DEVELOPMENT OF A ROBUST DIGITAL IMAGE WATERMARKING TECHNIQUE IN DISCRETE ORTHONORMAL STOCKWELL TRANSFORM DOMAIN BASED ON PHOTON POLARIZATION

BY

Daniel ALIU

DEPARTMENT OF COMPUTER ENGINEERING
FACULTY OF ENGINEERING
AHMADU BELLO UNIVERSITY ZARIA, NIGERIA

SEPTEMBER, 2018

DEVELOPMENT OF A ROBUST DIGITAL IMAGE WATERMARKING TECHNIQUE IN DISCRETE ORTHONORMAL STOCKWELL TRANSFORM DOMAIN BASED ON PHOTON POLARIZATION

By

Daniel ALIU B.Eng. (FUT., MINNA) 2010, MSc (ABU) 2015
P15EGCP9004
danfranal12@yahoo.com

A THESIS SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES, AHMADU BELLO UNIVERSITY, ZARIA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF DOCTOR OF PHILOSOPHY (Ph.D) DEGREE IN COMPUTER ENGINEERING

DEPARTMENT OF COMPUTER ENGINEERING

FACULTY OF ENGINEERING

AHMADU BELLO UNIVERSITY, ZARIA

NIGERIA

SEPTEMBER, 2018

DECLARATION

I, **Aliu Daniel** hereby declare that the work in this thesis entitled "**Development of a Robust Digital Image Watermarking Technique in Discrete Orthonormal Stockwell Transform Domain Based on Photon Polarization"** has been carried out by me in the Department of Computer Engineering. The information derived for the literature has been duly acknowledged in the text and a list of references provided. No part of this thesis was previously presented for any degree or diploma at this or any other institution.

Daniel ALIU _____ _____

(Student) Signature Date

CERTIFICATION

This thesis entitled "DEVELOPMENT OF A ROBUST DIGITAL IMAGE WATERMARKING TECHNIQUE IN DISCRETE ORTHONORMAL STOCKWELL TRANSFORM DOMAIN BASED ON PHOTON POLARIZATION" by Daniel ALIU meets the regulations governing the award of the degree of Doctor of Philosophy in Computer Engineering of the Ahmadu Bello University, Zaria and is approved for its contribution to knowledge and literary presentation.

Dr. E. A. Adedokun (Chairman, Supervisory Committee)	Signature	Date
Professor M. B. Mu'azu (Member, Supervisory Committee)	Signature	Date
Dr. I. J. Umoh (Member, Supervisory Committee)	Signature	Date
Professor M. B. Mu'azu (Head of Department)	Signature	Date
Professor S. Z. Abubakar (Dean, School of Postgraduate Studies)	Signature	Date

DEDICATION

This research is dedicated to God Almighty for His guidance, kindness, grace and mercy and to my Saviour Jesus Christ and to the kind hearted people, those who in one way or the other make a significant difference in an ordinary person's life.

ACKNOWLEDGEMENT

I thank God Almighty for His mercies, faithfulness, divine protection; for being my shepherd and light under my foot and for His love throughout my life and the period of this research.

I express my gratitude and sincere thanks to my supervisor and counselor Dr. E. A. Adedokun for his constant motivation, valuable contributions, and support throughout this research work. I appreciate his touch of expertise, advice, and all the valuable corrections without which this work would have not made it to this end. I sincerely wish to express my profound gratitude and appreciation to my role model, mentor, guide, and pathfinder supervisor Prof M. B. Mu'azu for his motivation, unending patience, expertise, exuberance, unquantifiable knowledge, and contributions to this research. I am greatly indebted to you sir for your valuable technical guidance, organization of the work, and moral support throughout this research work. Your inestimable guidance aided me shape the research problem, constantly enlightened me towards actualizing the research, and writing of the thesis. Without this support, this thesis would have not been completed. I thank my supervisor Dr. I. J. Umoh for his support and guidance throughout the research work. I am honoured and privileged of having a tremendous supervisory committee.

To my fellow researchers in the Control and Computer Group, I earnestly appreciate your observations and contributions during those numerous research group meetings.

I would also like to acknowledge with much appreciation the crucial role of Dr. A. D. Usman for creating time out of his tight scheduled to critically brainstorm with me over the possible ways of addressing the research problem. Thank you sir for the immense contributions you made in this research. Dr. A. T. Salawudeen, Dr. B. O. Sadiq, Dr. B. Yahaya, I. Yusuf, Z. M. Abubakar, Dr. Y. A. Sha'aban, Dr. M. B. Abdulrazaq, Dr. I. A. Bello, Dr. T. H. Sikiru, Dr. A.

M. S. Tekanyi for their valuable contributions during seminar and for creating time out of their tight schedule to go through my manuscripts. I am indepted to all the lecturers of the Department, and all those whose names could not be mentioned.

Special thanks go to Mrs O.O. Sule, Department of Computer Science, NILEST for unyielding support. Many thanks goes to all my fellow researchers whose names are too numerous to mention. Thank you all for the spirit of togetherness and for all the assistance and contributions to realize my dream in Ahmadu Bello University.

My appreciation goes to my lovely father late Mr, Aliu Francis Olakpe for the ideas he inculcated in me and brought me up in the ways of God, may your soul continue to rest in the bosom of the Lord until we meet to part no more. My lovely mother, Mrs. Esther Francis Aliu, thank you for your unyielding support, morally, financially and otherwise, I am most grateful. Also, I wish to extend my profound gratitude to Adeji Glory and my entire family. May God bless and protect all of you.

Finally, my deepest appreciation goes to my special and beloved friends: U. Abgalla. Abdulrashid, A. Tijani, O. Elvin, O. Rabiu, Soja A. C. Valentine, Arafat, Y. Abdulmumuni, Ibrahim and those whose names could not be mentioned. Your continuous support and contributions toward the success of this research would never be forgotten, May God reward you and strengthen our friendship.

Daniel. ALIU
September, 2018

ABSTRACT

This thesis presents the development of novel digital image watermarking technique for the shielding of intellectual property rights of digital images. Because of their digital nature, multimedia data can be duplicated, modified, and transformed. In this context, it is essential to develop a watermarking –based technique for copyright protection and authentication of digital images. The major problem of watermarking technique is how to achieve an optimal-tradeoff between robustness and imperceptibility. A robust digital image watermarking technique has been developed based on cascaded Discrete Orthonormal Stockwell Transform (DOST), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD) using private key obtained from the implementation of a Quantum Key Distribution (QKD) scheme and optimal scaling factor selection using Particle Swarm Optimization (PSO) algorithm. The colour images acquired are standard colour Lena, Pepper, Mandril, and Nepal Telecom logo. The colour images were decomposed into the respective three colour channels, of Red (R), Green (G), and Blue (B). The developed technique is achieved by applying DOST scheme on each channel of the cover and watermark images to obtain DOST transformed coefficients, these are then fed to the DWT for further transformation by decomposing the coefficients up to third level for complete representation and interpretation of the images in order to produce robust and scalable images. The images are modified by applying SVD to improve the security. A key length of 64-bits generated from the implementation of QKD scheme is used to encrypt the transformed watermark to further enhance the security of the technique. The watermark is reshuffled by affine transform by redistributing the pixel values to different locations using four 8-bit keys for it to be robust to attacks. The unintelligible transformed image by affine transform is divided into 2 pixels x 2 pixels blocks and each of the block is encrypted using XOR operation by four 8-bit keys. The optimal scaling factor obtained is used to embed and extract the watermark. The performance of the scheme is evaluated using Peak Signal to Noise Ratio (PSNR), Normalized Correlation Coefficient (NCC), and Structural Similarity Index Measure (SSIM) as performance metrics for imperceptibility and robustness. The results of the PSNR obtained for accessing the fidelity of the watermarked image when subjected to Gaussian, salt and pepper, speckle, rotated at 45°, 5°, and 90°, and crop attacks are 50.2752dB, 47.7293dB, 45.6404dB, 46.8626dB, 44.6045dB, 47.9442dB and 46.4067dB respectively, indicating that perceptual quality has been improved. The NCC values are 1, 1, 1, 0.9997, 1, 1 and 1, signifying high resistance to attacks. The SSIM values are 1, 1, 1, 0.99998, 0.9996, 0.9999 and 0.9987, respectively. The developed scheme with the QKD scheme delivered an imperceptibility improvement when compared with ITU-R standard value of 35dB for watermarking technique by 30%, 27%, 23%, 25%, 22%, 27% and 25% respectively. Comparison of the developed algorithm with the work of Bajracharya & Koju (2017) in terms of perceptual quality of the watermarked image showed an average PSNR value of 64.3580dB as against 48.1819, representing about 25% improvement of imperceptibility. The NCC values of the work of Bajracharya & Koju (2017) when subjected to the following attacks: Gaussian, salt and pepper, speckle, rotated at 45°, 5°, and 90°, and crop attacks are 1, 0.9996, 0.9999, 0.9999, 1 and 1. This demonstrates that the developed scheme gave an average improvement of about 14% robustness to attacks when compared with the work of Bajracharya & Koju (2017).

TABLE OF CONTENTS

TITLE PAGE **i**

DECLARATION i

CERTIFICATION ii

DEDICATION iii

ACKNOWLEDGEMENT iv

LIST OF FIGURES xii

LIST OF TABLES xxi

LIST OF ABBREVIATION xxii

CHAPTER ONE: INTRODUCTION

1.1 Background of Research 1

1.2 Motivation 10

1.3 1.3 Significance of Research 12

1.4 Statement of Problem 13

1.5 Aim and Objectives 14

1.6 Scope of the Research 15

1.7 Thesis Organization 15

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction 16

2.2 Review of Fundamental Concepts 16

2.2.1 Digital Image Watermarking 16

2.2.3 Characteristics of Digital Image Watermarking 17

2.2.3.1 Imperceptibility 17

2.2.3.2 Capacity 18

2.2.3.3 Security 18

2.2.3.4 Robustness 19

2.2.3.5 Computational Complexity 20

2.2.3.6 Verifiability 20

2.2.4 Applications of Digital Image Watermarking 21

2.2.5 Digital image watermarking techniques 22

2.2.5.1 Discrete Wavelet Transform (DWT) 25
2.2.5.2 Discrete Fourier Transform (DFT) 28
2.2.5.3 Singular Value Decomposition (SVD) 28
2.2.5.4 Stockwell Transform (ST) 30
2.2.5.5 Discrete Orthonormal Stockwell Transform (DOST) 32
2.2.6 Comparison between Digital Image Watermarking Techniques 36
2.2.7 Attack on Digital Image Watermarking 39
2.2.7.1 Signal Processing Attacks 40
2.2.7.2 Geometric Attacks 40
2.2.8 Performance Evaluation Metrics 41
2.2.9 Cryptography 42
2.2.9.1 Challenges of Classical Key Distribution 44
2.2.9.2 Quantum Cryptography 45
2.2.9.3 Quantum Key Distribution (QKD) 47
2.2.10 Bennet and Brassard 1984 (BB84) Protocol 50
2.2.10.1 Steps of QKD Processes Based on the BB84 Protocol 52
2.2.10.2 Suitable Selection of Scaling Factor 55
2.2.11 Particle Swarm Optimization 55
2.3 Review of Similar Works 57

CHAPTER THREE : MATERIALS AND METHODS

3.1 Introduction 73
3.2 Materials 73
3.3 Important Assumptions 73
3.4 Methodology 74
3.4.1 Development of a Digital Image Watermarking Technique 76
3.4.2 Application of 2D DOST on the Cover and Watermark images 77

CHAPTER FOUR: RESULTS AND DISCUSSION

4.1 Introduction 97
4.2 Decomposition of the Cover and Watermark Images 97
4.3 Determination of Scaling Factor 98
4.4 Definition of Different Scenarios 98
4.4.1 Robustness and Imperceptibility Results for Case I 99

4.4.2 Robustness and Imperceptibility Results for Case II 100
4.4.3 Robustness and Imperceptibility Results for Case III 101
4.4.4 Robustness and Imperceptibility Results for Case IV 102
4.4.5 Robustness and Imperceptibility Results for Case V 104
4.4.6 Robustness and Imperceptibility Results for Case VI 106
4.4.7 Robustness and Imperceptibility Results for Case VII 108
4.5 Other Scenarios Considered for Comparison 111
4.5.1 Robustness and Imperceptibility Results for Case VIII 111
4.5.2 Robustness and Imperceptibility Results for Case IX 112
4.5.3 Robustness and Imperceptibility Results for Case X 113
4.5.4 Robustness and Imperceptibility Results for Case XI 114
4.6 Determination of Optimal Scale Factor Based on Individual Attack Scenarios using PSO 116
4.7 Definition of Different Scenarios 117
4.7.1 Robustness and Imperceptibility Results for Case I 118
4.7.2 Robustness and Imperceptibility Results for Case II 119
4.7.3 Robustness and Imperceptibility Results for Case III 120
4.7.4 Robustness and Imperceptibility Results for Case IV 121
4.7.5 Robustness and Imperceptibility Results for Case V 122
4.7.5 Robustness and Imperceptibility Results for Case VI 123
4.8 Definition of Different Scenarios 125
4.8.1 Robustness and Imperceptibility Results for Case I 126
4.8.2 Robustness and Imperceptibility Results for Case II 127
4.8.3 Robustness and Imperceptibility Results for Case III 129
4.8.4 Robustness and Imperceptibility Results for Case IV 130
6.8.5 Robustness and Imperceptibility Results for Case V 131
4.8.6 Robustness and Imperceptibility Results for Case VI 132
4.8.7 Robustness and Imperceptibility Results for Case VII 133
4.9 Definition of Different Scenarios 135
4.9.1 Robustness and Imperceptibility Results for Case I 136
4.9.2 Robustness and Imperceptibility Results for Case II 138
139
4.9.3 Robustness and Imperceptibility Results for Case III 139
4.9.4 Robustness and Imperceptibility Results for Case IV 141
4.9.5 Robustness and Imperceptibility Results for Case V 143

4.9.6 Robustness and Imperceptibility Results for Case VI 144
4.9.6 Robustness and Imperceptibility Results for Case VII 145
4.10 Performance Evaluation of the Developed Algorithm 148
4.11 Comparison of Results 149
4.11.1 Comparison of PSNR, NCC and SSIM Results of Various Defined Scenarios under No Attack 149
4.11.2 Comparison of PSNR, NCC and SSIM Results of Various Defined Scenarios under Gaussian Attack 152
4.11.3 Comparison of PSNR, NCC and SSIM Results of Various Defined Scenarios under Salt and Pepper Attack 154
4.11.4 Comparison of PSNR, NCC and SSIM Results of Various Defined Scenarios under Speckle Attack 157
4.12 Validation 159

CHAPTER FIVE: CONCLUSION AND RECOMMENDATION

5.1 Summary 163
5.3 Conclusion 164
5.4 Significant Contributions 167
5.5 Limitations 167
5.6 Recommendations for future work 168

REFERENCES 170
APPENDIX A 177
Complete M File for Host Image Decomposition Using DOST 177
APPENDIX B 179
Complete M File for Binary bits Generation 179
APPENDIX C 180
Complete M File for Generating and Sending of Quantum bits to Receiver 180
APPENDIX D 181
Complete M File for Receiving Quantum bits from Sender 181
APPENDIX E 183
Complete M File for performing the various phases of Error Detection and Correction 183
APPENDIX F 185
Complete M File for performing Error Reconciliation 185

APPENDIX G 188
Complete M File for performing Error Reconciliation process on the key obtained 188
APPENDIX H 191
Complete M File for Watermark Encryption with Generated Key 191
APPENDIX I 192
Complete M File for Application of transformation Technique 192
APPENDIX J 193
Complete M File for Performing the Fitness Function 193
APPENDIX K 194
Complete M File for Decrypting the watermark image 194
APPENDIX L 195
Complete M File for using PSO to obtain optimal Scale factor based on Fitness Function 195
APPENDIX M 196
Complete M File for Watermarking Process 196
APPENDIX N 198
Complete M File for Host Image Recovering Using Inverse DOST 198
APPENDIX O 200
Complete M File for Application of Inverse Transformation 200
APPENDIX P 201
Complete M File for Generating the watermarking simulation user interface 201
APPENDIX Q 203
Summary of results obtained for the various Attack scenarios 203
APPENDIX R 204
Summary of results obtained of Optimal Scaling Factor under different Attack Scenarios 204
APPENDIX S 206
Comparison of the random bits generated by Alice, Alice randomly chooses polarization basis, transmitted Qubits by Alice and Bob measures Qubits 206

LIST OF FIGURES

Figure 1.1: Watermark Embedding process 5

Figure 1.2: Watermark Extraction Process 6

Figure 1.3: Watermarking System 6

Figure 2.1: 1- level DWT Decomposition 26

Figure 2.2: 2- level DWT Decomposition 26

Figure 2.3: 3- level DWT Decomposition 27

Figure 2.4: Time – Frequency of DOST Coefficients of Signal length of 16 34

Figure 2.5: 2D Visualization of DOST coefficients of signal length of 64 35

Figure 2.6: QKD model using two channels to Generate Random key 48

Figure 2.7: Polarization Bases 50

Figure 2.8: Diagonal and Rectilinear Filters 50

Figure 2.9: Photon polarization 51

Figure 3.1: Lena as Original Cover Image and Mandril as Watermark Image 76

Figure 3.2: Cover Image Channels and the Logarithm of their DOST coefficients 78

Figure 3.3: Watermark Image Channels and the Logarithm of their DOST coefficients 79

Figure 3.4: Number and size of Blocks Generated at each Pass in Error reconciliation Process 84

Figure 3.5: Flowchart of the PSO – Based Scheme 91

Figure 3.6: Flow chart of Developed Watermark Embedding Process Algorithm 92

Figure 3.7: Flowchart of Developed Watermark Extraction Process Algorithm 94

Figure 4.1: Decomposition of Cover Image into RGB Channels 97

Figure 4.2: Decomposition of Watermark Image into RGB Channels 98

Figure 4.3: Comparison of Visual Similarity between Original Cover Image and Watermarked Image 99

Figure 4.4: Comparison of Original Cover Image Watermarked Images under no Attack 100

Figure 4.5: Comparison of Original Watermark Image and Extracted Watermark Image under No Attack with an optimal Scaling factor of 0.1208 100

Figure 4.6: Comparison of Original Cover Image, Watermarked Image and Watermarked Images under Gaussian Attack 101

Figure 4.7: Comparison of Original and Extracted Watermark Images under Gaussian Attack with an optimal Scaling factor of 0.1208 101

Figure 4.8: Comparison of Original Cover Image, Watermarked Image and Watermarked Images under Salt and Pepper Attack 102

Figure 4.9: Comparison of Original Watermark Image and Extracted Watermark Image under Salt and Pepper Attack with an optimal Scaling factor of 0.1208 102

Figure 4.10: Comparison of Original Cover Image, Watermarked Image and Watermarked Images under Speckle Attack 103

Figure 4.11: Comparison of Original Watermark Image and Extracted Watermark Image Under Speckle Attack 103

Figure 4.12: Comparison of the Results of PSNR, NCC and SSIM obtained using optimal Scaling factor of 0.1208 104

Figure 4.13: Encrypted Watermarked Image based on an Estimated Private Key 105

Figure 4.14: Comparison of Original Cover Image, Watermarked Image and Watermarked Image that contains the Encrypted Image under Speckle Attack 105

Figure 4.15: Recovered Encrypted Watermark Image under Speckle Attack 106

Figure 4.16: Comparison of Extracted Decrypted Watermark Image and Original Watermark Image under Speckle Attack 106

Figure 4.17: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Salt and Pepper Attack with an optimal Scaling factor of 0.1208 using Encrypted Watermark Image 107

Figure 4.18: Recovered Encrypted Watermark Image under Salt and Pepper Attack 107

Figure 4.19: Comparison of Extracted Decrypted Watermark Image and Original Watermark Image under Salt and Pepper Attack 108

Figure 4.20: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Gaussian Attack with an optimal Scaling factor of 0.1208 using Encrypted Watermark Image 108

Figure 4.21: Recovered Encrypted Watermark Image under Gaussian Attack 109

Figure 4.22: Comparison of Extracted Decrypted Watermark Image and Original Watermark Image under Gaussian Attack 109

Figure 4.23: Comparison of the results of PSNR, NCC and SSIM using the Encrypted Watermark and optimal Scaling factor 0f 0.1208 110

Figure 4.24: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under No Attack with a manual selected Scaling Factor of 0.0121 111

Figure: 4.25: Comparison of Original Watermark and Extracted Watermark Images under No Attack 112

Figure 4.26: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Gaussian Attack with a manual selected Scaling Factor of 0.0121

112

Figure 4.27: Comparison of Original Watermark and Extracted Watermark Images under Gaussian Attack 113

Figure 4.28: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Salt and Pepper Attack with a manual selected Scaling Factor of 0.0121 113

Figure 4.29: Comparison of Original Watermark and Extracted Watermark Images under Salt and Pepper Attack 114

Figure 4.30: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Speckle Attack with a manual selected Scaling Factor of 0.0121 114

Figure 4.31: Comparison of Original Watermark and Extracted Watermark Images under Speckle Attack 115

Figure 4.32: Comparison of the Results of PSNR, NCC and SSIM obtained using manually Selected Scaling Factor of 0.0121 116

Figure 4.33: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Gaussian Attack using different optimal Scaling factors obtained From Different Attack scenarios 118

Figure 4.34: Comparison of Original Watermark and Extracted Watermark Images under Gaussian Attack 119

Figure 4.35: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under salt and Pepper Attack using different optimal Scaling factors obtained From Different Attack scenarios 119

Figure 4.36: Comparison of Original Watermark and Extracted Watermark Images under Salt and Pepper Attack 120

Figure 4.37: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Speckle Attack using different optimal Scaling factors obtained From Different Attack scenarios 120

Figure 4.38: Comparison of Original Watermark and Extracted Watermark Images under Speckle Attack 121

Figure 4.39: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under 30° rotation Attack using different optimal Scaling factors obtained From Different Attack scenarios 121

Figure 4.40: Comparison of Original Watermark and Extracted Watermark Images under

30° rotation 122

Figure 4.41: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under 20° rotation Attack using different optimal Scaling factors obtained From Different Attack scenarios 122

Figure 4.42: Comparison of Original Watermark and Extracted Watermark Images under 20° rotation 123

Figure 4.43: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under crop Attack using different optimal Scaling factors obtained From Different Attack scenarios 123

Figure 4.44: Comparison of Original Watermark and Extracted Watermark Images under Crop Attack 124

Figure 4.45: Comparison of Results of PSNR, NCC and SSIM obtained using Optimal Scaling Factor under different Attack Scenarios 125

Figure 4.46: Depicts Pepper as Original Cover Image and Nepal Telecom as Watermark Image 126

Figure 4.47: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Gaussian Attack using different optimal Scaling factors obtained From Different Attack scenarios 127

Figure 4.48: Comparison of Original Watermark and Extracted Watermark Images under Gaussian Attack 127

Figure 4.49: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Salt and Pepper Attack using different optimal Scaling factors obtained From Different Attack scenarios 128

Figure 4.50: Comparison of Original Watermark and Extracted Watermark Images under Salt and Pepper Attack 128

Figure 4.51: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Speckle Attack using different optimal Scaling factors obtained From Different Attack scenarios 129

Figure 4.52: Comparison of Original Watermark and Extracted Watermark Images under Speckle Attack 130

Figure 4.53: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under 45° rotation Attack using different optimal Scaling factors obtained From Different Attack scenarios 130

Figure 4.54: Comparison of Original Watermark and Extracted Watermark Images under 45° rotation 131

Figure 4.55: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under 5° rotation Attack using different optimal Scaling factors obtained From Different Attack scenarios 131

Figure 4.56: Comparison of Original Watermark and Extracted Watermark Images under 5° rotation 132

Figure 4.57: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under 90° rotation Attack using different optimal Scaling factors obtained From Different Attack scenarios 132

Figure 4.58: Comparison of Original Watermark and Extracted Watermark Images under 90° rotation 133

Figure 4.59: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Crop Attack using different optimal Scaling factors obtained From Different Attack scenarios 133

Figure 4.60: Comparison of Original Watermark and Extracted Watermark Images under Crop Attack 134

Figure 4.61: Comparison of Results of PSNR, NCC and SSIM obtained using the optimal Scaling factor under various Attack Scenarios 134-135

Figure 4.62: Encrypted Watermark Image based on the key obtained from Implementation Of QKD Scheme 136

Figure 4.63: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Gaussian Attack based on its optimal scaling factor using Encrypted Watermark Image 136

Figure 4.64: Recovered Extracted Watermark Image under Gaussian Attack 137

Figure 4.65: Comparison of Original Watermark and Extracted Decrypted Watermark Images under Gaussian Attack 137

Figure 4.66: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Salt and Pepper Attack based on its optimal scaling factor using Encrypted Watermark Image 138

Figure 4.67: Recovered Extracted Watermark Image under Salt and Pepper Attack 139

Figure 4.68: Comparison of Original Watermark and Extracted Decrypted Watermark Images under Salt and Pepper Attack 139

Figure 4.69: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Speckle Attack based on its optimal scaling factor using Encrypted Watermark Image 140

Figure 4.70: Recovered Extracted Watermark Image under Speckle Attack 140

Figure 4.71: Comparison of Original Watermark and Extracted Decrypted Watermark Images under Speckle Attack 141

Figure 4.72: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under 45° rotation based on its optimal scaling factor using Encrypted Watermark Image 141

Figure 4.73: Recovered Extracted Watermark Image under 45 degree Rotation Images under 45° Rotation 142

Figure 4.74: Comparison of Original Watermark and Extracted Decrypted Watermark Images under 45°Rotation 142

Figure 4.75: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under 5° rotation based on its optimal scaling factor using Encrypted Watermark Image 143

Figure 4.76: Recovered Extracted Watermark Image under 45 degree Rotation Images under 5° Rotation 143

Figure 4.77: Comparison of Original Watermark and Extracted Decrypted Watermark Images under 5° Rotation 144

Figure 4.78: Comparison of Original Cover Image, Watermarked Image and Watermarked

Image under 90° rotation based on its optimal scaling factor using Encrypted Watermark Image 145

Figure 4.79: Comparison of Original Watermark and Extracted Decrypted Watermark Images under 90° Rotation 145

Figure 4.80: Comparison of Original Cover Image, Watermarked Image and Watermarked Image under Crop Attack based on its optimal scaling factor using Encrypted Watermark Image 146

Figure 4.81: Comparison of Original Watermark and Extracted Decrypted Watermark Images under Crop Attack 146

Figure 4.82: Comparison of Results of PSNR, NCC and SSIM obtained using optimal Scaling factor and key under various Attack Scenarios 147

Figure 4.83: Comparison of Results of PSNR obtained on various Defined Scenarios under No Attack 150

Figure 4.84: Comparison of Results of NCC obtained on various Defined Scenarios under No Attack 151

Figure 4.85: Comparison of Results of SSIM obtained on various Defined Scenarios under No Attack 152

Figure 4.86: Comparison of Results of PSNR obtained on various Defined Scenarios under Gaussian Attack 153

Figure 4.87: Comparison of Results of NCC obtained on various Defined Scenarios under Gaussian Attack 153

Figure 4.88: Comparison of Results of SSIM obtained on various Defined Scenarios under Gaussian Attack 154

Figure 4.89: Comparison of Results of PSNR obtained on various Defined Scenarios under Salt and Pepper Attack 155

Figure 4.90: Comparison of Results of NCC obtained on various Defined Scenarios under Salt and Pepper Attack 156

Figure 4.91: Comparison of Results of SSIM obtained on various Defined Scenarios under Speckle Attack 157

Figure 4.92: Comparison of Results of PSNR obtained on various Defined Scenarios under Speckle Attack 158

Figure 4.93: Comparison of Results of NCC obtained on various Defined Scenarios under Speckle Attack 158

Figure 4.94: Comparison of Results of SSIM obtained on various Defined Scenarios under Speckle Attack 159

Figure 4.95: Comparison of the Degree of Imperceptibility of the Developed Algorithm And Referenced Algorithm 161

Figure 4.96: Comparison of the Degree of Robustness of the Developed Algorithm And referenced Algorithm 162

LIST OF TABLES

Table 1.1: Classification of Digital Image Watermarking 10

Table 2.1: Comparison Between Spatial and Transform Domain 36

Table 2.2: Comparison between Individual Transform domain Techniques 37

Table 2.3: Procedure of BB84 Protocol of Key Generation 52

Table 4.7: Summary of Results based on the work of Referenced Algorithm 149

Table 4.8: Comparison of Results between Developed Algorithm and Referenced Algorithm 160

LIST OF ABBREVIATIONS

Acronyms	Definitions
AES	Advanced Encryption Scheme
BB84	Bennet and Brassard, 84
B92	Bennet, 92
CBT	Correlation Based technique
COW	Coherent one –way
DCT	Discret Cosine Transform
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DOST	Discrete Orthonormal Stockwell Transform
DPS-QKD	Differential Phase Shift-QKD
DST	Discrete Stockwell Transform
DWT	Discrete Wavelet Transform
2D	2- Dimensional
E91	Ekert, 91
FFT	Fast fourire Transform
ITU	International Telecommunication Union
HH	Diagonal high pass-Band
HL	Horizontal high pass-Band
LH	Vertical high pass-Band
LL	Low pass-Band
LSB	Least Significant Bit

LWT	Lifting Wavelet Transform
MATLAB	MAtrix LABoratory
MSE	Mean Square Error
NCC	Normalized-Correlation Coefficient
OTP	One Time Pad
PSNR	Peak Signal to Noise Ratio
PSO	Particle Swarm Optimization
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
Qubit	Quantum bit
RSA	Rivest Shamir and Adleman
SARG04	Sacrani, Acin, Ribordy and gisin, 04
SSIM	Structural Similarity Index Measured
SSM	Spread Spectrum Technique
SSP	Six-State Protocol
ST	Stockwell Transform
SVD	Singular Value Decomposition

CHAPTER ONE

INTRODUCTION

1.1 Background of Research

The rising demand for the production, storage and transmission of multimedia contents (such as image, audio, video and text) over secured and unsecured communication media in recent years poses a lot of security and privacy concerns to both the sender and receiver. The use of these multimedia contents (image, audio, video and text) is rapidly increasing with the high growth and widespread use of the Internet and information technology. Due to this fact, tampering with and illegal distribution of digital contents is inevitable and as such it becomes imperative to devise mechanisms to protect the copyright of such media. It has been established that present copyright laws are insufficient for addressing the security of digital contents (Chandramouli *et al.,* 2002). Furthermore, simple transfer and manipulation of digital data also institutes a real menace for information inventors, and copyright owners want to be recompensated every period their work is used. In addition, they want to be certain that their work is not deployed in an illegitimate means (for instance modified without their consent).

The introduction of Internet has resulted in numerous opportunities for the creation and transfer of contents (electronic advertising, web publishing, digital repositories and libraries, real-time video and audio delivery, etc.) in digital form (Chandramouli *et al.,* 2002). A pertinent issue that arises in these applications is the protection of the rights of all participants, such as copyright enforcement and content verification because the present copyright acts are insufficient in sharing digital messages (Chandramouli *et al.,* 2002). One solution to this threat would be to curb access to the data using encryption technique (Arnold *et al.,* 2003), even though it does not necessarily offer total protection. Once the encoded data are decoded,

they can be easily circulated or manipulated (Arnold *et al.,* 2003), this has led to the fascination of researchers in developing copy deterrence and protection mechanisms to overcome illegal manipulation of digital data (Kavitha & Shan, 2016).

Several mechanisms have been proposed for the protection of multimedia contents based on data hiding techniques. These techniques are as follows (Harish *et al.,* 2013):

1. Cryptography,
2. Steganography
3. Watermarking

A comprehensive review of the development of data hiding can be found in (Tanaka, Nakamura & Matsui, 1990).

Cryptography is not particularly focused on concealing the presence of data, but is also regarded as encryption (Challita & Farhat, 2011). Cryptography can be defined as the study of mathematical systems for solving two types of challenges, privacy and authentication (Diffie & Hellman, 1976). A privacy scheme precludes the extraction of information by unauthorized parties from data transferred over public channel, hence ensuring the sent message is being read only by the designated receiver (Diffie & Hellman, 1976). An authentication scheme is to forestall an unauthorized injection of messages into public channel, ascertaining the recipient of a message of the legitimacy of its sender (Diffie & Hellman, 1976).

Steganography means the study of techniques for concealing the existence of a secondary message in the presence of a primary message (Arnold *et al.,* 2003), i.e. by inserting a private message in a cover image (Challita & Farhat, 2011). Where the carrier signal depicts the primary message and the secondary message is the payload signal or payload message. Steganography is a mechanism that is used for offering confidentiality and deniability, both of

which can be satisfied exclusively through cryptographic ways (Arnold *et al.,* 2003). In steganography, messages which are secreted has no connection with the cover channel or image and the condition for steganography is that no intuition should arise that a channel is conveying any concealed data (Challita & Farhat, 2011). The aim of steganography is to have covert communication between two parties, that is, presence of the communication is unknown to a potential assailant, and only a fruitful attack can notice the existence of this conversation.

One of such mechanisms that have been attracting major interest is digital watermarking (Averkiou, 2002). Watermarking has provides one of the best solutions among steganography and cryptography mechanisms (Harish *et al.,* 2013). Watermarking has shown resilient property that overcomes covert communication as in steganography (Harish *et al.,* 2013). The interest in watermarking actually started in 1990 with the development of the multimedia systems and the necessity of transferring data over the internet (Araghi *et al.,* 2016). Digital watermarking is a technique that is used to preclude duplicating or to shield digital data by invisibly hiding lawful marked message into the original data (Lai *et al.,* 2013). Digital watermarking can also be defined as the act of concealing information connected to a digital signal (which could be a video, song and image) inside the signal itself (Bajracharya & Koju, 2017). Watermarking attempts to hide a message interrelated to the actual content of the digital signal (Bajracharya & Koju, 2017). Such information is embedded for various reasons such as (Nin & Ricciardi, 2013):

1. Copyright protection
2. Source tracking
3. Broadcast monitoring

4. Telemedicine
5. Piracy deterrence etc.,

The categorization of watermarking scheme into four phases is based on the kind of information to be watermarked; this information can be any of (Sinha *et al.*, 2017):

1. Video watermarking
2. Image watermarking
3. Text watermarking
4. Audio watermarking

Image watermarking was considered in this research work but any of the other watermarking types can be used.

A model of bits fixed into a digital audio, video, image, or text file that is unambiguously used to identify the owner of a specific image is refered to as watermark and its main steps are embedding and extraction (Cherian & Mereena, 2016; Nyeem *et al.*, 2014).

1. Embedding Processing: Embedding is a method of inserting a watermark within the host image in order to create the watermarked image and the process is carried out at the sender's side (Navas *et al.*, 2008)

   A typical watermark embedding is represented as follows (Chandramouli *et al.*, 2002):

$$X' = E_k(X, W) \tag{1.1}$$

Where:

X is the original image

W is the watermark information being embedded

k is the user's insertion key

E represents the watermark insertion function

X’ depicts the watermark variant

2. Extracting Processing: Extracting is the method of recovering the watermark and the host image from the watermarked image and this process happens at the receiver’s end A generic watermark extraction is represented as follows (Chandramouli *et al.*, 2002):

$$\widehat{W} = D_{K'}(\widehat{X}') \quad (1.2)$$

where:

$\widehat{X}'$ represents the possible corrupted watermarked image

K' denotes the extraction key

D depicts the watermark extraction /detection function

$\widehat{W}$ represents the extracted watermark information

The two processes are shown in Figures 1.1 and 1.2 respectively.

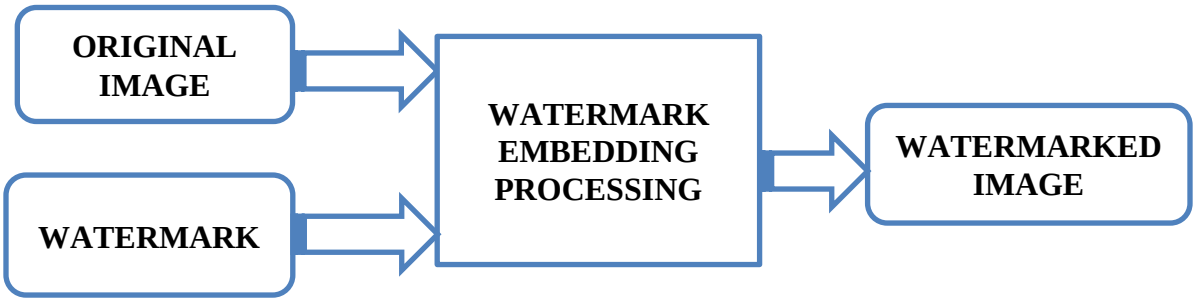


Figure 1.1: Watermark Embedding Process (Chanda & Choudhury, 2016)

Figure 1.1 depicts the watermarking embedding process where the original image represents the carrier signal or message that hosts the watermark while the watermark is the hidden data. The watermarked image is the media which contains the watermark and is generated by using an embedding function to insert the watermark into the original image. This operation is executed from the sender’s end (Chanda & Choudhury, 2016).

Figure 1.2 depicts the watermarking extraction phase where the watermarked image undergoes extraction process with a view to recovering the original watermark at the receiver's side.

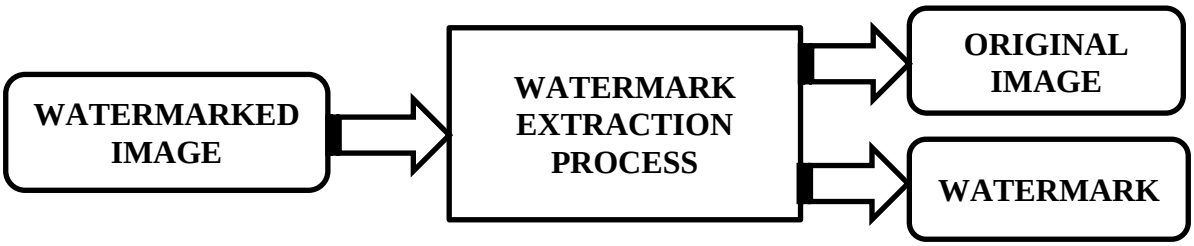


Figure 1.2: Watermark Extraction Process (Chahal & Khurana, 2013)

Figure 1.3 depicts the complete representation of the components of a watermarking process which comprises of embedding, detection and extraction processes.

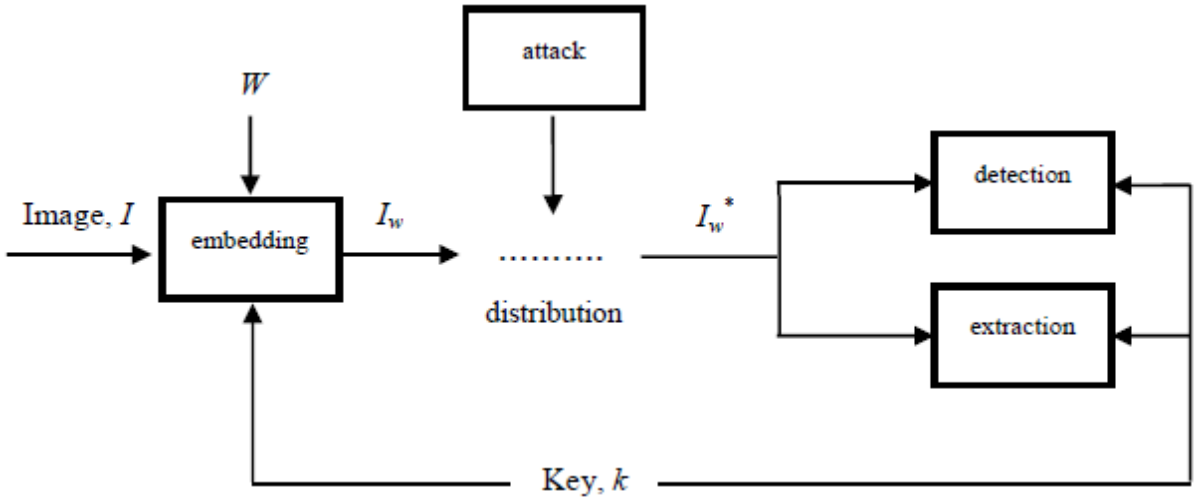


Figure 1.3: Watermarking System (Tao & Eskicioglu, 2004)

Detection is the procedure deployed for identifying whether the given media contains the watermark or not (Tao & Eskicioglu, 2014). Attack is an artificial process used intentionally or non-intentionally to duplicate or modify the watermark within the cover image. This modifies the watermarked image and destroys or alters watermark in the data. Key is a bit of information or parameter that controls the embedding and extraction processes (Tao & Eskicioglu, 2014).

where: I depicts the host image, W Denotes the watermark image, I_W represents the watermarked image, I_W* *represents* the distorted image, K depicts embedding and extraction key

The two key groups of digital image watermarking are as follows (Sathik & Sujatha, 2012):

1. Visible digital image watermarking technique
2. Invisible digital image watermarking technique

Information is perceptible in the multimedia content which identifies the owner of the document in detectible watermarking. The visible watermarking should be perceptible (easy to discern the concealed data) (Santhi & Arulmozhivarman, 2013).

In invisible watermarking information is inserted as digital data to multimedia content, such that, it is imperceptible to observers. The invisible watermarking requirements are imperceptibility and robustness. The invisible watermarks are categorized as follows (Chandramouli *et al.,* 2002):

1. Fragile watermarks
2. Semi fragile watermarks
3. Robust watermarks

Several techniques have been proposed for copyright protection of digital images and these are categorized into two domains as follows (Sathik & Sujatha, 2012):

1. Spatial domain techniques
2. Transform domain techniques

In spatial domain techniques the pixel values of the host image are changed directly by inserting the watermark bits (Araghi *et al.,* 2016). The spatial domain techniques are simply implemented with little cost of operation, quick, computationally uncomplicated and

straightforward while there is no need for cover image to be transformed. Nevertheless, they are vulnerable to simple image processing operations such as noise, compression and filtering due to watermark insertion in selected locations of the image or other geometric attacks. The spatial domain techniques comprise of the following (Lai & Tsai, 2010; Zheng, Liu, Zhao, & Saddik, 2007):

1. Least significant bit (LSB)
2. Spread spectrum technique (SSM)
3. Correlation based technique (CBT)

In transform domain technique the coefficients of the host image is modified where the watermark is inserted for embedding in transform domain. At first the cover image is transformed and then the watermark is inserted to the coefficients of the transformed image. In order to retrieve the original image, an inverse transform of the modified coefficients needs to be performed (Araghi *et al.*, 2016). The transform domain techniques comprise of the following (Rahman, 2013 and Cherian & Mereena, 2016):

1. Discrete Orthonormal Stockwell Transform (DOST)
2. Singular Value Decomposition (SVD)
3. Lifting Wavelet Transform (LWT)
4. Discrete Stockwell Transform (DST)
5. Discrete Cosine Transform (DCT)
6. Discrete Wavelet Transform (DWT)
7. Discrete Fourier Transform (DFT)
8. Fast Fourier Transform (FFT)

The information concealing and recovery operations of these transform algorithms are comparatively complicated, however, due to their strong anti-attack abilities, they are suitable for the copyright protection of multimedia data (Araghi *et al.*, 2016). These methods in handling image and common signal processing attacks achieve higher imperceptibility and robustness, although, the cost of computation is higher than that of the spatial domain watermarking schemes (Cherian & Mereena, 2016).

