

ON SECURITY OF TWO DIMENSIONAL DATA (IMAGE DATA & VIDEO DATA)

DEEP CHANDRA MISHRA



DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
JANUARY 2018

ON SECURITY OF TWO DIMENSIONAL DATA (IMAGE DATA & VIDEO DATA)

by
DEEP CHANDRA MISHRA

Department of Mathematics

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the



Indian Institute of Technology Delhi
January 2018

*Dedicated to Lord
Ganpati*



Certificate

*This is to certify that the thesis entitled of “**On Security of Two Dimensional Data (Image Data & Video Data)**” being submitted by **Mr. Deep Chandra Mishra** to the Indian Institute of Technology Delhi for the award of the degree of **Doctor of Philosophy** is a record of bona fide research work carried out by him under my guidance and supervision. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.*

The results contained in this thesis have not been submitted elsewhere, either in part or full, for the award of any degree or diploma.

Dr. R. K. Sharma

Professor

Department of Mathematics

Indian Institute of Technology Delhi

Acknowledgements

Firstly, my sincere thanks to Lord Ganpati and Maa Saraswati for giving me the strength and unlimited mercies to complete this work.

I would like to express my sincere gratitude to my supervisor Dr. R. K. Sharma, Professor and former Head, Department of Mathematics, Indian Institute of Technology Delhi, for his overwhelming support and guidance during my candidature. He has always encouraged and given continuous support during the work of my thesis. In spite of his busy schedule. He allowed me wide freedom in my choice of research area and guided me to study the same. I am fortunate that Prof. Sharma introduced me to such an interesting and challenging topic for the thesis. I could not have imagined having a better advisor and mentor for my Ph.D study. I am thankful to God for providing me Prof. R. K. Sharma Sir as my supervisor.

I am grateful to Prof. S. Dharmaraja, Head, Department of Mathematics, IIT-Delhi, for providing me necessary facilities for the completion of this work. I would like to express my deep sense of gratitude to the SRC members, Dr. Aparna Mehra, Department of Mathematics, IIT-Delhi, Dr. Ritumoni Sarma, Department of Mathematics, IIT-Delhi and Prof. M. P. Gupta, Head, DMS, IIT-Delhi, for their encouragement and invaluable suggestions. I am also thankful for my research collaborator Prof. M. Hanmadlu, Department of Electrical Engineering, IIT-Delhi who helped me as a part of this research work. I express my gratitude to all the faculty members

of the Department of Mathematics, IIT-Delhi. I am also thankful to Prof. Kumkum Rautela, Principal, Govt. P. G. College Lansdowne, Uttarakhand, for supporting me to manage my job along with in thesis completion.

I express my extreme indebtedness to my parents, brothers, and friends for the patience and encouragement shown by them during this period, to whom I dedicate this thesis.

Lastly, I would like to extend my gratitude to CSIR, New Delhi, Govt. of India, Under Grant No. F. No. 09/086(1068)/2010-EMR-I for providing financial support.

Deep Chandra Mishra

Abstract

In this world of internet which is full of eavesdropping, modification of private information, safety of information is a major concern. Secure and appropriate transmission of two dimensional digital data (Image Data and Video Data) over open networks is an important and valuable agenda for research work in the area of security. In this thesis, we have presented various approaches for the security system of color image data and video data for appropriate and secured transmission in the open network without any loss of information over the geometrical domain, co-ordinate domain and frequency domain. The existing techniques discuss the security of image data or video data on the basis of keys only (which provides only one layer of security for image data or video data) in the geometrical domain, co-ordinate domain or frequency domain, but in this thesis we have presented multi-layers of security for RGB image data and video data in all domains (geometrical, co-ordinate and frequency domains). In this thesis, keys and arrangement of parameters are imperative for the correct decryption process. If an attacker knows about all possible correct keys but is not aware of the correct arrangement of the used parameters of geometrical domain, co-ordinate domain and frequency domain then he/she cannot recover the original information (original RGB image data or video data) from the encrypted data or ciphered data. The robustness of the presented approaches, not only depends on the possible correct keys, but also depends on the correct arrangement of parameters.

Some chapters of the thesis provide security of image data and video data by the symmetric-key-cryptosystem, while some chapters provide security of data through public-key-cryptosystem. Thus, the work in this thesis focuses on the security of RGB image data and video data using:

- (i) Symmetric-key-security system, and*
- (ii) Public-key-security system.*

Experimental results and security analysis on the standard examples of the presented security system are given for the justification of the robustness of the proposed cryptosystems for RGB images and videos. These methods or algorithms will be of potential use in digital RGB image processing and for secured and appropriate transmission of two dimensional data like image data and video data from one end (Sender) to the other end (Receiver).