Watermarking system is classified based on three vital criteria, namely the type of domain, watermark and information required in the recovery or extraction process. The classification according to these criteria is shown in Table 1.1

Table 1.1: Classification of Digital Watermarking Technique (Araghi *et al.,* 2016):

Criterion	Class	Description
Domain type	Spatial	Pixels values are adjusted to enclose the secret message.
	Transform	Transform constants are modified to insert the classified message. Present popular transforms are DCT, DWT, and DFT etc.
Watermark type	Pseudo random number (PRN) sequence (having a normal distribution with zero mean and unity variance)	Let the detector to statistically determine the existence or nonexistence of a watermark. A PRN series is created by serving the generator with an underground seed.
	Visual watermark	The watermark is essentially reassembled, and its visual value is evaluated.
Information type	Non-blind	Both the original image and the undisclosed key(s) are require for watermark extraction process
	Semi-blind	The watermark and the secret key(s) are require for the extraction process
	Blind	Only the secret key(s) is require for the extraction process

1.2 Motivation

The use of digital data (image, audio, video and text) is rapidly rising with the high growth and widespread use of the Internet and information technology. Due to this fact, tampering

and illegal distribution of digital contents is inevitable and as such it becomes imperative to devise mechanisms to protect such contents. It has been established that present copyright laws are insufficient in dealing with the security of digital data (Chandramouli *et al.,* 2002). Information hiding and copyright protection have also become vital challenges on the issue of sharing digital data over public network; this is the principal motivation for this research work. In order to address these challenges watermarking technology is adopted. Several researchers had worked in the area of watermarking for its usefulness (Al-Mansoori & Kunhu 2012, Gattani & Warnekar, 2014; Chanda & Choudhury 2016; Ouazzane *et al.,* 2017). Work in this area has led to development of several watermarking techniques such as spatial domain based techniques and transform domain based techniques. Image watermarking scheme should possess the requirements of imperceptibility between the watermarked image and original image and robustness (Tao *et al.,* 2014). Robustness is the ability of the digital watermarking method to withstand common image manipulations like compression, filtering, rotation, scaling, cropping and other digital signal processing operations (Tao *et al.,* 2014, Mehto & Mehra, 2015). Normally used frequency domain transforms include the DFT, DWT, DCT, and SVD (Chan & Cheng, 2004). Currently DOST has been developed and applied to image texture characterization, image compression, decomposition. DWT has the capability of producing temporal resolution and captures frequency and location information, these properties of DWT make its suitable for the application of de-noising, compression and phase analysis. Although, the self-similarity restraint amongst the wavelet basis functions ruins the phase information; as such coefficients supply single locally referenced phase information. SVD is a transform technique that addressed the challenge associated with DWT transform technique. SVD offers a robust method of watermarking with little or no distortion based on

the singular value of the image. This makes it resilient to noise and geometric attack, even though, it suffers from false positive outcome. DOST has the ability to retain phase reference information of the signal absolutely, that is, the reference is constantly at zero time. With this, it gives the accumulation of the coefficients for a static frequency that yields the precise Fourier coefficient for that frequency. However, the non-redundancy nature ascribable to DOST, make it provides a preferably coarse time–frequency representation with its frequency resolution proportionally scaled to the logarithm of the frequency. Such an illustration may not be constantly simple to interpret and be sufficient to disclose all the details within a specific signal. Therefore, the cascade of DOST, DWT and SVD is utilized in this work in order to compensate for the deficiencies of each other, with a view to achieving an effective watermarking technique. The watermark is encrypted with a private key to further enhance the security of the watermarking algorithm. Therefore, the proposed watermarking technique is expected to achieve an optimal balance between imperceptibility and robustness when subjected to attacks.

1.3 Significance of Research

In recent years the nature of digital network systems means that digital contents can be duplicated and shared with ease to large spectrum of people with no cost over internet. Due to current advances in information technologies, these multimedia data can easily be downloaded, duplicated and manipulated by hackers in order to modify the original contents (Kalarikkal *et al.*, 2017). The major challenges is how to protect the ownership right of these multimedia contents transmitted over internet and prevent duplication of the contents, which still remains a major challenge to researchers. In addressing these challenges, researchers introduced a copy deterrence mechanism called digital watermarking. In order for digital

watermarking technique to be useful, it must satisfy imperceptibility and robustness requirements for protection. Therefore, this thesis is focused on the development of a robust digital image watermarking algorithm in DOST domain by employing DWT in conjunction with SVD based on photon polarization with a view to protecting the copyright of multimedia data, with the hope of striking a balance between imperceptibility and robustness.

The unique features of the developed technique are as follows:

1. The watermarking algorithm is blind since the original cover image is not involve during the recovery process.
2. The watermarking algorithm is robust against variety of attacks.
3. The watermark is invisible and causes no distortion to the cover image.

1.4 Statement of Problem

The rising pace in the transmission of multimedia contents (such as image, audio, video and text) over secured and unsecured communication media poses a lot of security and privacy concerns to both the sender and the receiver. It has been established that present copyright laws are insufficient for dealing with the security of digital data (Chandramouli *et al.*, 2002). This has led to the development of a copy deterrence and protection mechanism called digital watermarking (Kavitha & Shan, 2016). Most works reported in literature using different techniques only concentrated on achieving the watermark robustness by compromising image fidelity or vice versa. In other words, those techniques were based on some sort of trade-off between robustness and imperceptibility of the watermarked image. Hence, this research sets to develop a novel approach of robust digital image watermarking technique in DOST domain using DWT and SVD. The scaling factor, which is critical to imperceptibility and robustness, is optimally obtained using Particle Swarm Optimization (PSO). The secret key is obtained

using quantum key distribution (QKD) based on the principle of photon polarization in order to mitigate the effect of both signal processing manipulation and geometric attacks, with the hope of simultaneously satisfying both robustness and imperceptibility requirements.

1.5 Aim and Objectives

This research is aimed at developing a robust digital image watermarking technique in DOST domain based on the principle of photon polarization in order to strike a balance between imperceptibility and robustness to obtain the copyright protection of a digital image.

In order to accomplish the stated aim, the following objectives were adopted:

1. To develop a digital image watermarking algorithm in 2D DOST domain using DWT and SVD for decomposition of the cover image and watermark for both embedding and extraction processes.
2. To develop a scheme for the generation of the secret key from quantum key distribution using the principle of photon polarization based on the BB84 protocol
3. To determine the optimal scaling factor by applying particle swarm optimization (PSO)-based approach required to ascertain the strength of the embedded watermarked image
4. To generate a watermarked image by performing inverse DWT and 2D DOST on the transformed coefficients (obtained from 1 modified by the key and scaling factor obtained from 2 and 3 respectively). Extraction of the watermark is to be carried out by performing the inverse of the process described.
5. To validate the developed technique by comparing with the ITU benchmark and techniques developed by Bajracharya & Koju (2017 in terms of robustness and

imperceptibility using peak signal to noise ratio (PSNR), normalized-correlation coefficient (NCC) and structural similarity index (SSIM) as performance metrics.

1.6 Scope of the Research

The scope of this research work which developed a new data hiding algorithm (digital watermarking technique) inspired by the proliferation of duplicating and modifying of intellectual properties on daily basis without the consent of the rightful owner. The scope that encapsulates this developed algorithm is enumerated as follows:

1. The research only considered DOST, DWT and SVD for images transformation and as such no other transform domain techniques were considered.
2. The research only considered affine transform and XORed operation technique in encryption and decryption of the watermark image.
3. An optimal scaling factor selected by the application of PSO only for embedding the watermark is considered in this thesis.
4. The research only considered colour images

1.7 Thesis Organization

This thesis consists of five chapters, and is organized as follows: The introductory part of the thesis is discussed in chapter one. Chapter two provides an overview of the pertinent fundamental concepts in addition to a review of similar works. Chapter three describes the detailed steps of the methodology while results and discussions are presented in chapter four. Summary, conclusion and recommendations make up chapter five. Appendices and relevant references are presented at the end of this thesis.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter provides an insight to the fundamental concepts of the research, and comprises of two sub-sections. The first sub-section describes the overview of fundamental concepts which are pertinent to copyright protection. The second sub-section, covers review of similar works that are critical to the research.

2.2 Review of Fundamental Concepts

This subsection presents an overview of fundamental concepts relevant to the research such as digital watermarking, transform techniques, photon polarization, Particle Swarm Optimization and performance metrics for evaluating the validity of the developed watermarking technique.

2.2.1 Digital Image Watermarking

The rising pace of digital media (audio, image and video) production is creating an urgent need for copyright enforcement schemes (Cox *et al.,* 1997). In conventional cryptographic systems, only an authorized party is permitted access to secured data, but once such data is decoded there is no way to trail its duplication or retransmission. Therefore, classical cryptographic schemes (advanced encryption scheme (AES), Rivest, Shamir and Adleman (RSA), data encryption standard (DES) and one-time pad (OTP) etc.) provide little protection against data piracy, making publishers to face unauthorized reproduction of their content. In recent years a new cryptographic scheme, called quantum cryptography was developed, and it offers the following advantages over classical cryptography (Guenther, 2003):

1. Quantum cryptography: It is invulnerable to an increase in computing power, which makes brute force attack infeasible

2. Quantum cryptography: It detects the presence of an eavesdropper in the communication channels during key generation
3. The security of the key during key generation is absolutely guaranteed
4. The security of the key during key distribution is absolutely guaranteed

Digital watermarking was introduced to complement the cryptographic processes for enhanced data security. It involves the use of either a visible or invisible identification code embedded in the original data and which remains present within the data after any encryption process and is only separated from the original data after the decryption process (Cox *et al.*, 1997).

2.2.3 Characteristics of Digital Image Watermarking

The watermark systems have a number of characteristics (Mehto & Mehra, 2015), however, it is the requirements of a particular watermarking system that decides the comparative importance of each characteristic (Chahal & Khurana, 2013). Different applications need different properties of watermarking. Before designing any watermarking system the attributes described in the following sub-sections need to be taken into consideration (Tao *et al.*, 2014).

2.2.3.1 Imperceptibility

Imperceptibility is an important condition for digital watermarking that provides a visual similarity between the watermarked and original images. The perceptual worth of the original image should be transformed imperceptibly by the insertion of the watermark (Tao *et al.*, 2014). There are two major reasons why it is vital to keep the imperceptibility of the host data after the embedding with watermark media (Tao *et al.*, 2014).

1. The presence or absence of a watermark should not be differentiated from the fundamental purpose of the original image, even if the watermarked media is so badly distorted that its value is lost.
2. Suspicious perceptible artifacts may indicate the existence of a watermark and perhaps its precise location. This information may make it easy to distort, substitute or remove the watermark data maliciously, thereby making the information embedded in it no longer available.

2.2.3.2 Capacity

Capacity is also known as payload, can be defined as the total numbers of bits that are embedded into an original image (Chahal & Khurana, 2013). The number of bits could be different as the size of the watermark changes. Capacity defines the amount of the data that is embedded as the watermark and is detected during the extraction process. Watermark should be able to convey sufficient information to signify the uniqueness of the image. Dissimilar application has different capability desires (Thramboulidis, 2007).

2.2.3.3 Security

Security is a major interest where classified key has to be employed for insertion and detection process. Security is the capacity to repel intentional and unintentional attacks planned to change the role of embedding the watermark (Chahal & Khurana, 2013). A watermark should only be manageable by certified users and this is frequently accomplished by the use of cryptographic keys. Individual certified operators can legally detect, extract and even adjust the watermark, thus ensuring copyright protection (Singh & Chadha, 2013).

2.2.3.4 Robustness

Robustness is one of the most frequently measured attributes that gives an indication of how resilient the watermark embedded in data is to various attacks and common signal processing operations in digital watermarking systems (Tao *et al.*, 2014). Once some watermark signal is inserted in the original media, distortions may be applied to the signal unavoidably when the signal is encoded, decoded and distributed across the Internet. These distortions may be designed to apply the anticipated distortion to the watermarked signals or compress it before transmission, and they may or may not importantly disrupt the watermarked signals. It is difficult for a watermarking system to resist all signal processing operations where the condition is application subordinate and reliant.

A good watermarking method is likely to resist against noise addition, filtering processing, geometrical transformations such as scaling, translation and rotation, and also JPEG compression (Tao *et al.*, 2014). These methods can be classified as follows (Singh & Chadha, 2013):

1. Robust: this has to do with how to embed and recover watermark such that it would resist malicious or accidental attempts at removal (Chandramouli *et al.*, 2002). This type of watermarking can be used in copy control, fingerprinting, broadcast monitoring and copyright protection, (Liu & He, 2005).
2. Fragile: The watermark is planned to be ruined by any type of variation (even slight changes involving malicious and accidental attacks) to prevent any illegal manipulation (Abdullatif *et al.*, 2013 and Chandramouli *et al.*, 2002). Fragile watermarking is principally used for authentication applications such as integrity

protection, which must be very delicate to the changes of signal (Singh & Chadha, 2013).

3. Semi-fragile: Semi fragile watermarking is designed to tolerate some amount of modification to a watermarked image, such as the addition of quantization noise from lossy compression and is commonly used for image authentication (Singh & Chadha, 2013). (Chandramouli *et al.,* 2002).

2.2.3.5 Computational Complexity

Computational complexity describes the efficiency and cost in terms of time and space used by the algorithm. Computational complexity also describes the quantity of time a watermarking algorithm receipts to encrypt and decipher (Huang & Fang, 2010). It designates the overhead of using watermark embedders and detectors and as such the two main issues to be considered here are the time of embedding and detection and the amount of embedders and detectors (Abdullatif *et al., 2013*).

2.2.3.6 Verifiability

Watermark should be able to offer maximum and dependable evidence for the proprietorship of copyright-protected information products. Verifiability can be used to decide whether the object is to be protected, to monitor the extent of the data being protected, to ascertain the authenticity of the data and to control unlawful copying (Singh & Chadha, 2013).

However, the conditions of robustness, imperceptibility and capacity are conflicted and limited by each other. One may need to proliferate the watermarking strength in order to increase the robustness but this can result in a more observable watermark (Tao *et al.,* 2014). Consequently, one can decrease the capacity by reducing the amount of samples assigned to

each secreted bit but this is counterpoised by a loss of robustness. In other words, for any watermarking scheme, it is impossible to meet these three requirements simultaneously (Tao *et al.,* 2014). An optimal trade-off among these requirements in order to achieve improved watermarking is proposed in this research work.

2.2.4 Applications of Digital Image Watermarking

Digital image watermarking finds application in a wide range of areas that include the following:

1. **Copyright protection:** Watermarking can be used to prevent reallocation of copyrighted material over the unsecured network like Internet or one-to-one networks (Potdar *et al.,* 2005) and also to protect digital data against duplication. Copyright information can be embedded as a watermark whenever a new work is made and the watermark can be used as evidence, if any dispute in ownership of the digital data arises (Mehto & Mehra, 2015).
2. **Fingerprint:** In presentations where multimedia content is electronically shared through a network, the content possessor would like to discourage illegitimate replication and circulation by embedding a discrete watermark (or a fingerprint) in individual copy of the data. If, illegal copies of the data are discovered, at any time, then the source of the copy can be ascertained by recovering the fingerprint. In this application, the watermark needs to be imperceptible and must also be indestructible to deliberate attempts to forge, remove or invalidate it (Chandramouli *et al.,* 2002).
3. **Image and content authentication:** This is used to detect modifications to the image data. A digital signature can be used to proffer solution to this application which idea is derived from cryptography, as a message authentication method. Digital signature

represents some kind of summary of the original content (Mehto & Mehra, 2015). Integrity verification can be achieved by using fragile or semi fragile watermark which has low robustness to modification in an image (Singh & Chadha, 2013).

4. **Broadcast and publication monitoring:** This is refers to the technique of cross-verifying whether the content that was supposed to be broadcasted (on television (TV) or radio) is really what was broadcasted or not. Watermarking can also be used for broadcast monitoring, especially in commercial advertisement broadcasting where the entity that is advertising wants to monitor whether their advertisement was actually broadcasted at the right time and for right duration (Potdar *et al.*, 2005). Watermarking can also be used to monitor unauthorized broadcast stations (Jabade & Gengaje, 2011).
5. **Medical application:** Digital image watermarking can be adopted in medical images for various purposes. It used to protect the patient's information from unauthorized people, especially with the popularity of telemedicine, where images are easily distributed over the Internet (Chahal & Khurana, 2013).
6. **Covert communication:** The embedded data or watermark can be employed in the passing of secret messages from one person to another or from one computer to another computer stealthily (Katzenbeisser & Petitcolas, 2000 and Mehto & Mehra, 2015).

2.2.5 Digital image watermarking techniques

The field of digital watermarking has enkindled considerable interest in the research community due to its flexibility to convey necessary information that can be used to code the watermarks (Balasubramanya, 2016). There are numerous algorithms which are being used to

hide confidential information in watermarking processes. These algorithms are grouped into two major domains (Rahman, 2013):

1. Spatial Domain Technique

This technique applies the use of image pixels to embed an image (Balasubramanya., 2016). The process of embedding a watermark in the image therefore, involves the modification of the color value and intensity of the image of the pixels chosen. The spatial domain techniques do not require the secured images to be transformed and this makes them require low computational time for the watermark embedding and extraction processes (Araghi *et al.,* 2016). These techniques can easily be applied to many images although they are less robust against signal processing attacks than the transform domain techniques. The following are the spatial domain techniques (Deepti *et al.,* 2016):

a. Least Significant Bit (LSB) Technique

The LSB technique is mostly applied to embed watermark on randomly chosen pixels of the host image (Balasubramanya, 2016). The watermark is commonly inserted in the LSB of the chosen pixels. There are two types of LSB techniques. In the first method the LSB of the image is replaced with a pseudo-noise (PN) series while in the second a PN series is added to the LSB (Deepti *et al.,* 2016). This method is easy to use but not very robust against attacks

b. Patchwork Technique

In patchwork, *n* pairs of image points, (a, b), are randomly selected, where the image data in *a,* is lightened while that in *b* is darkened. Only very small amount of information can be hidden in this technique at a time even though it has a high level of robustness against different types of attacks (Deepti *et al.,* 2016).

c. Predictive Coding Scheme

In this scheme, a PN pattern say W (a, b) is summed to the cover image in order to increase the strength of the watermark by increasing the gain factor. However, image quality may decrease due to high increment in gain factor (Kester *et al.*, 2014).

2. Transform Domain Technique

In this technique, the images are represented in form of frequencies. This implies that the images will first be transformed before starting the watermark embedding process on the decomposed transform coefficients (Balasubramanya, 2016 and Mehto & Neelesh, 2015). The transform domain techniques provide greater robustness of the watermarked content to signal procedures attacks than the spatial domain algorithms since they hide private information in significant areas of the cover image. In order to obtain the watermark image, the inverse of the process used to embed is performed. The most used transform domain technique includes the following (Balasubramanya, 2016):

a. Discrete Wavelet Transform (DWT)
b. Discrete Fourier Transform (DFT)
c. Singular Value Decomposition (SVD)
d. Stockwell Transform (ST)
e. Discrete Orthonormal Stockwell Transform (DOST)

A more recent technique for image processing and analysis has been developed called the S-transform domain (Yan & Zhu, 2011). This technique comprises of Stockwell transform (ST), discrete Stockwell transform (DST) and discrete orthonormal Stockwell transform (DOST).

2.2.5.1 Discrete Wavelet Transform (DWT)

DWT is a mathematical tool for hierarchically splitting an image. It is valuable for processing of motion signals such as images, video and audio signals (Chanda & Choudhury, 2016). The transform is centered on little waves, called wavelets, of changing frequency and limited duration. The DWT is an improvement of DCT such that the technique analyses the signal at multiple resolutions, that is, it represents the image in multi resolutions form. The image is divided into two types of quadrants which include high frequency and low frequency quadrants signal (Chanda & Choudhury, 2016).

Wavelet sequence is an illustration of a square integral function of a sure orthonormal series produced by a wavelet (Paliwal & Jain, 2015). In two-dimensional dissociable dyadic DWT, each level of decomposition creates four bands of data, one equivalent to the low pass-band (LL), and three other corresponding to horizontal (HL), vertical (LH), and diagonal (HH) high pass-bands. The splitted image indicates a coarse approximation image in the lowest resolution low pass-band and three detailed images in higher bands. The low pass-band can further be splitted to obtain a new level of decomposition (Araghi *et al.,* 2016). This process can be sustained up to the preferred level of decomposition is determined by the kind of application that is of concern (Malonia & Agarwal, 2016). DWT can be performed by low pass and high pass filtering of an image, where the high pass filter creates detailed pixels of the image and low pass filter creates coarse approximation image pixels. The outputs are down-sampled by 2 after performing the low pass and high pass filtering. Owing to its exceptional spatial-frequency localization properties, the DWT is very appropriate in identifying the regions in the host image where a watermark can be inserted effectively (Koju

& Joshi, 2015). Examples of two dimensional applications for three different levels of DWT decomposition are depicted in Figures 2.1 to 2.3 (Chanda & Choudhury, 2016)

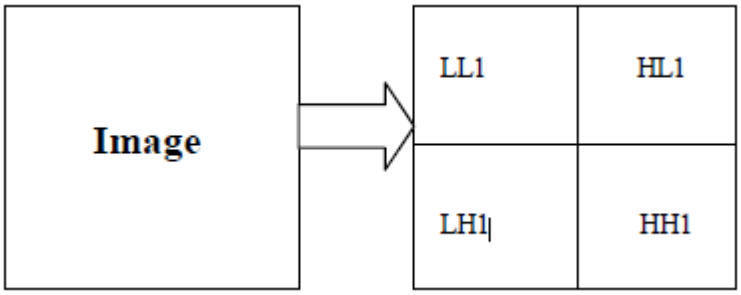


Figure 2.1: 1-Level DWT Decomposition

Figure 2.1 shows the first level decomposition of an image by DWT into four frequency sub-band. The four bands of data obtained represents low pass-band that denotes LL1 and the other corresponds to horizontal (HL1), vertical (LH1) and diagonal (HH1) high pass-band of the image respectively.

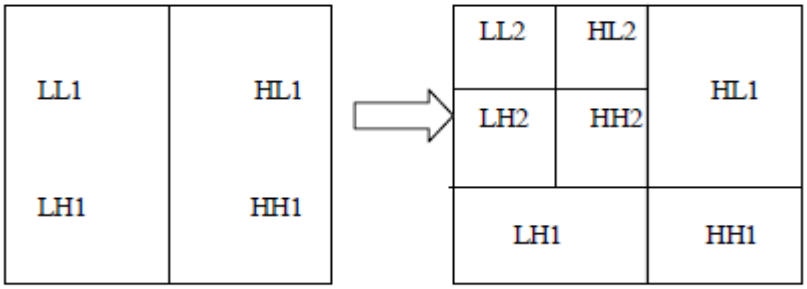


Figure 2.2: 2-Level DWT Decomposition

Figure 2.2 depicts the second level decomposition of an image by applying DWT to the low pass-band LL1 of the first level decomposition of the image to obtain second level frequency sub-bands. The four bands of data obtained represents low pass-band that denotes LL2 and the other corresponds to horizontal (HL2), vertical (LH2) and diagonal (HH2) high pass-band of the image.

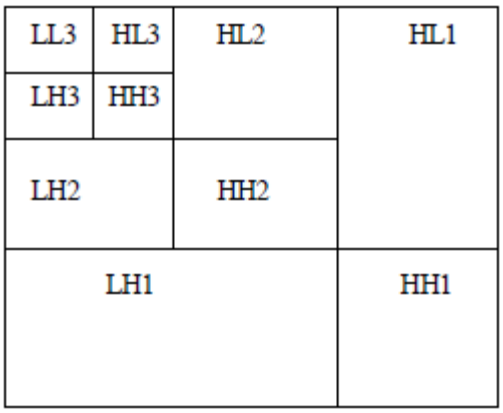


Figure 2.3: 3-Level DWT Decomposition

Figure 2.3 depicts the third level decomposition of an image by applying DWT to the low pass-band LL2 of the second level decomposition of the image to obtain third level frequency sub-bands. The four bands of data obtained represents low pass-band that depicts LL3 and the other corresponds to horizontal (HL3), vertical (LH3) and diagonal (HH3) high pass-band of the image respectively.

Therefore, two dimensional (2-D) forward DWT of image $f(x, y)$ of size $K \times L$ can be defined as (Venkatram *et al.*, 2014a):

$$w_{\varphi}(j_0, m, n) = \frac{1}{\sqrt{MN}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f(x, y) \varphi_{j_0,m,n}(x, y) \quad (2.1)$$

$$w_{\Psi}^{i}(j, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \Psi_{j,m,n}^{i}(x, y), \; i = (\mathrm{H}, \mathrm{V}, \mathrm{D}) \quad (2.2)$$

Where:

J, *m*, *n M*, *N* are integers, $i = (\mathrm{H}, \mathrm{V}, \mathrm{D})$

Where H depicts horizontal component of the image, V denotes the vertical component of the image and D represents the diagonal component of the image

j_0 *denotes an a*rbitrary starting scale ($j_0 = 0$)

$w_\varphi(j_0, m, n)$ depicts approximation coefficients of $f(x, y)$ at scale j_0

$w_\Psi^i(j, m, n)$ represents horizontal, vertical and diagonal detailed coefficients at scales

$j \geq j_0$ $M = N = 2^j, for\ j = 0,1,2, \dots, j-1, m, n = 0,1,2, \dots, 2^j - 1.$

Given w_φ and w_Ψ^i the image $f(x, y)$ can be recovered from 2-D inverse DWT as follows (Venkatram *et al.*, 2014b):

$$f(x,y) = \frac{1}{\sqrt{mn}} \sum_m \sum_n w_\varphi(j_0, m, n) \varphi_{j_0, m, n}(x, y) + \frac{1}{\sqrt{mn}} \sum_{i=H,D,V} \sum_{j=j_0}^{\infty} \sum_m \sum_n w_\Psi^i(j, m, n) \Psi^i_{j,m,n}(x, y) \quad (2.3)$$

There is a variety of prevalent wavelets including Daubechies, Mexican Hat, Haar, and Morlet (Chen & Zhan, 2008). These wavelets have the benefit of better resolution for efficiently varying time series, even though they are computationally difficult to implement (Chen & Zhan, 2008).

2.2.5.2 Discrete Fourier Transform (DFT)

DFT also converts an image from spatial domain to frequency domain and in this circumstance; it has the advantage of separating the magnitude and phase of an image in the frequency domain. The 2D-DFT of an image f(x, y) of size G×H can be defined as (Mehto & Mehra, 2015):

$$F(u, v) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi\left(\frac{ux}{M} + \frac{vy}{N}\right)} \quad (2.4)$$

2.2.5.3 Singular Value Decomposition (SVD)

SVD is implemented by decomposing the matrix of an image into two orthogonal matrices and one diagonal matrix consisting of the singular values of the original matrix (Kaur & Jindal, 2014). It is a worthwhile tool in computer vision as a decomposition matrix valuable

for image transformations (Rahman, 2013). The SVD of an image B with size $m \times m$ can be defined as (Lai *et al.*, 2013):

$$B = USV^T \tag{2.5}$$

where: U and V are orthogonal matrices, S = diag(λi) is a diagonal matrix of singular values λi, $i = 1, \ldots, m$, which is organized in declining order. It can be represented as (Rahman, 2013):

$$S = \begin{bmatrix} S_1 & 0 & \bullet & 0 & 0 \\ 0 & S_2 & \bullet & 0 & 0 \\ \bullet & \bullet & \bullet & \bullet & \bullet \\ 0 & 0 & \bullet & S_{n-1} & 0 \\ 0 & 0 & \bullet & 0 & S_n \end{bmatrix}$$

The columns of U are the left singular vectors, whereas the columns of V are the right singular vectors of the image B.

SVD of B can be written as (Lai *et al.*, 2013):

$$B = USV^T = \sum_{i=1}^{r} \lambda_i u_i v_i^T \tag{2.6}$$

Where: r denotes the rank of A, u_i represent left singular vector, v_i depicts right singular vectors.

It is vital to observe that the singular values identify the luminance of the image, whereas the equivalent pair of singular vectors specifies the geometry of the image. There are two key properties that is employed in SVD technique for digital-watermarking:

(i) There is no room for huge disparity of its singular value, when a minor disturbance is introduced to an image.

(ii) Intrinsic algebraic image properties signify the singular values

2.2.5.4 Stockwell Transform (ST)

ST is a transformation technique introduced in 1996 that offers a complete time (or space)-frequency decomposition of a signal (Ouazzane *et al.*, 2017). The actualization of ST is based on the fusion of the short-time Fourier transform (STFT) and the wavelet transforms (WT) that delivers a time-frequency depiction of a signal with a frequency-dependent resolution. The ST has recorded successes in many areas including geophysics and biomedicine (Yan & Zhu, 2011), due to its multi-resolution analysis, easy interpretation, and ability to maintain meaningful local phase information. In STFT, time-frequency analysis is introduced to deal with time distribution for different frequencies. However, the STFT cannot track the signal dynamics properly for non-stationary signals owing to the boundaries of fixed window width. WT is good at extracting information from both time and frequency domains, but is sensitive to noise (Wang, 2011). For instance, let a function *h(t),* the STFT of a signal *h(t)* can be defined as (Wang, 2010):

$$STFT(\tau, f) = \int_{-\infty}^{\infty} h(t) g(\tau - t) e^{-j2\pi f t} dt \tag{2.7}$$

where: τ and f denote the time of spectral localization and Fourier frequency, respectively and $g(t)$ denotes a window function.

The ST can be derived by replacing equation (2.8) with the window function $g(t)$ in equation (2.9) with the Gaussian function, defined as (Wang, 2010):

$$g(t) = \frac{|f|}{\sqrt{2\pi}} e^{\frac{t^2 f^2}{2}} \tag{2.8}$$

Therefore, the continuous ST of a signal *h(t)* can be shown as (Yan & Zhu, 2011):

$$S(\tau, f) = S\{h(t)\} = \int_{-\infty}^{\infty} h(t) \frac{|f|}{\sqrt{2\pi}} e^{-\frac{(\tau - t) f^2}{2}} e^{-j2\pi f t} dt \tag{2.9}$$

Where: *f* represents the frequency variable, *t* denotes the time variable, τ depicts the time translation

The evaluation of inverse fourier transform of *H*(*f*) recovered the original function *h(t)* (Wang & Orchard, 2009):

$$h(t) = S^{-1}\{S(\tau, f)\} = \int_{-\infty}^{\infty}\{\int_{-\infty}^{\infty} S(\tau, f)d\tau\}e^{i2\pi ft}df \quad (2.10)$$

Using the same frequency-domain description of the ST, the discrete ST (DST) can be defined as (Ouazzane *et al.*, 2017):

$$S\left[jT, \frac{n}{NT}\right] = \sum_{m=0}^{N-1} H\left[\frac{m+n}{NT}\right] e^{-2\pi^2 m^2/n^2} e^{i2\pi mj/N}, \text{n} \neq 0 \quad (2.11)$$

where, $H\left[\frac{n}{NT}\right]$ is the DFT of the N-point time sequence $h[kT]$, m and j = 0,1,…..,$N-1$and n=1, 2,….$N-1$.

For n =0, voice is the invariable:

$$S[jT, 0] = \frac{1}{N}\sum_{m=0}^{N-1} h[mT] \quad (2.12)$$

The DST has been applied in amongst others, the following areas (Wang & Orchard, 2009):

(i) In geophysics for examining inner atmospheric wave packets

(ii) In atmospheric studies characterization of seismic signals,

(iii)In global sea surface temperature analysis

(iv)In digital signal processing

ST and DST are redundant with respect to digital images and thus induce high computational difficulty for lengthy and multidimensional signals (Ouazzane *et al.*, 2017). The ST becomes exponentially more costly for higher-dimensional data. Due to these imperfections of the ST, a more efficient scientific measurable and computational efficient algorithm proposed to

pursue this time-frequency decomposition. This new proposed time-frequency decomposition is a non-redundant form of ST called DOST introduced in 2007 (Ouazzane *et al.*, 2017).

2.2.5.5 Discrete Orthonormal Stockwell Transform (DOST)

An orthonormal transformation takes an *N*-point time sequence to an *N*-point time-frequency illustration, consequently achieving the full efficiency of representation. Beside, every point of the outcome is linearly independent from any other point (Stockwell, 2007). The alteration matrix (taking the time series to the DOST depiction) is orthogonal, meaning that the inverse matrix is equal to the complex conjugate transpose. The vector norm is conserved in an orthonormal transformation domain according to the Parseval theorem (the norm of the time series equals the norm of the DOST). An energy preserving transform is referred to as orthonormal transform (Stockwell, 2007) since it reduces the information redundancy of the DST to nil leading to the maximum efficacy of a representation (Yan & Zhu, 2011). DOST sub-samples low frequencies while high frequencies are sampled with higher rates and utilizes this sample spacing arrangement to distribute its coefficients accordingly (Wang & Orchard, 2009).

Therefore, the efficient illustration of the S-transform can be stated as the inner products between a time series $h[kT]$ and a set of orthonormal basis functions evaluated as $[kT]$ as shown (Stockwell, 2007):

$$S\left\{h\left[kT\right]\right\} = S\left(\tau T, \frac{\nu}{NT}\right) = \sum_{k=0}^{k=N-1} h\left[kT\right] S_{[\nu,\beta,\tau]}\left[kT\right] \tag{2.13}$$

where; ν depicts the middle of a frequency band and similar to the "voice" of the wavelet transform).

β represent the breadth of the frequency band

τ denotes the time localization

The DOST is mainly founded on a set N of orthonormal basis vectors each denoting an exact section in the time (or space)-frequency domain (Ouazzane *et al.*, 2017). These basis functions $S_{[v,\beta,\tau]}[kT]$ for the general case are defined as (Stockwell, 2007):

$$S_{[v,\beta,\tau]}[kT] = \frac{ie^{-i\pi\tau}}{\sqrt{\beta}} \frac{\left\{ e^{-i2\pi\left(k/N - \tau/\beta\right)\left(v - \beta/2 - 1/2\right)} - e^{-i2\pi\left(k/N - \tau/\beta\right)\left(v + \beta/2 - 1/2\right)} \right\}}{2Sin\left[\pi\left(k/N - \tau/\beta\right)\right]} \tag{2.14}$$

Where; $k = 0,1 \ldots \ldots \ldots \ldots N-1$

It is presumed that orthogonality is proven through an appropriate selection of the parameters values (v, β, τ). An octave sampling of the time-frequency domain is also chosen to be twice the breadth of each increasing voice bandwidth (Ouazzane *et al.*, 2017).

At this period, the sampling of the time-frequency space has not hitherto been determined. In order to ensure sampling of the time-frequency space for orthogonality to occurred. The following conditions must be observed (Stockwell, 2007):

(i) Rule 1: τ*=0, 1, 2,…,* p *-1.*

(ii) Rule 2: v *and* β must be selected such that each Fourier frequency sample is adopted on only one ocassion

Normally, an octave number $p = 0,1,2, \ldots \ldots \log_2(N) - 1$ is used to define the parameters (v, β, τ) and each of the basis vectors is computed as follows (Ouazzane *et al.*, 2017):

When $p = 0$, $v = 0$, $\beta = 1$, $\tau = 0$,

and $S_{[v,\beta,\tau]}[kT] = 1$ (2.15)

when $p = 1$, $v = 1$, $\beta = 1$, and $\tau = 0$:

$$S(kT)_{[v,\beta,\tau]} = e^{-\frac{i2k\pi}{N}} \tag{2.16}$$

For $p = 2, .\log_2(N) - 1$, $v = 2^{(p-1)} + 2^{(p-2)}$, $\beta = 2^{(p-1)}$ and $\tau = 0,1, \ldots, 2^{(p-1)} - 1$

$$S(kT)_{[v,\beta,\tau]} = ie^{-i\pi\tau}\frac{e^{-i2\alpha\left(v-\beta/2-1/2\right)}-e^{-i2\alpha\left(v+\beta/2-1/2\right)}}{\sqrt[2]{\beta sin\alpha}} \quad (2.17)$$

N coefficients produced from N length signal by DOST can be organized as shown in Figure 2.4 (Ouazzane *et al.*, 2017):

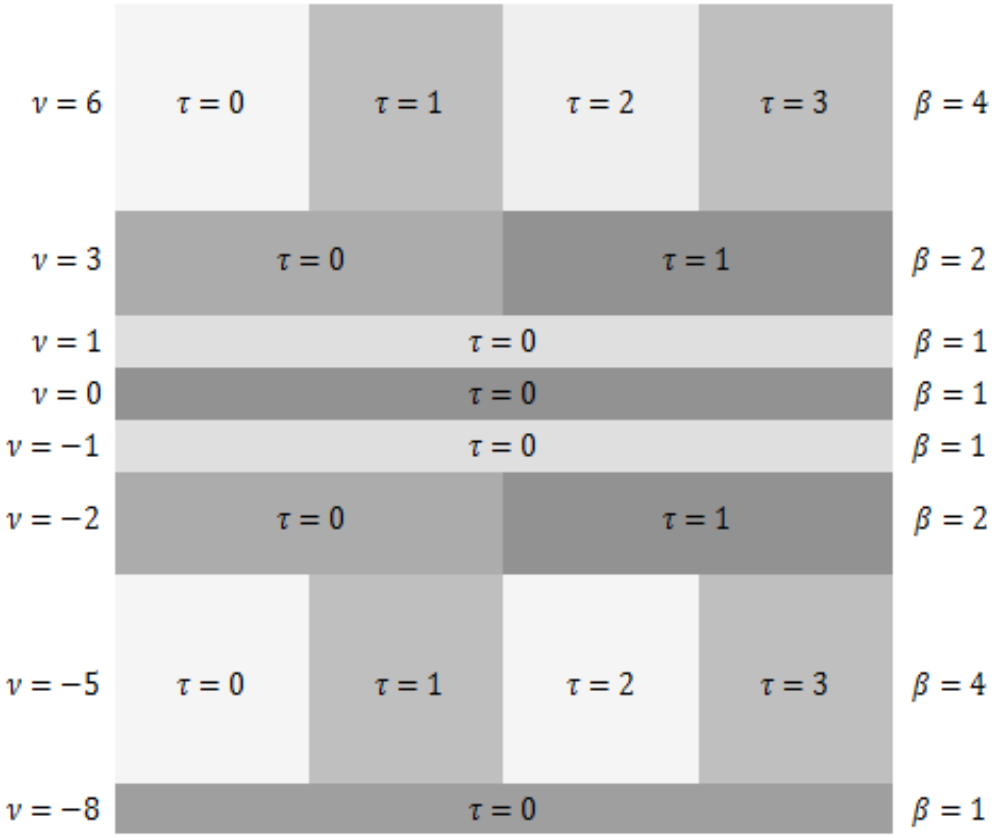


Figure 2.4: Time-Frequency of the DOST Coefficients of Signal Length of 16

The time localization index τ is negative for negative frequencies in Figure 2.4 in order to generate symmetry between positive and negative frequency components (Wang, 2011). The zero-frequency constituents are hence in the centre of Figure 2.4. The visualization of time-frequency DOST coefficients is realizable with respect to storage convention and computation, in which the DOST coefficients of a signal of size N can be stored in an N-tuple vector (Wang, 2011). However, it is more common to analyze the data in its 2D form and as

such the 2D visualization can be implemented according to the order of Figure 2.5 (Wang, 2011).

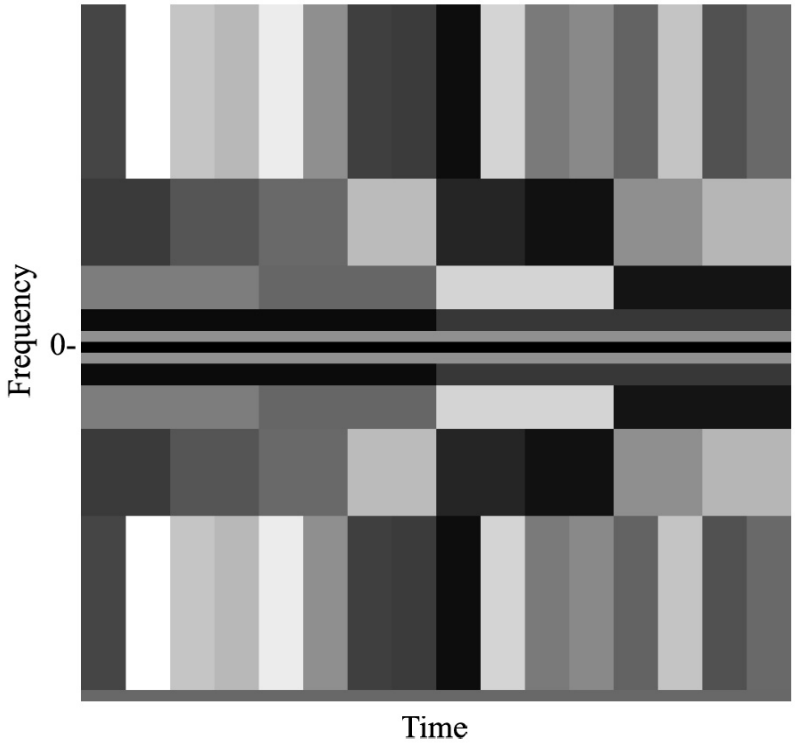


Figure 2.5: 2D Visualization of DOST Coefficients of Signal Length of 64

Figure 2.5 gives an outlook of this visualization, where the horizontal axis is consistent with the temporal index of the signal and the vertical axis is consistent with the ordered frequency bands (Wang, 2011). Based on the definition of ST in the equivalent frequency domain, the forward 2D-DOST of a $N\,X\,N$ image starts by defining the forward 2D-FT of a discrete function f(x,y) which is assumed to have a sampling interval of one in the x and y direction is represented as (Drabycz, Stockwell, & Mitchell, 2009):

$$H\left[m,n\right]=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}h\left[x,y\right]e^{-2\pi i\left(\frac{mx}{M}+\frac{ny}{N}\right)} \tag{2.18}$$

The original image can, therefore, be reconstructed by evaluating the inverse 2D-FT (Drabycz, Stockwell, & Mitchell, 2009):

$$h[x,y] = \frac{1}{MN} \sum_{n=-\frac{M}{2}}^{\frac{M}{2}-1} \sum_{n=-\frac{N}{2}}^{\frac{N}{2}-1} H[m,n] e^{2\pi i\left(\frac{mx}{M}+\frac{ny}{N}\right)} \quad (2.19)$$

where, $H(n,m)$ denotes the discrete 2-D Fourier coefficients, x ranges as $0,1,\dots,N-1$, y ranges as $0,1,\dots,M-1$, and $m\ and\ n\ ranges\ as\ 0,1,\dots N-1$.

The 2D DOST provides the convenience and the freedom to manipulate data over spatial and frequency domains. Since image signals have 2D data structure, 2D DOST is adopted in this research.

2.2.6 Comparison between Digital Image Watermarking Techniques

The distinction between individual candidate of spatial and transform domain in terms of their characteristics and the differences between the individual transform techniques are depicted in Tables 2.1 and 2.2 respectively.

Table 2.1: Comparison Between Spatial and Transform Domain (Araghi *et al.*, 2016)

Characteristics	Spatial Domain	Transform Domain
Capacity	High	Low
Imperceptibility	High	Low
Robustness	Fragile	More robust
Speed	Fast	Slow
Simplicity	Yes	No
Computational load	Low	High
Security	No	Yes

Table 2.2: Comparison between Individual Transform Domain Techniques (Araghi *et al.*, 2016, Yan & Zhu, 2011 and Stockwell, 2007)

Techniques	Merits	Demerits
DWT	1. Excellent spatial localization 2. Frequency spread (multi resolution) 3. Excellent time frequency analysis (DWT captures both frequency & location information) 4. Good energy compaction 5. Good for signal processing attacks 6. Compatible with jpeg2000 for compaction 7. Higher compression proportion which is pertinent to human sensitivity	1. Computational complexity 2. Less robustness against geometric attacks 3. Noise/blur close to edges of images or video frames
DFT	1. Good resistant against scaling and rotation attacks	1. Not robust to some geometric attacks like cropping & shearing 2. Loss of time frequency analysis can result to difficulties in processing 3. Not compatible with standard image compression techniques (JPEG, JPEG2000, etc.)
DCT	1. Good imperceptibility 2. Compatible with JPEG compression standards 3. Easier computation compared with DFT 4. Reasonable complexity with respect to execution time	1. Block effect (higher compression ratio makes the blocks visible) 2. Effect of picture cropping

SVD	1. Good resistance against geometric and signal processing attacks (high robustness) 2. High energy compaction 3. Low computation cost	1. High false positive outcomes
DST	1. Excellent time-frequency analysis of signal which perfectly maintains the absolutely referenced frequency and local phase information. 2. It is easy to interpret	1. Its redundant nature, makes the DST to double the dimension of the original data (or information), due to this redundancy , use of DST is computationally expensive and even infeasible for higher dimensional data such as images
DOST	1. Reduces the information redundancy of the DST to naught and leads to the maximal efficacy of a depiction. 2. High energy compaction.	1. Its non-redundancy provides a coarse time-frequency representation Such representation may not always be adequate to disclose all the details within a particular signal

It could be observed from Table 2.2 that the DOST offers the most vital merits due to the fact that it distinctively aggregates progressive resolution and absolutely-referenced information of phase of a signal collectively (Kumar & Agrawal, 2015). DWT is differentiated from DOST because of the presence of absolute reference phase property in DOST. In Wavelet Transform (WT), as the wavelet translates, the phase reference designate also translates (called locally referenced phase) however, the phase reference information of a signal in DOST is constantly referenced at turning point (Kumar & Agrawal, 2015). DOST suffer from inability to sufficiently reveal all the details within a given signal due to its coarse time-frequency

representation and such representation may not always be easy to interpret. DWT does not exhibit coarse time-frequency representation which enables it to reveal all the edge details of an image with suitable level of decomposition. The use of SVD will add an extra security layer because of its good resistance to both geometric and signal processing attacks and this would strengthen the security of the embedded watermark.

2.2.7 Attack on Digital Image Watermarking

Attacks as apply to this research can be defined as the introduction of noise and other geometric attack to watermarked image. Attack can be categorized as intentional or unintentional (Mehto & Mehra, 2015). Intentional attacks use all available resources to modify or destroy the watermark. The idea is to make it as difficult as possible to detect. The methods used in intentional attacks are as follows (Friedman, 1993):

1. Signal processing techniques
2. Cryptanalysis
3. Stag analysis.

Unintentional attacks, on the other hand, are inevitable as the transmission media are usually not perfect leading to noise which can cause distortions.

Apart from the intentional or unintentional attacks, there is also the approximation based attacks. In this case, estimates of either the watermark data or the original object can be achieved using random methods and the attacks can be categorized as removal, protocol, or desynchronization liable on the method used for the estimation (Friedman, 1993, Liu & He, 2005).

2.2.7.1 Signal Processing Attacks

Signal or image processing attacks are non-geometric attacks and include the following (Chahal & Khurana, 2013):

1. Noise: This is any random unwanted signal with a given distribution like Gaussian, salt and pepper, Poisson, etc. that is added to the image unintentionally. The noise may be added during the analog to digital conversion and vice-versa or as a result of transmission impairments.
2. Image Compression: In order to minimize the memory location and reduce the rate of bandwidth needed for transferring images, images are usually compressed with JPEG, JPEG2000, etc. compression techniques (Singh & Chadha, 2013). However, image compression techniques yield irretrievable variations to the watermarked images and as such the likelihood of reconstructing watermark information is very low.

Others include filtering, brightness, sharpening, printing, scanning and gamma correction

2.2.7.2 Geometric Attacks

These attacks are used to influence the watermarked image in such a manner that the detector cannot detect the watermark data (Mehto & Mehra, 2015). Unlike the non-geometric attacks, geometric attacks are meant to deform or distort the transformations of the watermarked image contents and not the removal of the embedded watermark (Singh & Chadha, 2013). For instance, rotation, translation and scaling in addition to line and column removal, cropping and warping are typical examples of this type of attack (Tao *et al.,* 2014). Two of the major attacks in this domain are discussed as follows (Malonia & Agarwal, 2016):

1. Cropping Attack: Refers to cutting a part (outer elements) of an image in order to boost framing.

2. Rotation Attack: Image rotation alters the original aspect of an image by a certain angle, which can destroy the synchronization of the watermark detector.

2.2.8 Performance Evaluation Metrics

Dissimilar statistical measures are used for the performance examination of watermarked image and extracted watermark. The watermark robustness hinges directly on the embedding strength, which in turn stimulates visual degradation of the image (Jabade & Gengaje, 2011). For benchmarking and performance evaluation, the following metrics are used:

1. **Mean square error (MSE):** MSE is measured by an average squared difference between reference image and watermarked image (Malonia & Agarwal, 2016). It is determined using (Mehto & Mehra, 2015):

$$\text{MSE} = \frac{1}{X \times Y} \sum_{j=1}^{X} \sum_{t=1}^{Y} (X(j,t) - X'(j,t))^2 \tag{2.20}$$

where: $X(j, t)$ = Original image, $X'(j, t)$ =Watermarked image, X = Number of rows in the image, Y = Number of columns in the image.

2. **Peak Signal to Noise Ratio (PSNR):** PSNR measures the degradation in the watermarked image with respect to the host image (i.e. the quality of a watermarked image)(Mehto & Mehra, 2015). It is determined using (Singh & Chadha, 2013):

$$PSNR = 10 \log_{10} \left(\frac{L^2}{MSE} \right) \tag{2.21}$$

Where, L is the peak signal value of the original image which is equivalent to 255 for 8 bit images.

If the PSNR value is greater than 35dB then the perceptual quality of the algorithm is satisfactory (Malonia & Agarwal, 2016).

3. **Correlation coefficient (CRC):** CRC is a metric, ranging from 0 to 1 that is used to evaluate the relationship between the original and recovered watermark (Jabade & Gengaje, 2011). The CRC defines the resemblance between the original and extracted watermark images used to depict the manner the algorithm is resilience to attack. The CRC is normalized by subtracting the mean and dividing by standard deviation. NCC can be defined as follows (Venkatram *et al.*, 2014a):

$$NCC = \frac{\sum_{y \in k} 1 \sum_{z \in j} I^{j}(\mathrm{y},\mathrm{z}) \times W^{ji}(\mathrm{y},\mathrm{z})}{\sqrt{\sum_{y \in k}\sum_{z \in j}\left[I^{j}(\mathrm{y},\mathrm{z})\right]^{2}}\sqrt{\sum_{y \in k}\sum_{z \in j}\left[W^{ji}(\mathrm{y},\mathrm{z})\right]^{2}}} \tag{2.22}$$

4. **Structural Similarity Index Measure (SSIM):** SSIM gives an indication of the similarity between two images. The closer the SSIM value is to 1, the more similar the original watermark and extracted watermark images will be (Benrhouma *et al.*, 2015). SSIM can be determined using (Kaur & Jindal, 2014):

$$SSIM(X,\mathrm{Y}) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{2.23}$$

5. **Bit Error Rate (BER):** BER is the proportion of the amount of incorrectly deciphered bits to the size of the binary series and can be determined using (Jabade & Gengaje, 2011):

$$BER = \frac{DB}{NB} \tag{2.24}$$

Where, DB is amount of wrongly decoded bits and NB is whole number of bits.

2.2.9 Cryptography

Cryptography is a field of applications that furnishes users with authentication, confidentiality and privacy (Scarani *et al.*, 2009). Cryptography can be defined as the skill of providing a

message indecipherable to any unapproved party (Weerasinghe, 2012). It is a part of the wider field of cryptology, which similarly contains cryptanalysis, the skill of code breaking. To attain this goal, an algorithm called cipher is employed to chain a message with some additional information known as a key and yield a cryptogram in a method called encryption (Weerasinghe, 2012). Therefore, a key is a bit of information or a parameter that ensures the task of a cryptographic algorithm as it stipulates the specific transformation of plaintext into cipher text, or vice versa during decryption (Sasirekha & Hemalatha, 2014**).**

There are three kinds of cryptographic schemes (Lokhande & Gulve, 2014):

1. **Symmetric Key System:** Symmetric (secret, session or private) key cryptography uses a single key or same set of keys for both sender and receiver to encrypt and decrypt data (Lokhande & Gulve, 2014). Its utility diminishes when the user wants to exchange keys on unsecured channels. Different set of keys must be maintained for different users. If there are 'n' number of peoples on the group then it is necessary to administer n(n-1)/2 set of keys which are distinct and private (Elboukhari *et al.*, 2010). Examples of a symmetric key system are data encryption standard (DES) and one-time-pad (OTP) (Weerasinghe, 2012).
2. **Asymmetric Key System:** This system includes the use of unlike keys for encryption and decryption and is generally known as public-key cryptosystems (Elboukhari *et al.*, 2010). The fundamental concept of public key distribution was principally introduced in 1976 by Whitfield Diffie and Martin Hellman (Weerasinghe, 2012). Examples of asymmetric key systems are Diffie Hellman and Ronald Rivest, Adi Shamir,and Leonard Adleman (RSA) (Kester *et al.*, 2014).

3. **Hash Function:** Hash function takes a relatively arbitrary amount of input and produces a fixed size of output. The properties of some hash functions can also be utilized to verify and confirm the source of a file or the integrity of any network packet or arbitrary data, therefore, contributing to an increase in the security level. By using the message digests generated by a cryptographic hash function, unauthorized changes in files can be detected. This is especially important when safeguarding critical system binaries and sensitive databases (Lokhande & Gulve, 2014).

After critical examination of the cryptographic encryption schemes in multimedia data, the asymmetric key algorithm has extreme computational costs which is usually unreasonable to be used for multimedia data (Nag *et al.,* 2011). Symmetric key encryption schemes are relatively low in cost and might be employed for multimedia contents (such as image, video and audio). However, the characteristics of multimedia contents are completely different from text data, due to absence of data redundancy while multimedia (such as images) possesses a lot of redundancy that enables the pixel values of a neigbouring pixel to be predicted accurately (Nag *et al.,* 2011). In order to enhance the computational overhead and security of this proposed algorithm, affine transform and XOR operation is adopted for the shuffling and encryption of the watermark image.

2.2.9.1 Challenges of Classical Key Distribution

The safety of the public key ciphers that are used to distribute symmetric keys relies on the strength of the mathematical algorithms and the capabilities of the attacker (Anghel, 2009). Classical cryptographic algorithms are conceived to be realistically secure founded on years of public scrutiny over the basis process of factoring large integers into their primes (Sharma & De, 2011). The safety of public key cryptography algorithms, however, is presently

centered on the unverified assumptions of the complexity of integer factorization or the discrete logarithm problem. This means that public key cryptography algorithms are possibly susceptible to improved and more computationally efficient algorithms (quantum computing) developed to solve both integer factorization and discrete logarithm problems (Haitjema, 2007). One of these efforts has led to the development of quantum cryptography that addresses these challenges by using quantum properties to exchange secret information over an insecure channel (Anghel, 2009).

2.2.9.2 Quantum Cryptography

Stephen Wiesner, who developed the concept of quantum cryptography (Gisin *et al.,* 2008), disclosed how to stock or transfer two messages by encoding them in two "conjugate observables", such as linear and circular polarization of light, so that any, but not both, may be received and decoded. This idea led to the development of unforgeable bank notes (Elboukhari *et al.,* 2010). Quantum cryptography relied on the fundamental and static principles of quantum mechanics and does not depend on the difficulty of factoring large numbers (Ajay, 2016). These principles comprise the Heisenberg uncertainty principle and the principle of photon polarization (Lo *et al.,* 2014) and the no-cloning theorem (where entangled quantum bits are used to share secret keys) (Holloway, 2012). The paramount application of quantum cryptography is quantum key distribution (QKD) which promises to achieve an enhanced security situation for communication systems (Gümüş *et al.,* 2008).

1. **Heisenberg Uncertainty Principle:** Uncertainty principle states that it is not likely to quantify the quantum state of any system without perturbing that system (Poels *et al.*, 2005). The uncertainty principle can be defined as follows (Poels *et al.*, 2005):

Suppose $\hat{A}$ and $\hat{B}$ are Hermitian operators representing the observables *A* and *B*. For the variances of *A* and *B* it then holds that

$$\sigma_A^2 \sigma_B^2 \geq \left(\frac{1}{2i}\langle[\hat{A}, \hat{B}]\rangle\right)^2 \tag{2.25}$$

This is the general uncertainty principle. If $\hat{A} = x \; and \; B = p$

where $[\hat{x}, \hat{p}] = i\hbar$ (2.26)

$$\sigma_x^2 \sigma_p^2 \geq \left(\frac{1}{2i} i\hbar\right)^2 = \frac{\hbar^2}{4} \tag{2.27}$$

and thus

$$\sigma_x \sigma_p \geq \frac{\hbar}{2} \tag{2.28}$$

This inequality is better known as the Heisenberg uncertainty principle.

2. **Photon Polarization:** Polarization of a photon (or light particle) can only be defined at the spot when it is quantified (Lo *et al.*, 2014). This principle plays the following roles (Lo *et al.*, 2014):
    a. Quantum cryptography aid avoidance of eavesdropping in a cryptosystem
    b. Depiction of how light photons can be oriented or polarized in particular directions.

    Furthermore, a photon filter with accurate polarization can only detect a polarized photon or else the photon will be damaged. It is this "one-way-ness" of photons along with the Heisenberg uncertainty principle that makes quantum cryptography a fascinating choice for certifying the secrecy of data and overcoming eavesdroppers.
3. **No cloning:** The no-cloning theorem states that it is impossible to duplicate a quantum state that is unknown (Holloway, 2012). This essentially means that a quantum state from a given set of states can be cloned only if the states within the set are mutually

orthogonal (Bhandari, 2014), such as |0>, |1>, |+>, |->, which are not mutually orthogonal in entangled photon.

2.2.9.3 Quantum Key Distribution (QKD)

Key distribution can be defined as a function that delivers a shared random secret key (which is used to encrypt and decrypt messages) to two parties who wish to communicate (Charjan & Kulkarni, 2015 and Bennett & Brassard, 1984). Therefore, it is pertinent to have a secure key distribution system because if the key gets compromised then the whole system gets compromised too (Charjan & Kulkarni, 2015). This has led to the development of more secured key distribution schemes like the QKD based on the fundamental principle of quantum physics.

QKD is a revolutionary security protocol which generates limitless numbers of symmetric keying material between two geographically divided parties (Mailloux *et al.,* 2017). QKD is well suited for high-security applications in banking, government, and military environments (Mailloux *et al.,* 2017) as it has an essential and sole attribute of quantum distribution and the capability of the two interactive parties to notice the existence of any third party trying to acquire knowledge of the key (Sinha *et al.*, 2017).

QKD can only be used to create and allot a key, not to transfer any message (Bennett *et al.,* 1990). The distributed key can be used with any selected encryption algorithm to encode or decode a message, which can then be transferred over a regular communication channel. One-time pad (OTP) algorithm is most usually linked with QKD, as it has proven to be safe when used with a secret, random key (Bennett *et al.,* 1990).

Quantum communication includes coding information in quantum states (qubits), contrary to classical communication's use of bits. Ordinarily, quantum states are obtained from photons.

QKD feats certain attributes of these quantum states to assure its security (Sinha *et al.*, 2017). For example, a QKD model, as in Figure 2.6, comprises a sender, "Alice", a recipient, "Bob", and an intruder eavesdropper, "Eve". Alice initiates by transmitting a message to Bob using a photon gun to drive a stream of photons arbitrarily selected in one of four polarization states corresponding to vertical, horizontal or diagonal in opposing directions (0º,45º,90º or 135º). A communications channel is obtained with the property that messages transmitted through it cannot in principle be reliably read or copied by an eavesdropper (Eve) ignorant of certain key information used in encrypting the transmission (Bennett & Brassard, 1984, Bennett *et al.*, 1990 and Sinha *et al.*, 2017).

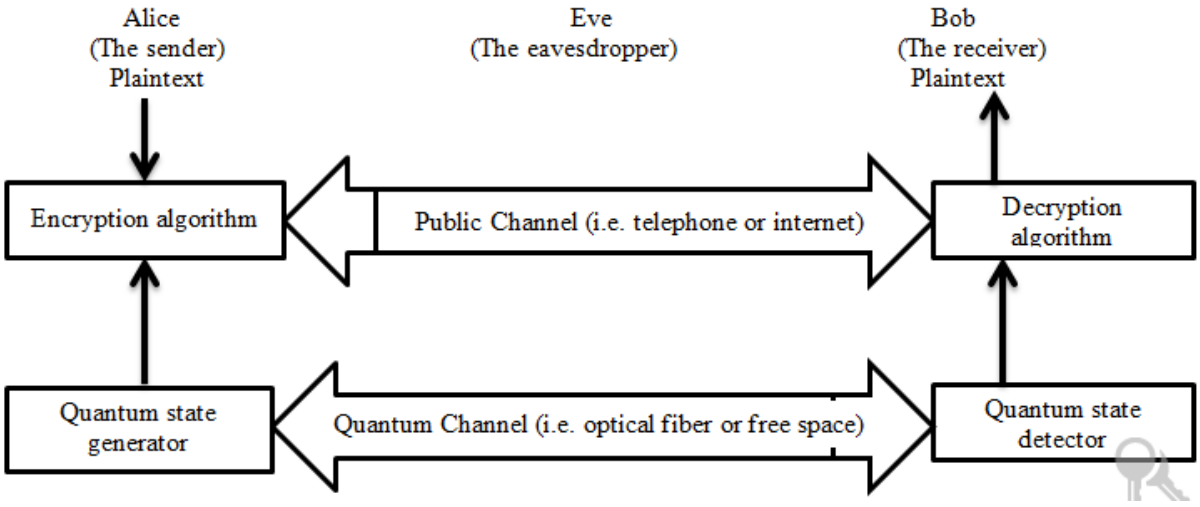


Figure 2.6: QKD Model using Two Channels to Generate Random Key (Sasirekha & Hemalatha, 2014)

QKD based protocols are basically (Sharma & De, 2011; Charjan & Kulkarni, 2015 and Mailloux *et al.*, 2017):

1. Non-orthogonal
    a. Bennett and Brassard, '84 (BB84)
    b. Bennett, '92 (B92)

c. Scarani, Acin, Ribordy, and Gisin, ’04 (SARG04)

d. Decoy state (passive or active)

e. Six-state protocol (SSP)

f. Differential phase shift-QKD (DPS-QKD)

g. Coherent one-way (COW)

2. Quantum-tangle

   a. Ekert, ’91 (E91)

The central goal of these protocols is to form an encryption key and allocate it to both parties in such a secure manner that a likely eavesdropping effort can be detected (Gümüş et al., 2008). However, for the purpose of this research, the BB84 protocol is the choice protocol because it remains the benchmark and is relatively easy to implement (Mailloux *et al.*, 2017). In order to get a vivid understanding of BB84 protocol, there is a need to get familiar with some terms associated with polarization in quantum cryptography (Gümüş *et al.*, 2008):

1. **Quantum** is the smallest unit of energy.
2. **Photon** is the quantum that can be transmitted in a wavelength. It is referred to as quantum of light. Photons are energy with massless particles.
3. **Polarization** is the orientation of electromagnetic field that a quantum particle has. For quantum cryptography, polarization of a photon is a characteristic feature that is used for secure communication.
4. **Qubit** is the value of a photon that is allotted according to photon’s orientation.
5. **Bases** these are special filters with polarization angles of 0º, 45º, 90º or 135º (as in Figure 2.5) which are adopted to polarize a photon produced by a beam source like a laser.



Figure 2.7: Polarization Bases with 0º, 45º, 90º or 135º
Polarization Angles (Gümüş *et al.*, 2008)

6. **Filter** is a system that is composed of two crosswise bases and used to recite the last polarization of a photon. There exist two types of filters as shown in Figure 2.6
    i. diagonal
    ii. rectilinear



Figure 2.8: Diagonal and Rectilinear Filters (Gümüş *et al.*, 2008)

2.2.10 Bennet and Brassard 1984 (BB84) Protocol

BB84 protocol was initially proposed by Charles Bennett and Gilles Brassard in 1984 (Hui & Chen, 2009) and is essentially the benchmark for subsequent QKD based protocols. BB84 protocol has been proven to be secure since it uses polarization-coding to realize the key distribution (Hui & Chen, 2009). The protocol enables two users to distribute an arbitrary secret key which is simply identified by them to encrypt and decrypt the message. The BB84 protocol is based four non-orthogonal polarization states (0º, 90º, 45º and 135º). In this protocol, sender (Alice) and receiver (Bob) have to connect in a quantum channel (fiber optic or free space) and public channel (Internet) (Mailloux *et al.*, 2017). The polarization matching of BB84 protocol is as depicted in Figure 2.9

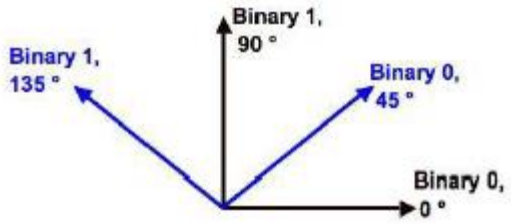


Figure 2.9: Photon Polarization (Hui & Chen, 2009)

From the photon polarization matching rule scheme of Figure 2.9, polarization angles of 90º and 135º represent a qubit with value of 1 and polarization angles of 45º and 0º represent a qubit with value of 0. The identical matching rule must be selected by both sides for a faultless communication process (Gümüş et al., 2008).

For systems that use the BB84 protocol, if an eavesdropper (Eve) attempts to recite the polarization status of a photon with a filter which covers a base with the identical polarization angle of this photon then the photon polarization stays unaltered. However, if Eve uses the incorrect kind of filter to read the polarization status of a photon, the photon's original polarization angle varies ± 45 degrees. This alteration can be understood when Alice and Bob equate their selected base/filter types for each photon and the presence of Eve suspected when the error rate (based on some qubit values) are compared with a threshold value.

There are two steps involved in key distribution for BB84 protocol (Hui & Chen, 2009):

1. One way Communication (via quantum channel)

   Step 1: Alice randomly choses polarized photon and sends it to Bob over a quantum channel

   Step 2: Bob receives photons using random basis (rectangular or diagonal)

2. Two way Communication (via public channel)

   Step 1: Alice will use public channel to inform Bob about the polarization chosen for each bit sent without divulging the bit value.

Step 2: Bob will match the polarization sequence received from Alice with the sequence produced.

Step 3: Bits of same orientation of those two sequences can be used as secret key.

Table 2.3 depicts the steps of how key can be generated from BB84 protocol.

Table 2.3: Procedure of BB84 Protocol of Key Generation (Hui & Chen, 2009)

Alice's photon polarization	↔	◿	↕	↔	◹	◿	↕	↕	◿	↔	◹
Alice's bit sequence	0	0	1	0	1	0	1	1	0	0	1
Bob's basis	✚	✚	✖	✚	✖	✖	✖	✚	✖	✖	✚
Bob's measured polarization	↔	↕	◹	↔	◹	◿	◹	↕	◿	◿	↔
Bob's sifted measured polarization	↔	?	?	↔	◹	◿	?	↕	◿	?	?
Alice and Bob's bit sequence	0			0	1	0		1	0		
Final key	0				1			1	0		

2.2.10.1 Steps of QKD Processes Based on the BB84 Protocol

In order to produce the ending key that will be used in any encryption process, the following are the required phases based on the BB84 protocol (Bhandari, 2014):

1. **Raw key extraction (key generation):** This phase deals with the eradication of wrong transferred bits and it is passed out over public channels (which are more susceptible to eavesdropping). Its application displays variances from protocol to protocol (Gümüş *et al.*, 2008). Hence, in order to generate identical keys, Alice and Bob will keep only those bits in their bit strings for which Alice's preparation basis and Bob's measurement basis are identical. Accordingly, they share the information of their bases (not the bit values) on the available classical channel, and discard those bits from their

bit strings for which the bases are not identical. Since for every qubit received, the probability of selecting the incorrect basis is 1/2, and bits corresponding to incorrect bases are discarded, Alice and Bob are left with a bit string that is roughly half the size of the raw key. This is called the sifted key (Bhandari, 2014).

2. **Error estimation:** The purpose of error estimation is to determine the percentage of errors in the key after quantum transmission and sifting have occurred. The percentage of errors is known as the quantum bit error rate (QBER) (Johnson, 2012). QBER can be defined as (Holloway, 2012):

$$QBER = \frac{N_{wrong}}{N_{total}} \tag{2.29}$$

where, N_{wrong} depicts the number of bits that are not identical bit and N_{total} is the total number of generated bits.

If both parties are using a QKD protocol over a noisy channel, this situation turns into an advantage for an eavesdropper. Because at any time slot, if both sides use the same type of filter for sending or reading process and they do not have the same qubit value then it indicates not only the existence of an eavesdropper but also physical noise in the transmission medium. This situation is conducive for attacks on QKD systems over noisy physical channels.

In order to avoid such attacks, both sides determine an error threshold value "Rmax" when they are sure that there is no eavesdropping on the transmission medium. Then after each QKD session, they compare some bits of their raw keys in order to calculate a transmission error percentage "R". In that way, R>Rmax indicates the existence of an eavesdropper (Gümüş *et al.*, 2008).

3. **Key reconciliation (Error Correction):** Key reconciliation is the process of resolving all errors in the key over the classical channel, after quantum transmission and sifting have occurred, without revealing an unreasonable amount of information about the key to a potential Eve (Johnson, 2012).

   Even for $Q \leq Q_{max}$, where Q is transmitted error rate, case, there could be incorrect bits in the keys. If this condition arises, key reconciliation is applied with a view to minimizing the error(s). The most common error correcting algorithms are (Johnson *et al.,* 2015):

   a. Cascade algorithm
   b. Winnow algorithm
   c. Low density parity check algorithm

   The most famous among these algorithms is the cascade protocol. Cascade protocol will be used in this research due to its effectiveness and simplicity of implementation (Johnson *et al.,* 2015**).**

4. **Privacy amplification:** This is the final stage in correcting the errors in a transmitted key. The purpose of this step is to account for any information exposed during the error reconciliation phase and ensure that any eavesdroppers present do not gain sufficient information to the point where they are able to reconstitute a significant part of the key (Johnson, 2012). Transmitter and receiver ends apply a reduction method to their bit series in a manner that an eavesdropper cannot employ any possible information obtained to reconstruct the bit sequences (Hui & Chen, 2009). A universal hash function will be considered as the shrinking method in this research because of its

ability to expose a hidden error and exponentially minimize it to the point of complete elimination.

2.2.10.2 Suitable Selection of Scaling Factor

Scaling factor denotes the enduringness of a watermark and it can be used along with the final key that will be generated from QKD to control the overall robustness, security and the quality of the image (Thakkar & Srivastava, 2017). Increasing the value of scaling factor increases the strength of the watermark but introduces a gradual perceivable distortion while decreasing the value would result in better hiding of the watermark and hence better quality but decreases the strength of the watermark (Vaidya & Mouli, 2015). An optimal value needs to be decided upon depending on the watermark and the key before embedding. Ascertaining the appropriate value of scaling factor is a challenging task. However, a systematic algorithm is essential for this goal. Therefore, an optimal approach using PSO algorithm will be adopted in this proposed research work to ascertain the scaling factor due to the following reasons (Thakkar & Srivastava, 2017):

i. PSO will enable the proposed technique to be dynamic to diversity of images and attacks due to the fact, that it simulates a variety of social behaviours such as fish schooling and bird flocking.
ii. The scheme will also be less complex given that PSO requires lower number of particles and iterations for any image compared to most other algorithms.

2.2.11 Particle Swarm Optimization

Particle swarm optimization is a population based stochastic optimization technique that was first introduced by Eberhart and Kennedy (Eberhart & Kennedy, 1995). The technique is a population based algorithm that imitates the swarm behavior of bird flocking and school of

fish (Eberhart & Kennedy, 1995). PSO is an algorithm that is easy to implement with good computational efficiency (Goudos, 2014). Overall, the PSO comprises population of particles over the search space. Individual particle symbolizes a candidate solution to be regarded as an optimization problem (Lai *et al.*, 2013). The *i*th particle has the following three features:

1. The current position in an *N*-dimensional search space $X_i = \left(x_{i,1,}\, x_{i,2,}\ldots\ldots x_{i,N}\right)$.
2. The current velocity $V_i = \left(v_{i,1,}\, v_{i,2,}\ldots\ldots v_{i,N}\right)$.
3. Each particle has its own best previous position $P_i = \left(p_{i,1,}\, p_{i,2,}\ldots\ldots p_{i,N}\right)$.

In order to specify information for every particle, the distributing information amongst conspecifics also shows a key function in searching solution. This can be accomplished by employing the publicized knowledge P_g (the global best particle), which denotes the best location found so far amongst all the particles in the swarm at iteration *x* (Lai *et al.*, 2013). Firstly, a population of arbitrary particles is generated and then optimum is searched by growing generations. In each iteration, a particle gains from the discoveries and former experience of other particles during the exploration. Hence, a new population is produced based on a preceding one and the particles are updated by the following equations (Lai *et al.*, 2013):

$$v_{i,j}(t+1) = wv_{i,j}(t) + c_1 r_1\left(p_{i,j} - x_{i,j}(t)\right) + c_2 r_2\left(p_{g,j} - x_{i,j}(t)\right), j = 1,2,\ldots\ldots N, \quad (2.30)$$

$$x_{i,j}(t+1) = x_{i,j}(t) + v_{i,j}(t+1), j = 1,2,\ldots\ldots N, \quad (2.31)$$

where:

w denotes the inertia factor that is used to control the convergence during iteration

c_1 and c_2 depict two constants for acceleration that control particle movement.

r_1 and r_2 represents two arbitrary numbers uniformly distributed in the interval of [0, 1].

Velocity values must be within an interval known by two parameters v_{min} and v_{max}, that is, a clamped velocity to prevent the particle from escaping the search space.

2.3 Review of Similar Works

Several researches have been undertaken in the area of watermarking and mechanisms to improve its imperceptibility and robustness with a view to enhancing the security of the system and some of the relevant ones are described as follows:

Shieh *et al.* (2004) developed an innovative robust watermarking technique using DCT based on genetic algorithm (GA). In this work, the GA was used to optimally select the frequency bands for embedding watermark into DCT based watermarking system. The algorithm was tested on Lena image as cover image of size 512 x 512 and rose of size 128 x128 as the watermark. The performance of the algorithm was measured using PSNR and normalized correlation NC to simultaneously evaluate imperceptibility and robustness. However, the proposed algorithm was susceptible to geometric attacks such as rotation and histogram equalization applied to fully establish the strength of its robustness.

Tao & Eskicioglu, (2004) implemented a generation algorithm by inserting visual secret messages in all four sub-bands at two different decomposition levels of DWT. The first level decomposition of the algorithm was examined on a grey scale goldhill (cover image) of size 512 x 512 and binary visual messages BC and A of size 256 x 256. The second level of decomposition was tested on same size of cover image at first level of decomposition and binary visual watermarks BC and A of size 128 x 128. The algorithm was tested against

fifteen different attacks. It was shown that the watermark embedded in low frequencies was resilience to attacks which included JPEG compression, blurring, inclusion of Gaussians noise and rescaling, while those embedded in high frequencies were robust to attacks such as gamma correction, intensity adjustment and histogram equalization. It was established that watermark embedded in at least two sub-bands at a certain DWT decomposition level made the algorithm tremendously withstand most of the malicious attempts or normal A/V processing. However, the scale factor was manually determined for each sub-band, which affected the embedding speed of the algorithm.

Navas *et al.* (2008), developed a non-blind transform domain watermarking based DWT-DCT-SVD. In this approach, DWT was used to decompose a grey scale (cover image) into four sub-bands, LL, HL, LH and HH. The DCT was employed in the selected coefficients obtained from DWT operation (LL and HH were selected). SVD was used to modify the DCT coefficients obtained from it applications. The watermark also underwent the same processes used on the cover image. Both the watermark and the modified cover image were together inserted in the host image. The inverse DCT followed by the inverse DWT were performed to btain the watermarked image. The algorithm was tested on a grey scale cover image (Cameraman) of size 256 X256 and watermark (Lena) of size 128 X 128. The evaluation of the algorithm was examined using PSNR and MSE to evaluate the imperceptibility of the watermarked image. It was found that the algorithm was resistance against attacks such as average filtering, Gaussian blur, and JPEG compression. The performance of the algorithm degraded when applied on colour images, and digital imaging, and communications in medicine DICOM images.

Al-Mansoori & Kunhu (2012) developed a robust image watermarking algorithm for inserting logo information into all DubaiSat-1 satellite images based on DCT. The odd and even technique was used to embed the watermark into the decomposed 2-D DCT coefficients of the cover image. The proposed algorithm comprises of three modules; for the first module, two bits of binary watermark logo are embedded inside the block based image with a secret key, while for the second module, two copies of two bits of binary watermark logo are embedded inside the block based image with a secret key and for the third module, three copies of two bits of binary watermark logo are embedded inside the block based image with a secret key. The performances of the three modules of the algorithm were evaluated based on their PSNR values using the following attacks: flipping, noise, resize and rotations. However, the performance of the algorithm when subjected to rotation, resize, translation and cropping attacks decreased.

Anitha & Velusamy (2012) developed an efficient technique for digitizing the authoritative documents of an individual based on secret key biometric watermarking. Biometric watermark for five different persons were generated from their iris and a total of 25 documents that belonged to these five people were selected. Each biometric watermark was embedded in all the 25 documents, that is, a person's biometric watermark was embedded in the person's documents. The embedding and extracting process were done with the aid of a secret key generated from cryptographic hash function. It was found that the technique showed accuracy in authenticating the genuine documents and was resistant against signal processing attacks. However, the performance analysis of the technique was evaluated under geometric attacks in order to ascertain the reliability of the model, and results showed it to be susceptible to geometric attacks.

Kashyap & Sinha (2012) Implemented 2-level 2-D DWT based digital mage watermarking technique, using alpha blending process to insert the watermark in the original image. A gray scale (original image) was decomposed using the second level 2-D DWT to obtain second level (low and high frequency) sub-bands. Watermark image was also decomposed using 2-level 2-D DWT to obtain 2-level (low and high frequency) sub-bands. The decomposed 2-level low-low (LL) frequency constituents of the host image and that of watermark image are manifold by scaling factors and then added using alpha blending formula. The watermarked image was created by performing inverse second level 2-D DWT. The performance of the algorithm was tested using gray scale images (Lena image) as original image and (cameraman) as the watermark. The images are of equal size of 256 x 256. The values of MSE and PSNR were calculated for different values of the scaling factors. Investigational results showed that the quality of the processed image was dependent on the scaling factors. However, robustness of the technique was trade-off for imperceptibility against intentional and unintentional attacks. This was due to the fact that the scaling factor was manually selected.

Kejgir & Kokare (2012) developed a robust digital image watermarking method based on lifting wavelet transform (LWT) and SVD. The LWT transformed the image into sub-bands with energy greater than a given threshold is selected for watermark embedding. The SVD is applied on the selected sub-band, where the selected sub-band is decomposed into three matrices and used to insert the watermark. The proposed algorithm was tested on five different host images (pepper, rose, Mandrill) of size 512 x 512 and cameraman of size 256 x 256 and watermark of digital signature of size 256 x 256. The technique was examined for robustness against eight different attacks on each of the five images. The performance of the

algorithm was evaluated using PSNR and CRC to show the simultaneous improvement of watermarked image quality and robustness respectively. The algorithm outperformed DWT and SVD when compared in terms of robustness and speed in real life applications. Nevertheless, the imperceptibility of the watermarked image which plays a vital role in digital watermarking was sacrificed for robustness.

Singh *et al.*, (2012) developed a DWT based digital image watermarking algorithm. A 4-level 2-D DWT was used to decompose cover image and the watermarks bits are then embedded into the mid frequencies of the decomposed cover image by modifying the coefficients in the block according to the embedding process. Inverse 4-level 2-D DWT was performed to obtain the watermarked image. The algorithm was examined on four different images (baboon, satellite, Lena and medical) as cover images and binary image as watermark information. The performance of the algorithm was measured using PSNR. The PSNR values were computed at different scaling factors and as the scaling factor value is increased, the PSNR value of the image decreased. However, evaluation of robustness of the proposed algorithm was vulnerable to poisson noise, filtering and JPEG compression attacks.

Lai *et al.* (2013) developed a robust feature-based image watermarking technique which hybridized DWT and SVD using PSO. The edge image information was utilized to embed the watermark. The PSO was used to optimally select a suitable scaling factor which was used to ascertain the robustness of the watermark. The watermarked image was obtained by applying inverse DWT. The technique was tested on the image of a boat of size 512 x 512 as cover image and a gray scale image (cameraman) of size 128 x 128 as watermark. The proposed algorithm was subjected to several attacks such as geometric attack, noise attack, denoising attack and image processing attack. The performance evaluation of the algorithm based on

imperceptibility and robustness were measured using PSNR and NC respectively. However, inability to integrate the characteristics of human visual system into the algorithm caused an adverse effect on the quality of the host image after embedding.

Rahman, (2013) developed watermarking algorithm using DWT, DCT and SVD transformation, where the host image was reshuffled using zigzag series and the DWT was applied on reshuffled image, in order to split the image into four sub-bands (LL, HL, LH and HH). DCT and SVD were applied on all the high sub-bands. The watermark was enclosed by the modification of singular value of both the host image and watermark and added together. The watermarked image was created by the application of inverse DCT and DWT. The performance of the technique was evaluated based on PSNR and NCC to measure the level of imperceptibility and robustness. It was established in this work that the mid sub-bands and high sub-bands ensured high visual quality and more robustness against different kinds of attacks. However, the algorithm was susceptible to Gaussian, salt and pepper, speckle and Poisson noise and in addition; its performance was degraded when tested on colour images.

Santhi & Arulmozhivarman, (2013) developed a novel and dynamic technique for perceptible and undetectable watermarking in frequency domain based on Hadamard transform and sigmoid function. The algorithm adaptively calculated the scaling factor centered on the content of underlying cover image. In the embedding procedure, RGB cover image was converted into YUV colour space and the Hadamard transform was used to transform the luminance channel Y and the watermark image was as well transformed based on the Hadamard transform. The secret image was embedded by modulating the transformed coefficients of shelter image with that of the watermark. The robustness of the technique was measured using median filtering, JPEG compression, noise, low pass filtering, high pass

filtering, cropping, and geometric attacks. However, the technique was found not to be robust against cropping and Gaussian noise and also as the JPEG compression ratio increased, the robustness tended to decrease likewise the perceptual quality of the watermarked images.

Sharma & Swami (2013) implemented a digital image watermarking based on 3-level DWT. Alpha blending technique was used to embed a multi-bit watermark into low frequency sub-band of the host image. The technique was tested on the original image (Lena) and watermark (bird) of same size 256 x 256. The performance of the technique was evaluated using PSNR and MSE. These measures were found to be better than those obtained using first and second levels of decomposition of DWT. However, the technique was easily distorted by geometric attacks, since the watermark was inserted in low frequency of the second level of decomposition.

Ahmad *et al.* (2014) implemented image watermarking algorithm in transform domain using DWT. In this approach, both the cover and watermark images were splitted using 3-level 2-D DWT and so LL sub band of decomposed watermark image was embedded into the LL sub band of decomposed host image based on alpha blending technique. Eventually, watermarked image was obtained by performing inverse 3-levels 2-D DWT. The performance of the algorithm was evaluated using PSNR and was examined on gray scale images of fruits as cover image and pepper image as watermark image. Although, the algorithm demonstrated a high performance in occasion of no attacks, but after subjecting it to various attacks, such as JPEG compression, adding noise and filtering attacks, the watermarked image quality was below PSNR value of 30 dB which is below the minimum required level.

Gattani & Warnekar, (2014) studied a new invisible digital watermarking scheme for colour images based on the merger of wavelet transform with SVD and Advanced encryption scheme (AES). In this approach, the watermark was embedded into the channels of the host image using a scaling factor lamda. This lamda was multiplied with singular matrix of watermark and added to the singular matrix of the host image. The AES was then used to encrypt the watermarked image in order to further enhance its security. The approach was tested on colour images (Lena) of size 512 X 512 as original image and watermark (Baboon) of size 256 X 256. The reliability of this approach was evaluated by PSNR and NCC. It was found that the application of SWT2 technique through SVD reduces distortion and the AES ensures the security of the image. Although, the embedding and extraction time of the watermark was very high.

Kaur & Jindal, (2014) proposed a new SVD-DWT video watermarking embedding technique. In this technique, third level DWT and SVD were applied on chosen frames and the watermark was embedded into randomly selected frames with the aid of private key to authenticate the video. The technique was tested with different variations using colour host video clips. Ten random features were selected and watermark (Penguin) of size 512 X 512 was embedded into the frames. The combined inverse DWT was performed to reconstruct the watermarked video. The robustness and quality of watermarked video were tested using different performance evaluation metrics such as SSIM, PSNR, MSE and BER. It was shown that the algorithm gave a high robustness and good quality watermarked video. Nevertheless, in this study public key was consider for embedding and extraction processes, because it has be established that secrete keys are more secure than dynamic keys. This exposes the algorithm to security treat.

Kester *et al.*, (2014) proposed a hybrid cryptographic and digital watermarking technique for securing digital images based on a generated symmetric key from the image features. In this technique, the encryption scheme made use of both digital image pixel displacement and visual cryptographic encryption schemes, in order to secure the digital images engaged in sequential embedding scheme and method used for authentication process of the image at the pixel level. The technique was examined on captured surveillance camera image. The operation of the algorithm was evaluated using NCC based on robustness and fidelity. It was reported in the work that the technique has a high robustness and good fidelity. However, the scheme has low capacity due to loss of pixel during encryption process.

Sharma & Jain, (2014) carried out a robust fusion watermarking scheme using SVD and DWT, where the watermark was embedded in the singular values of the red component of the cover image DWT coefficients. These coefficients were combined with the green and blue components to yield the watermarked image. The technique was examined on a colour Lena image of size 512 X 512 and cameraman of size 256 X 256 as watermark. The quality of the approach was evaluated using PSNR. In the work the quality and robustness of the watermarked image was high. However, it is susceptible to the human visual system.

Singh *et al.*, (2014) proposed a new robust digital image watermarking scheme in transform domain for image authentication based on DWT, DCT and SVD. In this approach, DCT was employed over DWT to improve robustness and imperceptibility. In the insertion process, first level 2-D DWT was employed to decompose the cover image and then DCT and SVD were applied on HH sub-band of the decomposed first level 2-D DWT cover image. Arnold transformation was used to scramble the watermark and subsequently decomposed by applying 1-level 2-D DWT and SVD on the HH sub band of the decomposed 1-level 2-D

DWT watermark image. The orthogonal matrix was used to embed SVD of watermark into SVD of host image and inverse DCT and inverse DWT were performed respectively to obtain the watermarked image. Nevertheless, the technique is complicated and when the watermark data is embedded in high frequency components of the image, high frequency content of an image behaves like added noise and hence, noise removal algorithms such as filtering and sharpening destroys it. JPEG compression algorithms also try to reduce the image size by removing the small details which correspond to high frequency content of the image.

Venkatram, *et al.* a(2014) developed RSA-DWT based medical image watermarking scheme. The watermark was encrypted with a public key generated from the RSA algorithm and the host image was decomposed up to second level of decomposition. Two scaling factors were used to insert the encrypted watermark into the host image and the private key for decryption is transmitted along with the embedded image. The watermarked image is created by applying inverse DWT. The technique was tested on a set of medical images using magnetic resonance imaging, computed tomography (MRI, CT and ultra-sound scans) as host image of standard resolution 256 x 256 and patient image of resolution 64 x 64 as watermark. PSNR and NCC were used as performance metrics. The results showed a good non-perceptible, high robustness and superior protection to normal DWT based watermarking scheme. However, the system was still vulnerable to noise when subjected to various types of geometric attacks.

Rahman & Rabbi. (2015) developed an image watermarking algorithm based on hybrid of DWT and SVD with decomposition error. A host colour image is separated into three respective colour channels (RGB) and 4-level 2-D DWT was employed to decompose R band of the host image and SVD was applied to the watermark matrices and embedded into the HL

sub-band of the decomposed R channel of the host image and eventually inverse 4-level 2-D DWT was performed to obtain the watermarked image. The performance of the algorithm was evaluated using RGB image of size 512 x 512 as a host image and secret matrices of size 64 x 64 as a watermark image. However, the scheme exhibited weak robustness against attacks such as rotation and Gaussian high pass filtering with PSNR values of below 30dB (which is benchmarked as a non-robust value).

Paliwal & Jain, (2015) implemented digital watermarking technique for embedding colour image using DWT with the aim of maintaining the quality of the image for which a signal is inserted. The inverse DWT was applied on the watermark to create the watermarked image. The performance of the technique was evaluated using PSNR and MSE. However, the results showed that the technique was vulnerable to low pass filtering.

Vaidya & Mouli. (2015) developed an adaptive robust watermarking algorithm for digital images based on DWT. The technique was adaptive in the sense that Bhattacharyya distance and Kurtosis were used in the embedding factor and scaling factor calculation**.** In the insertion period, the watermark was embedded into the LL sub-band of the transformed second level 2-D DWT host image. The algorithm was tested on eleven different gray scale images (airplane, Barbara, girl1, girl2, house1, house2, Lena, mandrill, original frame, peppers and tree) of size 256 x 256 and cameraman image of size 64 x 64 were used as cover images and watermark image respectively. The performance evaluation of the algorithm was based on robustness and imperceptibility using PSNR and NCC by applying different kinds of signal manipulations and geometric attacks to the watermarked image during communication such as noise attacks, cropping, rotation, scaling and translation. The approach was found to be robust to these attacks but at the cost of the imperceptibility of the watermarked image.

Azeem *et al.*, (2016) developed an effective robust video watermarking technique based on DCT. The video frame was decomposed into three video channels Y, U and V. The V channel was chosen for the embedding of the watermark and the 2D DCT was applied to all blocks of each frame in the V luminance. The watermarked video frame was created by combining the modified Y, U and V components and inverse 2D DCT was performed on the watermarked video to obtain the watermark. The presentation of the algorithm was evaluated using PSNR and MSE. The results showed that the algorithm was susceptible to geometric attacks such as cropping, warping, rotation, line and column removal.

Chanda & Choudhury (2016) implemented an image watermarking algorithm for copyright protection based on third level DWT. The watermark was inserted into the low frequency sub-band of the cover image by the use of alpha blending method. The watermarked image was obtained by performing inverse DWT. The technique was tested on host images (Lena, Sailboat, Rabindrama and Netaji) and cameraman as watermark. PSNR and RMSE were employed to evaluate the performance of the proposed technique, in terms of perceptual transparency and robustness. The results showed a high level of imperceptibility but that it was susceptible to geometric attacks since the watermark was inserted in the low frequency of the host image which made it less robust.