सार

इंटरनेट की इस दुनिया में जो छिपी हुई है, निजी जानकारी के रूपांतरण कथन, जानकारी की सुरक्षा एक प्रमुख चिंता का विषय है। खुले नेटवर्क पर दो आयामी डिजिटल डेटा (छवि डेटा और वीडियो डेटा) के सुरक्षित और उपयुक्त संचरण सुरक्षा के क्षेत्र में अनुसंधान कार्य के लिए एक महत्वपूर्ण और मूल्यवान एजेंडा है। इस थीसिस में, हमने विभिन्न तरीकों को प्रस्तुत किया है रंग छवि डेटा और वीडियो डेटा की सुरक्षा व्यवस्था को खुली नेटवर्क में उचित और सुरक्षित प्रसारण के लिए बिना किसी भी सूचना के नुकसान के ज्यामितीय डोमेन, समन्वय डोमेन और आवृत्ति डोमेन पर। मौजूदा तकनीक केवल चाबियाँ के आधार पर छवि डेटा या वीडियो डेटा की सुरक्षा पर चर्चा करते हैं (जो छवि डेटा या वीडियो डेटा के लिए सुरक्षा का केवल एक स्तर प्रदान करता है) ज्यामितीय डोमेन, समन्वय डोमेन या आवृत्ति डोमेन में, लेकिन इस थीसिस में हमने आरजीबी छवि डेटा और वीडियो डेटा के लिए सुरक्षा की बहु-परतें प्रस्तुत की हैं सभी डोमेन में (ज्यामितीय, समन्वय और आवृत्ति डोमेन में)। इस थीसिस में, सही डिक्रिप्शन प्रक्रिया के लिए चाबियाँ और पैरामीटर आवश्यक हैं। यदि कोई हमलावर सभी संभव सही कुंजी के बारे में जानता है लेकिन ज्यामितीय डोमेन के उपयोग किए गए पैरामीटर, समन्वय डोमेन और आवृत्ति डोमेन की सही व्यवस्था से अवगत नहीं है तो वह एन्क्रिप्टेड डेटा या साइफर्ड डेटा से मूल जानकारी (मूल आरजीबी छवि डेटा या वीडियो डेटा) को पुनर्प्राप्त नहीं कर सकता। प्रस्तुत दृष्टिकोणों की मजबूती, न केवल संभव सही कुंजी पर निर्भर करता है, बल्कि पैरामीटर की सही व्यवस्था पर भी निर्भर करता है। थीसिस के कुछ अध्याय छवि डेटा और वीडियो डेटा की सुरक्षा सममित-कुंजी-क्रिप्टो सिस्टम से प्रदान करते हैं, जबकि कुछ अध्याय सार्वजनिक कुंजी-क्रिप्टोसिस्टम के माध्यम से डेटा की सुरक्षा प्रदान करते हैं। इस प्रकार, इस थीसिस में कार्य केंद्रित है आरजीबी छवि डेटा और वीडियो डेटा की सुरक्षा का उपयोग करते हुए:

- (i) सममित-कुंजी-सुरक्षा प्रणाली, और
- (ii) सार्वजनिक-कुंजी-सुरक्षा प्रणाली।

मानक उदाहरणों पर प्रायोगिक परिणाम और सुरक्षा विश्लेषण प्रस्तुत सुरक्षा प्रणाली के आरजीबी छवियों और वीडियो के लिए प्रस्तावित क्रिप्टो तंत्रों की मजबूती के औचित्य कथन के लिए दिए गए हैं। संभवतः इन पद्धतियों या एल्गोरिदम का उपयोग डिजिटल आरजीबी इमेज प्रोसेसिंग में, छवि डेटा और वीडियो डेटा जैसे दो आयामी डेटा के सुरक्षित और उचित संचरण एक सिरे से (प्रेषक) दूसरे छोर (रिसीवर) तक के लिए होंगे।

Contents

	i
Certificate	iii
Acknowledgements	v
Abstract	vii
List of Figures	xv
List of Tables	xxi
1 Introduction	1
1.0.1 Notations	1
1.0.2 Definitions	2
1.0.3 Introduction of Security System	4
2 An Approach for Security of Color Image Data	13
2.1 Introduction	14
2.2 Mathematical Formulation of the Proposed Security System	15
2.2.1 Random Matrix Shift Cipher	15