Malonia & Agarwal. (2016) developed a digital image watermarking algorithm in frequency domain using DWT and arithmetic progression (AP) techniques. AP was used to insert the binary watermark bits into the cover image. In the embedding period, 1-level 2-D DWT was applied to decompose RGB host image and then the secret bits were embedded into the HH, HL and LH sub-bands of the decomposed host image. The performance of the technique was examined on different host images (Lena, Baboon, Barbara) of size 512 x 512 and a quick

response (QR) code image of size 48 x 48 as watermark image. It was found that by performing different signal processing manipulations and geometric attacks on watermarked images, PSNR and SSIM values (above 50dB and 0.2 respectively) were obtained. However, in this technique imperceptibility was traded-off for robustness during performance evaluation.

Salama & Mokhtar, (2016) developed an improved technique (IMD-WC-T) that combined DWT and DCT. The host image was disintegrated into four multi-resolution sub-bands that are non-overlapping up to second level of decomposition. The watermark signal was inserted into the second level sub-band of the cover image and DCT was then applied on the second level sub-band. Watermarking was then carried out in the sub-band. The technique was tested on a host image (Lena) of size 512 x 512 and a binary image of size 20 x 50 as watermark. The watermarked image was achieved by the application of inverse DCT and DWT respectively. The performance of the technique was measured based on PSNR, NC, MSE and watermark document ratio (WDR). It was established that the technique offered improved performance against separate DCT and DWT respectively in terms of fidelity and robustness. However, the technique was found to be vulnerable to rotation and scaling.

Bajracharya & Koju (2017) developed a DWT and SVD based digital watermarking using alpha blending and Arnold transformation in the colour images. The cover image was converted from RGB colour space to YCbCr colour space. DWT was applied on the chosen Y channel of the cover image, which was used to subdivide the image into low frequency and high frequency sub-bands up to the fourth level of decomposition. The high frequency sub-band was selected for embedding the watermark, that is, HH4. R channel was extracted from RGB of the watermark. Arnold transformation was used to scramble the R colour channel to

improve the safety of the watermark image. DWT was applied on the scramble R channel of the watermark image, which was used to subdivide the image into low frequency and high frequency sub-bands up to the third level of decomposition. The high frequency sub-band of the watermark was selected, that is, HH3. The SVD was applied to the coefficients of DWT of both the cover image and watermark in order to modify them for embedding. Alpha blending scheme was used to embed the watermark in the cover image. The inverse DWT was performed on the modified SVD to generate the watermarked image. While in the reconstruction process the inverse DWT and anti-Arnold transformation were performed on the watermarked image to obtain the original watermark. The technique was tested on images (pepper and Lena) as cover image and Nepal Telecom logo as watermark information. The performance of the technique was measured using PSNR and NCC with a view to evaluating imperceptibility and robustness. It was found that the algorithm had accepted imperceptibility and robustness levels. Nevertheless, the capacity of the technique was very low, which implied that the cover image got distorted with increasing data.

Loukhaoukha *et al.*, (2017) showed how redundant wavelet transform (RDWT) and SVD resisted two ambiguity attacks. They performed one level RDWT to decompose the original image into four sub-bands and SVD was applied to all the sub-bands. The singular values for each sub-band were modified in order to enclose the watermark. The reverse RDWT was done on the modified singular values to obtain the watermarked image. The algorithm was tested on an original image (Lena and Pepper) of size 256 x 256, owners and attackers watermarks of cameraman were of the same size. The performance of the algorithm was evaluated on two different attacks referred to as ambiguity attack using PSNR and NC. However, it was established that the algorithm was not suitable to be used for ownership identification and

authentication due to the fact that the algorithm failed when subjected to two ambiguity attacks.

Ouazzane *et al.*, (2017) explored the extended use of DOST in image watermarking by suggesting a fragile and blind medical image watermarking scheme that embedded the secret image based on dual symmetric high frequency sub-bands of the two dimensional DOST illustration of the original image. The technique was examined on 14 DICOM images of separate modalities. The secret images that were explored in this technique were bit series and the performance of the scheme was evaluated in order to measure the transparency of the misrepresentations presented to the original image by the insertion of the watermark using PSNR and RMSE. It was evaluated that the DOST watermarking obtained a good tradeoff between fidelity and payload when compared with DWT watermarking in blind insertion technique. However, it was not shown how the approach would behave when tamper localization capacity is added in order to ascertain modified areas and achieve enhanced integrity of the image.

In view of the aforementioned imperfections associated with the reviewed works and the need to overcome the inefficiencies of the traditional watermarking techniques such as inability to obtain an optimal trade-off between imperceptibility and robustness and to withstand mostly geometric attacks. It is evident from the reviewed works that the major challenges in digital image copyright protection have been the effects of both geometric attacks and signal processing manipulations on watermarked images. Researchers have concentrated on the development of robust techniques to mitigate these effects. Most works focused on enhancing the robustness and imperceptibility of the watermarking technique by using frequency domain techniques such as, DCT, DWT and SVD. Recently DST and DOST have been introduced in

image transformation. DCT, DWT, and SVD have been identified to possess limited properties. Such properties are less robust to geometric attacks, blur near edges of images, false positive outcome, and insufficient revelation of all the details within an image. These make them to be vulnerable to some attacks. Hence, combining the transforms recompense for the downsides of each other, resulting in effective watermarking. Therefore, the development of an enhanced robust digital image watermarking technique is here proposed. The proposed technique is to employ the combination of DOST, DWT, SVD (for which the critical scaling factor is optimally obtained based on PSO) and QKD (based on photon polarization) to strengthen the watermarked image, in order to optimally satisfy the enhanced robustness and imperceptibility of the watermarked image.

CHAPTER THREE

MATERIALS AND METHODS

3.1 Introduction

This chapter describes the detailed procedure of the methods and materials used to develop the digital image watermarking in this research work. The developed digital image watermarking algorithm is based on DOST, DWT, SVD techniques, PSO and key and is experimentally implemented in MATLAB R2015b simulation environment.

3.2 Materials

The materials needed in this research work includes; colour images of Lena, Pepper, Mandril, and Nepal Telecom logo for cover and watermark images respectively obtained from a data set of University of Southern California (Signal and Image Processing Institute), MATLAB, DELL laptop with processor Intel core i3 2.3GHz, x64-based processor and 4GB RAM

3.3 Important Assumptions

Important assumptions adopted for the successful development and implementation of the proposed robust digital image watermarking technique are itemized as follows:

1. An unsecure public network was used for the transmission of the created watermarked data between two geographically separated communicating parties, Alice and Bob.
2. A 0.05 quantum channel error probability was assumed for the quantum channel used to transmit quantum bits between two geographically separated communicating parties during QKD scheme for key generation and distribution.
3. A perfect transmission error estimation between two geographically separated communicating parties in the final key agreed by both parties.

3.4 Methodology

The step by step processes adopted to attain the proposed robust digital image watermarking algorithm are enumerated as follows:

1. **Development of a digital image watermarking technique**
    a. Acquisition of digital images for both cover and watermark images. The images were acquired from signal and image processing institute, university of Southern California.
    b. Decomposition of cover and watermark images into three colour channels, namely red(R), green(G) and blue(B) from the cover and watermark images
    c. Application of 2D DOST on each of the three colour channels of both the cover image and watermark in order to obtain DOST coefficients (that is, two symmetric high frequency sub-bands)
    d. Application of 3-level 2D DWT on the DOST coefficients that decomposes the coefficients of each colour channel into four sub-bands (LL, HL, LH and HH) up to the third desire level.
    e. Application of SVD on each of the four sub-bands at the third level of decomposition of all the three colour channels that were obtained from DWT
2. **Development of a scheme for secrete key generation**
    a. Generation of secrete key from quantum key distribution using the principle of photon polarization based on BB84 protocol.

    The following steps will be adopted in order to generate the final key that will be used in the encryption process.

    (i) Raw key extraction

(ii) Error estimation

(iii)Key reconciliation

(iv)Privacy amplification

3. **Determination of optimal scaling factor base on PSO approach**
   a. Generation of random particles from initial population
   b. Formulation of fitness function based on cover image, watermark image, watermarked image and extracted watermark.
4. **Modification of transform coefficients and embedded process**
   a. Diagonal singular value coefficients obtained in item (e) step (1) is modified
   b. Embedding the watermark into the cover image with the use of scaling factor and key obtained in step (2) and (3). The pixels values of watermark image was shuffle using affine transform and encrypted with the key based on XORed operation of the modified SVD of the watermark and multiply with the scaling factor and added to the modified SVD of the cover image.
5. **Generation of watermarked image**
   a. Combination of all the modified coefficients
   b. Performation of inverse DWT and DOST on all the combine modified coefficients
   c. Watermarked imaged is obtain by combining all the three colour planes R, G and B on term (b) step 5
6. **Extraction of watermark from the watermarked image**
   a. The procedures that were carried out on steps 1 (b, c, d, e,), 4 and 5 is repeated on the watermarked image and the cover image
   b. The procedure in step 4 is divided by the scaling factor in the extraction process.

7. **Validation**

   a. The performance of the developed technique will be evaluated by comparing with the ITU benchmark and techniques developed by Bajracharya & Koju (2017) in terms of robustness and imperceptibility using the following performance metrics:

      (i) PSNR

      (ii) NCC

      (iii)SSIM

The following subsections provide detailed steps of the methodology adopted in carrying out the research.

3.4.1 Development of a Digital Image Watermarking Technique

In the proposed watermarking technique, the following steps are employed for the actualization of the technique.

1. Colour Lena and Mandril images stand for cover and watermark images respectively. The size of images is 512 x 512 x 3, the images are acquired from Signal and image processing institute, University of Southern California as shown in Figure 3.1



(a) Lena (b) Mandril

Figure 3.1: Original Cover and Watermark Images

2. Both images are decomposed into their respective channels, red (R), green (G) and blue (B) accordingly based on the following equations:

$$I_{A_d} = \sum_{1}^{d} C_{I_A}\left[R, G, B\right] \tag{3.1}$$

$$I_{B_d} = \sum_{1}^{d} C_{I_B}\left[R, G, B\right] \tag{3.2}$$

Where**:** I_{A_d} depicts cover image, I_{B_d} depicts watermark image, C_{I_A} represents each channel of the cover image, C_{I_B} represents each channel of the watermark and d denotes the maximum level of decomposition, which is 3

3.4.2 Application of 2D DOST on the Cover and Watermark images

The following are the steps for the application of DOST on the cover and watermark images:

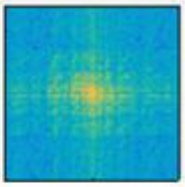
1. The 2D DOST is applied on each of the three colour channels of both the cover and watermark images in order to obtain DOST coefficients (that is, two symmetric high frequency sub-bands). The forward DOST host image decomposition and inverse DOST host image reconstruction is achieved using equations (2.17) and (2.18) respectively. The following pseudo code is used for the implementation of forward DOST decomposition and inverse DOST reconstruction of both the cover and watermark images.

Start
Input images
Apply forward DOST to transform input images
Output Dost coefficients
Apply inverse DOST to DOST coefficients to obtain reconstructed images
Output reconstructed image
End

Figures 3.2 and 3.3 depict the logarithm of the magnitude of the 2D DOST coefficients for each channel of the cover and watermark images (Lena and Mandril respectively) of size 512 x 512 x 3. As could be seen, the coefficients decay very rapidly, which makes the DOST a prevailing tool for image decomposition, compaction and other usages. Although, the DOST coefficients decay in a consistent way, it can still be observed from the log-scale magnitude plot, that there are small components of “Lena and Mandril ” at each corner of the plot. The stretched edges of “Lena and Mandril” are also visible within the square and rectangular blocks inside the plot, where frequency bands with respect to different spatial axes of the image overlap. Due to the side-lobes seen in the plot of the DOST basis function, the 2D DOST coefficients are non-zero almost everywhere, even for the one-dot image. This dispersion has created difficulties in using the DOST for some applications. However, the extent of the temporal side-lobes is the price that must be paid for perfect frequency banding.



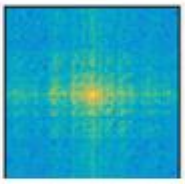
(a) Red Channel of Cover Image



(b) Log of the norm of dost2 red channel



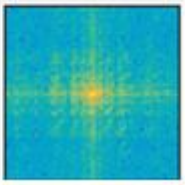
(c) Green Channel of Cover Image



(d) Log of the norm of dost2 green channel



(e) Blue Channel of Cover Image

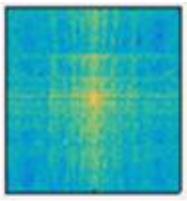


(f) Log of the norm of dost2 blue channel

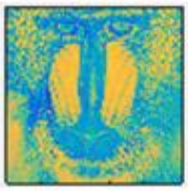
Figure 3.2: Cover Image Channels and the Logarithm of their DOST Coefficients



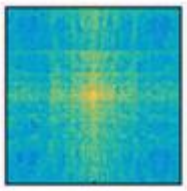
(a) Red Channel of Watermark Imag



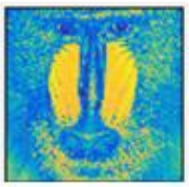
(b) Log of the norm of dost2 red channel



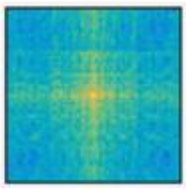
(c) Green Channel of Watermark Imag



(d) og of the norm of dost2 green channel



(e) Blue Channel of Watermark Image



(f) Log of the norm of dost2 blue channel

Figure 3.3: Watermark Image Channels and the Logarithm of their DOST Coefficients

2. For the purpose of enhancing the security of the watermarked image, a QKD is employed to produce and distribute a symmetric key to encrypt the watermark image. Based on the procedure of Table 2.3 random key length of 500-bits are generated. Final key lengths of 64-bits are obtained by adopting the steps of QKD based on BB84 protocol in sub-section 2.2.8.1. Alice and Bob assumed an estimated error rate of 0.0500 in quantum transmission channel, for the purpose of communicating quantum bit between them in order to share a secret message. The random bits generated by Alice for transmission are presented in appendix S and the first 20 bits are as shown:

1 0 0 0 0 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0

In order for Alice to secretly transmit the bits through quantum channel, Alice randomly chooses polarization basis and generate bases to encode the bits to form quantum bits (qubits) with a view to transmitting the qubits to Bob through a quantum channel of an estimated error rate of 0.0500. Alice randomly chooses polarization basis are presented in appendix S and the first 20 basis in correspondence to the first 20 bits are depicted as shown:

+ x x x + x + + x + x x + + x x + x x +

The transmitted qubits by Alice are shown in appendix S and the corresponding qubits to the first 20 basis is represented as follows:

| / / / - \ | | \ | / \ - - / / - / / - |

The qubits received by Bob is almost the same qubits transmitted by Alice with an estimated error rate. The pseudo code for qubits received by Bob is as follows:

```
Start
     Bob.Qubits = Alice.Qubits;
          Bob = Bob.receiveQubits(Alice.Qubits, errorRate);
     Bob.Qubits
End
```

Bob randomly chooses polarization basis and compare it with that of Alice basis. Consequently, Bob measures the qubits and also compares it with that of Alice qubits. The bases are as depicted in appendix S and the first 20 measured bases by Bob are as follows:

| / / / - \ | | \ | / \ - - / / - / / -

Alice and Bob communicate through public channel discussion to compare the polarization sequence received from Alice with the sequence generated. At this point Bob reports bases of received bits to Alice.

Alice communicates back those bit positions for which Bob chose correctly. The communicating parties keep the match bit positions for which they chose rightly and discard those that are mismatch. At this stage, Bob reveals some bits at random. The mathematical formula for revealing bits at random is as given by:

$$nRB = \left\lceil \left(\frac{nCB}{3} \right) \right\rceil \tag{3.3}$$

where, nRB depicts the number of revealed bases position and nCB denotes the number of correct bases position.

Alice confirms all revealed bits from Bob and keeps the corresponding bits as secret bits. 128 bits length with a transmission error rate of 0.0435 was obtained as the secret bits or key by both parties at the end of the QKD session. Although, the obtained transmission error rate p_t is less than the estimated error rate E_r ($p_t \leq E_r$) in the shared secret bits, there could be erroneous bits in the keys. As a result of the erroneous bits, there is quest to further subject the shared secret bits or key to error reconciliation in order to resolve all errors in the key over the public channel, after quantum transmission and sifting have happened. The error reconciliation is pertinent in order to avert revealing undue amount of information about the secret information to potential attacker (eavesdropper).

The mathematical expression for obtaining the transmission error rate p_t is as shown:

$$p_t = \sum_{i=0}^{n} \left(\frac{A \sim = B}{nRB} \right) \tag{3.4}$$

where: p_t denotes the transmission error rate, $A \sim = B$ depicts the shared secret bits between Alice and Bob, nRB depicts the number of revealed bases position

The error correcting algorithm used is cascade, the process used by the algorithm for identifying an error and correcting the error in a transmission channel is as follows:

The first stage of the protocol is that, Alice and Bob agreed on a random permutation and reverse permutation, in public channel. Permutation was performed on the shared secret keys between them in order to evenly distribute any errors within the channel. The secret key is divided into blocks of size k, where k is the initial block size, such that each block has error not more than one, based on the transmission error rate obtained in comparison with the estimated error rate. The initial block size k is taken to be 8 because of the consideration of colour image which has 24bits that depicts 8 red, 8 green and 8 blue in order to obtain a suitable block size. At this state, a single bit parity of each block is calculated and shared publicly in the first pass. If parities are in accordance, it is assumed that there are no errors in that block, and the process continues. However, if the parity disagrees between both parties, then a binary search is performed on the blocks in order to identify the single bit error, which is then rectified. After rectification, a permutation is applied, the block size is doubled by $2 \bullet k_i$, and another pass is performed indistinguishable to the first. For any errors identified and corrected in the second pass, there is at least one corresponding error that is domiciled in the same block in the previous pass, since neither error was found nor corrected in that pass. For this purpose, in each correction made in any pass after the first pass, a binary search is rerun on the block containing that corrected bit in all previous passes, in order to identify any potential corresponding errors. At any period a new error is identified, it reveals error in a previous pass, hence the process is

repeated, and the error is detected and corrected. At this time Alice and Bob will find that all their parity comparisons are in agreement. The mathematical expression for obtaining the quantity of blocks in a pass is as follows:

$$n_i = \frac{N}{k_i} \tag{3.5}$$

where: N denotes the number of secret bits obtained by Alice and Bob, k represents the initial block size, k_1 denotes the block size in pass one, n_i depicts the number of blocks in ith pass, k_i is the block size in ith pass , p_i implies the number of ith pass

where i ranges as 1,2, . . . 5

Figure 3.4 succinctly describe how the sifted keys were divided into blocks of various sizes, and how the single bit parity check for each block is calculated and distributed publicly. It could be observed that as the number of pass increases there is a corresponding increase in blocks size and matching decrease in the number of blocks. This leads to a single block size that contains the reconcile key at the end of the reconciliatory process in pass 5. The process in Figure 3.4 is as follows: After the first pass, a permutation is applied, the block size is doubled by $2 \bullet k_i$ in the second pass, and is performed indistinguishable to the first pass. An error is identified in block 10 in second pass and corrected, there is at least one corresponding error that is domiciled in the same block in the first pass, since neither error was found or corrected in first pass. For this purpose, in each correction made in any pass after the first pass, a binary search is rerun on block 10 that contains the corrected bit in first pass, in order to identify any potential corresponding errors. At any period a new error is identified, it reveals error in a previous pass, hence the process is repeated, and the error is detected and

corrected. At the end of pass 5 a reconciled key length of 64 bits was obtained, which was used to encrypt the watermark image.

==========pass 1==========

block-1

block-2

block-3

block-4

block-5

block-6

block-7

block-8

block-9

block-10

block-11

block-12

block-13

block-14

Figure 3.4: Number and size of Block Generated at each Pass in Error Reconciliation Process

block-15

block-16

==========pass 2==========

block-1

pass-1-block-10

block-2

block-3

block-4

block-5

block-6

block-7

block-8

==========pass 3==========

block-1

block-2

block-3

block-4

==========pass 4==========

block-1

block-2

==========pass 5==========

block-1

Figure 3.4: Number and size of Block Generated at each Pass in Error Reconciliation Process

In order to use the symmetric key obtained to encrypt the watermark image, a symmetric encryption algorithm is employed. The algorithm is of two modules, encryption and decryption, which are based on shuffling the image pixels using affine transform and encrypting the image using XOR operation. A key of 64-bit length is then generated. The affine transform fractures the correlation between adjacent pixels of the image.

The encryption and decryption algorithms based on the 64 bits key length are described in algorithms 1 and 2 respectively.

Algorithm 1: Encryption Algorithm

Input: A Mandril watermark image of size 512 x 512 x 3 is converted to a gray level of secret image denoted as S and a 64-bit secret key

Output: A gray level cipher image of size 512 x 512 x 3

a. Split 64-bit secret key into:

   $K_0, K_1, K_2, K_3, K_4, K_5, K_6$ *and* K_7

   K_0 = bin2dec(key(1:8));

   K_1 = bin2dec(key(9:16));

   K_2 = bin2dec(key(17:24));

   K_3 = bin2dec(key(25:32));

   K_4 = bin2dec(key(33:40));

   K_5 = bin2dec(key(41:48));

   K_6 = bin2dec(key(49:56));

   K_7 = bin2dec(key(57:64));

b. For each pixel $P_{x,y}$ transform the location (X,Y) in S to (x',y') in C based on:

$$x' = (k_0 + k_1 \times x) \bmod M \tag{3.6}$$

$$y' = (k_2 + k_3 \times y) \bmod N \tag{3.7}$$

c. Decompose C into M/2 x N/2 number of 2 x 2 blocks

d. For each block Bi,j of C do:

   P11 = bitxor(B(1,1), K_4);

   P12 = bitxor(B(1,2), K_5);

P21 = bitxor(B(2,1), K_6);

P22 = bitxor(B(2,2), K_7);

e. End

Algorithm 2: Decryption Algorithm

Input: A cipher image of size 512 x 512 x 3 depicted as C and a 64-bit secret key

Output: A secret image S

a. Split 64-bit secret key into:

   $K_0, K_1, K_2, K_3, K_4, K_5, K_6$ *and* K_7

   K_0 = bin2dec(key(1:8));

   K_1 = bin2dec(key(9:16));

   K_2 = bin2dec(key(17:24));

   K_3 = bin2dec(key(25:32));

   K_4 = bin2dec(key(33:40));

   K_5 = bin2dec(key(41:48));

   K_6 = bin2dec(key(49:56));

   K_7 = bin2dec(key(57:64));

b. Decompose C into M/2 x N/2 number of 2 x 2 blocks

c. For each block Bi,j of C do:

   P11 = bitxor(B(1,1), K_4);

   P12 = bitxor(B(1,2), K_5);

   P21 = bitxor(B(2,1), K_6);

   P22 = bitxor(B(2,2), K_7)

d. For each pixel $P_{x,y}$ transform the location (x',y') in C to (X,Y) in S based on:

$$x = \left(x^{1} + \left(-k_0\right)\right) \times k_1^{-1} \right) \bmod M \tag{3.8}$$

$$y = \left(y^{'} + \left(-k_2\right)\right) \times k_3^{-1} \right) \bmod N \tag{3.9}$$

e. End

3. The coefficients of DOST transformations on each channel of the cover and encrypted watermark images are then fed into DWT for further transformation. This is necessary due to the fact that the DOST transformation output is not always easy to interpret and may not be sufficient enough to reveal all the details within a specific signal. The DWT is able to mitigate this limitation in DOST by decomposing the output of DOST transformation up to c^{th} level of decomposition into the following sub-bands (LL, LH, HL, HH), for complete representation and interpretation, where c is the number of levels a wavelet is supposed to be decomposed and in this work, c = 1, 2, and 3. The forward DWT host image decomposition is achieved using equations (2.4) and (2.5). The MATLAB code for implementation of forward 2D DWT for third level of decomposition of DOST transformation output is presented in appendix I

4. The transformed cover and encrypted watermark images are modified by applying SVD based on equations (2.7) and (2.8) in order to stabilize and increase the quality of the images. The following MATLAB commands show the modification of the singular component that is, the diagonal matrix, left and right vectors of the cover and encrypted watermark images respectively. The left component represents the horizontal details of the image while the right component depicts the vertical details of the image:

```
[Ua(:,:,c), Sa(:,:,c), Va(:,:,c)] = svd(Ia_transform(:,:,c));
[Ub(:,:,c), Sb(:,:,c), Vb(:,:,c)] = svd(Ib_transform(:,:,c));
```

5. The robustness and imperceptibility of any technique relies on the value of the scaling factor. A small value of scale factor increases the imperceptibility of the watermarked image while demeaning the fidelity of the extracted watermark and a large value decreases the imperceptibility of the watermarked image while improving the fidelity of the extracted watermark. A PSO-based scheme is used to optimally tune the scale factor.

   The PSO is incorporated in the watermarking algorithm, where an initial population is generated using a random function. The population is initialized with population size of 10 and the population of particles in swarm varies from 1 to 200. Each of these elements are then selected as the scaling factor and the encrypted watermark image is embedded inside the diagonal component of the cover image. Different noise attacks are applied to the generated watermarked images and the watermarks are extracted using the developed algorithm. The performance of each scaling factor is evaluated using the fitness function as shown in equation (3.10). The maximum value of the fitness discovered and the respective element is the global best particle, represented as P_{best}. in the first generation, particle acts as individual best particle which connotes P_{best}. the growing generation is created from the particles of the presence generation using equations (2.29) and (2.30). The performance of the particles of this generation is evaluated once more using the fitness function. The obtained values of the corresponding fitness functions are compared with the values of the fitness function from earlier generation of respective elements. The elements that offer the maximum fitness values are known as P_{best} particles, and the best of these global best particles is

the global best particle called G_{best}. The process is repeated till the desired number of iteration is executed.

In this research, maximum fitness is obtained at the end of the final iteration. The mathematical expression for the fitness function is as shown in:

$$Fitness = \max\left[\frac{corr2(I_b, I_{br}) + corr2(I_a, I_{ar})}{2}\right] \tag{3.10}$$

where: Corr depicts normalized correlation coefficient, I_b represents watermark image, I_{br} denotes decrypted image, I_a denotes cover image, I_{ar} depicts watermarked image

The acceleration coefficients C_1 and C_2 are given as 2. The lowest and highest velocities V_{lst} and V_{hst} are valued as 20 and 40 correspondingly. The overall quantity of particles is 200, and the number of iterations is 1000. The opening values of velocity *V* and inertia weight *W* are 2 and 1.5 accordingly. The flowchart of PSO-based scheme is as shown in Figure 3.5

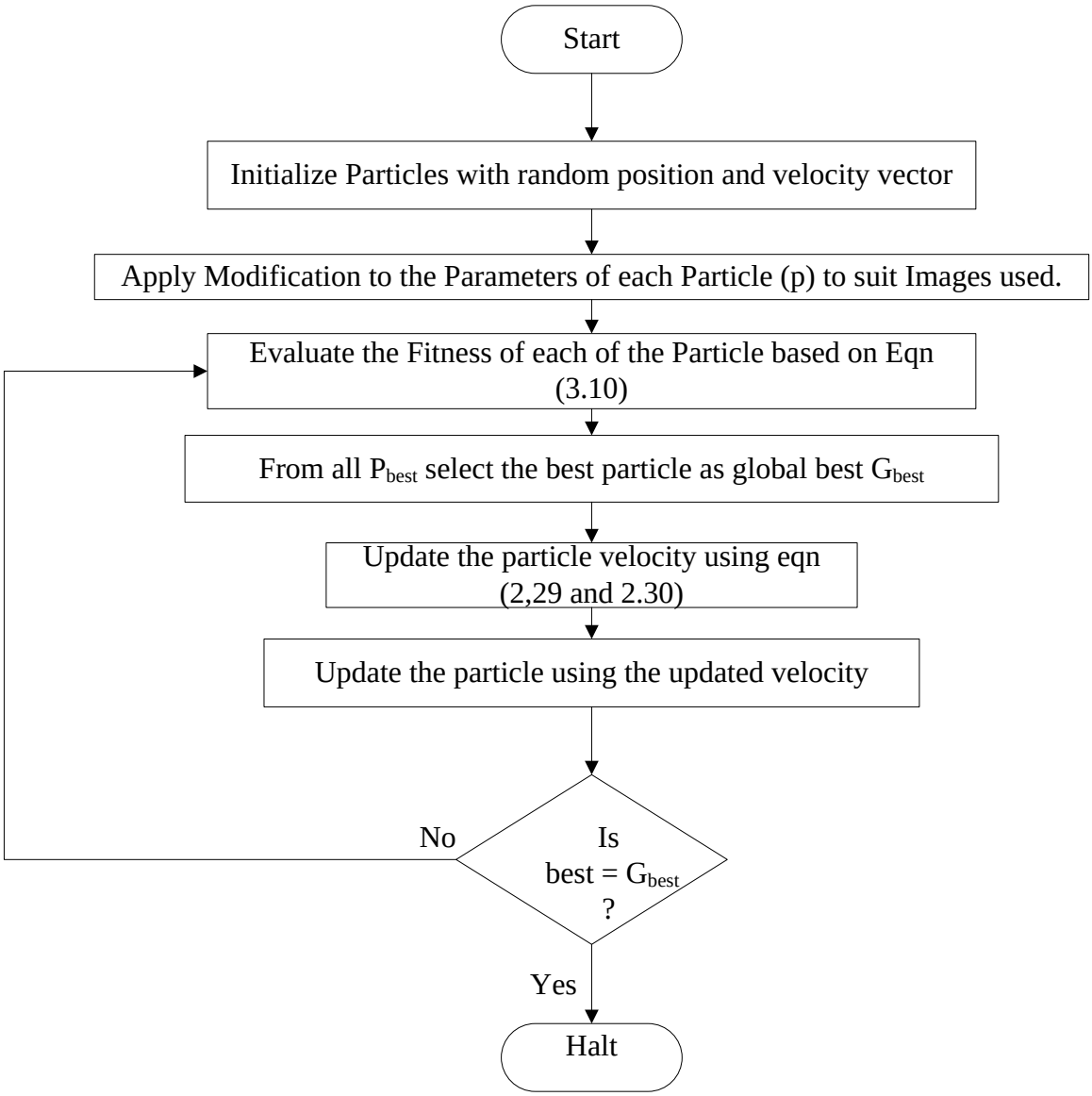


Figure 3.5: Flowchart of the PSO-Based Scheme

The steps adopted for the developed watermark embedding technique are described using the flowchart of Figure 3.6.

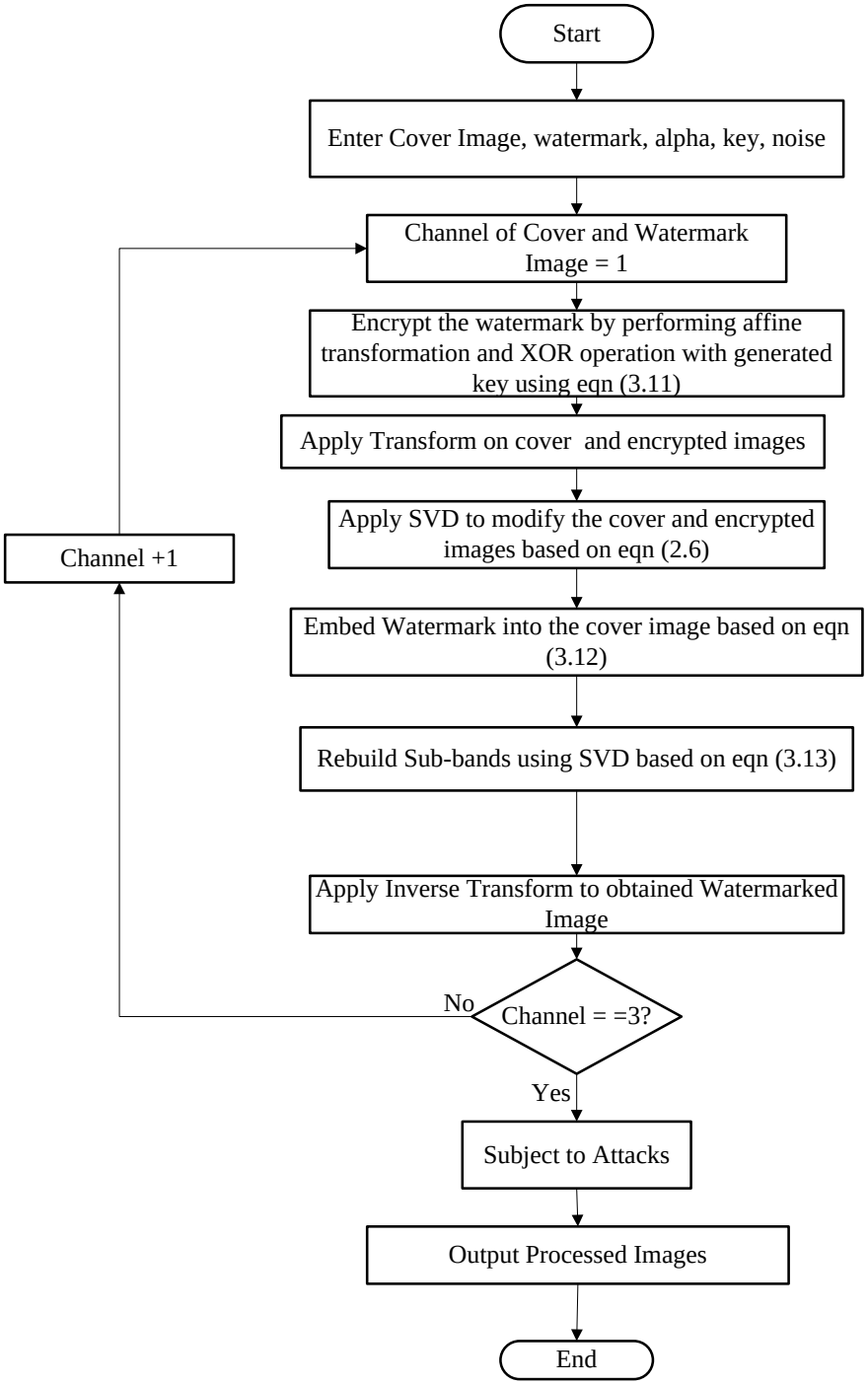


Figure 3.6: Developed Watermark Embedding Process

The encryption equation is given by:

$$eI_{b(c)} = I_b \otimes K \tag{3.11}$$

where: $eI_{b(c)}$ depicts encrypted image,

I_b denotes the watermark image,

K represents the generated key,

$\otimes$ depicts XOR operation

The embedding equation is given by:

$$S_{a(i,j)embeded} = S_a I_a + S_b eI_{b(c)} \times \alpha \tag{3.12}$$

where: $S_{a(i,j)embeded}$ represents the embedded image

$S_a I_a$ denotes the diagonal component of the cover image which is the singular values of the image

$S_b eI_{b(c)}$ represents the diagonal component of the encrypted image which depict the singular values of the image

α depicts the value of the scaling factor obtained with PSO

The rebuild equation is given by:

$$I_{CR_{c,w(i,j)}} = u_a \times s_{a_embedded} \times v_a^{'} \tag{3.13}$$

where: $I_{CR_{c,w(i,j)}}$ denotes the rebuild of the sub-bands, u_a is the left singular value of the cover image, $s_{a_embedded}$ is the singular value of the embedded image, $v_a^{'}$ represents the transpose of the right singular value of the cover image

6**.** The watermarked image degrades depending on the nature of the noise attack and can end up becoming a noisy watermarked image. This algorithm is described using the flowchart of Figure 3.7.

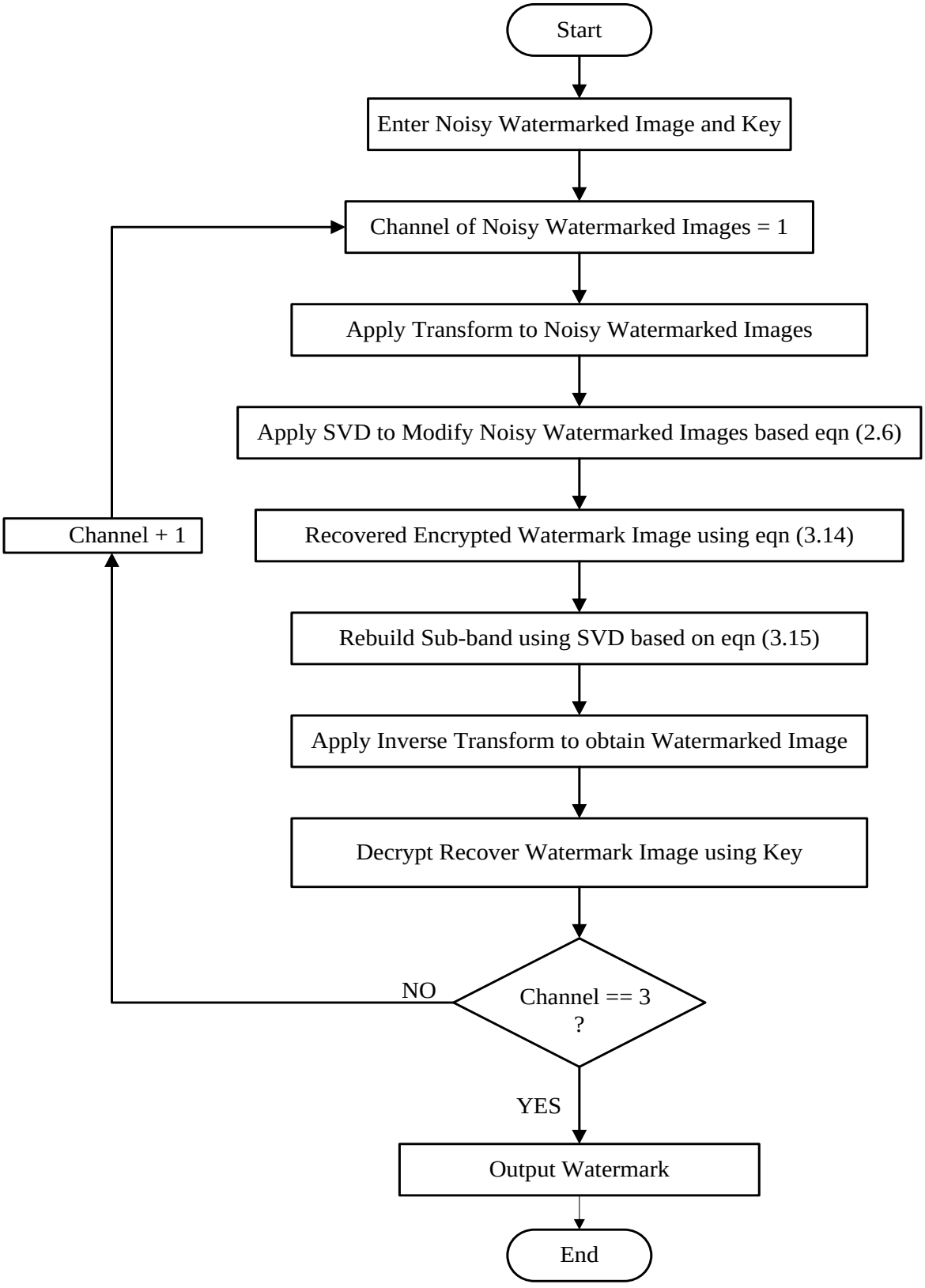


Figure 3.7: Developed Watermark Extraction Process

Figure 3.7 shows the systematic steps of the extraction process of the developed watermarking algorithm with a view to recovering the original watermark with little or no distortion to the watermark.

The recover equation is given by:

$$S_{br_encrypted} = \frac{S_w I_{w(i,j)} - S_a I_{a(i,j)}}{\alpha} \tag{3.14}$$

The rebuild sub-band equation is given by:

$$I_{br_rebuild} = u_b \times s_{br_encrypted} \times v_b \tag{3.15}$$

The following MATLAB function files (m.file) forms the structure of the proposed QKD-based watermarking process for the algorithm used in this research.

a. dost2.m: Decomposes the channel of each cover and encrypted watermark images

b. generateKey.m: Function that performs generation of binary bits

c. Senderclass.m: Function that performs the sending of quantum bits to receiver

d. **Receiverclass.m:** Function that performs the receiving of quantum bits from the sender

e. **Performpass.m:** Performs the various phases of error detection and correction

f. **Cascade.m:** Performs error reconciliation

g. **main.m1:** Performs error reconciliation process on obtained key

h. encryption.m: Encrypt the watermark image

i. applytransform.m: Transformation of the cover and encrypted watermark images by DOST, DWT and SVD

j. **objfun.m:** The PSO based evaluation of fitness function

k. **decryption.m:** The function that decrypt the encrypted watermark image

l. **main.m:** PSO based for obtaining the maximum scale factor (alphavalue) fitness function

m. **Watermarking process.m:** Performs the transformation, embedding and extraction process of the watermark

n. **idost:** perform inverse DOST transformation

o. **applyinverse Transform.m:** Perform the inverse transformation of the transformation techniques

p. **test.m:** Generate the watermarking simulation user interface

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents the results obtained from the developed watermarking algorithm used in carrying out experiment of robust digital image watermarking technique and their discussions. A number of scenarios were simulated and the results is presented based on the scaling factors (alpha value) determined by PSO-based scheme. Various images with and without noise attacks are used to evaluate the enhancement of the developed watermarking algorithm and pertinent results reported, and discussed

4.2 Decomposition of the Cover and Watermark Images

The output of the cover and watermark images decomposition into RGB components are shown in Figures 4.1 and 4.2 respectively. The DOST uses these as inputs and transforms each channel of the cover image.



(a) Cover Image



(b) Red Channel of Cover Image



(c) Green Channel of Cover Image



(d) Blue Channel of Cover Image

Figure 4.1: Decomposition of Cover Image into RGB Component



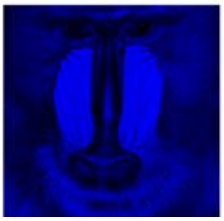
(a) Watermark Image



(b) Red Channel of Watermark Image



(c) Green Channel of Watermark Image



(d) Blue Channel of Watermark Image

Figure 4.2: Decomposition of Watermark Image into RGB

4.3 Determination of Scaling Factor

The optimal value of the scale factor obtained by PSO-based scheme, which in this case is the best value after 1000 runs, is 0.1208. It is this value that is used for the embedding and extraction processes in the different attack scenarios considered as follows:

4.4 Definition of Different Scenarios

The following are the different scenarios considered in evaluating the robustness and imperceptibility of the developed digital watermarking technique whilst using the optimal scaling factor for the different attacks to evaluate the level of distortion the attack will cause to watermark embedded inside the cover image:

1. **Case I:** The scenario where the watermarked image is under no attack
2. **Case II:** The scenario where the watermarked image is under Gaussian attack
3. **Case III:** The scenario where the watermarked image is under salt and pepper attack
4. **Case IV:** The scenario where the watermarked image is under speckle attack

5. **Case V:** The scenario where the watermark image is encrypted with a 64-bit private key that is generated using binary number generator and the watermarked image is under speckle attack
6. **Case VI:** The scenario where the watermark image is encrypted with a 64-bit private key and the watermarked image is under salt and pepper attack
7. **Case VII:** The scenario where the watermark image is encrypted with a 64-bit private key and the watermarked image is under Gaussian attack

4.4.1 Robustness and Imperceptibility Results for Case I

The original cover and watermark images that are used for inserting and recovering procedures in this scenario are as shown in Figure 3.1. Figure 4.3 depicts the visual similarity between the original cover and watermarked images. The original cover image is used to host the private information (watermark image) that forms the watermarked image.



(a) Original Cover Image



(b) Watermarked Image

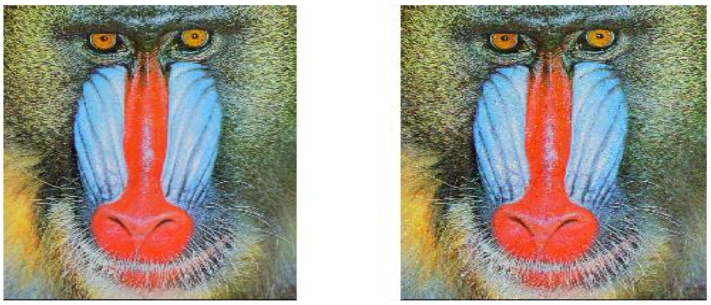
Figure 4.3: Comparison of Visual Similarity between Original Cover and Watermarked Image Based on PSNR Value

Figure 4.4 shows the watermarked image under no attack. It can be observed that the watermarked image under no attack depict clear similarity between the original cover and watermarked images with reference from Figure 4.3 which signifies high level of imperceptibility with a PSNR value of 47.2805dB.