2.2.2	Two Dimensional Discrete Fractional Fourier Transform for Data Security	17
2.3	Procedure of Encryption and Decryption	20
2.4	Robustness Analysis	36
2.4.1	Histogram Analysis	36
2.4.2	Mean Square Error, NPCR, and UACI Analysis	40
2.5	Comparison with Existing Methods	42
2.6	Conclusion	45
3	RGB Image Encryption and Decryption by Random Matrix Affine Cipher and Discrete Wavelet Transform	47
3.1	Introduction	48
3.2	Random Matrix Affine Cipher and Discrete Wavelet Transform	50
3.3	Process of Encryption and Decryption using RMAC associated with DWT	54
3.4	Demonstration of the Procedure	56
3.5	Security Analysis	59
3.5.1	Key Sensitivity Analysis	59
3.5.2	Robustness Against Known-plaintext Attack and Chosen-ciphertext Attack	60
3.5.3	Appropriateness for Sparse and Circular Image Data	61
3.5.4	Entropy Analysis	62
3.5.5	Robustness of the encrypted image at 50% and 75% pixels when cropped	64
3.5.6	Histogram Analysis	65
3.5.7	Mean Square Error, NPCR, and UACI Analysis	68
3.6	Comparison Analysis	71
3.7	Conclusion	74

4 Security of RGB Image using Hill Cipher associated with Two Dimensional Discrete Wavelet Transform	75
4.1 Introduction	76
4.1.1 Organization of the Chapter	79
4.2 Two-Dimensional Discrete Wavelet Transform and Random Hill Cipher	79
4.3 Procedure and Results of the Proposed Cryptosystem	84
4.4 Sensitivity Analysis	88
4.5 Statistical Analysis	90
4.5.1 Mean Square Error, Peak Signal-to-Noise Ratio and Correlation Analysis	90
4.5.2 Pixel Intensity Distributions at Horizontal, Vertical, and Diagonal Direction	94
4.5.3 Histogram Analysis of RGB Image Data	99
4.6 Security Analysis of the Proposed Cryptosystem	103
4.6.1 Key's Space Analysis	104
4.6.2 Robustness Against Cryptanalysis	104
4.6.3 Encrypted RGB Image Data Occluded with 25% and 50% Pixels	106
4.6.4 Entropy, NPCR, and UAIC Analysis	109
4.7 Comparison of the Proposed Technique with Existing Methods	110
4.8 Conclusion	112
5 Multi-layer Security for RGB Image Data by Affine Hill Cipher over $SL_n(F_q)$ and $M_n(F_q)$ Domains with Arnold Transform	115
5.1 Introduction	116
5.1.1 Organization of the Chapter	118
5.2 Affine Hill Cipher Combined with Arnold Transform for RGB Images	119
5.3 Encryption and Decryption Processes	122
5.4 Demonstration of the Procedure	124
5.5 Security Analysis of the Presented Technique	133

5.5.1	Key Space of the Cryptosystem	133
5.5.2	Sensitivity Analysis of the Presented Approach	134
5.5.3	Robustness of the Approach when Encrypted RGB Image Data Occluded	135
5.6	Statistical Analysis	138
5.6.1	Histogram Analysis of RGB Image Data	138
5.6.2	Mean Square Error, Peak Signal-to-Noise Ratio and Correla- tion Analysis	140
5.6.3	Pixels Intensity Distributions at Horizontal, Vertical and Di- agonal pixels	143
5.6.4	Entropy, NPCR, and UAIC Analysis	148
5.7	Comparison Analysis	150
5.8	Conclusion	152
6	Multi-layer Security for Color Image based on Chaotic System com- bined with RP2DFrFT and Arnold Transform	155
6.1	Introduction	156
6.1.1	Organization of the Chapter	158
6.2	Mathematical Formulation of the Presented Cryptosystem	158
6.2.1	Chaotic Map and Cyclic Shift	158
6.2.2	Two Dimension Discrete Fractional Fourier Transform	160
6.2.3	Two Dimension Arnold Transform for Image Data	163
6.3	Procedures of Encryption and Decryption	164
6.4	Results of the Presented Cryptosystem	166
6.4.1	Results of the Cryptosystem for Baboon Color Image Data	167
6.4.2	Results of the Cryptosystem for Lena Color Image Data	168
6.5	Security Analysis	170
6.5.1	Sensitivity Analysis for Baboon Color Image Data	170