Figure 4.4: Watermarked Image under No Attack

The resemblance between the original watermark and recovered watermark images is as shown in Figure 4.5. The level of similarity between the images shows the level of robustness of the algorithm to the attack with NCC value of 0.9804 and SSIM value of 0.9998 that depicts the visual similarity between them.



(a) Original Watermark (b) Extracted Watermark

Figure 4.5: Comparison of Original and Extracted Watermark Images under No Attack

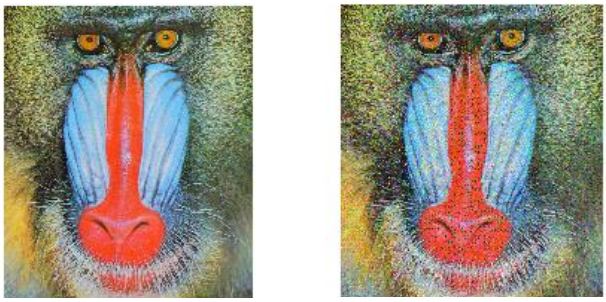
4.4.2 Robustness and Imperceptibility Results for Case II

The original cover and watermark images before any form of transformation are as shown in Figure 3.1. Figure 4.6 shows the watermarked image under Gaussian attack. The watermarked image under Gaussian attack depicts the visual resemblance between the original and watermarked images with referenced to Figure 4.3. It shows a high level of imperceptibility for this scenario which signifies a PSNR value of 45.4202dB.



Figure 4.6: Watermarked Image under Gaussian Attack

The resemblance between the original watermark and recovered watermark images under Gaussian attack is as shown in Figure 4.7. The level of similarity between the images shows the level of robustness of the algorithm under Gaussian attack that represents an NCC value of 0.9147 and SSIM value of 0.9564.



(a) Original Watermark (b) Extracted Watermark

Figure 4.7: Comparison Original and Recovered Watermark Images under Gaussian Attack

4.4.3 Robustness and Imperceptibility Results for Case III

Figure 4.8 shows the watermarked image under salt and pepper attack. The level of similarity between the watermarked image under salt and pepper attack, original cover image and watermarked image as shown from Figure 4.3 explains the level of resistance of the algorithm to this attack with reference to ITU-R bench mark of 35dB, which highlights the high level of imperceptibility of the technique with a PSNR value of 46.4406dB.



Figure 4.8: Watermarked Image under Salt and Pepper Attack

The similarity between the original watermark and extracted watermark images under salt and pepper attack is as shown in Figure 4.9. The level of similarity between the images shows the level of robustness of the algorithm under salt and pepper attack with an NCC value of 0.7254 and SSIM value of 0.8626.



(a) Original Watermark Image (b) Extracted Watermark Image

Figure 4.9: Comparison of Original Watermark and Extracted Watermark Images under Salt and Pepper Attack

4.4.4 Robustness and Imperceptibility Results for Case IV

Figure 4.10 shows the watermarked image under speckle attack. The level of similarity between the watermarked image under speckle attack in comparison with original cover image shown in Figure 4.3 explains the level of resistance of the algorithm to this attack, which highlights the high level of imperceptibility of the technique with a PSNR value 45.5727dB.



Figure 4. 10: Watermarked Image under Speckle Attack

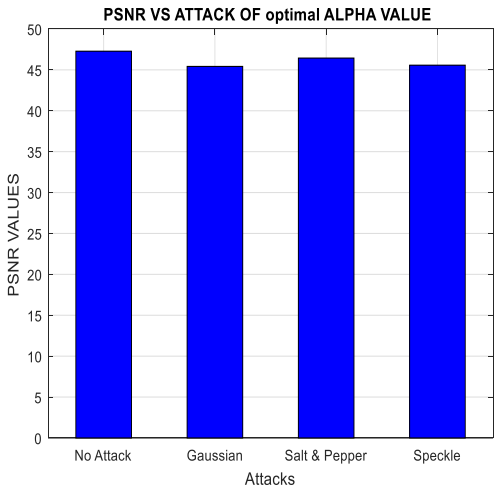
The match between the original watermark and recovered watermark images under speckle attack is as shown in Figure 4.11. The level of similarity between the images shows the level of robustness of the algorithm under speckle attack with an NCC value of 0.8588 and SSIM value of 0.9293.



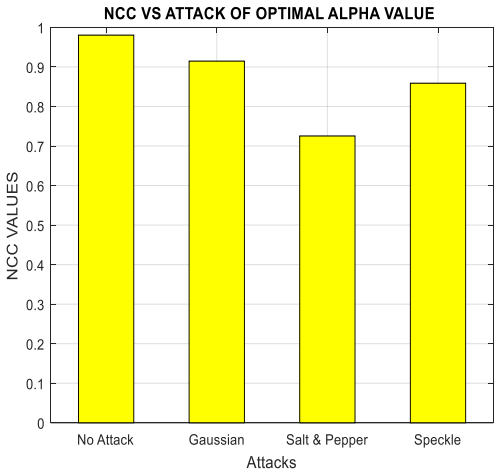
(a) Original Cover Image (b) Extracted Watermark

Figure 4.11: Comparison of Original Watermark Image and Extracted Watermark Image under Speckle Attack

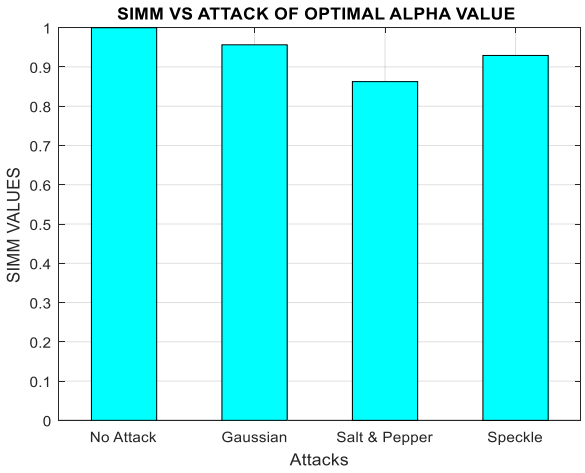
The summary of results of this scenario is depicted in Table 4.1 as shown in appendix Q. Figure 4.12 shows the histogram of the performance metrics results obtained for evaluating the robustness and imperceptibility of the developed digital watermarking technique whilst using the optimal scaling factor under no attack, Gaussian, salt and pepper and speckle attacks. The height of individual bar in PSNR values for each attack connotes the degree of imperceptibility which implies the level to which the watermark is hidden from an observer. SSIM exhibits same characteristics. The height of individual bar in NCC illustrates the level of robustness of the algorithm to specific attack.



(a) PSNR Values for Watermarked Ima



(b) NCC Values for Watermark



(c) SSIM Values for Watermark

Figure 4.12: Comparison of the Results of PSNR, NCC and SSIM Obtained using the Optimal Scale Factor

4.4.5 Robustness and Imperceptibility Results for Case V

The 64-bit key generated is used to encrypt the watermark image before the embedding process is as shown in Figure 4.13.

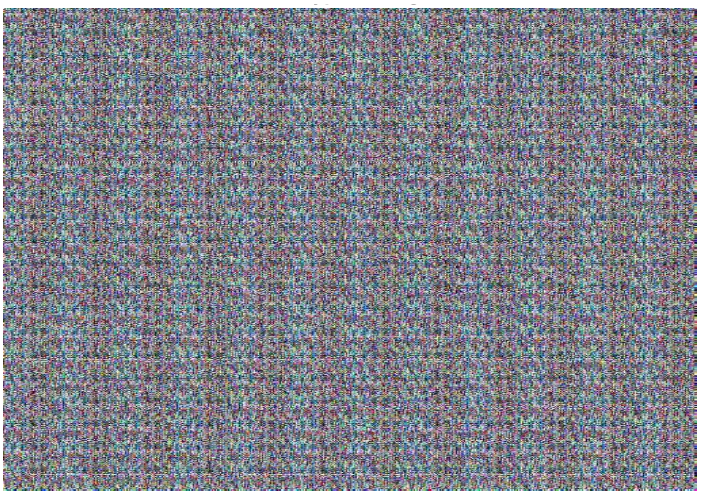


Figure 4.13: Encrypted Watermark Image (Mandril)

The watermarked image that contains the encrypted watermark image under speckle attack is as shown in Figure 4.14(b). The degree of similarity between the watermarked image under speckle attack, and original cover image with referenced to Figure 4.3 in comparison with watermarked image given in Figure 4.14 (b) explains the level of resistance of the algorithm to this attack, which highlights the high level of imperceptibility of the technique with a PSNR value of 46.3648dB.



(a) Watermarked Image that contains the Encrypted Watermark Image



(b) Watermarked Image under Speckle Attack

Figure 4.14: Comparison between Watermarked and Watermarked Images under Speckle Attack

The recovered encrypted watermark image under speckle attack is as shown in Figure 4.15.

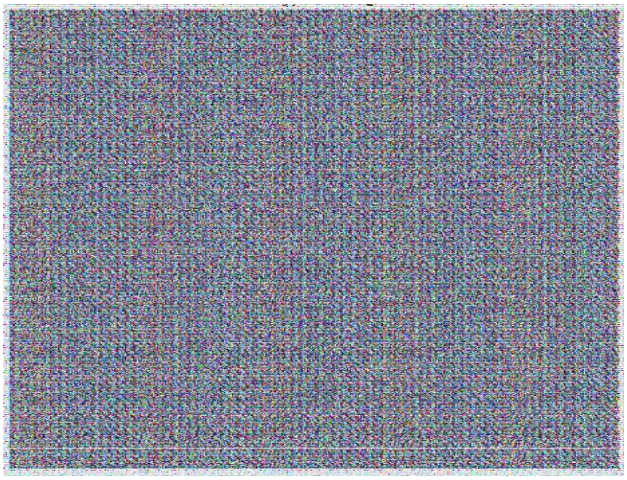
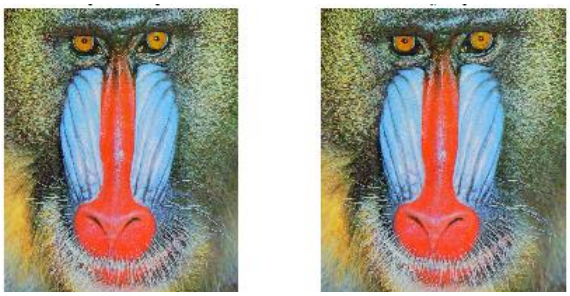


Figure 4.15: Recovered Encrypted Watermark Image under Speckle Attack

The high level of visual relationship between the original and extracted decrypted watermark images under speckle attack as shown in Figure 4.16 shows the robustness of the developed technique against such attack with an NCC value of 0.8863 and SSIM value of 0.9293.



(a) Original Watermark (b) Extracted Decrypted Watermark

Figure 4.16: Extracted Decrypted Watermark Image under Speckle Attack

4.4.6 Robustness and Imperceptibility Results for Case VI

The 64-bit key encrypted watermark image before the embedding process is as shown in Figure 4.13. The watermarked image that contains the encrypted watermark image under salt and pepper attack is as shown in Figure 4.17. The degree of similarity between the

watermarked image under salt and pepper attack, and original cover image with reference to Figure 4.3 explains the level of similarity of these images, indicates the level of resistance of the algorithm to this attack in terms of imperceptibility with a PSNR value of 46.4406dB.



Figure 4.17: Watermarked Image under Salt and Pepper Attack

Figure 4.18 shows the recovered encrypted watermark image under salt and pepper attack.

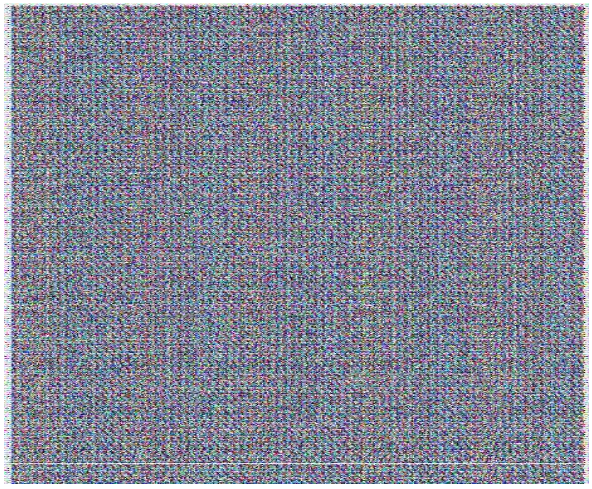
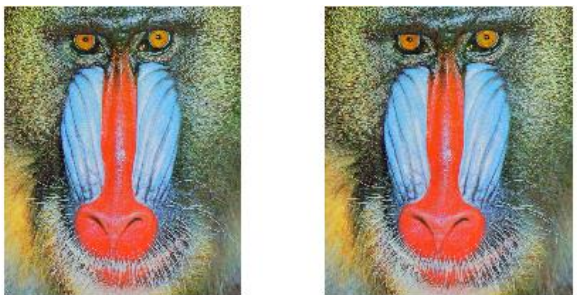


Figure 4.18: Recovered Encrypted Watermark Image under Salt and Pepper Attack

The high level of visual resemblance between the original watermark and extracted decrypted watermark under salt and pepper attack as shown in Figure 4.19 depicts the robustness of the developed technique against such attack with an NCC value of 0.8010 and SSIM value of 0.9003 respectively.



(a) Original Watermark (b) Extracted Decrypted Watermark Image

Figure 4.19: Extracted Decrypted Watermark Image under Salt and Pepper Attack

4.4.7 Robustness and Imperceptibility Results for Case VII

The 64-bit key encrypted watermark image before the embedding process is as shown in Figure 4.13. The watermarked image that contains the encrypted watermark image under Gaussian attack is as shown in Figure 4.20. The degree of similarity between the watermarked image under Gaussian attack, and original cover image as shown in Figure 4.3 highlights the level of robustness of the technique with a PSNR value of 46.8875dB.



Figure 4.20: Watermarked Image Under Gaussian Attack

The recovered encrypted watermark image after subjected to Gaussian attack is as shown in Figure 4.21.

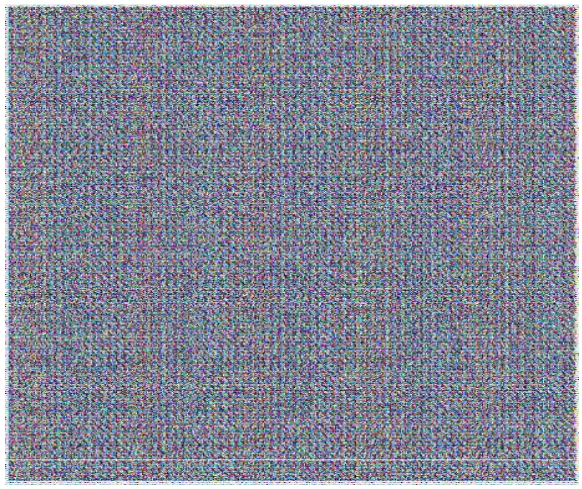
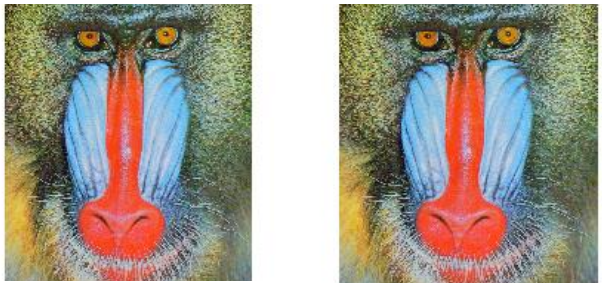


Figure 4.21: Recovered Encrypted Watermark Image under Gaussian Attack

The high level of visual similarity between the original and extracted decrypted watermark images under Gaussian attack as shown in Figure 4.22 indicates the robustness of the developed technique against such attack with an NCC value of 0.8846 and SSIM value of 0.9422 respectively.

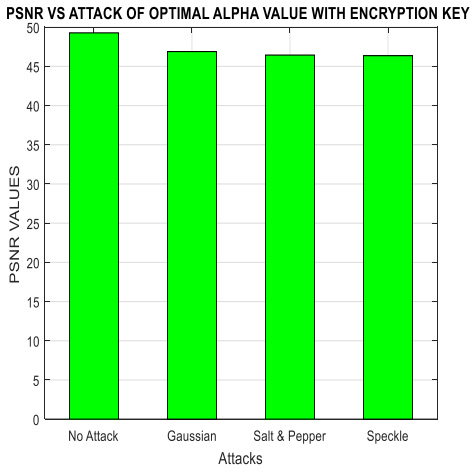


(a) Original Watermark Imag (b) Decrypted Watermark Image

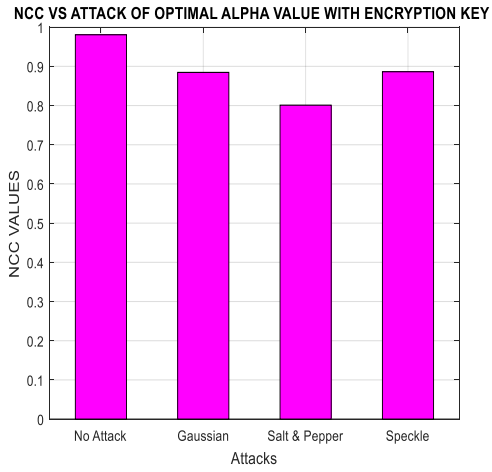
Figure 4.22: Comparison of Original Watermark Image and Extracted Decrypted Watermark Image under Gaussian Attack

The summary of results of this scenario is depicted in table 4.2 as shown in appendix Q

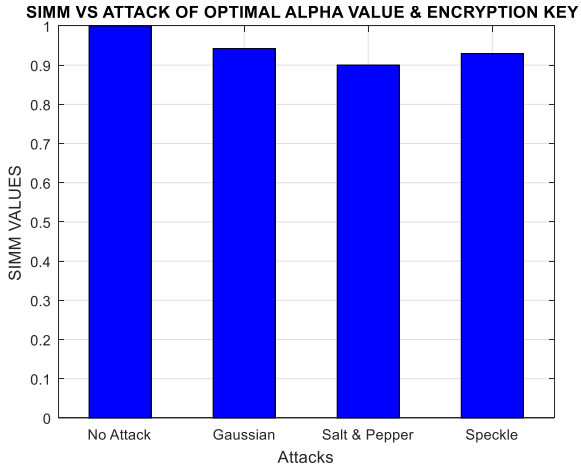
Figure 4.23 shows the summary of the performance metrics for evaluating the robustness and imperceptibility of the developed digital watermarking technique, based on encrypted watermark image with 64-bit key whilst using the optimal scale factor. The height of individual bar in PSNR values for each attack connotes the degree of imperceptibility which implies the level in which the data is concealed from an observer. SSIM exhibits same characteristics. The height of individual bar in NCC illustrates the level of robustness of the algorithm to specific attack.



(a) PSNR Values for Watermarked Image



(b) NCC Values for Watermark



(c) SSIM Values for Watermark

Figure 4.23: Comparison of the Results of PSNR, NCC and SSIM Obtained using the Encrypted Watermark and Optimal Scale Factor

4.5 Other Scenarios Considered for Comparison

The following are the other scenarios considered in order to be able to evaluate the robustness and imperceptibility of the developed digital watermarking technique whilst using a selected manual scaling factor of 0.0121:

1. **Case VIII:** The scenario where the watermarked image is under no attack
2. **Case IX:** The scenario where the watermarked image is under Gaussian attack
3. **Case X:** The scenario where the watermarked image is under salt and pepper attack
4. **Case XI:** The scenario where the watermarked image is under speckle attack

4.5.1 Robustness and Imperceptibility Results for Case VIII

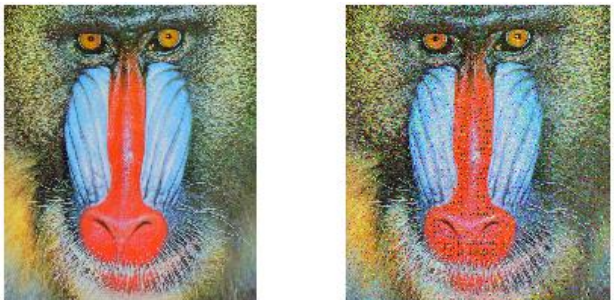
The comparison of the watermarked image under no attack obtained with a manually selected scaling factor of 0.0121 shown in Figure 4.24 with the original cover image with reference to Figure 4.3. It can be observed that the three images are visually similar with a PSNR value of 79.6917dB. This denotes the level at which the watermark is hidden from an observer or attacker.



Figure 4.24: Watermarked Image under No Attack

The similarity between the original watermark and recovered watermark images under no attack is as shown in Figure 4.25. It can be perceived that the recovered watermark image still contains some form of noise, despites the fact that it was not subjected to any form of attack

since an NCC value of 1 was not obtained. This implies that robustness had been traded-off for imperceptibility with an NCC value of 0.9191 and SSIM value of 0.9595.



(a) Original Watermark Image (b) Extracted Watermark Image

Figure 4.25: Original Watermark and Recovered Watermark Images under No Attack

4.5.2 Robustness and Imperceptibility Results for Case IX

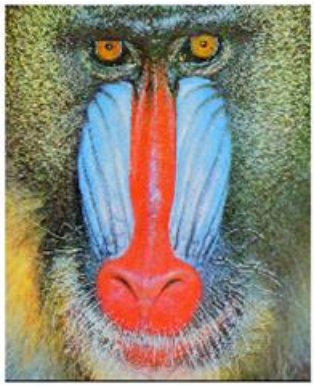
The watermarked image under Gaussian attack with a manually selected scaling factor of 0.0121 is as shown in Figure 4.26. The degree of similarity between the watermarked image under Gaussian attack, original cover image as shown in Figure 4.3 and watermarked image as given in Figure 4.24 (a) highlights the level of imperceptibility of the technique. It can be observed that the three images are visually similar with a PSNR value of 64.8475dB.



Figure 4.26: Watermarked Image under Gaussian Attack

The similarity between the original watermark and recovered watermark images under Gaussian attack is as shown in Figure 4.27. It can be seen that the recovered watermark image contains some form of noise that depicts high visual difference between the original

watermark image and recovered watermark image. This implies that robustness had been traded-off for imperceptibility that represents an NCC value of 0.3289 and SSIM value of 0.1584.



(a) Original Watermark Image



(b) Extracted Watermark Image

Figure 4.27: Comparison of Original Watermark and Recovered Watermark Images under Gaussian Attack

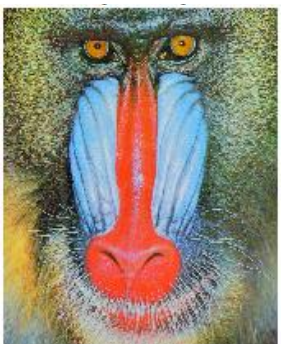
4.5.3 Robustness and Imperceptibility Results for Case X

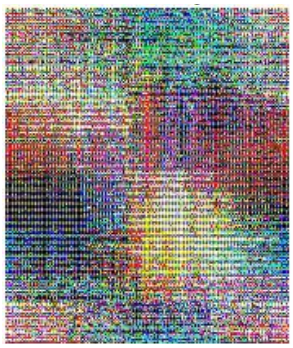
The watermarked image under salt and pepper attack with a manually selected scaling factor of 0.0121 is as shown in Figure 4.28. The level of similarity between the watermarked image under salt and pepper attack, watermarked image as given in Figure 4.24 (a) and original cover image as shown in Figure 4.3 highlights the level of imperceptibility of the technique. It can be observed that the three images are visually similar, although, small spots are found to be distributed on the image under the salt and pepper attack with a PSNR value of 56.8566dB.



Figure 4.28: Watermarked Image under Salt and Pepper Attack

The visual similarity between the original watermark and recovered watermark images under salt and pepper attack is as shown in Figure 4.29. It can be observed the recovered watermark image contains some form of noise that depicts high visual difference between the original watermark image and recovered watermark image. This implies that robustness had been traded-off for imperceptibility with an NCC value of 0.1105 and SSIM value of 0.0759.





(a) Original Watermark Image (b) Extracted Watermark Image

Figure 4.29: Original Watermark and Recovered Watermark Images under Salt and Pepper Attack

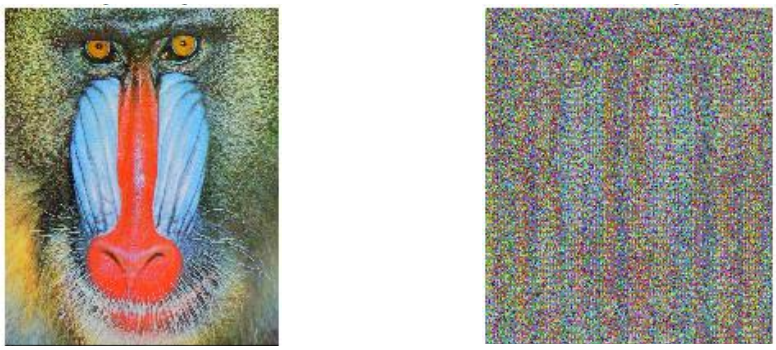
4.5.4 Robustness and Imperceptibility Results for Case XI

The watermarked image under speckle attack with a manually selected scaling factor of 0.0121 is as shown in Figure 4.30. The level of similarity between the watermarked image under speckle attack, watermarked image as given in Figure 4.24 (a) and original cover image as shown in Figure 4.3 indicates the level of imperceptibility of the technique. It can be observed that the three images are visually similar, although, small spots are found on the image under the speckle attack that signifies a PSNR value of 60.1784dB



Figure 4.30: Watermarked Image under Speckle Attack

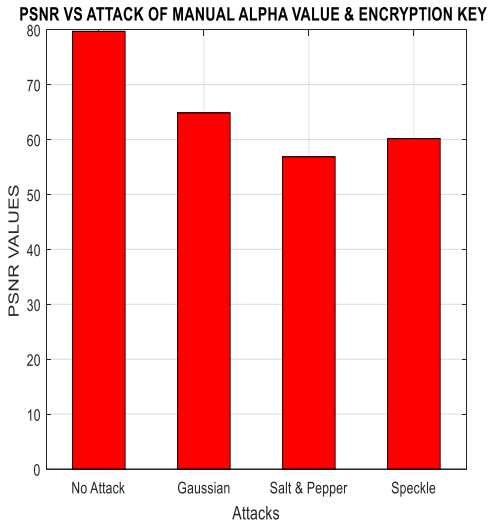
The similarity between the original watermark and recovered watermark images under speckle attack is as shown in Figure 4.31. It can be observed the recovered watermark image contains some form of noise that depicts high visual difference between the original watermark image and recovered watermark image. This implies that robustness had been traded-off for imperceptibility which corresponds to an NCC value of 0.1636 and SSIM value of 0.1115.



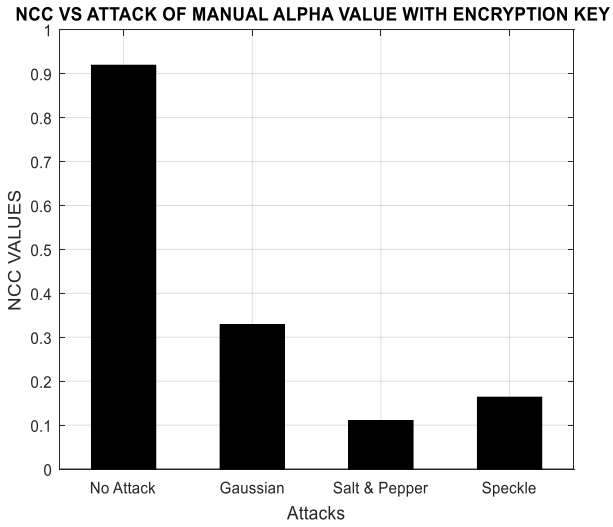
(a) Original Watermark Image (b) Extracted Watermark Image

Figure 4.31: Comparison of Original Watermark and Recovered Watermark Images under Speckle Attack

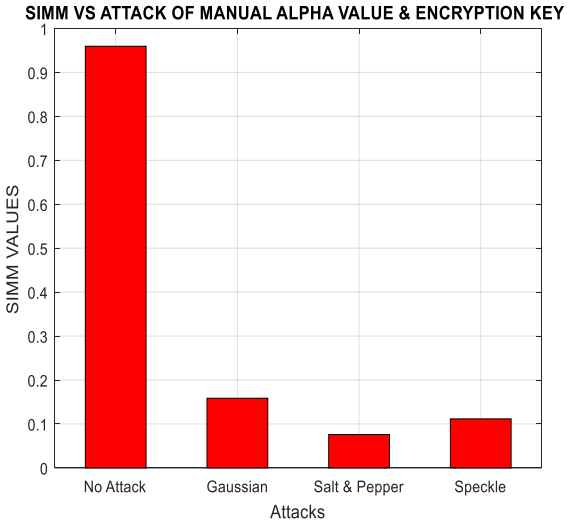
The summary of results of this scenario is depicted in table 4.3 as shown in appendix Q. Figure 4.32 shows the summary of results obtained of the performance metrics for evaluating the robustness and imperceptibility of the developed digital watermarking technique, whilst using a manually selected scaling factor of 0.0121. The height of individual bar in PSNR values for each attack connotes the degree of imperceptibility which implies the level in which the watermark is concealed from an observer. SSIM exhibits same characteristics. The height of individual bar in NCC illustrates the level of robustness of the algorithm to specific attack.



(a) PSNR Values for Watermarked Image



(b) NCC Values for Watermark



(c) SSIM Values for Watermark

Figure 4.32: Comparison of the Results of PSNR, NCC and SSIM Obtained using the Selected Scale Factor

4.6 Determination of Optimal Scale Factor Based on Individual Attack Scenarios using PSO

Different optimal value of scaling factors is obtained by PSO-based scheme under specific attack, in the quest to achieve an optimal balance between imperceptibility and robustness. Which in this case colour Lena and Pepper Images are adopted as cover images of same size.

Mandril and Nepal Telecom logo as watermark images. The varying values of optimal scaling factors obtained when standard RGB colour Lena is employed as the cover image and Mandril as the watermark image of same size 512 x 512 x 3 and subjected to Gaussian, salt and pepper, speckle, rotate at 30°, 20° and crop are as follows 0.4362, 1, 0.3708, 1, 1 and 0.3746 respectively. The various optimal values of scale factors obtained when Pepper is adopted as the cover image and Nepal Telecom logo as watermark image of same size 512 x 512 x 3 and subjected to Gaussian, salt and pepper, speckle, rotate at 45°, 5°, 90° and crop attack are as follows 0.1183, 1, 1, 0.2478, 0.1308, 1 and 1 respectively. The different optimal values of scale factors obtained when Pepper is adopted as the cover image of size 512 x 512 x 3 and Nepal Telecom logo as watermark image of size 256 x 256 x 3 and subjected to Gaussian, salt and pepper, speckle, rotate at 45°, 5°, 90° and crop attack are 0.2283, 1, 1, 0.2478, 0.1408, 1 and 1 accordingly. It is these various values that were used for embedding and extraction processes in the different scenarios considered in these cases.

4.7 Definition of Different Scenarios

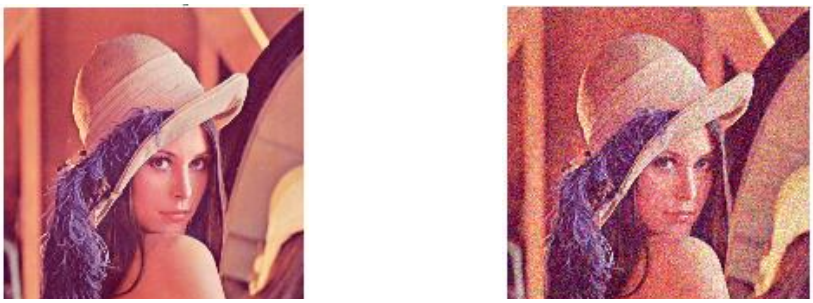
The following are the different scenarios considered in evaluating the robustness and imperceptibility of the developed digital watermarking technique whilst using the peculiar optimal scaling factor obtained by adopting Lena and Mandril of same size 512 x 512 x 3 under each of the following attack scenarios:

1. **Case I:** The scenario where the watermarked image is under Gaussian attack
2. **Case II:** The scenario where the watermarked image is under salt and pepper attack
3. **Case III:** The scenario where the watermarked image is under speckle attack
4. **Case IV:** The scenario where the watermarked image is rotated at 30° attack
5. **Case V:** The scenario where the watermark image is rotated at 20° attack

6. **Case VI:** The scenario where the watermark image is under crop attack

4.7.1 Robustness and Imperceptibility Results for Case I

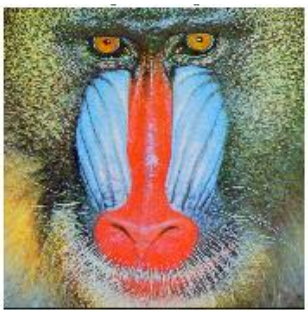
The original cover and watermark images that are used for embedding and extraction procedures are as presented in Figure 3.1. The original cover image is used to host the private information (watermark image) that forms the watermarked image. Henceforth, for the purpose of comparison from case I to case VI, Figure 3.1 is referenced while comparing watermarked image and extracted watermark image with original cover and watermark images. Figure 4.33 illustrates the comparison between the watermarked image under Gaussian attack and original cover image as shown in Figure 4.3. It can be observed that the three images depict visual similarity between them which signifies high level of imperceptibility, that is, the degree at which the secret information is hidden without notice with a PSNR value of 46.9152dB.



(a) Watermarked Image (b) Watermarked Image under Gaussian Attack

Figure 4.33: Comparison of Cover, Watermarked and Watermarked Images Under Gaussian

The visual relationship between the original watermark and recovered watermark images under Gaussian attack is as shown in Figure 4.34. The level of visual similarity between the images shows the degree of robustness of the algorithm under Gaussian attack with an NCC value of 0.9842 and SSIM value of 0.9739. This implies that the original watermark and extracted watermark images are almost the same since the NCC is close to 1.



(a) Original Watermark Image



(b) Extracted Watermark Image

Figure 4.34: Comparison of Original Watermark and Extracted Watermark Images under Gaussian attack

4.7.2 Robustness and Imperceptibility Results for Case II

Figure 4.35 illustrates the assessment between the watermarked image under salt and pepper attack and original cover image as given in Figure 4.3. It can be observed that the three images depict visual similarity between them which signifies high level of imperceptibility, that is, the degree at which the private information is hidden without notice with a PSNR value of 43.6528dB.



(a) Watermarked Image



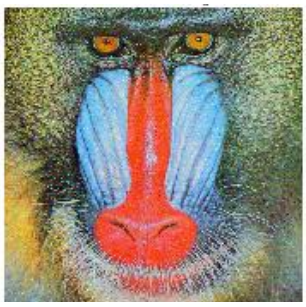
(b) Watermarked Image under Salt and Pepper

Figure 4.35: Comparison of Watermarked Image and Watermarked Image under Salt and Pepper Attack

The visual similarity between the original watermark and recovered watermark images under salt and pepper attack is as shown in Figure 4.36. The degree of visual similarity between the images shows the level of robustness of the algorithm under salt and pepper attack with an NCC value of 0.9582 and SSIM value of 0.9557. This depicts that the original watermark and extracted watermark images are almost alike since the NCC value obtained is close to 1.



(a) Original Watermark Image



(b) Extracted Watermark Image

Figure 4.36: Comparison of Original Watermark and Extracted Watermark Images under Salt and Pepper Attack

4.7.3 Robustness and Imperceptibility Results for Case III

Figure 4.37 shows the evaluation between watermarked image under speckle attack and original cover image as given in Figure 4.3. It can be observed that the three images depict visual similarity between them which signifies high degree of imperceptibility, that is, the level at which the secret information is concealed without notice with a PSNR value of 41.3768dB.



(a) Watermarked Image



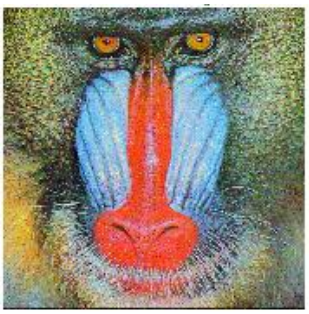
(b) Watermarked Image under Speckle Attack

Figure 4.37: Comparison of Original Cover Image, Watermarked and Watermarked Image under Speckle Attack

The visual similarity between the original watermark and recovered watermark images under speckle attack is as shown in Figure 4.38. The degree of visual similarity between the images shows the level of robustness of the algorithm under speckle attack with an NCC value of 0.9688 and SSIM value of 0.9404. This depicts that the original watermark and extracted watermark images are almost similar since the NCC value obtained is close to 1.



(a) Original Watermark Image



(b) Extracted Watermark Image

Figure 4.38: Comparison of Original watermark and Extracted Watermark images under Speckle Attack

4.7.4 Robustness and Imperceptibility Results for Case IV

Figure 4.39 shows the evaluation between watermarked image under which the watermarked image is rotated at 30° and original cover image as given in Figure 4.3. It can be observed that the three images depict visual similarity between them which signifies high degree of imperceptibility, even after the watermarked image is subjected to 30° rotation, that is, the level at which the secret information is concealed without notice with a PSNR value of 42.9160dB.



(a) Watermarked Image



(b) Watermarked Image Rotated at 30°

Figure 4.39: Comparison of Original Cover Image, Watermarked and Watermarked Image Rotated at 30°

The visual similarity between the original watermark and recovered watermark images when rotated at 30° is as shown in Figure 4.40. The degree of visual similarity between the images shows the level of robustness of the algorithm under geometric attack with an NCC value of

0.8877 and SSIM value of 0.7960. This depicts that the original watermark and extracted watermark images shows how close the recovered watermark is to the original watermark.

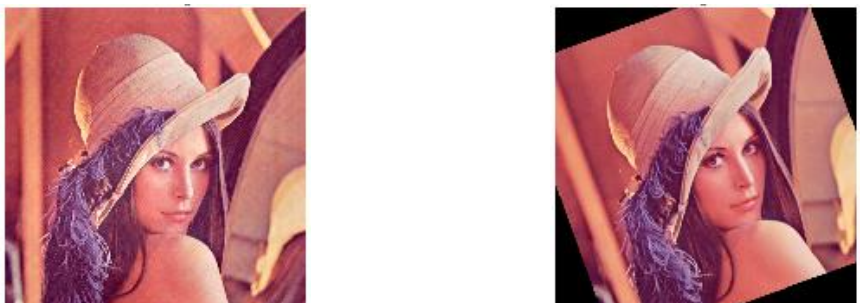


(a) Original Watermark Image (b) Extracted Watermark Image

Figure 4.40: Comparison of Original watermark and Extracted Watermark images under 30° Rotation

4.7.5 Robustness and Imperceptibility Results for Case V

Figure 4.41 shows the evaluation between watermarked image under which the watermarked image is rotated at 20° and original cover image as given in Figure 4.3. It can be observed that the three images depict visual similarity between them which signifies high degree of imperceptibility, even after the watermarked image is subjected to 20° rotation, that is, the level at which the secret information is concealed without notice with a PSNR value of 43.8328dB.



(a) Watermarked Image (b) Watermarked Image Rotated at 20°

Figure 4.41: Comparison of Original Cover Image, Watermarked and Watermarked Image Rotated at 20°

The visual similarity between the original watermark and recovered watermark images when rotated at 20° is as shown in Figure 4.42. The degree of visual similarity between the images shows the level of robustness of the algorithm under geometric attack with an NCC value of

0.8681 and SSIM value of 0.7587. This depicts that the original watermark and extracted watermark images shows how near the recovered watermark is to the original watermark.



(a) Original Watermark Image



(b) Extracted Watermark Image

Figure 4.42: Comparison of Original watermark and Extracted Watermark images under 20° Rotation

4.7.5 Robustness and Imperceptibility Results for Case VI

Figure 4.43 depicts the assessment between watermarked image, watermarked image subjected to crop attack and original cover image as given in Figure 4.3. It can be observed that the three images depict visual similarity between them which signifies high degree of imperceptibility, that is, the level at which the secret information is hidden without notice with a PSNR value of 43.2816dB.



(a) Watermarked Image



(b) Extracted Watermarked Image

Figure 4.43: Comparison of Original Cover Image, Watermarked and Watermarked Image under Crop Attack

The visual similarity between the original watermark and recovered watermark images when subjected to crop attack is depicted in Figure 4.44. The degree of visual similarity between the images shows the level of robustness of the algorithm under geometric attack with an NCC value of 0.9631 and SSIM value of 0.8096. This shows that the original watermark and

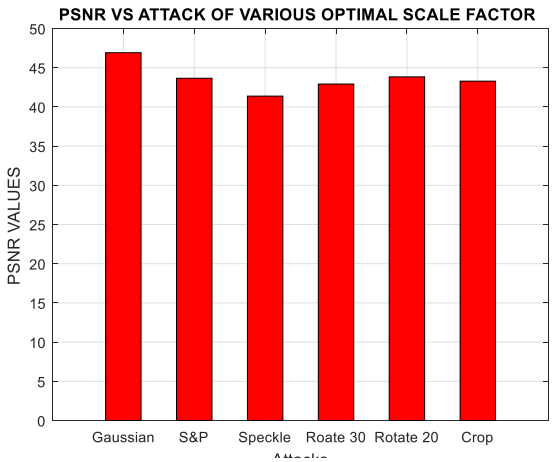
extracted watermark images shows how close the recovered watermark is to the original watermark.



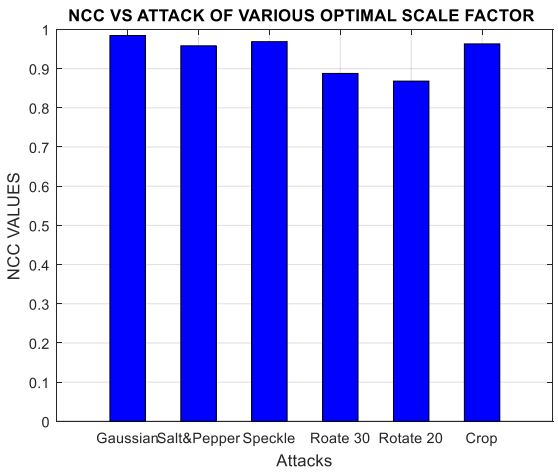
(a) Original Watermark Image (b) Extracted Watermark Image

Figure 4.44: Comparison of Original watermark and Extracted Watermark images under Crop Attack

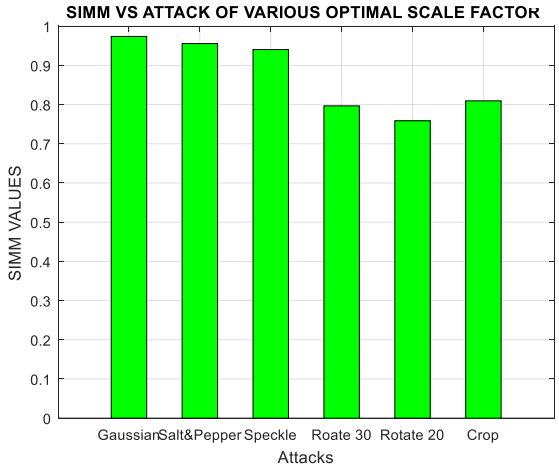
The summary of results of the various scenarios is depicted in Table 4.4 as shown in appendix R. Figure 4.45 shows the summary of the performance metrics for evaluating the robustness and imperceptibility of the developed digital watermarking technique, whilst using a selected scale factor from various scenarios. The height of individual bar in PSNR values for each attack denotes the degree of imperceptibility a measure of the level in which the watermark is hidden from an observer. The height of individual bar in NCC illustrates the level of robustness of the algorithm to specific attack.



(a) PSNR Values for Watermarked Image



(b) NCC Values for Watermark



(c) SSIM Values for Watermark

Figure 4.45: Comparison of the Results of PSNR, NCC and SSIM Obtained using the Optimal Scaling Factor under various Attacks

4.8 Definition of Different Scenarios

The following are the different scenarios considered in evaluating the robustness and imperceptibility of the developed digital watermarking technique whilst using the peculiar optimal scale factor obtained by adopting Pepper and Nepal Telecom Logo of same size 512 x 512 x 3 based on different attack scenarios:

1. **Case I:** The scenario where the watermarked image is under Gaussian attack
2. **Case II:** The scenario where the watermarked image is under salt and pepper attack
3. **Case III:** The scenario where the watermarked image is under speckle attack

4. **Case IV:** The scenario where the watermarked image is rotated at 45° attack
5. **Case V:** The scenario where the watermarked image is rotated at 5° attack
6. **Case VI:** The scenario where the watermarked image is rotated at 90° attack
7. **Case VII:** The scenario where the watermarked image is under crop attack

4.8.1 Robustness and Imperceptibility Results for Case I

The original cover and watermark images that are used for embedding and extraction processes are as shown in Figure 4.46. The size of the two images adopted is 512 x 512 x 3. The original cover image is used to host the private information (watermark image) that forms the watermarked image. Henceforth, for the purpose of comparison from case I to case VII Figure 4.46 is referenced while comparing watermarked image and extracted watermark image with original cover and watermark images.



(a) Original Cover Image (b) Original Watermark Image

Figure 4.46: Original Cover and Watermark Images

Figure 4.47 depicts the evaluation between watermarked image subjected Gaussian attack and original cover image as given in Figure 4.46(a). It can be observed that the three images depict visual similarity between them which signifies high degree of imperceptibility, that is, the level at which the secret information is hidden without notice with a PSNR value of 48.2791dB.



(a) Watermarked Image



(b) Watermarked Image under Gaussian Attack

Figure 4.47: Comparison of Original Cover Image, Watermarked and Watermarked Image under Gaussian Attack

Figure 4.48 depicts extracted watermark image when the watermarked image is subjected to Gaussian attack, by comparing the visual similarity between extracted watermark and original watermark images as referenced in Figure 4.46(b). The degree of visual similarity between the images shows the level of robustness of the algorithm under this attack with an NCC value of 0.9790 and SSIM value of 0.9043. This shows that the original watermark and extracted watermark images are almost similar since the NCC value obtained is close to 1.



Extracted Watermark Image

Figure 4.48: Comparison of Original watermark and Extracted Watermark images under Gaussian Attack

4.8.2 Robustness and Imperceptibility Results for Case II

Figure 4.49 depicts the comparison between watermarked image, watermarked image under salt and pepper attack and original cover image as shown in Figure 4.46(a). It can be observed that the three images denote visual similarity between them which signifies high degree of

imperceptibility, that is, the level at which the secret information is hidden without notice with a PSNR value of 46.3012dB.



(a) Watermarked Image (b) Watermarked Image under Salt and Pepper Attack

Figure 4.49: Comparison of Original Cover Image, Watermarked and Watermarked Image under Salt and Pepper Attack

Figure 4.50 depicts extracted watermark image when the watermarked image is subjected to salt and pepper attack, by comparing the visual similarity between extracted watermark and original watermark images as shown in Figure 4.46(b). The degree of visual similarity between the images shows the level of robustness of the algorithm under this attack with an NCC value of 0.9600 and SSIM value of 0.9230. This shows that the original watermark and extracted watermark images are almost similar since the NCC value obtained is close to 1.



Extracted Watermark Image

Figure 4.50: Comparison of Original watermark and Extracted Watermark images under Salt and Pepper Attack

4.8.3 Robustness and Imperceptibility Results for Case III

Figure 4.51 shows the comparison between watermarked image, watermarked image under speckle attack and original cover image as shown in Figure 4.46(a). It can be observed that the three images denote visual similarity between them which signifies high degree of imperceptibility, that is, the level at which the secret information is concealed without notice with a PSNR value of 43.3887dB.



(a) Watermarked Image (b) Extracted Watermarked Image

Figure 4.51: Comparison of Original Cover Image, Watermarked and Watermarked Image under Speckle Attack

Figure 4.52 depicts extracted watermark image when the watermarked image is under speckle attack, by comparing the visual similarity between extracted watermark and original watermark images as shown in Figure 4.46(b). The degree of visual similarity between the images shows the level of robustness of the algorithm under this attack with an NCC value of 0.9596 and SSIM value of 0.8204. This shows that the original watermark and extracted watermark images are almost similar since the NCC value obtained is close to 1.



Extracted Watermark Image

Figure 4.52: Comparison of Original watermark and Extracted Watermark images under Speckle Attack

4.8.4 Robustness and Imperceptibility Results for Case IV

Figure 4.53 shows the comparison between watermarked image, when the watermarked image is rotated at 45° and original cover image as given in Figure 4.46(a). It can be observed that the three images denote visual similarity between them apart from the rotation of the watermarked image at 45°. This signifies high degree of imperceptibility, that is, the level at which the secret information is concealed without notice with a PSNR value of 42.5491dB.



(a) Watermarked Image (b) Watermarked Image Rotated at 45°

Figure 4.53: Comparison of Original Cover Image, Watermarked and Watermarked Image Rotated at 45°

Figure 4.54 depicts extracted watermark image when the watermarked image is rotated at 45°, by comparing the visual similarity between extracted watermark and original watermark images as shown in Figure 4.46(b). The degree of visual similarity between the images shows the level of robustness or resilience of the algorithm under this geometric attack with an NCC value of 0.9084 and SSIM value of 0.5116. This shows that the original watermark and extracted watermark images are almost similar since the NCC value obtained is close to 1.



Extracted Watermark Image

Figure 4.54: Comparison of Original watermark and Extracted

6.8.5 Robustness and Imperceptibility Results for Case V

Figure 4.55 shows the scenario where the watermarked image is rotated at 5° in comparison with original cover image with reference to Figure 4.46(a) . It can be observed that the three images depict visual similarity between them apart from the rotation of the watermarked image at 5°. This signifies high degree of imperceptibility, that is, the level at which the secret information is hidden without notice with a PSNR value of 42.8439dB.



(a) Watermarked Image (b) Watermarked Image Rotated at 5°

Figure 4.55: Comparison of Original Cover Image, Watermarked and Watermarked Image Rotated at 5°

The visual similarity between the original watermark image as shown in Figure 4.46(b) and extracted watermark image when rotated at 5° is given in Figure 4.56. The degree of visual similarity between the images shows the level of resilience of the algorithm under this geometric attack with an NCC value of 0.9300 and SSIM value of 0.4901. This shows that the original watermark and extracted watermark images are almost similar since the NCC value obtained is close to 1.



Extracted Watermark Image

Figure 4.56: Comparison of Original watermark and Extracted Watermark images Rotated at 5°

4.8.6 Robustness and Imperceptibility Results for Case VI

Figure 4.57 depicts the comparison in a scenario where the watermarked image and in which the watermarked image is rotated at 90° and original cover image with reference to Figure 4.46(a). It can be observed that the three images depict visual similarity between them apart from the rotation of the watermarked image at 90°. This signifies high degree of imperceptibility, that is, the level at which the secret information is concealed without notice with a PSNR value of 43.2148dB.



(a) Watermarked Image



(b) Extracted Watermarked Image

Figure 4.57: Comparison of Original Cover Image, Watermarked and Watermarked Image Rotated at 90°

The visual similarity between the original watermark image as shown in Figure 4.46(b) and extracted watermark image when rotated at 90° is given in Figure 4.58. The degree of visual similarity between the images shows the level of resilience of the algorithm under this attack with an NCC value of 0.9184 and SSIM value of 0.7126. This shows that the original

watermark and extracted watermark images are almost similar since the NCC value obtained is close to 1.



Extracted Watermark Image

Figure 4.58: Comparison of Original watermark and Extracted Watermark images Rotated at 90°

4.8.7 Robustness and Imperceptibility Results for Case VII

Figure 4.59 depicts the comparison in a scenario where the watermarked image and in which the watermarked image is subjected to crop attack and original cover image with reference to Figure 4.46(a). It can be observed that the three images denote visual similarity between them which signifies high degree of imperceptibility, that is, the level at which the secret information is concealed without notice with a PSNR value of 43.0859dB.



(a) Watermarked Image



(b) Watermarked Image under Crop Attack

Figure 4.59: Comparison of Original Cover Image, Watermarked and Watermarked Image under Crop Attack

The visual similarity between the original watermark image as shown in Figure 4.46(b) and extracted watermark image under crop attack is given in Figure 4.60. The degree of visual similarity between the images shows the level of resilience of the algorithm under this attack

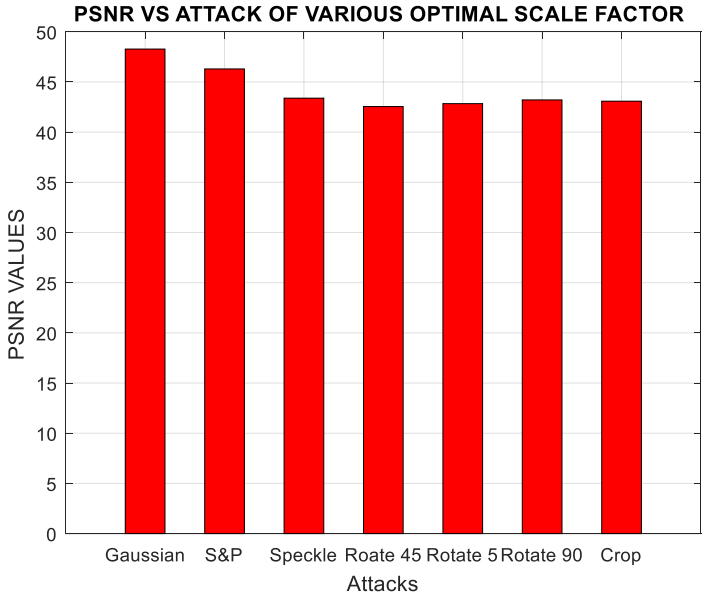
with an NCC value of 0.9643 and SSIM value of 0.4183. This shows that the original watermark and extracted watermark images are almost similar since the NCC value obtained is close to 1.



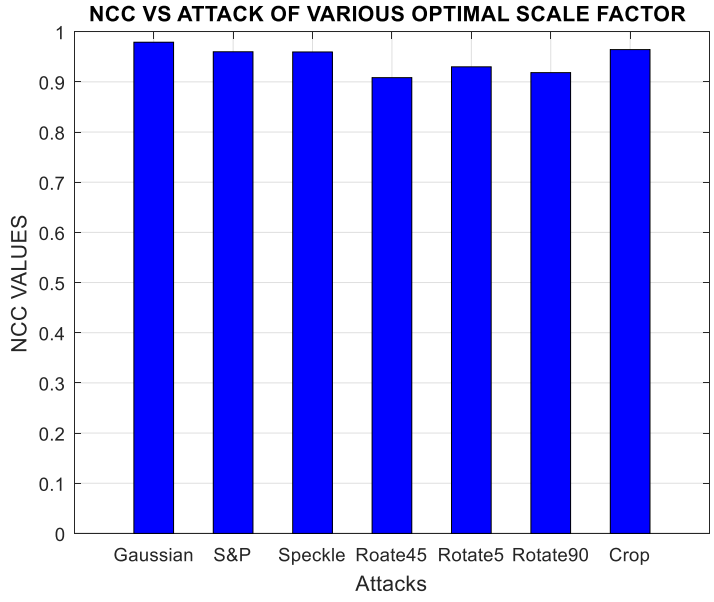
Extracted Watermark Image

Figure 4.60: Comparison of Original watermark and Extracted Watermark image under Crop Attack

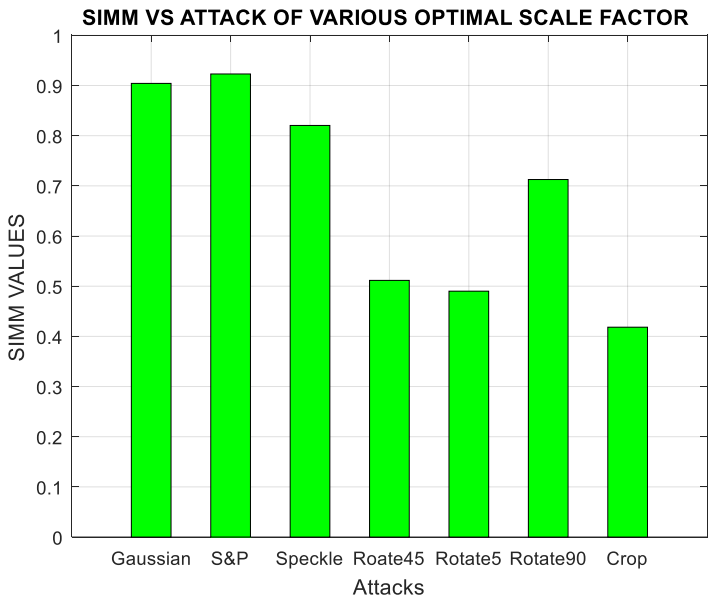
R. Figure 4.61 shows the summary of results obtained of the performance metrics for evaluating the robustness and imperceptibility of the developed digital watermarking technique, whilst using a selected optimal scaling factor from various attack scenarios.



(a) PSNR Values for Watermark Image



(b) NCC Values for Watermark



(c) SSIM Values for Watermark

Figure 4.61: Comparison of the Results of PSNR, NCC and SSIM Obtained using the Optimal Scale Factor under various Attacks

4.9 Definition of Different Scenarios

The following are the different scenarios considered in evaluating the robustness and imperceptibility of the developed digital watermarking technique, based on 64-bit key obtained from the implementation of QKD whilst using the peculiar optimal scale factor obtained with reference to subsection 4.6 by adopting Pepper of size 512 x 512 x 3 as cover image and Nepal Telecom Logo of size 512 x 512 x 3 as watermark image based on different attack scenarios:

1. **Case I:** The scenario where the watermarked image is under Gaussian attack
2. **Case II:** The scenario where the watermarked image is under salt and pepper attack
3. **Case III:** The scenario where the watermarked image is under speckle attack
4. **Case IV:** The scenario where the watermarked image is rotated at 45° attack
5. **Case V:** The scenario where the watermarked image is rotated at 5° attack

6. **Case VI:** The scenario where the watermarked image is rotated at 90° attack
7. **Case VII:** The scenario where the watermarked image is under crop attack

4.9.1 Robustness and Imperceptibility Results for Case I

The 64-bit key obtained from QKD is used to encrypt the watermark image before the embedding process. The encrypted watermark image with 64-bit key is as shown in Figure 4.62.

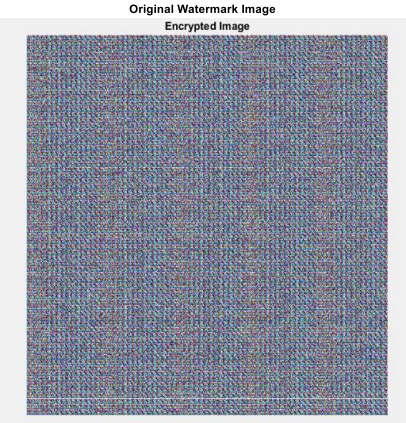


Figure 4.62: Encrypted Watermark Image

The original cover image as given in Figure 4.46(a), watermarked image and watermarked image that contains the encrypted watermark image under Gaussian attack are as shown in Figure 4.63. The level of similarity between the three images highlights the level of imperceptibility of the technique with a PSNR value of 50.2752dB.



(a) Watermarked Image (b) Watermarked Image under Gaussian Attack

Figure 4.63: Comparison of Original Cover Image, Watermarked and Watermarked Image under Gaussian Attack

The recovered encrypted watermark image after the watermarked image is subjected to Gaussian attack is as shown in Figure 4.64.

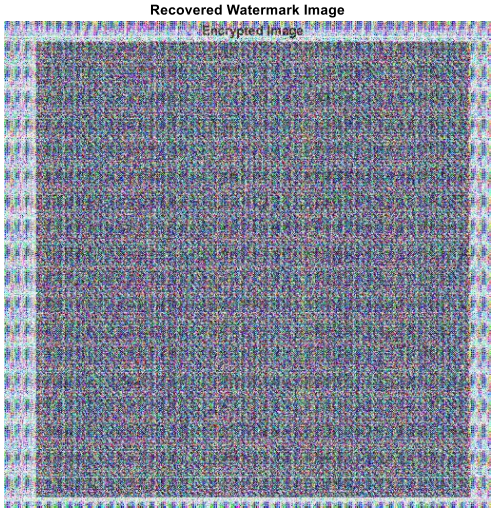


Figure 4.64: Recovered Encrypted Watermark Image under Gaussian Attack

The high level of visual match between the original and extracted decrypted watermark images under Gaussian attack as shown in Figure 4.65 shows the robustness of the developed technique against such attack with an NCC value of 1 and SSIM value of 1. Since the values of NCC obtained is 1 it depicts total similarity between the original watermark image and extracted decrypted watermark image.



(a) Original Watermark Image (b) Extracted Decrypted Watermark Image

Figure 4.65: Comparison of Original Watermark Image and Extracted Decrypted Watermark Image under Gaussian Attack

4.9.2 Robustness and Imperceptibility Results for Case II

The 64-bit key obtained from the implementation of QKD is used to encrypt the watermark image before the embedding process. The encrypted watermark image with 64-bit key is referenced in Figure 4.62.

The original cover image as given in Figure 4.46(a), watermarked image and watermarked image that contains the encrypted watermark image under salt and pepper attack are as shown in Figure 4.66. The level of similarity between the three images highlights the level of imperceptibility of the technique with a PSNR value of 47.7293dB.



(a) Watermarked Image



(b) Watermarked Image under Salt and Pepper Attack

Figure 4.66: Comparison of Original Cover Image, Watermarked and Watermarked Image under Salt and Pepper Attack

The recovered encrypted watermark image after the watermarked image is subjected to salt and pepper attack is as shown in Figure 4.67.

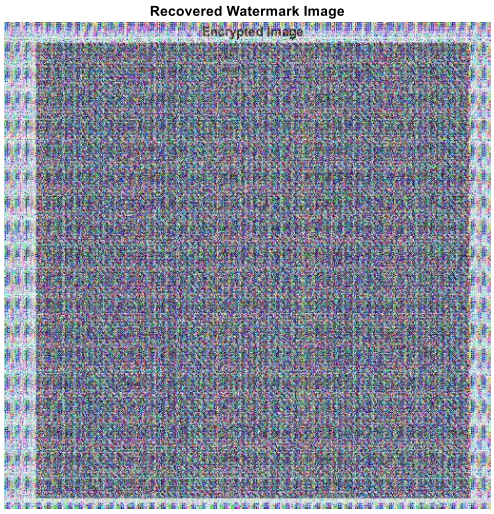


Figure 4.67: Recovered Extracted watermark image under Salt and Pepper Attack

The high level of visual similarity between the original and extracted decrypted watermark images under salt and pepper attack as shown in Figure 4.68 shows the robustness of the developed technique against such attack with an NCC value of 1 and SSIM value of 1. Since the value of NCC obtained is 1 it depicts total similarity between the original watermark image and extracted decrypted watermark image.



(a) Original Watermark Image (b) Extracted Decrypted Watermark Image

Figure 4.68: Comparison of Original Watermark Image and Extracted Decrypted Watermark Image under Salt and Pepper Attack

4.9.3 Robustness and Imperceptibility Results for Case III

The 64-bit key obtained from QKD is used to encrypt the watermark image before the embedding process. The encrypted watermark image with 64-bit key is referenced in Figure 4.62. The original cover image as given in Figure 4.46(a), watermarked image and

watermarked image that contains the encrypted watermark image under speckle attack are as shown in Figure 4.69. The level of similarity between the three images highlights the level of imperceptibility of the technique with a PSNR value of 45.6404dB.



(a) Watermarked Image



(b) Watermarked Image under Speckle Attack

Figure 4.69: Comparison of Original Cover Image, Watermarked and Watermarked Image under Speckle Attack

The recovered encrypted watermark image after the watermarked image is subjected to speckle attack is as shown in Figure 4.70.

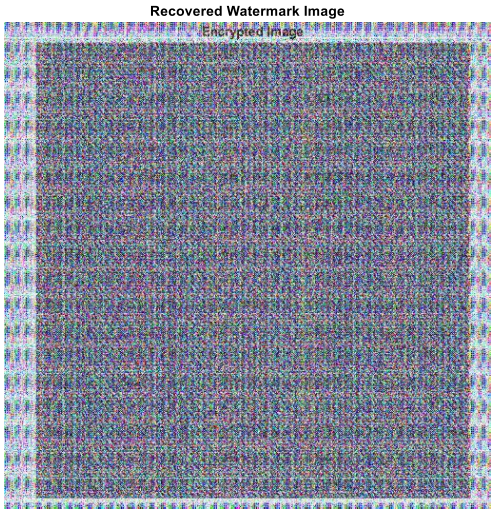


Figure 4.70: Recovered Extracted Watermark Image under Speckle Attack

The visual similarity between the original and extracted decrypted watermark images under speckle attack is shown in Figure 4.71 shows the resilience of the developed technique against such attack with an NCC value of 1 and SSIM value of 1. Since the value of NCC obtained is

1 it depicts complete relationship between the original watermark image and extracted decrypted watermark image.



(a) Original Watermark Image



(b) Extracted Decrypted Watermark Image

Figure 4.71: Comparison of Original Watermark Image and Extracted Decrypted Watermark Image under Speckle Attack

4.9.4 Robustness and Imperceptibility Results for Case IV

The 64-bit key obtained from the implementation of QKD scheme is used to encrypt the watermark image before the embedding procedure. The encrypted watermark image with 64-bit key is referenced in Figure 4.62. The original cover image with referenced to Figure 4.46(a), watermarked image and watermarked image that contains the encrypted watermark image when rotated at 45° are as shown in Figure 4.72. The level of similarity between the three images highlights the level of imperceptibility of the technique even after the watermark is rotated at 45° with a PSNR value of 46.8626dB.



(a) Watermarked Image



(b) Watermarked Image Rotated at 45°

Figure 4.72: Comparison of Original Cover Image, Watermarked and Watermarked Image Rotated at 45°

The recovered encrypted watermark image after the watermarked image is rotated at 45° is as shown in Figure 4.73.

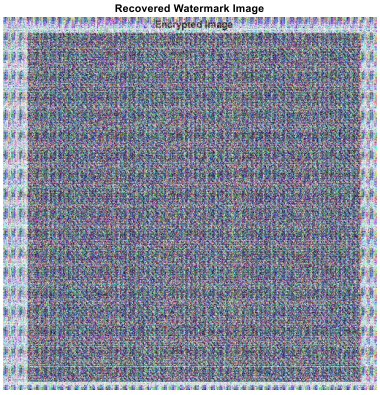


Figure 4.73: Recovered Extracted Watermark Image under 45° Rotation

The visual similarity between the original and extracted decrypted watermark images under 45° rotation as shown in Figure 4.74 depicts the resilience of the developed technique against such attack with an NCC value of 0.9997 and SSIM value of 0.9998. Since the value of NCC obtained is close to 1 it depicts almost similarity between the original watermark image and extracted decrypted watermark image.



(a) Original Watermark Image (b) Extracted Decrypted Watermark Image

Figure 4.74: Comparison of Original Watermark Image and Extracted Decrypted Watermark Image under 45° Rotation

4.9.5 Robustness and Imperceptibility Results for Case V

The 64-bit key obtained from the implementation of QKD is used to encrypt the watermark image before the embedding process. The encrypted watermark image with 64-bit key is referenced in Figure 4.62. The original cover image with reference to Figure 4.46(a), watermarked image and watermarked image that contains the encrypted watermark image when rotated at 5° are as shown in Figure 4.75. The level of similarity between the three images highlights the level of how the watermark image has been concealed in the cover image with a PSNR value of 44.6045dB.



(a) Watermarked Image (b) Watermarked Image Rotated at 5°

Figure 4.75: Comparison of Original Cover Image, Watermarked, and Watermarked Image Rotated at 5°

The recovered encrypted watermark image after the watermarked image is rotated at 5° is as shown in Figure 4.76.

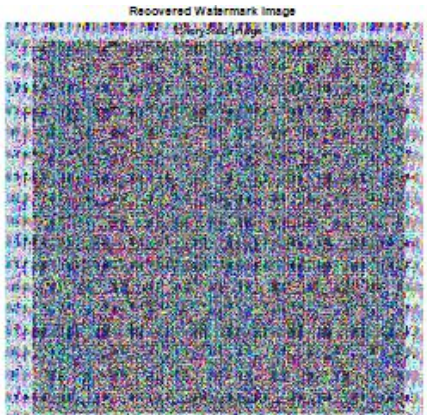
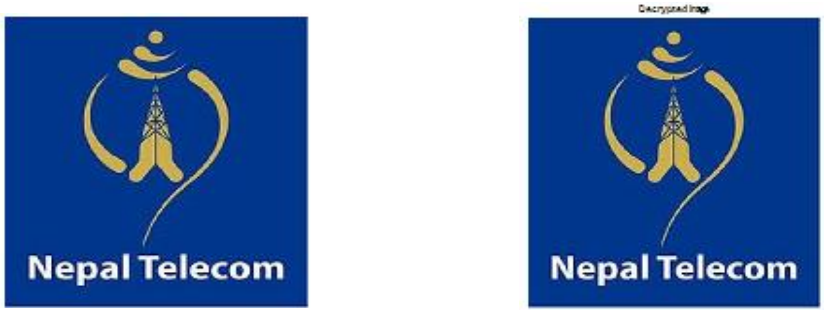


Figure 4.76: Recovered Extracted Encrypted Watermark Image under 5° Rotation

The visual similarity between the original and extracted decrypted watermark images under 5° rotation is shown in Figure 4.77, this illustrates the resilience of the developed technique against such attack with an NCC value of 1 and SSIM value of 0.9996. Since the value of NCC is 1 it depicts total similarity between the original watermark image and extracted decrypted watermark image.



(a) Original Watermark Image (b) Extracted Decrypted Watermark Image

Figure 4.77: Comparison of Original Watermark Image and Extracted Decrypted Watermark Image under 5° Rotation

4.9.6 Robustness and Imperceptibility Results for Case VI

The 64-bit key obtained from QKD is used to encrypt the watermark image before the embedding process. The encrypted watermark image with 64-bit key is referenced in Figure 4.62. The original cover image with reference to Figure 4.46(a), watermarked image and watermarked image that contains the encrypted watermark image when rotated at 90° are as shown in Figure 4.78. The level of similarity between the three images highlights the level of how the watermark image has been concealed in the cover image with a PSNR value of 47.9442dB.



(a) Watermarked Image



(b) Watermarked Image Rotated at 90°

Figure 4.78: Comparison of Original Cover Image, Watermarked and Watermarked Image Rotated at 90°

The visual similarity between the original and extracted decrypted watermark images under 90° rotation is shown in Figure 4.79, this shows the resilience of the developed technique against such attack with an NCC value of 1 and SSIM value of 0.9999. Since the value of NCC is 1 it depicts total similarity between the original watermark image and extracted decrypted watermark image.



(a) Original Watermark Image



(b) Extracted Decrypted Watermark Image at 90°

Figure 4.79: Comparison of Original Watermark Image and Extracted Decrypted Watermark Image under 90° Rotation

4.9.6 Robustness and Imperceptibility Results for Case VII

The 64-bit key obtained from QKD is used to encrypt the watermark image before the embedding process. The encrypted watermark image with 64-bit key is referenced in Figure 4.62. The original cover image with reference to Figure 4.46(a), watermarked image and watermarked image that contains the encrypted watermark image is subjected to crop attack are as shown in Figure 4.80. The level of similarity between the three images highlights the

level of how the watermark image has been concealed in the cover image with a PSNR value of 46.4067dB.



(a) Watermarked Image (b) Watermarked Image under Crop Attack

Figure 4.80: Comparison of Original Cover Image, Watermarked and Watermarked Image under Crop Attack

The visual similarity between the original and extracted decrypted watermark images under crop attack is shown in Figure 4.81, this shows the resilience of the developed technique against such attack with an NCC value of 1 and SSIM value of 0.9987. Since the value of NCC is 1 it depicts total similarity between the original watermark image and extracted decrypted watermark image.

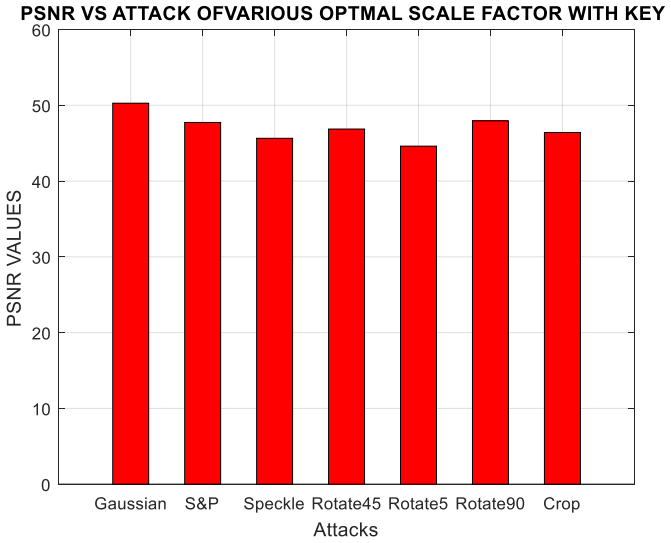


(a) Original Watermark Image (b) Extracted Decrypted Watermark Image

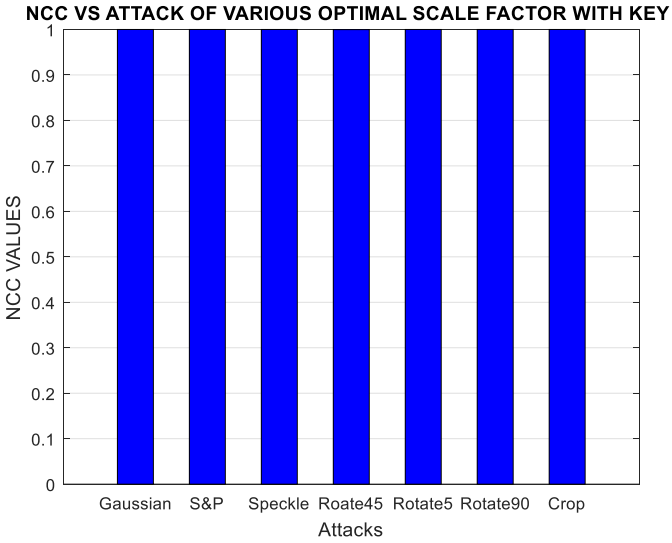
Figure 4.81: Comparison of Original Watermark Image and Extracted Decrypted Watermark Image under Crop Attack

The summary of results of the various scenarios is depicted in table 4.6 as shown in appendix R. Figure 4.82 shows the summary of results obtained of the performance metrics for evaluating the robustness and imperceptibility of the developed digital watermarking technique, whilst using a selected scale factor from various scenarios. The height of individual

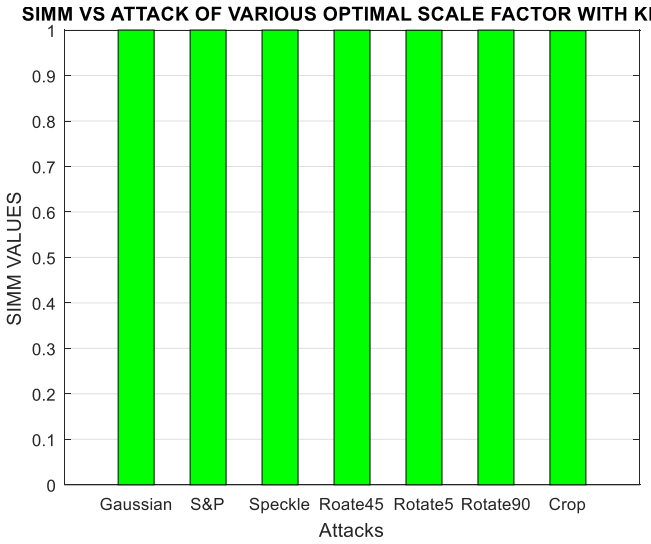
bar in PSNR values for each attack denotes the degree of imperceptibility which implies the level in which the watermark is concealed from an attacker. SSIM exhibits same characteristics. The height of individual bar in NCC illustrates the level of robustness of the algorithm to specific attack.



(a) PSNR Values for Watermark Image



(b) NCC Values for Watermark



(c) SSIM Values for Watermark

Figure 4.82: Comparison of the Results of PSNR, NCC and SSIM Obtained using the Optimal Scale Factor and Key under various Attacks

The recorded PSNR values of various scenarios display a vivid demonstration of the level of how the secret information has been concealed in the host image without causing any scintilla distortion to the host image. It also ensures that the host image goes unnoticed without revealing that it contains vital information. This performance metric evaluates the visual similarity between the original cover image and watermarked image. The obtained and recorded values of NCC which are close to 1 and values which are 1 implies how the developed technique is resilient to different attacks without exposing the secret information, or deformation of the secret information within the host image. This metric evaluates the visual similarity between the original watermark image and extracted watermark image.

4.10 Performance Evaluation of the Developed Algorithm

This subsection describes the performance of the developed algorithm evaluated by comparing the results obtained based on the different scenarios with the published work of Bajracharya & Koju (2017). Figure 4.3 to 4.82 presented are based on the developed algorithm that represents the degree of attacks of different scenarios to which the secret information are hidden within the cover image without visible to the human vision which is evaluated by PSNR. Secondly the degree to which the algorithm can resist any form of malicious attack without the attacker gaining access to the information, this is evaluated by NCC with a view to comparing between the original watermark image and extracted watermark image. In order to carryout comparison, the performance measures obtained for developed algorithm were compared with performance measures of Bajracharya & Koju (2017). The same cover image and watermark image were adopted in the developed algorithm. Table 4.7 depicts the summary of the results obtained for various attacks as shown in appendix R using the data published by Bajracharya & Koju (2017).

Table 4.7: Summary of Results based on the data Published in the Work of Bajracharya & Koju (2017) using the Developed Algorithm

sn	Cover Image	Watermark Image	Attacks	Alpha (α)	PSNR (dB)	NCC	SSIM
1	Pepper	Nepal Logo	No	0.1324	76.8139	1	1
2	Pepper	Nepal Logo	Gaussian	0.2283	71.8747	1	1
3	Pepper	Nepal Logo	Salt and Pepper	1	66.2485	1	1
4	Pepper	Nepal Logo	Rotate 45 degree	0.2478	61.0996	0.9997	0.9998
5	Pepper	Nepal Logo	Rotate 5 degree	0.1408	61.2046	1	0.9996
6	Pepper	Nepal Logo	Rotate 90 degree	1	63.4722	1	0.9999
7	Pepper	Nepal Logo	Crop	1	62.2485	1	0.9987

4.11 Comparison of Results

The performance of the developed algorithm is evaluated by comparing the results obtained of various defined scenarios based on generalized optimal scaling factor, generalized optimal scaling factor and estimated key, manually selected scaling factor, optimal scaling factor based on individual attack and optimal scaling factor based on individual attack and key obtained from the implementation of QKD protocol.

4.11.1 Comparison of PSNR, NCC and SSIM Results of Various Defined Scenarios under No Attack

The results obtained were evaluated using PSNR, NCC and SSIM as performance metrics. Figure 4.83 shows the PSNR results obtained based on the scaling factor on each bar as shown in Figure 4.83 from different defined scenarios under no attack. The height of each bar depicts the level of the perceptual quality of the watermarked image. It can be observed from Figure

4.83 that the bar based on manually selected scaling factor is the highest follows by the bar based on optimal scaling factor according to individual attack alongside the key obtained from the implementation of QKD protocol. This implies that the bar based on manually selected scaling factor exhibits the highest level of imperceptibility. However, it demonstrated that the algorithm tradeoff robustness for imperceptibility. The bar based on optimal scale factor according to individual attack alongside key obtained from the implementation of QKD protocol achieved an optimal balance between imperceptibility and robustness as shown in Figures 4.83 and 4.84. This demonstrated that the primary aim of this thesis has been achieved.

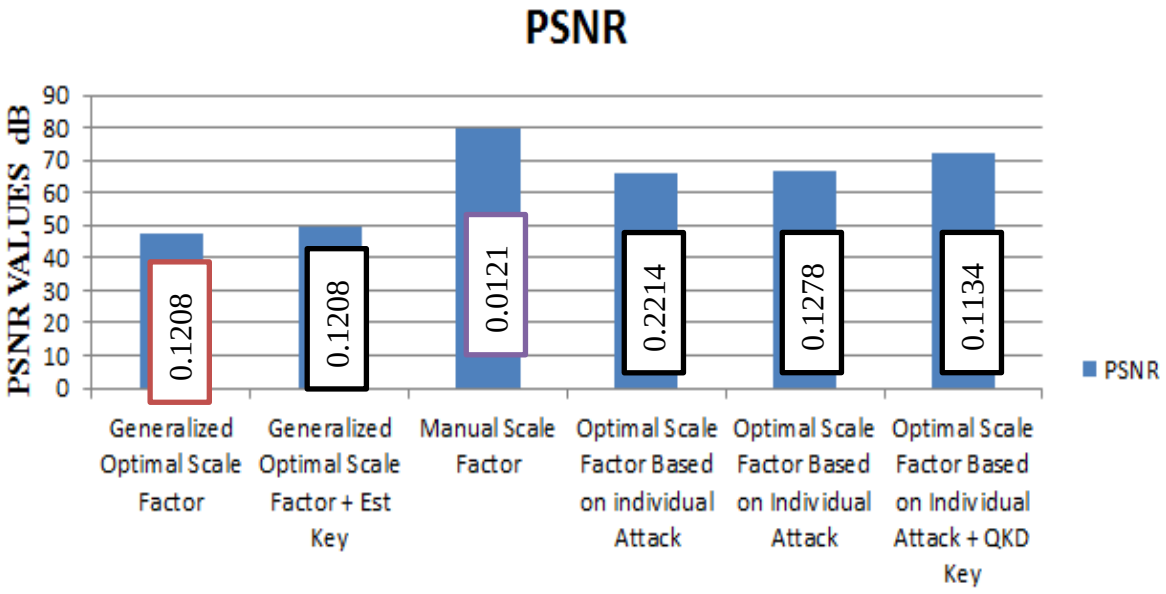


Figure 4.83: Comparison of Results of PSNR obtained Based on Various Defined Scenarios under No Attack

Figure 4.84 shows the NCC results obtained based on the scaling factor on each bar as shown in Figure 4.83 from different defined scenarios under no attack. The values of NCC obtained were based on the respective scaling factors in Figure 4.83. The height of each bar depicts the degree at which the algorithm is robust or contains little or no noise. It can be observed from Figure 4.84 that the bar based on optimal scaling factor according to individual attack

alongside the key obtained from the implementation of QKD protocol contains no noise. The other respective bars from manually to generalized scaling factor still contain some high level of noise under no attack.

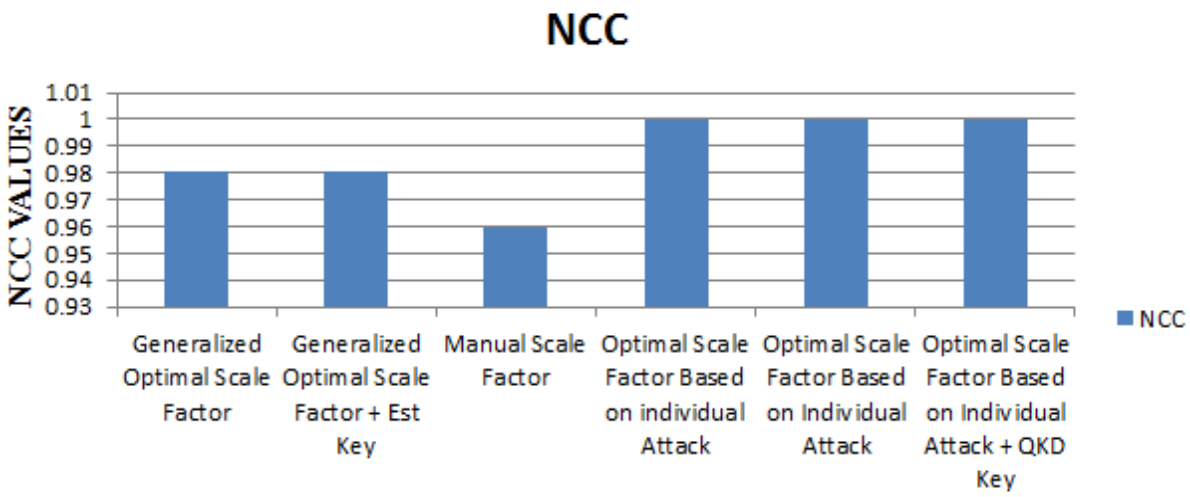


Figure 4.84: Comparison of Results of NCC obtained Based on Various Defined Scenarios under No Attack

Figure 4.85 shows the SSIM results obtained using the scaling factor on each bar as shown in the Figure from different defined scenarios under no attack. The values of SSIM obtained were based on the respective scaling factors in Figure 4.83. The SSIM exhibits the same characteristics as NCC, although the SSIM denotes the visual similarity between the original cover image and watermarked image. It can be observed from Figure 4.85 apart of the bar from manually selected scaling factor, the other respective bar depicts same visual similarity between the original cover image and watermarked image under no attack.

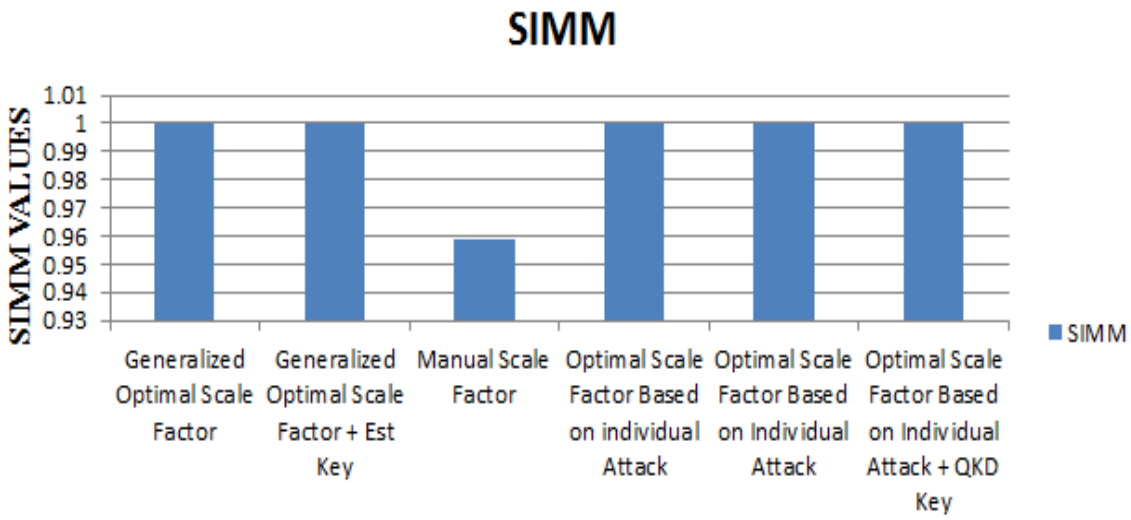


Figure 4.85: Comparison of Results of SSIM obtained Based on Various Defined Scenarios under No Attack

4.11.2 Comparison of PSNR, NCC and SSIM Results of Various Defined Scenarios under Gaussian Attack

The results obtained were evaluated using PSNR, NCC and SSIM as performance metrics. Figure 4.86 depicts the PSNR results obtained based on the scaling factor on each bar as shown in Figure 4.86 from different defined scenarios under Gaussian attack. The height of each bar depicts the level of the perceptual quality of the watermarked image. It can be observed from Figure 4.86 that the bar based on manually selected scaling factor is the highest follows by the bar based on optimal scaling factor according to individual attack alongside the key obtained from the implementation of QKD protocol. The bar based on manually selected scaling factor exhibits the highest level of imperceptibility. However, it demonstrated that the algorithm trades off robustness for imperceptibility. The bar based on optimal scaling factor according to individual attack alongside key obtained from the implementation of QKD protocol achieved an optimal balance between imperceptibility and robustness as shown in Figures 4.86 and 4.87. This has attested that the developed algorithm achieved an optimal balance between imperceptibility and robustness.

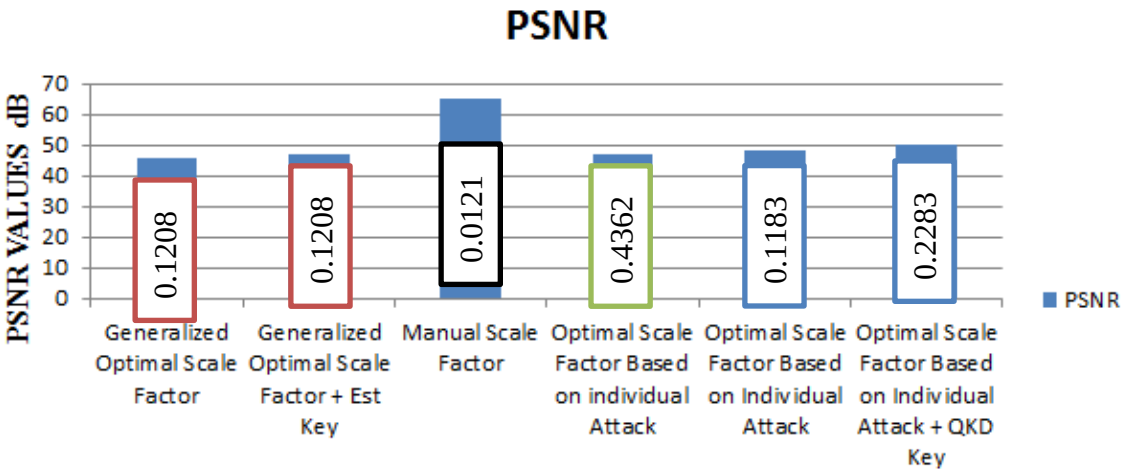


Figure 4.86: Comparison of Results of PSNR obtained Based on Various Defined Scenarios under Gaussian Attack

Figure 4.87 illustrates the NCC results obtained based on the scaling factor on each bar as shown in Figure 4.86 from different defined scenarios under Gaussian attack. The values of NCC obtained were based on the respective scaling factors in Figure 4.86. The height of each bar depicts the degree at which the algorithm is robust or contains little or no noise. It can be observed from Figure 4.86 that the bar based on optimal scaling factor according to individual attack alongside the key obtained from the implementation of QKD protocol contains no noise. The other respective bars from manually to generalized scaling factor still contain some level of noise under Gaussian attack.