6.5.2	Sensitivity Analysis of the Proposed Cryptosystem for Lena Color Image Data	174
6.6	Statistical Analysis	175
6.6.1	Histogram Analysis of Color Image Data	175
6.6.2	Mean Square Error, Peak Signal-to-Noise Ratio and Correlation Analysis	183
6.6.3	Entropy Analysis	187
6.6.4	Cropping Analysis	188
6.6.5	Distributions in Pixels Intensity at Horizontal, Vertical, and Diagonal directions	190
6.7	Conclusion	198
7	Asymmetric-key Security System for RGB Images	201
7.1	Introduction	202
7.1.1	Organization of the Chapter	204
7.2	Asymmetric-key Security-system for Images	205
7.2.1	Public-key Algorithm (RSA) for RGB Image Data	205
7.2.2	Reality Preserving Fractional Fourier Transform	207
7.3	Encoding and Decoding of RGB Image	207
7.4	Sensitivity Analysis of the Presented Algorithm	214
7.5	Statistical Analysis	216
7.5.1	Histogram Analysis of Color Image Data	216
7.5.2	Mean Square Error, Peak Signal-to-Noise Ratio and Correlation Analysis	219
7.5.3	Entropy, NPCR, and UAIC Analysis	221
7.5.4	Pixels Intensity in Horizontal, Vertical, and Diagonal Directions	221
7.6	Comparison Analysis	227
7.7	Conclusion	230

8	Secure Cryptosystem for Color Video Data	231
8.1	Introduction	232
8.1.1	Organization of the Chapter	234
8.2	Matrix Affine Cipher and 2D-DWT for Security of Video Data	235
8.2.1	Matrix Affine Cipher for Security of Video Data	235
8.2.2	Two-Dimensional DWT for Security of Video Data	236
8.3	Encoding and Decoding of color Video	239
8.4	Sensitivity Analysis of the Proposed Approach	245
8.5	Statistical Analysis	246
8.5.1	Histogram Analysis of RGB Video Data	246
8.5.2	Mean Square Error, Peak Signal-to-Noise Ratio and Correlation Analysis of RGB Video	250
8.5.3	Entropy, NPCR, and UAIC Analysis	253
8.5.4	Pixel Intensity Distributions of Two Neighboring Pixels at Horizontal, Vertical and Diagonal pixels of the Frame	256
8.6	Comparison with Existing Techniques	259
8.7	Conclusion	263
9	Conclusion and Future Directions	265
9.1	Conclusion	265
9.2	Future Directions	268
	Bibliography	269
	BIO-DATA	277

List of Figures

1.1	Basic model of a cryptosystem or a security system.	5
1.2	Procedure of transmission of secured data and keys in a symmetric-key-cryptosystem.	7
1.3	Procedure of transmission of encrypted data and confidential information through an asymmetric-key-cryptosystem.	8
2.1	Procedure for RMSC on color image data.	16
2.2	Encoding procedure (from left to right).	21
2.3	Decoding procedure (from left to right).	22
2.4	Encoding and decoding results for Lena image	23
2.5	Encoding and decoding results for Barbara image	23
2.6	Histogram analysis	37
2.7	Histogram analysis	38
2.8	Histogram analysis	39
2.9	Histogram analysis	40
2.10	Comparison analysis	42
2.11	Comparison analysis	43
2.12	Comparison analysis	43
2.13	Comparison analysis	44

2.14	Comparison analysis	44
2.15	Comparison analysis	45
3.1	Structure of random matrix affine cipher on an RGB image of size $n \times m$	52
3.2	Tree structure of wavelet decomposition at different levels.	53
3.3	Encryption procedure for color image Data.	55
3.4	Decryption process for an RGB image.	56
3.5	Encryption and decryption results	57
3.6	Results for sparse image	61
3.7	Results for circular image	61
3.8	Cropping results	64
3.9	Histogram analysis	66
3.10	Histogram analysis	67
3.11	Histogram analysis	68
3.12	Comparison analysis	71
3.13	Comparison analysis	72
3.14	Comparison analysis	72
3.15	Comparison analysis	73
4.1	Transmission of secure data though an insecure network.	78
4.2	Tree structure of wavelet decomposition in forward direction.	81
4.3	Tree structure of wavelet reconstruction in backward direction.	82
4.4	Process of block creation	83
4.5	Encoding procedure for each channel of RGB image data.	85
4.6	Decoding procedure for each channel of RGB image data.	86
4.7	Encryption and decryption results	87
4.8	Results for sparse images	88
4.9	Results for circular images	88

4.10 Sensitivity analysis	89
4.11 Pixel intensity distribution analysis	95
4.12 Pixel intensity distribution analysis	96
4.13 Pixel intensity distribution analysis	97
4.14 Pixel intensity distribution analysis	98
4.15 Histogram analysis	100
4.16 Histogram analysis	101
4.17 Histogram analysis	102
4.18 Histogram analysis	103
4.19 Robustness against cryptanalysis	105
4.20 Data occluded with 25% pixels	107
4.21 Data occluded with 25% pixels	107
4.22 Data occluded with 50% pixels	108
4.23 Data occluded with 50% pixels	108
5.1 Procedure of transmission of information though open network.	117
5.2 Procedure for creation of a block matrix	121
5.3 Encoding procedure for each component of RGB image data.	123
5.4 Decoding procedure for each component of RGB image data.	124
5.5 Experimental results on Lena image	126
5.6 Sensitivity analysis	135
5.7 Encrypted RGB image data occluded	136
5.8 Encrypted RGB image data occluded	136
5.9 Encrypted RGB image data occluded	137
5.10 Histogram analysis	139
5.11 Histogram analysis	140
5.12 Pixels intensity distribution	144
5.13 Pixels intensity distribution	145
5.14 Pixels intensity distribution	146

5.15	Pixels intensity distribution	147
5.16	Comparison analysis	150
5.17	Comparison analysis	151
5.18	Comparison analysis	151
6.1	Procedure of transmission of information though open network.	157
6.2	Encryption procedure for each channel of color image.	165
6.3	Decryption procedure for each channel of color image.	166
6.4	Encryption and decryption results for Baboon color image	167
6.5	Encryption and decryption results for Lena color image	169
6.6	Sensitivity analysis for Baboon color image	171
6.7	Sensitivity analysis for Baboon color image	172
6.8	Sensitivity analysis for Baboon color image	173
6.9	Sensitivity analysis for Baboon color image	174
6.10	Sensitivity analysis for Lena color image	174
6.11	Histogram analysis	176
6.12	Histogram analysis	177
6.13	Histogram analysis	178
6.14	Histogram analysis	179
6.15	Histogram analysis	180
6.16	Histogram analysis	181
6.17	Histogram analysis	182
6.18	Cropping analysis	189
6.19	Cropping analysis	190
6.20	Pixels intensity for Baboon color image	191
6.21	Pixels intensity for Baboon color image	192
6.22	Pixels intensity for Baboon color image	193
6.23	Pixels intensity for Baboon color image	194
6.24	Pixels intensity for Lena color image	196

6.25	Pixels intensity for Lena color image	197
7.1	Process of transmission of encrypted color images through insecure networks.	204
7.2	Encryption and decryption process for RGB images of the presented cryptosystem.	208
7.3	Encoding and decoding results	210
7.4	Sensitivity analysis	215
7.5	Histogram analysis	217
7.6	Histogram analysis	218
7.7	Histogram analysis	219
7.8	Pixels intensity distribution	223
7.9	Pixels intensity distribution	224
7.10	Pixels intensity distribution	225
7.11	Pixels intensity distribution	226
7.12	Pixels intensity distribution	227
7.13	Comparison analysis	228
7.14	Comparison analysis	228
8.1	Procedure of matrix affine cipher for RGB video data.	235
8.2	Structure of DWT for RGB video data at forward direction.	237
8.3	Structure of inverse DWT for RGB video data.	238
8.4	Original frames of Carphone.mpeg video	240
8.5	Process of encoding for color video data.	241
8.6	Encrypted frames of Carphone.mpeg video	242
8.7	Process of decoding for color video data.	243
8.8	Decrypted frames of Carphone.mpeg video	244
8.9	Sensitivity analysis	246
8.10	Histogram analysis	247

8.11 Histogram analysis	248
8.12 Histogram analysis	249
8.13 Pixels intensity distribution	257
8.14 Pixels intensity distribution	258
8.15 Comparison analysis	260
8.16 Comparison analysis	261
8.17 Comparison analysis	262
8.18 Comparison analysis	262
8.19 Comparison analysis	263