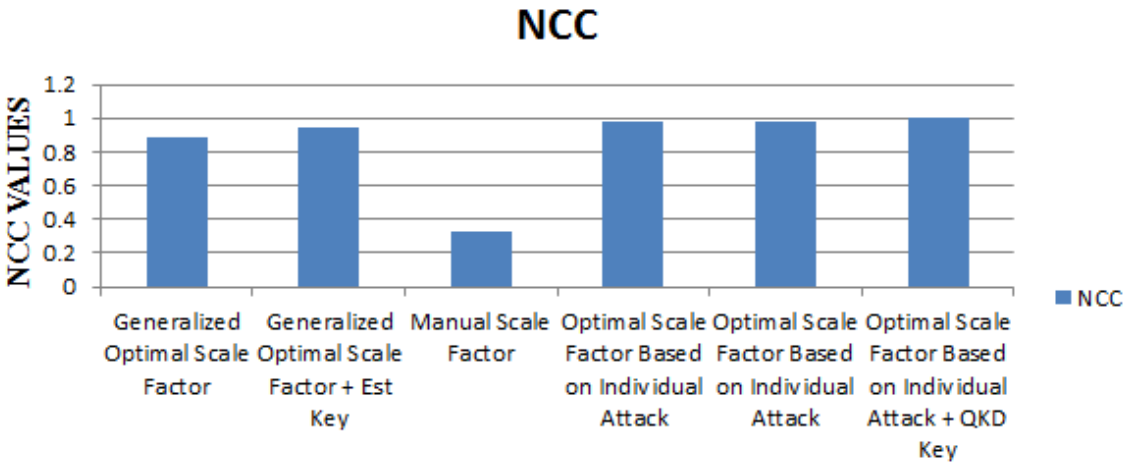


Figure 4.87: Comparison of Results of NCC obtained Based on Various Defined Scenarios under Gaussian Attack

Figure 4.88 shows the SSIM results obtained based on the scaling factor on each bar as shown in the Figure from different defined scenarios under Gaussian attack. The values of SSIM obtained were based on the respective scaling factors in Figure 4.86. The SSIM exhibits the same characteristics as NCC, although the SSIM denotes the perceptual quality similarity between the original cover image and watermarked image. It can be observed from Figure 4.88 apart of the bar from manually selected scaling factor, the other respective bar depicts same visual similarity between the original cover image and watermarked image under Gaussian attack.

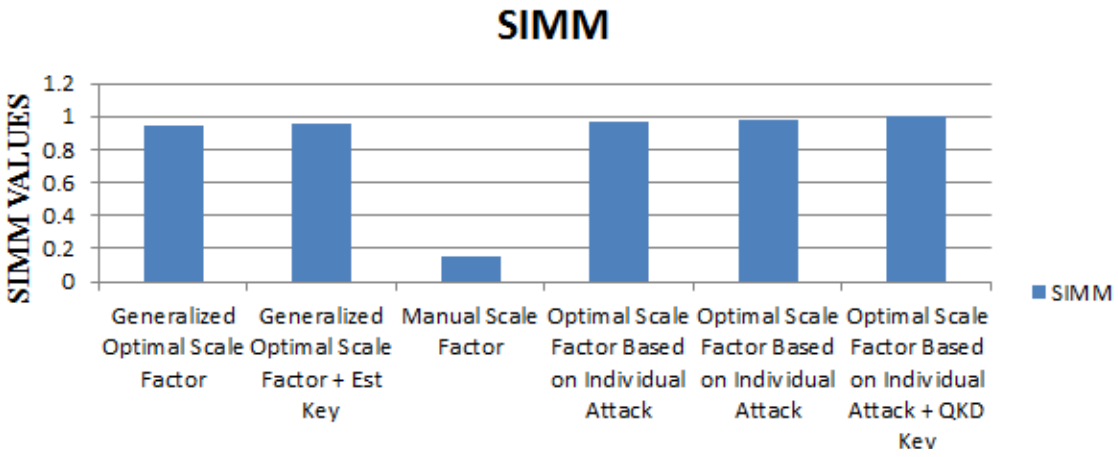


Figure 4.88: Comparison of Results of SSIM obtained Based on Various Defined Scenarios under Gaussian Attack

4.11.3 Comparison of PSNR, NCC and SSIM Results of Various Defined Scenarios under Salt and Pepper Attack

The results obtained were evaluated using PSNR, NCC and SSIM as performance metrics. Figure 4.89 depicts the PSNR results obtained based on the scaling factor on each bar as shown in the Figure from different defined scenarios under salt and pepper attack. The height of each bar depicts the level of the perceptual quality of the watermarked image. It can be

observed from Figure 4.89 that the bar based on manually selected scaling factor is the highest followed by the bar based on optimal scaling factor according to individual attack alongside the key obtained from the implementation of QKD protocol. The bar based on manually selected scaling factor exhibits the highest level of imperceptibility. However, it demonstrated that the algorithm trades off robustness for imperceptibility. The bar based on optimal scale factor according to individual attack alongside key obtained from the implementation of QKD protocol achieved an optimal balance between imperceptibility and robustness as shown in Figures 4.89 and 4.90. This has attested that the developed algorithm achieved an optimal balance between imperceptibility and robustness.

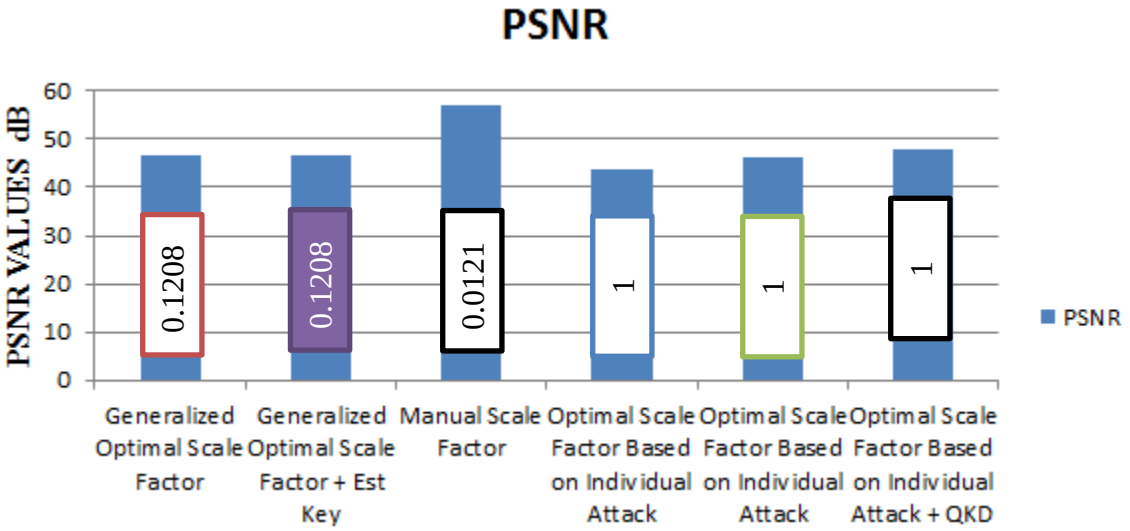


Figure 4.89: Comparison of Results of PSNR obtained Based on Various Defined Scenarios Under Salt and Pepper Attack

Figure 4.90 gives the NCC results obtained based on the scaling factor on each bar as shown in Figure 4.89 from different defined scenarios under salt and pepper attack. The values of NCC obtained were based on the respective scaling factors in Figure 4.89. The height of each bar depicts the degree at which the algorithm is robust or contains little or no noise. It can be observed from Figure 4.90 that the bar based on optimal scaling factor according to individual attack alongside the key obtained from the implementation of QKD protocol contains no

noise. The other respective bars from manually to generalized scaling factor still contain some level of noise under salt and pepper attack.

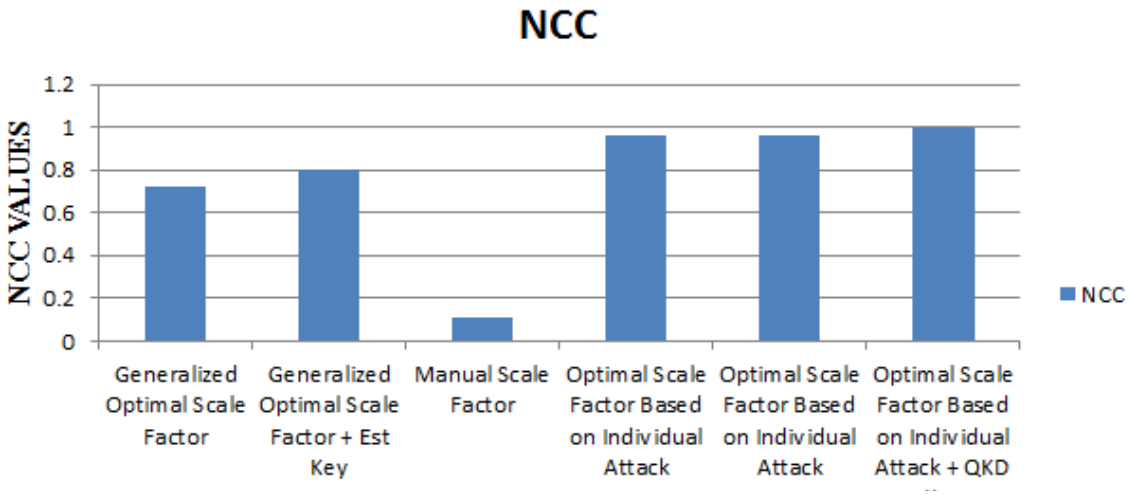


Figure 4.90: Comparison of Results of NCC obtained Based on Various Defined Scenarios under Salt and Pepper Attack

Figure 4.91 denotes the SSIM results obtained based on the scaling factor on each bar as shown in the Figure from different defined scenarios under salt and pepper attack. The values of SSIM obtained were based on the respective scaling factors in Figure 4.89. The SSIM exhibits the same characteristics as NCC, although the SSIM denotes the perceptual quality similarity between the original cover image and watermarked image. It can be observed from Figure 4.91 apart of the bar from manually selected scaling factor, the other respective bar depicts high level of visual similarity between the original cover image and watermarked image under salt and pepper attack.

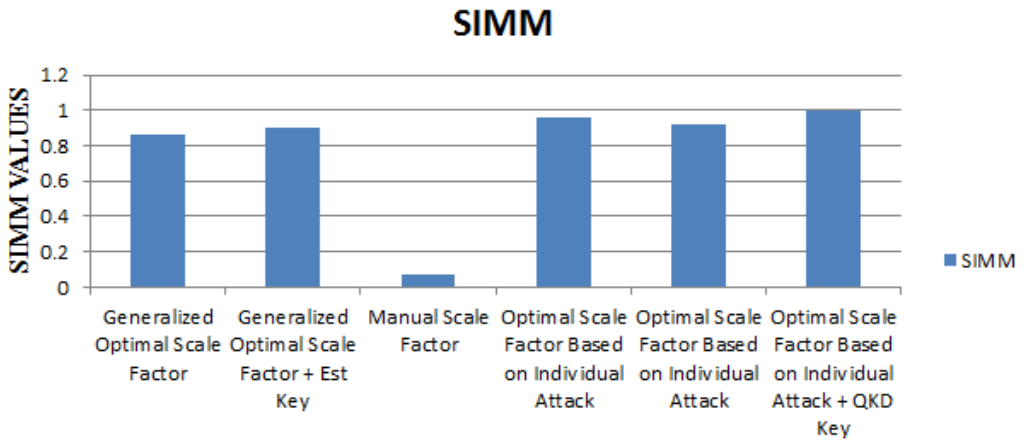


Figure 4.91: Comparison of Results of SSIM obtained Based on Various Defined Scenarios Under Salt and Pepper Attack

4.11.4 Comparison of PSNR, NCC and SSIM Results of Various Defined Scenarios under Speckle Attack

The results obtained were evaluated using PSNR, NCC and SSIM as performance metrics. Figure 4.92 depicts the PSNR results obtained based on the scaling factor on each bar as shown in the Figure from different defined scenarios under speckle attack. The height of each bar depicts the level of the perceptual quality of the watermarked image. It can be observed from Figure 4.92 that the bar based on manually selected scaling factor is the highest followed by the bar based on optimal scaling factor according to individual attack alongside the key obtained from the implementation of QKD protocol. The bar based on manually selected scaling factor exhibits the highest level of imperceptibility. However, it demonstrated that the algorithm trades off robustness for imperceptibility. The bar based on optimal scaling factor according to individual attack alongside key obtained from the implementation of QKD protocol achieved an optimal balance between imperceptibility and robustness as shown in Figures 4.92 and 4.93. This has attested that the developed algorithm achieved an optimal balance between imperceptibility and robustness.

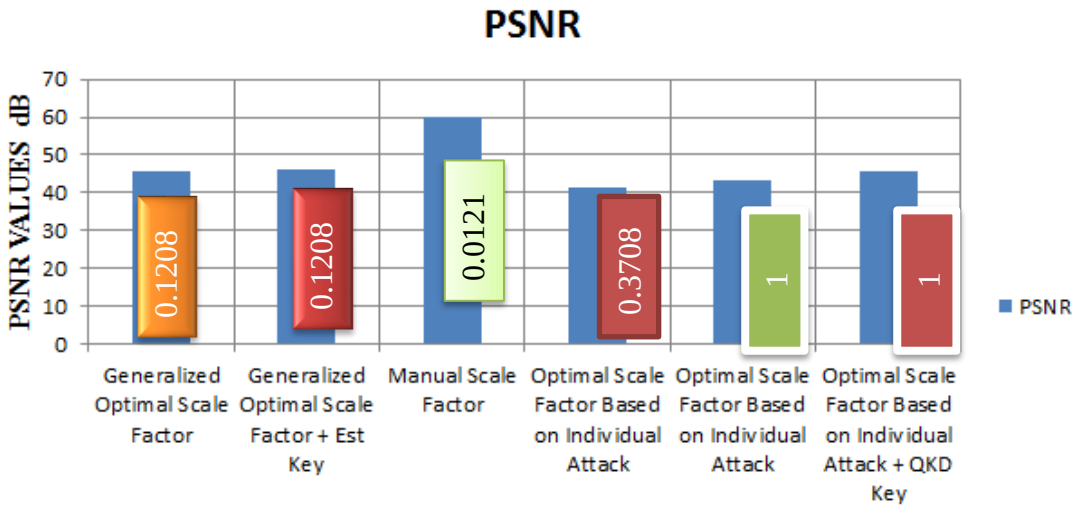


Figure 4.92: Comparison of Results of PSNR obtained Based on Various Defined Scenarios under Speckle Attack

Figure 4.93 depicts the NCC results obtained based on the scaling factor on each bar as shown in the Figure from different defined scenarios under speckle attack. The values of NCC obtained were based on the respective scaling factors in Figure 4.92. The height of each bar depicts the degree at which the algorithm is robust or contains little or no noise. It can be observed from Figure 4.93 that the bar based on optimal scaling factor according to individual attack alongside the key obtained from the implementation of QKD protocol contains no noise. The other respective bars from manually to generalized scaling factor still contain some level of noise under speckle attack.

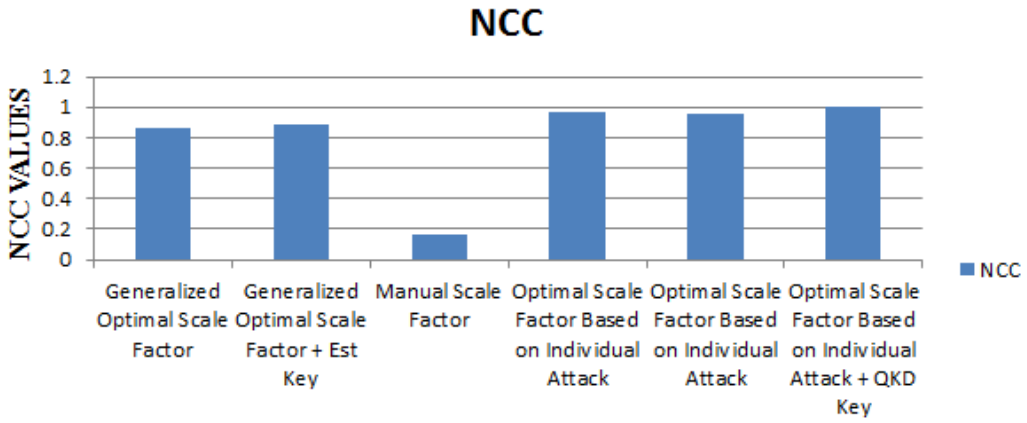


Figure 4.93: Comparison of Results of NCC obtained Based on Various Defined Scenarios Under Speckle Attack

Figure 4.94 denotes the SSIM results obtained based on the scaling factor on each bar as shown in the Figure from different defined scenarios under speckle attack. The values of SSIM obtained were based on the respective scaling factors in Figure 4.92. The SSIM exhibits the same characteristics as NCC, although the SSIM denotes the perceptual quality similarity between the original cover image and watermarked image. It can be observed from Figure 4.94 apart of the bar from manually selected scaling factor, the other respective bar depicts high level of visual similarity between the original cover image and watermarked image under speckle attack.

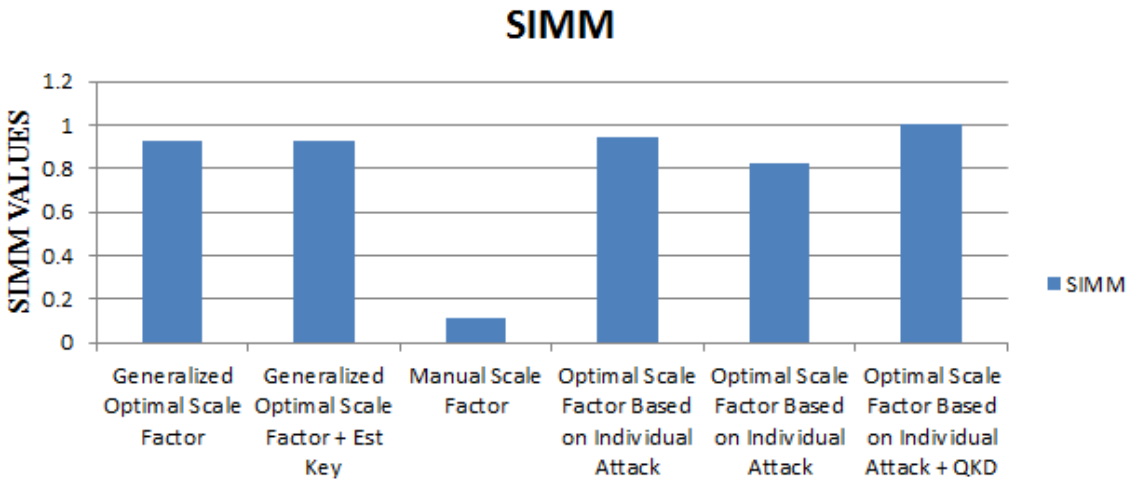


Figure 4.94: Comparison of Results of SSIM obtained Based on Various Defined Scenarios Under Speckle Attack

4.12 Validation

For validation, the results obtained using the data set based on the work of Bajracharya & Koju (2017) were compared with those of the developed algorithm. The deliverables used for comparison were imperceptibility and robustness. The average best of imperceptibility of the developed algorithm evaluated using PSNR is 64.3580dB. The average best of imperceptibility of referenced algorithm evaluated using PSNR is 48.1819dB. The developed

algorithm achieved 25% improvement in term of imperceptibility when compared with the referenced algorithm. The developed algorithm achieved 14% improvement in term of robustness when compared with referenced algorithm. Table 4.8 shows the summary of comparison of results of developed algorithm and that of referenced algorithm.

Table: 4.8: Comparison of Robustness Results between Developed Algorithm and Bajracharya & Koju (2017)

s/n	Attacks	Developed Algorithm (NCC)	Bajracharya & Koju (2017) (NCC)
1	Gaussian	1	1
2	Salt and Pepper	1	0.9996
3	45 degree Rotation	0.9997	0.9999
4	5 degree Rotation	1	0.9999
5	90 degree Rotation	1	1
6	Crop	1	1

The values of NCC of the developed algorithm showed that the algorithm is more robust or resilience to attacks highlighted in table 4.8 than that of the work of Bajracharya & Koju (2017).

Figure 4.95 depicts an average improvement of imperceptibility of the developed algorithm when compared with the work of Bajracharya & Koju (2017).

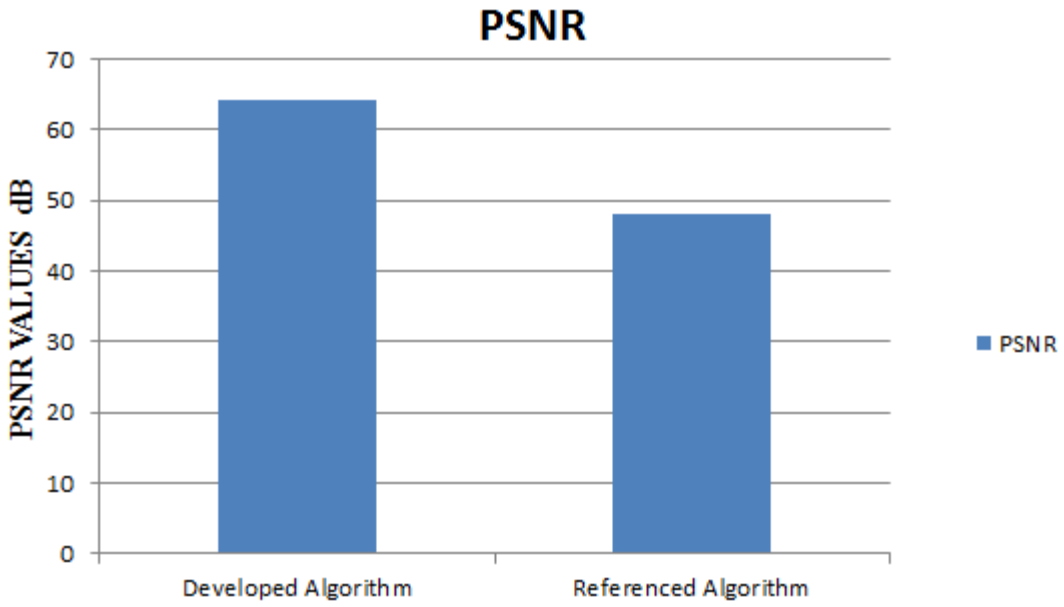


Figure 4.95: Comparison of Imperceptibility of the Developed Algorithm with the work of Bajracharya & Koju, (2017)

Figure 4.96 shows comparison of the different results obtained with respect to the various attacks the algorithms are subjected to in order to ascertain the robustness of the developed algorithm with the work of Bajracharya & Koju (2017) against under these attacks. The developed algorithm is observed to be better for almost all attacks, apart from 45° when the work of Bajracharya & Koju (2017) is observed to perform better than the developed algorithm. This is due to the fact, that the diagonal detail coefficient (HH) of an image that has been established to withstand such geometric attack was not fuse into the third level decomposition of DWT of the image.

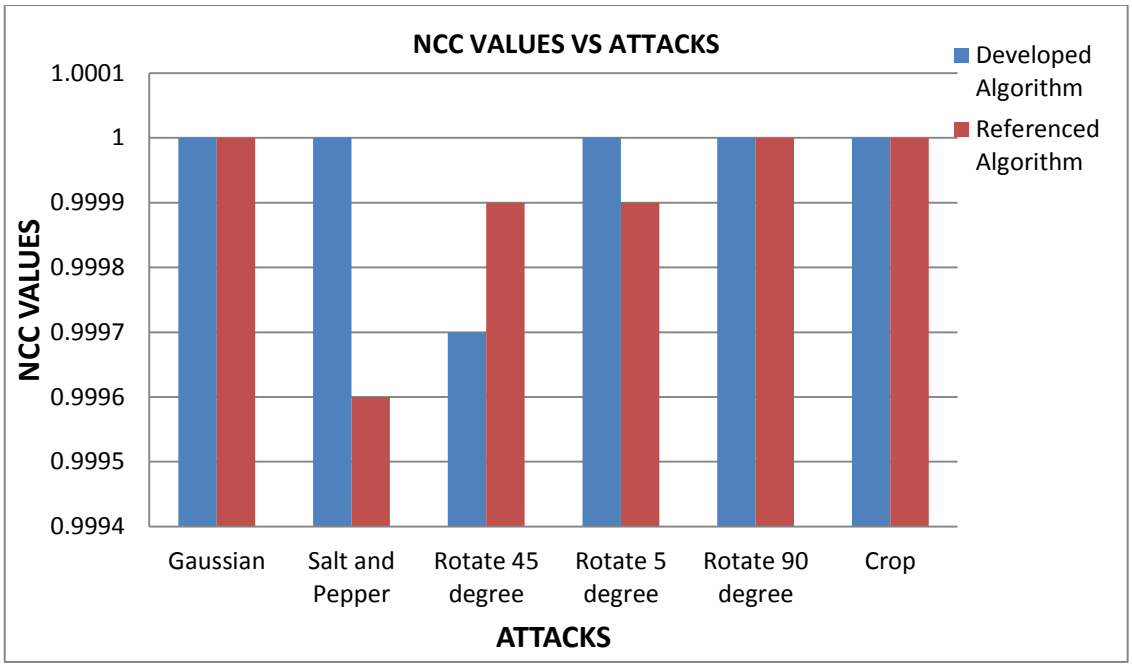


Figure 4.96: Comparison of Robustness of the Developed Algorithm with the work of Bajracharya & Koju, (2017)

The algorithm concealed secret information better than the referenced algorithm. In addition, the developed algorithm makes the watermarked image more imperceptible than the referenced algorithm when viewed by human vision. Figure 4.96 shows the level at which the developed algorithm resist attacks or robust to attacks. In most cases, results show that 100% watermark recovery is guaranteed whilst maintaining a high quality of the image.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 Summary

This thesis aimed at developing a robust digital image watermarking algorithm for images with a view to enhancing Digital image watermarking technique. The design of the algorithm was motivated by the growing threat of illegal duplication of intellectual property right, as a result of distribution of multimedia data over World Wide Web (WWW) or public network. In this research work, development of a novel digital image watermarking technique based on concatenation of DOST, DWT and SVD using private key obtained from QKD scheme has been presented. Also, an optimal scaling factor determined by PSO scheme was equally adopted in the algorithm for embedding and extraction. Standard colour Lena and Pepper images were employed as the cover images. Standard Mandril and Nepal Telecom logo images were employed as the watermark images. In this algorithm the watermark images (secret information) were embedded in the frequency domain of colour cover images. The RGB colour images were decomposed into its three components and the red, green and blue channels were used for watermark embedding. A shuffle method called affine transform was used to transform the watermark images into an incomprehensible form. The incomprehensible image is encrypted based on the private key obtained from QKD using XOR operation with a view to increasing the robustness against attacks. This further enhances the security of the scheme. Optimal scale factor determined by PSO scheme was used to insert the private message in the selected cover image coefficients. The effectiveness of using optimal scale factor is to ensure optimal balance between robustness and perceptual invisibility. After subjecting the watermarked image to series of attacks, the watermark is

invisible to human vision and extractable at all times. Modifications of the frequency components supplied by DOST and DWT were implemented by applying SVD to the diagonal constituents of the original cover image and watermark image in order to enhance the robustness while maintaining the perceptual hiddenness. For this, the developed scheme guarantees protected watermark embedding and easy reconstruction of the image. The watermark is imperceptible to human vision and extractable at all times.

In the developed algorithm, objective experiments were carried out to ascertain the fidelity of the watermarked image and the recovered watermark. The observation made from the results confirmed that the watermarked images sustain their quality with fruitful recoverable of the extracted watermark.

5.3 Conclusion

This thesis focused on the development of novel digital image watermarking technique in DOST domain in conjunction with DWT and SVD based on the principle of photon polarization using optimal scaling factor. The developed algorithm is applied on colour images. The cover images used are standard colour Lena and Pepper images of same size (512 x 512 x 3). The watermark information adopted includes standard colour Mandril image of size (512 x 512 x 3) and Nepal Telecom logo of size (512 x 512 x 3). The algorithm was developed and implemented in MATLAB R2015b.

It was experimentally observed that the use of private key obtained from QKD scheme with concatenated DOST, DWT and SVD using optimal scaling factor offers improvements in robustness against attacks. The improvement occurred when compared to the technique of embedding without private key generated from QKD scheme and optimal scaling factor. This arrangement gives additional adaptability in controlling the optimal balance between

watermark robustness and the perceptual superiority of the watermarked image. Although, the balance between the two deliverables is made possible because of the optimal scaling factor adopted using PSO scheme.

The performance of the algorithm is evaluated to ascertain watermarked image quality and honest reconstruction of the extracted watermark using PSNR, NCC and SSIM as performance metrics. The PSNR with a good value of at least 35dB defines the imperceptibility indicating the degree of visual similarity between the cover image and watermarked image. A high value of NCC (one or almost one) defines the robustness of the algorithm after subjecting the watermarked image to different attacks and this depicts the level of similarity between the original watermark and extracted watermark. The SSIM also exhibited similar characteristics with the NCC as it showed the similarity between the original cover image and watermarked images. The results of the PSNR values when the encrypted watermark image was embedded in the cover image (watermarked image) and subjected to Gaussian, salt and pepper, speckle, rotated at 45 degree, rotated at 5 degree, rotated at 90 degree and crop attacks are 50.2752dB, 47.7293dB, 45.6404dB, 46.8626dB, 44.6045dB, 47.9442dB and 46.4067dB respectively, this proves that the perceptual quality has been improved. The NCC values are 1, 1, 1, 0.9997, 1, 1 and 1, and this signifies that the algorithm is highly resistance to attacks. The SSIM values are 1, 1, 1, 0.99998, 0.9996, 0.9999 and 0.9987 respectively. Therefore, the developed watermarking technique delivered an imperceptibility improvement when compared with the ITU-R standard value of 35dB for digital image watermarking technique by 30%, 27%, 23%, 25%, 22%, 27% and 25% respectively. The technique is also shown to be robust since NCC values obtained are 1s except 5 degree rotation which is 0.9997 when compared with the ITU-R standard of 1 for

digital image watermarking technique. This showed 100% improvement in almost all the attacks except the 5 degree rotation. Comparison of the developed algorithm with the work of Bajracharya & Koju (2017) confirms that the developed algorithm offers superior performance. This is in terms of perceptual quality of the watermarked image using PSNR with an average value of 64.3580dB as against the referenced algorithm of 48.1819. This represents 25% improvement of imperceptibility when compared with the referenced algorithm. The NCC values of the referenced algorithm when subjected to the following attacks: Gaussian, salt and pepper, rotated at 45 degrees, rotated at 5 degrees, rotated at 90 degrees and crop are 1, 0.9996, 0.9999, 0.9999, 1 and 1. This demonstrated that the algorithm developed offered an average value of 14% improvement robustness to attacks when compared with the referenced algorithm.

It is deduced that the developed algorithm offered superior performance with respect to perceptual fidelity of the watermarked image and robustness to attacks, whilst incurring computational overhead with both the embedding and extraction stages. The originality of the technique enables it to achieve significant robustness compared to established watermarking technique and standard. The developed algorithm produced an optimal balance between perceptual deformation (imperceptibility) induced by insertion and robustness against attacks.

In conclusion, the developed algorithm could deliver pertinent merits to the field of digital watermarking and offer extra gains to the copyright protection sector.

5.4 Significant Contributions

The significant contributions of this thesis, which aims at the development of novel digital image watermarking technique motivated by the illegal duplication of intellectual copyright property, are highlighted as follows:

1. A robust digital image watermarking technique based on cascading of DOST, DWT and SVD using QKD scheme and optimal scaling factor has been developed. In actualization of the technique, the watermark data were embedded in the three colour channel of the cover images instead of a single channel of the cover images of the developed algorithm; this increases the robustness of the algorithm to different attacks.
2. The developed algorithm achieved a perceptual quality improvement of watermarked image by 30%, 27%, 23%, 25%, 22%, 27% and 25% respectively, when validated with ITU-R benchmark.
3. The developed algorithm achieved 25% improvement in term of imperceptibility and an average of 14% improvement on robustness to attacks when compared with the work of Bajracharya & Koju (2017).

5.5 Limitations

The limitation of this thesis work is itemized as follows:

1. The developed algorithm is minimally vulnerable to some geometric attack, for instance when the watermarked image was rotated at 5°. This is as a result of inability to combine all the transform coefficients of the images.

5.6 Recommendations for future work

There are numerous areas of this work that would benefit from further extension and experimentation in order to improve performance. Suggestions and recommendations for further finding are itemized as follows:

1. The developed algorithm is quit vulnerable to geometric attacks such as forgery attack and JPEG compression. This is caused by the fact that the diagonal coefficients of the transform images were unable to be combined with a view to forming a reconstructed image. Further development is required in this direction. One possible way is to develop a new technique by being able to fuse all the transform coefficients in order to resist a variety of attacks.
2. Development of an improved algorithm based on reduction of embedding and extraction of overhead processing time can be investigated. This is because the processing time of hiding and recovering the secret data is significantly high.
3. The developed algorithm in this work is for still images, this algorithm could be extended to audio and video files. This multimedia data could be implemented on hardware platform.
4. Development of an improved algorithm to handle higher resolution images such 2048 x 2048 and 1024 X 1024 pixels to assess their performance. Higher resolution of host image can handle numerous watermarking payloads.
5. This thesis was carried out using DOST, DWT and SVD transform; other transformation technique could also be investigated, such as integer wavelet transform (IWT).

6. The computational overhead of the developed algorithm is unreasonably high because the watermark data were embedded in the three channels of the cover images, with regards to this, it is recommended for the algorithm to be improved in order to reduce to computational overhead of embedding and extracting the watermark.

REFERENCES

Abdullatif, M., Zeki, A. M., Chebil, J., & Gunawan, T. S. (2013). *Properties of digital image watermarking.* Paper presented at the Signal Processing and its Applications (CSPA), 2013 IEEE 9th International Colloquium on.

Ahmad, A., Sinha, G., & Kashyap, N. (2014). 3-level DWT Image watermarking against frequency and geometrical attacks. *International Journal of Computer Network and Information Security, 6*(12), 58.

Al-Mansoori, S., & Kunhu, A. (2012). Robust watermarking technique based on DCT to protect the ownership of DubaiSat-1 images against attacks. *International Journal of Computer Science and Network Security (IJCSNS), 12*(6), 1.

Alléaume, R., Treussart, F., Messin, G., Dumeige, Y., Roch, J.-F., Beveratos, A., . . . Grangier, P. (2004). Experimental open-air quantum key distribution with a single-photon source. *New Journal of physics, 6*(1), 92.

Anghel, C. (2009). Base selection and transmission synchronization algorithm in quantum cryptography. *arXiv preprint arXiv:0909.1315*, p1-4.

Anitha, V., & Velusamy, R. L. (2012). Authentication of digital documents using secret key biometric watermarking. *InternationalJournal of Communication Network Security, 1*(4), 5-11.

Araghi, T. K., Manaf, A. B. A., Zamani, M., & Araghi, S. K. (2016). A survey on digital image watermarking techniques in spatial and transform domains. *Int. J. Adv. Image Process. Techn.–IJIPT, 3*(1), 6-10.

Arnold, M. K., Schmucker, M., & Wolthusen, S. D. (2003). *Techniques and applications of digital watermarking and content protection*: Artech House.

Averkiou, M. Digital Watermarking. *PDF). Source: https://www. cl. cam. ac. uk/teaching/0910, 8*, 1.

Azeem, N., Ahmad, I., Jan, S. R., Tahir, M., Ullah, F., & Khan, F. (2016). A New Robust Video Watermarking Technique Using H. 264/AAC Codec Luma Components Based On DCT. *International Journal of Advance Research and Innovative Ideas in Education, Online ISSN-2395-4396*.

Bajracharya, S., & Koju, R. (2017). An Improved DWT-SVD Based Robust Digital Image Watermarking for Color Image. *IJEM-International Journal of Engineering and Manufacturing (IJEM), 7*(1), 49.

Bennett, C. H., Brassard, G., & Robert, J.-M. (1988). Privacy amplification by public discussion. *SIAM journal on Computing, 17*(2), 210-229.

Benrhouma, O., Hermassi, H., & Belghith, S. (2015). Tamper detection and self-recovery scheme by DWT watermarking. *Nonlinear Dynamics, 79*(3), 1817-1833.

Bhandari, R. (2014). Quantum Error Correcting Codes and the Security Proof of the BB84 Protocol. *arXiv preprint arXiv:1409.1452*, p1-89.

Canale, M. (2014). Classical processing algorithms for Quantum Information Security. *Ph.D. School in Information Engineering Information Science and Technology XXVI Class*, p1-142.

Chahal, J. S., & Khurana, S. (2013). A Review on Digital Image Watermarking. *International Journal of Emerging Technology and Advanced Engineering, 3*(12), p482-484.

Challita, K., & Farhat, H. (2011). Combining steganography and cryptography: new directions. *International Journal of New Computer Architectures and their Applications (IJNCAA), 1*(1), 199-208.

Chanda, P. B., & Choudhury, J. P (2016). Secure Data Transmission using DWT Based Image Watermarking Scheme. *International Journal of Engineering Trends and Technology, 35*(10), p453-459.

Chandramouli, R., Memon, N., & Rabbani, M. (2002). Digital watermarking. *Encyclopedia of Imaging Science and Technology*, 1-21.

Chen, X.-y., & Zhan, Y.-y. (2008). Multi-scale anomaly detection algorithm based on infrequent pattern of time series. *Journal of Computational and Applied Mathematics, 214*(1), 227-237.

Cherian, J., & Mereena, A. T. (2016). A Survey on DWT and LWT based Digital Image Watermarking. *International Journal of Research in Computer Application and Information Technology, 4*(3), p27-32.

Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE transactions on image processing, 6*(12), 1673-1687.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory, 22*(6), 644-654.

Eberhart, R., & Kennedy, J. (1995). *A new optimizer using particle swarm theory.* Paper presented at the Micro Machine and Human Science, 1995. MHS'95., Proceedings of the Sixth International Symposium on.

Elboukhari, M., Azizi, M., & Azizi, A. (2010). Quantum Key Distribution Protocols: A Survey. *International Journal of Universal Computer Science, 1*(2), p59-67.

Elliott, C., Pearson, D., & Troxel, G. (2003). *Quantum cryptography in practice.* Paper presented at the Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications.

Eramian, M., Schincariol, R., Stockwell, R. G., Lowe, R. P., & Mansinha, L. (1997). *Review of applications of 1D and 2D S-transforms.* Paper presented at the Proc. SPIE.

Friedman, G. L. (1993). The trustworthy digital camera: Restoring credibility to the photographic image. *IEEE Transactions on consumer electronics, 39*(4), 905-910.

Gattani, P. V., & Warnekar, C. (2014). Security and Watermarking of Color Images. *International journal on Recent and Innovation Trends in Computing and Communication, 2*(6), 1471-1475.

Gelasca, E. D. (2005). *Full-reference objective quality metrics for video watermarking, video segmentation and 3D model watermarking.* Ph. D. thesis, EPFL.

Goudos, S. K. (2014). Evolutionary Algorithms for Wireless Communications—A Review of the State-of-the art (pp. 1-11).

Guenther, C. (2003). The relevance of quantum cryptography in modern cryptographic systems. *GSEC Partical Requirements (v1. 4b). http://www. giac. org/practical/GSEC/Christoph Guenther GSEC. pdf*. P1-27

GÜMÜŞ, E., Aydin, G. Z., & Aydin, M. A. (2008). Quantum cryptography and comparison of quantum key distribution protocols. *IU-Journal of Electrical & Electronics Engineering, 8*(1), 503-510.

Gupta, V., & Barve, A. (2014). A review on image watermarking and its techniques. *International Journal of Advanced Research in Computer Science and Software Engineering, 4*(1), 92-97.

Haitjema, M. (2007). A Survey of the Prominent Quantum Key Distribution Protocols (pp. p1-7): URL: http://www. cse. wustl. edu/~ jain/cse571-07/ftp/quantum (дата обращения 18.10. 2013).

Harish, N., Kumar, B., & Kusagur, A. (2013). Hybrid robust watermarking technique based on DWT, DCT and SVD. *International Journal of Advanced Electrical and Electronics Engineering, 2*(5), 137-143.

Huang, H.-C., & Fang, W.-C. (2010). Techniques and applications of intelligent multimedia data hiding. *Telecommunication Systems, 44*(3), 241-251.

Hui, Q., & Chen, X. (2009). Simulation of BB84 Quantum Key Distribution in depolarizing channel. *Proceeding of 14th Youth Conference on Communication*, p483-487.

Jabade, V. S., & Gengaje, D. S. R. (2011). Literature review of wavelet based digital image watermarking techniques. *International Journal of Computer Applications, 31*(1), 28-35.

Johnson, J. S. (2012). An Analysis of Error Reconciliation Protocols for use in Quantum Key Distribution (pp. p1-178): AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT.

Johnson, J. S., Grimaila, M. R., Humphries, J. W., & Baumgartner, G. B. (2015). An analysis of error reconciliation protocols used in quantum key distribution systems. *The Journal of Defense Modeling and Simulation, 12*(3), 217-227.

Kashyap, N., & Sinha, G. (2012). Image watermarking using 3-level discrete wavelet transform (DWT). *International Journal of Modern Education and Computer Science, 4*(3), 50.

Katzenbeisser, S., & Petitcolas, F. (2000). *Information hiding techniques for steganography and digital watermarking* (5th Edition ed.): Artech house.

Kaur, P., & Jindal, S. (2014). A New approach of SVD-DWT Video Watermarking Embedding Algorithm. *International Journal of Recent Advances in Engineering and Technology, 2*(5), p36-40.

Kavitha, K., & Shan, B. P. (2016). An Introduction to the Digital Watermarking. *International Journal of Advanced Engineering Research and Science, 3*(6), p 157-160.

Kejgir, S. G., & Kokare, M. (2012). Lifting wavelet transform with singular value decomposition for robust digital image watermarking. *International Journal of Computer Applications, 39*(18), 10-18.

Kester, Q.-A., Nana, L., Pascu, A. C., Gire, S., Eghan, J. M., & Quaynor, N. N. (2014). A Hybrid Cryptographic and Digital Watermarking Technique for Securing Digital Images based on a Generated Symmetric Key. *International Journal of Computer Applications, 94*(19), p19-27.

Koju, R., & Joshi, S. R. (2015). Comparative analysis of color image watermarking technique in RGB, YUV, and YCbCr Color Channels. *Nepal Journal of Science and Technology, 15*(2), 133-140.

Kumar, M., & Agrawal, S. (2015). Color image encoding in DOST domain using DWT and SVD. *Optics & Laser Technology, 75*, 138-145.

Ladan, J., & Vrscay, E. R. (2013). *The Discrete Orthonormal Stockwell Transform and Variations, with Applications to Image Compression.* Paper presented at the International Conference Image Analysis and Recognition.

Lai, C.-C., Chan, C.-F., Ouyang, C.-S., & Chiang, H.-F. (2013). *A robust feature-based image watermarking scheme.* Paper presented at the Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2013 14th ACIS International Conference on.

Lai, C.-C., & Tsai, C.-C. (2010). Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on instrumentation and measurement, 59*(11), 3060-3063.

Liu, J., & He, X. (2005). *A review study on digital watermarking.* Paper presented at the Information and Communication Technologies, 2005. ICICT 2005. First International Conference on.

Lo, H.-K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. *Nature Photonics, 8*(8), 595-604.

Lokhande, U., & Gulve, A. (2014). Steganography using Cryptography and Pseudo Random Numbers. *International Journal of Computer Applications, 96*(19), p40-46.

Loukhaoukha, K., Refaey, A., & Zebbiche, K. (2017). Ambiguity attacks on robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *Journal of Electrical Systems and Information Technology*, p1-10.

Lukin, M. (2003). Colloquium: Trapping and manipulating photon states in atomic ensembles. *Reviews of Modern Physics, 75*(2), 457.

Malonia, M., & Agarwal, S. K. (2016). *Digital Image Watermarking using Discrete Wavelet Transform and Arithmetic Progression technique.* Paper presented at the Electrical, Electronics and Computer Science (SCEECS), 2016 IEEE Students' Conference on.

Martinez-Mateo, J., Pacher, C., Peev, M., Ciurana, A., & Martin, V. (2014). Demystifying the information reconciliation protocol Cascade. *arXiv preprint arXiv:1407.3257, 15*(5&6), p453-476.

Mayers, D. (2001). Unconditional security in quantum cryptography. *Journal of the ACM (JACM), 48*(3), 351-406.

Mehto, A., & Mehra, N. (2015). Techniques of digital image watermarking: A review. *International Journal of Computer Applications, 128*(9), 21-33.

Nag, A., Singh, J. P., Khan, S., Ghosh, S., Biswas, S., Sarkar, D., & Sarkar, P. P. (2011). *Image encryption using affine transform and XOR operation.* Paper presented at the 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies.

Navas, K., Ajay, M. C., Lekshmi, M., Archana, T. S., & Sasikumar, M. (2008). *Dwt-dct-svd based watermarking.* Paper presented at the Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on.

Niemiec, M. (2011). *Design, Construction and Verification of High-level Security Protocol Allowing to Apply the Quantum Cryptography in Communication Networks: Ph. D. Thesiss*: AGH University of Science And Technology. Faculty of Electrical

Engineering, Automatics, Computer Science and Electronics. Department of Telecomunications.
Niemiec, M., & Pach, A. R. (2012). *The measure of security in quantum cryptography.* Paper presented at the Global Communications Conference (GLOBECOM), 2012 IEEE.
Nin, J., & Ricciardi, S. (2013). *Digital watermarking techniques and security issues in the information and communication society.* Paper presented at the Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on.
Ouazzane, H., Mahersia, H., & Hamrouni, K. (2017). *How to extend the use of the discrete orthogonal stockwell transform to image watermarking.* Paper presented at the Proceedings of the Symposium on Applied Computing.
Padgett, J. (2002). Multimedia Rights Protection Digital Image Watermarking Techniques. *Leeds University*.
Paliwal, M., & Jain, Y. K. (2015). Digital Watermarking Algorithm for Embedding Color Image using Two Level DWT. *International Journal of Computer Applications, 116*(13).
Poels, K., Schoenmakers, I. L., & Tuyls, P. (2005). Quantum Key Exchange Using Squeeze State. p1-120.
Potdar, V. M., Han, S., & Chang, E. (2005). *A survey of digital image watermarking techniques.* Paper presented at the Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on.
Prashanth, H., Shashidhara, H., & KN, B. M. (2009). *Image scaling comparison using universal image quality index.* Paper presented at the Advances in Computing, Control, & Telecommunication Technologies, 2009. ACT'09. International Conference on.
Pratt, W. K. (2013). *Introduction to digital image processing* (Third Edition ed.): CRC Press.
Rahman, M. (2013). A DWT, DCT and SVD based watermarking technique to protect the image piracy. *arXiv preprint arXiv:1307.3294*.
Rahman, M. A., & Rabbi, M. F. (2015a). DWT-SVD based New Watermarking Idea in RGB Color Space. *International Journal of Signal Processing, Image Processing and Pattern Recognition, 8*(6), 193-198.
Rahman, M. A., & Rabbi, M. F. (2015b). Non-Blind DWT-SVD based Watermarking Technique for RGB Image. *Global Journal of Research In Engineering, 15*(4), p1-5.
Salama, A. S., & Mokhtar, M. A. (2016). *Combined technique for improving digital image watermarking.* Paper presented at the Computer and Communications (ICCC), 2016 2nd IEEE International Conference on.
Santhi, V., & Arulmozhivarman, P. (2013). Hadamard transform based adaptive visible/invisible watermarking scheme for digital images. *Journal of Information Security and Applications, 18*(4), 167-179.
Sathik, M. M., & Sujatha, S. (2012). A Novel DWT Based Invisible Watermarking Technique for Digital Images. *Int. Arab J. e-Technol., 2*(3), 167-173.
Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics, 81*(3), 1301.

Sharma, P., & Jain, T. (2014). *Robust digital watermarking for coloured images using SVD and DWT technique.* Paper presented at the Advance Computing Conference (IACC), 2014 IEEE International.

Sharma, P., & Swami, S. (2013). *Digital image watermarking using 3 level discrete wavelet transform.* Paper presented at the Conference on Advances in Communication and Control Systems.

Sharma, R. D., & De, A. (2011). *A new secure model for quantum key distribution protocol.* Paper presented at the Industrial and Information Systems (ICIIS), 2011 6th IEEE International Conference on.

Shieh, C.-S., Huang, H.-C., Wang, F.-H., & Pan, J.-S. (2004). Genetic watermarking based on transform-domain techniques. *Pattern recognition, 37*(3), 555-565.

Singh, A. K., Dave, M., & Mohan, A. (2012). *A novel technique for digital image watermarking in frequency domain.* Paper presented at the Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on.

Singh, B., Sharma, K. D., & Jatav, L. S. (2014). *New robust watermarking approach for image authentication.* Paper presented at the Consumer Electronics (GCCE), 2014 IEEE 3rd Global Conference on.

Singh, P., & Chadha, R. (2013). A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT), 2*(9), 165-175.

Sinha, R. K., Mishra, M., & Sahu, S. (2017). Quantum Key Distribution: Simulation of BB84 Protocol in C. *Internal Journal of Electronics, Electrical and Computational System, 6*(1), p57-60.

Stockwell, R. G. (2007). A basis for efficient representation of the S-transform. *Digital Signal Processing, 17*(1), 371-393.

Tanaka, K., Nakamura, Y., & Matsui, K. (1990). *Embedding secret information into a dithered multi-level image.* Paper presented at the Military Communications Conference, 1990. MILCOM'90, Conference Record, A New Era. 1990 IEEE.

Tao, H., Chongmin, L., Zain, J. M., & Abdalla, A. N. (2014). Robust image watermarking theories and techniques: a review. *Journal of applied research and technology, 12*(1), 122-138.

Tao, P., & Eskicioglu, A. M. (2004). *A robust multiple watermarking scheme in the discrete wavelet transform domain.* Paper presented at the Proc. SPIE.

Thakkar, F., & Srivastava, V. K. (2017). A particle swarm optimization and block-SVD-based watermarking for digital images. *Turkish Journal of Electrical Engineering & Computer Sciences, 25*(4), 3273-3288.

Thramboulidis, K. (2007). IEC 61499 in factory automation *Advances in Computer, Information, and Systems Sciences, and Engineering* (pp. 115-124): Springer.
Trippe, S. (2014). Polarization and polarimetry: A review. *arXiv preprint arXiv:1401.1911*, p1-25.

Vaidya, S. P., & Mouli, P. C. (2015). Adaptive digital watermarking for copyright protection of digital images in wavelet domain. *Procedia Computer Science, 58*, 233-240.

Venkatram, N., Reddy, L., Kishore, P., & Shavya, C. (2014a). RSA-DWT BASED MEDICAL IMAGE WATERMARKING FOR TELEMEDICINE APPLICATIONS. *Journal of Theoretical & Applied Information Technology, 65*(3).

Venkatram, N., Reddy, L., Kishore, P., & Shavya, C. (2014b). RSA-DWT BASED MEDICAL IMAGE WATERMARKING FOR TELEMEDICINE APPLICATIONS. *Journal of Theoretical & Applied Information Technology, 65*(3), p801-812.

Wang, Y. (2011). Efficient stockwell transform with applications to image processing. p1-131.

Wang, Y., & Orchard, J. (2009). Fast discrete orthonormal Stockwell transform. *SIAM Journal on Scientific Computing, 31*(5), p4000-4012.

Weerasinghe, W. M. (2012). Quantum Cryptography. *https://www.researchgate.net/publication/305768369*, 1-26.

Yan, Y., & Zhu, H. (2011). *The generalization of discrete Stockwell transforms.* Paper presented at the Signal Processing Conference, 2011 19th European.

Zhao, Y., Qi, B., Ma, X., Lo, H.-K., & Qian, L. (2006). *Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber.* Paper presented at the Information Theory, 2006 IEEE International Symposium on.

Zheng, D., Liu, Y., Zhao, J., & Saddik, A. E. (2007). A survey of RST invariant image watermarking algorithms. *ACM Computing Surveys (CSUR), 39*(2), 5.

APPENDIX A

Complete M File for Host Image Decomposition Using DOST

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% dost2
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%
% this function computes the dost coefficients of a 2-dimensional signal.
% It works using the dost on rows and columns.
%

function dost_coefficients = dost2(input_signal)

dost_coefficients = dost(dost(input_signal).').';

end


%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% dost
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%
% this function computes the 1-dimensional discrete orthonormal Stockwell
% coefficients of a given time series
%
function dost_coefficients = dost(time_series)
% time_series should be a column vector, if not we take its transpose
if isrow(time_series) == 1
    time_series = time_series';
else
end

% look at the number of rows of the input
size_time_series = size(time_series);
rows_time_series = size_time_series(1);

% inizialize the output (same output size as the input).
dost_coefficients = zeros(size_time_series);

% partition of the frequency space, see details in the
% band_width_partitioning function explanation below.
[number_of_freq_bands, band_widths] =
band_width_partitioning(rows_time_series);

% compute the Fourier transform of the input using the fft. More details on
% this can be found on the Fourier function explanation below.
Fx = Fourier(time_series);

% compute the reverse transform of the cutted Fourier transform
% of the input signal
counter = 0;
for ll = 1:number_of_freq_bands
    % choose the bandwidth you are interested in and call it
```

```
    % frequency_width_cutter
    frequency_width_cutter = band_widths(ll);
    % cut all the Fourier coefficients Fx in the frequency band
    % counter + 1: counter + frequency_width_cutter
    cut_Fx = Fx(counter + 1: counter + frequency_width_cutter, : );
    % perform the inverse Fourier transform just on the selected frequency
    % band.
    % Notice that you have to pay attention on the length of the cut_Fx.
    % If it is just 1 we do not do nothing, otherwise we take the inverse
    % Fourier transform.
    if frequency_width_cutter == 1
            dost_coefficients(counter + 1 : counter +
frequency_width_cutter , : ) = cut_Fx;
    else
        dost_coefficients(counter + 1 : counter + frequency_width_cutter ,
: ) = iFourier(cut_Fx);
    end
    % update the starting position for the band
    counter = counter + frequency_width_cutter;
end
%
end
```

APPENDIX B

Complete M File for Binary bits Generation

```
function key = generateKey(A, L, M, N)
ind = 1;
while true
    key = A(ind:L);
    K1 = key(9:16);
    K3 = key(25:32);
    if isequal(gcd(bin2dec(K1),M), 1) && ...
            isequal(gcd(bin2dec(K3),N), 1)
        break

    else
        ind = ind+1;
    end
end
end
```

APPENDIX C

Complete M File for Generating and Sending of Quantum bits to Receiver

```
classdef SenderClass
    properties
        Bits
        Bases
        Qubits
        SecretBits

    end

    methods
        function obj = generateBits(obj, L, M, N)
                obj.Bits = strrep(num2str(randi([0,1], 1,L)), ' ', '');
        end

        function obj = generateBases(obj, L)
                basis = ['x' '+'];
                index = randi([1,2], 1,L);
                obj.Bases = basis(index);
        end

        function obj = generateQubits(obj, L)
            obj.Qubits = repmat('*', 1, L);
            for i=1:L
               if strcmp(obj.Bits(i), '0')
                   if strcmp(obj.Bases(i), '+')
                       obj.Qubits(i) = '-';
                   else
                       obj.Qubits(i) = '/';
                   end
               else
                   if strcmp(obj.Bases(i), '+')
                       obj.Qubits(i) = '|';
                   else
                       obj.Qubits(i) = '\';
                   end
               end
            end
        end

        function obj = getSecretBits(obj, sIndex)

            obj.SecretBits = obj.Bits(sIndex);
        end
    end
end
```

APPENDIX D

Complete M File for Receiving Quantum bits from Sender

```
classdef ReceiverClass
    properties
        Bits
        Bases
        Qubits
        ReceivedBases
        SecretBits
    end

    methods
         function obj = receiveQubits(obj, Qubits, errorRate)
            obj.Qubits = Qubits;
            L = numel(obj.Qubits);
            for i=1:L
                if rand < errorRate
                    if obj.Qubits(i) == '/'
                        obj.Qubits(i) = '\';
                    elseif obj.Qubits(i) == '\'
                        obj.Qubits(i) = '/';
                    elseif obj.Qubits(i) == '-'
                        obj.Qubits(i) = '|';
                    elseif obj.Qubits(i) == '|'
                        obj.Qubits(i) = '-';
                    end
                end
            end
        end

        function obj = generateBases(obj, L)
            basis = ['x' '+'];
            index = randi([1,2], 1,L);
            obj.Bases = basis(index);
        end

        function obj = measureQubits(obj)
            L = length(obj.Qubits);
            obj.Bits = repmat('-', 1, L);
            for i=1:L
                if ismember(obj.Qubits(i), ['-' '|']) && ...
                        strcmp(obj.Bases(i), '+')
                    if  strcmp(obj.Qubits(i), '-')
                        obj.Bits(i) = '0';
                    else
                        obj.Bits(i) = '1';
                    end
                elseif ismember(obj.Qubits(i), ['/' '\']) && ...
                        strcmp(obj.Bases(i), 'x')
                    if  strcmp(obj.Qubits(i), '/')
                        obj.Bits(i) = '0';
                    else
                        obj.Bits(i) = '1';
```

```
                    end
                else
                    obj.Bits(i) = ' ';
                end
            end
        end

        function obj = reportBases(obj)
            obj.ReceivedBases = obj.Bases;
            L = length(obj.Bases);
            for i=1:L
                if strcmp(obj.Bits(i), ' ')
                     obj.ReceivedBases(i) = ' ';
                end
            end
        end

       function obj = getSecretBits(obj, sIndex)

            obj.SecretBits = obj.Bits(sIndex);
        end
    end
end
```

APPENDIX E

Complete M File for performing the various phases of Error Detection and Correction

```
function [Ap, Bp, count] = performPass(P, Ap, Bp, k, n, permArray,
rPermArray)
count = 0;

for b=1:n
    display(['block-', num2str(b)])
    ind1 = k*(b-1) + 1;
    ind2 = k * b;
    Ab = Ap(ind1:ind2);
    Bb = Bp(ind1:ind2);
    AParityCheck = mod(numel(find(Ab == '1')),2);
    BParityCheck = mod(numel(find(Bb == '1')),2);

    if (AParityCheck ~= BParityCheck)
        %   perform binary search on that block in order
        %   to identify the single bit error
        eInd = find(Ab~=Bb);
        ne = numel(eInd);
        Bb(eInd) = Ab(eInd);
        Bp(ind1:ind2) = Bb;
        count = count + ne;


        % perform binary search rerun on the block containing
        % the corrected bit in previous passes
        for i=1:numel(eInd)
            Pprev = P - 1;
            ck = k;
            cAp = Ap;
            cBp = Bp;
            cInd = ind1+(eInd(i)-1);
            while Pprev >= 1

                pInd = permArray(cInd);

                pk = ck/2;
                pb = ceil(pInd/pk);
                display(['pass-', num2str(Pprev), '-block-', num2str(pb)])
                pind1 = pk*(pb-1) + 1;
                pind2 = pk * pb;
                pAp = cAp(rPermArray);
                pBp = cBp(rPermArray);

                Ab = pAp(pind1:pind2);
                Bb = pBp(pind1:pind2);

                %             AParityCheck = mod(numel(find(Ab == '1')),2);
                %             BParityCheck = mod(numel(find(Bb == '1')),2);

                ind = find(Ab~=Bb);
```

```
                ne = numel(ind);
                Bb(ind) = Ab(ind);
                pBp(pind1:pind2) = Bb;
                count = count + ne;

                %                       cAp = pAp(permArray);
                %                       cBp = pBp(permArray);


                Pprev = Pprev - 1;
                ck = pk;
                cAp = pAp;
                cBp = pBp;
                cInd = pInd;
            end

            for j=1:P-1
                nAp = cAp(permArray);
                nBp = cBp(permArray);

                cAp = nAp;
                cBp = nBp;
            end
            Ap = cAp;
            Bp = cBp;

        end
    end

end
```

APPENDIX F

Complete M File for performing Error Reconciliation

```
function [Aprime, Bprime] = cascade(A,B,p,k, permArray, rPermArray)

N = length(A);

display('==============pass 1===========')
% pass 1
% Alice and Bob decide on a arbitrary permutation
Ap1 = A(permArray);
Bp1 = B(permArray);

% Alice and Bob then divides their sifted keys into blocks of size k
% the single bit parity check for each block is calculated and shared
publicly
k1 = k;
n1 = N/k1;
P = 1;
[Ap1, Bp1, count1] = performPass(P, Ap1, Bp1, k1, n1, permArray,
rPermArray);

% if count1 == 28
%    return
% end

display('==============pass 2===========')
% pass 2
% Alice and Bob permute their new key
Ap2 = Ap1(permArray);
Bp2 = Bp1(permArray);

% the block size is increased
k2 = k1*2;
n2 = N/k2;
P = 2;

% Alice and Bob then divides their sifted keys into blocks of size k
% the single bit parity check for each block is calculated and shared
publicly
[Ap2, Bp2, count2] = performPass(P, Ap2, Bp2, k2, n2, permArray,
rPermArray);



display('==============pass 3===========')
% pass 3
% Alice and Bob permute their new key
Ap3 = Ap2(permArray);
Bp3 = Bp2(permArray);

% the block size is increased
k3 = k2*2;
```

```
n3 = N/k3;
P = 3;

% Alice and Bob then divides their sifted keys into blocks of size k
% the single bit parity check for each block is calculated and shared
publicly
[Ap3, Bp3, count3] = performPass(P, Ap3, Bp3, k3, n3, permArray,
rPermArray);


display('==============pass 4===========')
% pass 4
% Alice and Bob permute their new key
Ap4 = Ap3(permArray);
Bp4 = Bp3(permArray);

% the block size is increased
k4 = k3*2;
n4 = N/k4;
P = 4;

% Alice and Bob then divides their sifted keys into blocks of size k
% the single bit parity check for each block is calculated and shared
publicly
[Ap4, Bp4, count4] = performPass(P, Ap4, Bp4, k4, n4, permArray,
rPermArray);


display('==============pass 5===========')
% pass 5
% Alice and Bob permute their new key
Ap5 = Ap4(permArray);
Bp5 = Bp4(permArray);

% the block size is increased
k5 = k4*2;
n5 = N/k5;
P = 5;

% Alice and Bob then divides their sifted keys into blocks of size k
% the single bit parity check for each block is calculated and shared
publicly
[Ap5, Bp5, count5] = performPass(P, Ap5, Bp5, k5, n5, permArray,
rPermArray);


count = count1 + count2 + count3  + count4  + count5;


for i5=k5:k5:N
    Ap5(i5) = ' ';
    Bp5(i5) = ' ';
end
Ap4 = Ap5(rPermArray);
```

```
Bp4 = Bp5(rPermArray);

for i4=k4:k4:N
    Ap4(i4) = ' ';
    Bp4(i4) = ' ';
end
Ap3 = Ap4(rPermArray);
Bp3 = Bp4(rPermArray);

for i3=k3:k3:N
    Ap3(i3) = ' ';
    Bp3(i3) = ' ';
end
Ap2 = Ap3(rPermArray);
Bp2 = Bp3(rPermArray);

for i2=k2:k2:N
    Ap2(i2) = ' ';
    Bp2(i2) = ' ';
end

Ap1 = Ap2(rPermArray);
Bp1 = Bp2(rPermArray);

for i1=k1:k1:N
    Ap1(i1) = ' ';
    Bp1(i1) = ' ';
end
Aprime = Ap1(rPermArray);
Bprime = Bp1(rPermArray);

Aprime = Aprime(find(Aprime ~= ' '));
Bprime = Bprime(find(Bprime ~= ' '));

end
```

APPENDIX G

Complete M File for performing Error Reconciliation process on the key obtained

```
      clc
clear

errorRate = 0.05

%initialization
Alice = SenderClass;
Bob = ReceiverClass;

% % read original image and watermark
% Ia_original = imread('../dan/lena.png');
% Ib_original = imread('../dan/mandril.png');
% L = 64;                       %key length
% % [M,N,~] = size(Ib_original);


% % Quantum Transmission
display('generating random bits ...')
% Alice generate appropriate length random bits
L = 500;
Alice = Alice.generateBits(L);
Alice.Bits
pause

% Alice randomly chooses polarization basis
Alice = Alice.generateBases(L);
Alice.Bases
pause

display('transmiting qubits ...')
% Alice generate and transmits qubit
Alice = Alice.generateQubits(L);
Alice.Qubits
pause

% Bob receives qubits
% Bob.Qubits = Alice.Qubits;
Bob = Bob.receiveQubits(Alice.Qubits, errorRate);
Bob.Qubits
pause

% Bob randomly chooses polarization basis
Bob = Bob.generateBases(L);
Bob.Bases
pause

% Bob measures qubits
Bob = Bob.measureQubits();
Bob.Bits
```

```
pause

% % Public Discussion
display('sifting bits ...')
% Bob reports bases of received bits
Bob = Bob.reportBases();
Bob.ReceivedBases
pause

% ALice communicates those bit positions for which bob chose correctly
correctBasesPos = find(Alice.Bases == Bob.ReceivedBases);
sharedInfo = repmat(' ', 1, L);
sharedInfo(correctBasesPos) = Alice.Bits(correctBasesPos);

% Bob reveals some key bits at random
nCB = length(correctBasesPos);
nRB = ceil(nCB/3);
% comb = nchoosek(correctBasesPos, nRB);
% rIndex = comb(randi(length(comb)),:);

rIndex = correctBasesPos(sort(randi(nCB, 1, nRB)));


revealedBits = repmat(' ', 1, L);
revealedBits(rIndex) = Bob.Bits(rIndex)

% Alice confirms them
confirmRevealedBits = repmat(' ', 1, L);
confirmRevealedBits(rIndex) = Alice.Bits(rIndex)

% eER = sum(revealedBits ~= confirmRevealedBits)/ nRB
pause

display('display remaining shared secret bits')
% % Outcome
% Remaining shared secret bits

sIndex = setdiff(correctBasesPos,rIndex);

Alice = Alice.getSecretBits(sIndex);
Bob = Bob.getSecretBits(sIndex);

A = Alice.SecretBits(1:128)
B = Bob.SecretBits(1:128)


display('error reconciliation')
% error reconciliation

p = sum(A ~= B)/ nRB
k= 8; %floor(0.73/p)
N = length(A);

permArray = randperm(N);
```

```
[~, rPermArray] = sort(permArray);

[Aprime, Bprime] = cascade(A,B,p,k, permArray, rPermArray)
length(Aprime)
sum(Aprime ~= Bprime)
pause

display('privacy amplification')
% privacy amplification

%obtain key
L = 64;
M = 512;
N = 512;
key = generateKey(Aprime, L, M, N)
```

APPENDIX H

Complete M File for Watermark Encryption with Generated Key

```
function C = encryption(S, key)
% clear;
% clc;
% close all
% L = 64;
%
% I = imread('Mandril.png');
% S = rgb2gray(I);
% [M,N,~] = size(S);
% key = generateKey(L, M, N);

 [M, N] = size(S);
% Split 64 bits secret key into
% K0, K1, K2, K3, K4, K5, K6 and K7
K0 = bin2dec(key(1:8));
K1 = bin2dec(key(9:16));
K2 = bin2dec(key(17:24));
K3 = bin2dec(key(25:32));
K4 = bin2dec(key(33:40));
K5 = bin2dec(key(41:48));
K6 = bin2dec(key(49:56));
K7 = bin2dec(key(57:64));

% For each pixel Pxy, transform the location
% (x, y) in S to (x_prime, y_prime) in C
C = zeros(M,N);
for x = 0:M-1
    for y = 0:N-1
        x_prime = mod((K0+K1*x), M);
        y_prime = mod((K2+K3*y), N);
        C(x_prime+1, y_prime+1) = S(x+1,y+1);
    end
end

% Figure; imshow(uint8(C));

% Decompose C into M/2 X N/2 number of 2 X 2
% blocks
for i = 1:2:M
    for j = 1:2:N
        B = C(i:i+1, j:j+1);
        P11 = bitxor(B(1,1), K4);
        P12 = bitxor(B(1,2), K5);
        P21 = bitxor(B(2,1), K6);
        P22 = bitxor(B(2,2), K7);

        C(i:i+1, j:j+1) = [P11, P12; P21, P22];
    end
end
C = uint8(C);
% Figure; imshow(C);
End
```

APPENDIX I

Complete M File for Application of transformation Technique

```
function transformOutput = applyTransform(I)
    %apply dost
    Idost = dost2(I);

% Idost = I;
    %apply dwt thrice
    [cA1,cH1,cV1,cD1] = dwt2(Idost,'haar');
    [cA2,cH2,cV2,cD2] = dwt2(cA1,'haar');
    [cA3,cH3,cV3,cD3] = dwt2(cA2,'haar');
%     It = cA3;

    transformOutput = {};
    transformOutput.dost = Idost;

    transformOutput.dwtL1.cA = cA1;
    transformOutput.dwtL1.cH = cH1;
    transformOutput.dwtL1.cV = cV1;
    transformOutput.dwtL1.cD = cD1;

    transformOutput.dwtL2.cA = cA2;
    transformOutput.dwtL2.cH = cH2;
    transformOutput.dwtL2.cV = cV2;
    transformOutput.dwtL2.cD = cD2;

    transformOutput.dwtL3.cA = cA3;
    transformOutput.dwtL3.cH = cH3;
    transformOutput.dwtL3.cV = cV3;
    transformOutput.dwtL3.cD = cD3;

    transformOutput.It = cA3;
end
```

APPENDIX J

Complete M File for Performing the Fitness Function

```
function fitness = objFun(Ia_original, Ib_original, alpha, key, noise)

% Watermarking process
[Ia_watermarked, Ibr_decrypted, Ian_watermarked]...
    = watermarkingProcess(Ia_original, Ib_original, alpha, key, noise);

% Normalised correlation coefficient
fitness = (corr2(rgb2gray(Ib_original), rgb2gray(Ibr_decrypted)) ...
    + corr2(rgb2gray(Ia_original), rgb2gray(Ia_watermarked))) / 2;

end
```

APPENDIX K

Complete M File for Decrypting the watermark image

```
function S = decryption(C,key)
[M, N] = size(C);
% divid 64 bits secret key into
% K0, K1, K2, K3, K4, K5, K6 and K7
K0 = bin2dec(key(1:8));
K1 = bin2dec(key(9:16));
K2 = bin2dec(key(17:24));
K3 = bin2dec(key(25:32));
K4 = bin2dec(key(33:40));
K5 = bin2dec(key(41:48));
K6 = bin2dec(key(49:56));
K7 = bin2dec(key(57:64));

[~,U1,~] = gcd(K1,M);
K1_inv = mod(U1,M);
[~,U3,~] = gcd(K3,M);
K3_inv = mod(U3,M);

% Decompose C into M/2 X N/2 number of 2 X 2
% blocks
for i = 1:2:M
    for j = 1:2:N
        B = C(i:i+1, j:j+1);
        P11 = bitxor(B(1,1), K4);
        P12 = bitxor(B(1,2), K5);
        P21 = bitxor(B(2,1), K6);
        P22 = bitxor(B(2,2), K7);

        C(i:i+1, j:j+1) = [P11, P12; P21, P22];
    end
end

% Figure; imshow(uint8(C));

% For each pixel Pxy, transform the location
% (x, y) in S to (x_prime, y_prime) in C
S = zeros(M,N);
for x_prime = 0:M-1
    for y_prime = 0:N-1
        x = mod(((x_prime-K0)*K1_inv), M);
        y = mod(((y_prime-K2)*K3_inv), N);
        S(x+1, y+1) = C(x_prime+1,y_prime+1);
    end
end

S = uint8(S);
% Figure; imshow(S);
end
```

APPENDIX L

Complete M File for using PSO to obtain optimal Scale factor based on Fitness Function

```
clc
clear
close all

% read original image and watermark
Ia_original = imread('lena.png');
Ib_original = imread('mandril.png');

% Generate key, alpha and noise
L = 64;                      %key length
[M,N,~] = size(Ib_original);
key = generateKey(L, M, N);

noise = '';          %Gaussian | salt & pepper | speckle

fun = @(alpha) -objFun(Ia_original, Ib_original, alpha, key, noise);

nvars = 1;
lb = 0;
ub = 1;
options = optimoptions('particleswarm', 'SwarmSize',50, 'MaxIter', 10,
'Display','iter');
[alpha, fval] = particleswarm(fun, nvars, lb, ub, options)
```

APPENDIX M

Complete M File for Watermarking Process

```
function [Ia_watermarked, Ibr_decrypted, Ian_watermarked]...
    = watermarkingProcess(Ia_original, Ib_original, alpha, key, noise)

d = size(Ia_original,3);
%for each channel in original image and watermark
for c = 1:d
    % encrypt watermark
    Ib_encrypted(:,:,c) = encryption(Ib_original(:,:,c), key);

    % apply transform
    transformOutputA{c} = applyTransform(Ia_original(:,:,c));
    transformOutputB{c} = applyTransform(Ib_encrypted(:,:,c));

    Ia_transform(:,:,c) = transformOutputA{c}.It;
    Ib_transform(:,:,c) = transformOutputB{c}.It;

    %apply svd
    [Ua(:,:,c), Sa(:,:,c), Va(:,:,c)] = svd(Ia_transform(:,:,c));
    [Ub(:,:,c), Sb(:,:,c), Vb(:,:,c)] = svd(Ib_transform(:,:,c));

    %embed encrypted watermark
     Sa_embedded(:,:,c) = Sa(:,:,c) + alpha*Sb(:,:,c);

    %Rebuild the sub-bands using SVD
    Ia_rebuid(:,:,c) = Ua(:,:,c)*Sa_embedded(:,:,c)*Va(:,:,c)';

    %Apply inverse transform to get watermarked image
    Ia_watermarked(:,:,c) = applyInverseTransform(Ia_rebuid(:,:,c),
transformOutputA{c});

end

Ia_watermarked = uint8(Ia_watermarked);
% Figure; imshow(Ia_watermarked); title('Watermarked Image');

%  % add noise to watermarked image

if length(noise)>1
    Ian_watermarked = imnoise(Ia_watermarked,noise);
else
    Ian_watermarked = Ia_watermarked;
end

%  Figure; imshow(Ian_watermarked);
% title(['Watermarked Image with',blanks(1), noise, blanks(1), 'noise']);


 %Extraction Process
for c=1:d
```

```
    % apply transform
     transformOutputW{c} = applyTransform(Ian_watermarked(:,:,c));

     Iw_transform(:,:,c) = transformOutputW{c}.It;

     %apply svd
     [Uw(:,:,c), Sw(:,:,c), Vw(:,:,c)] = svd(Iw_transform(:,:,c));

     %recover encrypted watermark
     Sbr_encrypted(:,:,c) = (Sw(:,:,c) - Sa(:,:,c))/alpha;

     %Rebuild the sub-bands using SVD
      Ibr_rebuid(:,:,c) = Ub(:,:,c)*Sbr_encrypted(:,:,c)*Vb(:,:,c)';

     %Apply inverse transform to get watermarked image
     Ib_recovered(:,:,c) = applyInverseTransform(Ibr_rebuid(:,:,c),
transformOutputB{c});
     Ib_recovered(:,:,c) = uint8(real(Ib_recovered(:,:,c)));

     % decrypt recover watermark
     Ibr_decrypted(:,:,c) = decryption(Ib_recovered(:,:,c), key);
end

% Figure; imshow(Ibr_decrypted); title('Recovered Watermark Image');
end
```

APPENDIX N

Complete M File for Host Image Recovering Using Inverse DOST

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% idost2
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%
% this function reconstruct a 2-dimensional signal from its dost
% coefficients. It works using the idost on rows and columns.
%
function reconstructed_signal = idost2(dost_coefficients)

reconstructed_signal = idost(idost(dost_coefficients).').';

end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% idost
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%
% this function reconstruct a 1-dimensional signal from its dost
% coefficients.
%
function reconstructed_signal = idost(dost_coefficients)

if isrow(dost_coefficients)== 1
        dost_coefficients = dost_coefficients';
else
end

si = size(dost_coefficients);
rows_dost_coefficients = si(1);

% inizialize the output
reconstructed_signal = zeros(si);

% initialize a temporary output
temp_signal = reconstructed_signal;

% partition of the frequency space, see details in the
% band_width_partitioning function explanation below.
[number_of_freq_bands, band_widths] =
band_width_partitioning(rows_dost_coefficients);

counter = 0;
for ll = 1:number_of_freq_bands
    % choose the bandwidth you are interested in and call it
    % frequency_width_cutter
    frequency_width_cutter = band_widths(ll);
    % cut all the Fourier coefficients Fx in the frequency band
    % counter + 1: counter + frequency_width_cutter
    cut_x = dost_coefficients(counter + 1 : counter +
frequency_width_cutter, : );
```

```
    % perform the Fourier transform just on the selected frequency
    % band.
    % Notice that you have to pay attention on the length of the cut_Fx.
    % If it is just 1 we do not do anything, otherwise we take its
    % Fourier transform.
    if frequency_width_cutter == 1
     temp_signal(counter + 1 : counter + frequency_width_cutter,:) = cut_x;
    else
            temp_signal(counter + 1 : counter + frequency_width_cutter,:) =
Fourier(cut_x);
    end
    % update the starting position for the band
    counter = counter + frequency_width_cutter;
end
 % take the inverse Fourier transform on the whole temp_signal
reconstructed_signal = iFourier(temp_signal);

end
```

APPENDIX O

Complete M File for Application of Inverse Transformation

```
function Iw = applyInverseTransform(Ir, transformOutput)
% Idost = transformOutput.dost;

% cA1 = transformOutput.dwtL1.cA;
cH1 = transformOutput.dwtL1.cH;
cV1 = transformOutput.dwtL1.cV;
cD1 = transformOutput.dwtL1.cD;

% cA2 = transformOutput.dwtL2.cA;
cH2 = transformOutput.dwtL2.cH;
cV2 = transformOutput.dwtL2.cV;
cD2 = transformOutput.dwtL2.cD;

% cA3 = transformOutput.dwtL3.cA;
cH3 = transformOutput.dwtL3.cH;
cV3 = transformOutput.dwtL3.cV;
cD3 = transformOutput.dwtL3.cD;

cA3_r = Ir;
cA2_r = idwt2(cA3_r,cH3,cV3,cD3,'haar');
cA1_r = idwt2(cA2_r,cH2,cV2,cD2,'haar');
Idost_r = idwt2(cA1_r,cH1,cV1,cD1,'haar');

Iw = idost2(Idost_r);

% Iw = Idost_r;
end
```

APPENDIX P

Complete M File for Generating the watermarking simulation user interface

```
clc
clear
close all

% read original image and watermark
Ia_original = imread('lena.png');
Ib_original = imread('encrypt.png');

% Ib_original= imresize(Ib_original, 0.5);

Figure; imshow(Ia_original); title('Original Image');
Figure; imshow(Ib_original); title('Original Watermark Image');

% Generate key, alpha and noise
L = 64;
[M,N,~] = size(Ib_original);
key = generateKey(L, M, N);

alpha = 0.1208; %0.1208;

noise = 'speckle';          %Gaussian | salt & pepper | speckle

% Watermarking process
[Ia_watermarked, Ibr_decrypted, Ian_watermarked]...
    = watermarkingProcess(Ia_original, Ib_original, alpha, key, noise);

Figure; imshow(Ia_watermarked); title('Watermarked Image');

Figure; imshow(Ian_watermarked);
title(['Watermarked Image with',blanks(1), noise, blanks(1), 'noise']);

Figure; imshow(Ibr_decrypted); title('Recovered Watermark Image');

fitness = (corr2(rgb2gray(Ib_original), rgb2gray(Ibr_decrypted)) ...
    + corr2(rgb2gray(Ia_original), rgb2gray(Ia_watermarked))) / 2


% Calculate the PSNR for cover Image and watermarked image
display('Metrics for cover Image and watermarked image')
[peaksnr, snr] = psnr(rgb2gray(Ia_original), rgb2gray(Ia_watermarked));
fprintf('\n The Peak-SNR value is %0.4f', peaksnr);
fprintf('\n The SNR value is %0.4f \n', snr);

display('Metrics for the embedded watermark and extracted')
% Calculate correlation coefficient
r = corr2(rgb2gray(Ib_original), rgb2gray(Ibr_decrypted));
fprintf('\n The correlation coefficient value is %0.4f', r);

% Calculate the PSNR.
```

```
[peaksnr, snr] = psnr(rgb2gray(Ibr_decrypted), rgb2gray(Ib_original));
fprintf('\n The Peak-SNR value is %0.4f', peaksnr);
fprintf('\n The SNR value is %0.4f \n', snr);

% Calculate the global SSIM value for the image and local SSIM values for
each pixel.
[ssimval, sSSIMap] = ssim(rgb2gray(Ibr_decrypted),rgb2gray(Ib_original));
fprintf('The SSIM value is %0.4f.\n',ssimval);
```

APPENDIX Q

Summary of results obtained for the various Attack scenarios

Table 4.1: Summary of Results of Developed Watermarking Technique (Under optimal scale factor 0.1208)

	Cover Image	Watermark	Attack	PSNR (dB)	NCC	SSIM
1	Lena	Mandril	No Attack	47.2805	0.9804	0.9998
2	Lena	Mandril	Gaussian	45.4202	0.9147	0.9564
3	Lena	Mandril	Salt and Pepper	46.4406	0.7254	0.8626
4	Lena	Mandril	Speckle	45.5727	0.8588	0.9293

Table 4.2: Summary of Results of Developed Watermarking Technique based on Encrypted Watermark (under Optimal Scale Factor of 0.1208)

s/n	Cover Image	Watermark	Attack	PSNR (dB)	NCC	SSIM
1	Lena	Mandril	No Attack	49.2752	0.9806	1
2	Lena	Mandril	Gaussian	46.8875	0.8846	0.9422
3	Lena	Mandril	Salt and Pepper	46.4406	0.8010	0.9003
4	Lena	Mandril	Speckle	46.3648	0.8863	0.9293

Table 4.3: Summary of Results of Developed Watermarking Technique (Manual determination of scale factor of 0.0121)

s/n	Cover Image	Watermark	Attack	PSNR (dB)	NCC	SSIM
1	Lena	Mandril	No Attack	79.6917	0.9191	0.9595
2	Lena	Mandril	Gaussian	64.8475	0.3289	0.1584
3	Lena	Mandril	Salt and Pepper	56.8566	0.1105	0.0759
4	Lena	Mandril	Speckle	60.1784	0.1636	0.1115

APPENDIX R

Summary of results obtained of Optimal Scaling Factor under different Attack Scenarios

Table 4.4: Summary of results of Developed Technique using Optimal Scale factor values obtained under various Attacks

s/n	Cover Image	Watermark Image	Attacks	Alpha (α)	PSNR(dB)	NCC	SSIM
1	Lena	Mandril	No	0.2214	65.6820	0.9999	0.9998
2	Lena	Mandril	Gaussian	0.4362	46.9152	0.9842	0.9739
3	Lena	Mandril	Salt and Pepper	1	43.6528	0.9582	0.9557
4	Lena	Mandril	Speckle	0.3708	41.3768	0.9688	0.9404
5	Lena	Mandril	Rotate at 30 degree	1	42.9168	0.8877	0.7968
6	Lena	Mandril	Rotate at 20 degree	1	43.8328	0.8681	0.7582
7	Lena	Mandril	Crop	0.3746	43.2816	0.9631	0.8096

Table 4.5: Summary of results of Developed Technique using Optimal Scale factor values obtained under Different Attacks

s/n	Cover Image	Watermark Image	Attacks	Alpha (α)	PSNR(dB)	NCC	SSIM
1	Pepper	Nepal Logo	No	0.1278	66.7556	0.9999	0.9999
2	Pepper	Nepal Logo	Gaussian	0.1183	48.2791	0.9790	0.9043
3	Pepper	Nepal Logo	Salt and Pepper	1	46.3012	0.9600	0.9230
4	Pepper	Nepal Logo	Speckle	1	43.3887	0.9596	0.8204
5	Pepper	Nepal Logo	Rotate at 45 degree	0.2478	42.5491	0.9084	0.5116
6	Pepper	Nepal Logo	Rotate at 5 degree	0.1308	42.8439	0.9300	0.4901
7	Pepper	Nepal Logo	Rotate at 90 Degree	1	43.2148	0.9184	0.7126
8	Pepper	Nepal Logo	Crop	1	43.0859	0.9643	0.4183

Table 4.6: Summary of results of Developed Technique using Encryption key and Optimal Scale factor values obtained under various Attacks

s/n	Cover Image	Watermark Image	Attacks	Alpha (α)	PSNR (dB)	NCC	SSIM
1	Pepper	Nepal Logo	No	0.1134	71.8747	1	1
2	Pepper	Nepal Logo	Gaussian	0.2283	50.2752	1	1
3	Pepper	Nepal Logo	Salt and Pepper	1	47.7293	1	1
4	Pepper	Nepal Logo	Speckle	1	45.6404	1	1
5	Pepper	Nepal Logo	Rotate 45 degree	0.2478	46.8626	0.9997	0.9998
6	Pepper	Nepal Logo	Rotate 5 degree	0.1408	44.6045	1	0.9996
7	Pepper	Nepal Logo	Rotate 90 degree	1	47.9442	1	0.9999
8	Pepper	Nepal Logo	Crop	1	46.4067	1	0.9987

Table 4.7: Summary of Results based on the data Published in the Work of Bajracharya & Koju (2017) using the Developed Algorithm

s/n	Cover Image	Watermark Image	Attacks	Alpha (α)	PSNR (dB)	NCC	SSIM
1	Pepper	Nepal Logo	No	0.1324	76.8139	1	1
2	Pepper	Nepal Logo	Gaussian	0.2283	71.8747	1	1
3	Pepper	Nepal Logo	Salt and Pepper	1	66.2485	1	1
4	Pepper	Nepal Logo	Rotate 45 degree	0.2478	61.0996	0.9997	0.9998
5	Pepper	Nepal Logo	Rotate 5 degree	0.1408	61.2046	1	0.9996
6	Pepper	Nepal Logo	Rotate 90 degree	1	63.4722	1	0.9999
7	Pepper	Nepal Logo	Crop	1	62.2485	1	0.9987

APPENDIX S

Comparison of the random bits generated by Alice, Alice randomly chooses polarization basis, transmitted Qubits by Alice and Bob measures Qubits

Random Bits Generated by Alice for Transmission

1000011111010000000001011101010001111000010011010111010101010001000011 01

111110101010011001011001011100000110111101010001000111111001100010000010

010000011001001110011011001101011110000110010110111100010110001010001001

011110101001010011101111001110100000011100110111010110010001100101001111

110001100111010000110110101010010010101110101000110000111001001011000110

001000001001010101110000011110100100000101001001111001110011001001001 0111

01100011001110111110111011111000111111000011100010000001010110101111

Alice Randomly Chooses Polarization Basis

+xxx+x++x+xx++xx+xx+x+xxx++++++x+xx+xx+xxxx+++x+x+xx++++x+xxx+x++x+x

xx+++x+++x+x+x+x++++xxxxxxx+x+++xx++x+++xx+x+xxxx++++x+x+x+++x++x++

xx++x+x+x+++x++xx+++++xx+x+xx++xx++x+x+++xx++xxxx+xxxxx+xx+++x++++xx

+xx+++x+x+x+x+x+xx+++x+++xx+++xx++x++x+x+xxx++++xxxx++xxxxx++xxx+++x

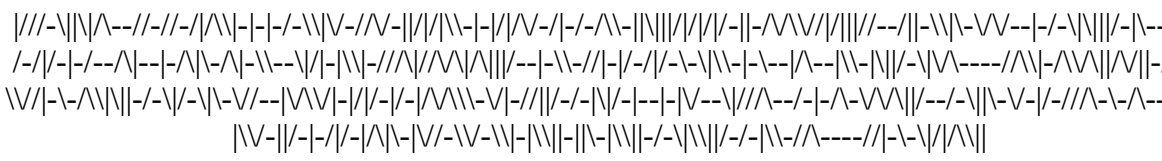
++x+xxxx++x+xxx+x+++x+x+x+x+x+xxx+++xxxxx+++x+x++x++xxxxxx+xx++xx++x

+x++x+x+++++++xx++x+xxxx++x+++xx+xxxxx++x++x+x++x+xx++x+xxxx+x+xx+++

x++x++xxx+++x+++x+x++xx+x++xxx+xxx+xx+++xx+++++x++xx+++x+x+xx++x+x+

+xx+xxx++++xx++x+x+x+xxx++

Transmitted Qubits by Alice



Bob Measures Qubits