List of Tables

2.1	The eigenvalues assignment rule for DFrFT kernel matrix	19
2.2	NPCR and UAIC results.	41
3.1	Entropy values for red, green, and blue component of RGB image data.	63
3.2	Mean Square Error of encrypted image (Fig. 3.5(b)).	69
3.3	Mean Square Error of correctly decrypted image (Fig. 3.5(c)).	69
3.4	Mean Square Error value of Fig. 3.5(f).	69
3.5	Mean Square Error of encrypted image Figs. 3.6(b) and 3.7(b).	70
3.6	Mean Square Error of decrypted image Figs. 3.6(c) and 3.7(c).	70
3.7	The Mean Square Error values of the Red, Green, and Blue channels of Fig. 3.8.	70
3.8	NPCR and UAIC results.	71
4.1	Statistical analysis between Fig. 4.7(c) and Fig. 4.7(a).	92
4.2	Statistical analysis between Fig. 4.7(d) and Fig. 4.7(a).	92
4.3	Statistical analysis between Fig. 4.7(e) and Fig. 4.7(a).	92
4.4	Statistical analysis between Fig. 4.7(f) and Fig. 4.7(a).	92
4.5	Statistical analysis between Fig. 4.8(c) and Fig. 4.8(a).	92
4.6	Statistical analysis between Fig. 4.9(c) and Fig. 4.9(a).	93
4.7	Statistical analysis between Fig. 4.10(b) and Fig. 4.7(a).	93

4.8	Statistical analysis between Fig. 4.10(c) and Fig. 4.7(a).	93
4.9	Statistical analysis between Fig. 4.10(d) and Fig. 4.7(a).	93
4.10	Statistical analysis between Fig. 4.10(e) and Fig. 4.7(a).	93
4.11	Statistical analysis between Fig. 4.10(f) and Fig. 4.7(a).	94
4.12	Entropy values of red, green, and blue component of RGB image data.	110
4.13	NPCR and UAIC results.	110
5.1	Statistical analysis between Fig. 5.5(b) and Fig. 5.5(a).	141
5.2	Statistical analysis between Fig. 5.5(c) and Fig. 5.5(a).	141
5.3	Statistical analysis between Fig. 5.5(d) and Fig. 5.5(a).	142
5.4	Statistical analysis between Fig. 5.5(e) and Fig. 5.5(a).	142
5.5	Statistical analysis between Fig. 5.5(f) and Fig. 5.5(a).	142
5.6	Statistical analysis between Fig. 5.6(b) and Fig. 5.5(a).	142
5.7	Statistical analysis between Fig. 5.6(c) and Fig. 5.5(a).	142
5.8	Entropy values of red, green and blue component of RGB image data Fig. 5.5.	148
5.9	Entropy values of red, green and blue component of RGB image data Fig. 5.6.	148
5.10	Entropy values of red, green and blue component of RGB image data Fig. 5.7.	149
5.11	Entropy values of red, green, and blue component of RGB image data Fig. 5.8.	149
5.12	Entropy values of red, green, and blue component of RGB image data Fig. 5.9.	149
5.13	NPCR and UAIC results.	150
6.1	Statistical analysis between Fig. 6.4(b) and Fig. 6.4(a).	184
6.2	Statistical analysis between Fig. 6.4(c) and Fig. 6.4(a).	184
6.3	Statistical analysis between Fig. 6.4(d) and Fig. 6.4(a).	184

6.4	Statistical analysis between Fig. 6.4(f) and Fig. 6.4(a).	184
6.5	Statistical analysis between Fig. 6.4(g) and Fig. 6.4(a).	184
6.6	Statistical analysis between Fig. 6.4(h) and Fig. 6.4(a).	185
6.7	Statistical analysis between Fig. 6.6(d) and Fig. 6.4(a).	185
6.8	Statistical analysis between Fig. 6.7(d) and Fig. 6.4(a).	185
6.9	Statistical analysis between Fig. 6.8(d) and Fig. 6.4(a).	185
6.10	Statistical analysis between Fig. 6.9(d) and Fig. 6.4(a).	185
6.11	Statistical analysis between Fig. 6.5(b) and Fig. 6.5(a).	186
6.12	Statistical analysis between Fig. 6.5(c) and Fig. 6.5(a).	186
6.13	Statistical analysis between Fig. 6.5(d) and Fig. 6.5(a).	186
6.14	Statistical analysis between Fig. 6.5(f) and Fig. 6.5(a).	186
6.15	Statistical analysis between Fig. 6.5(g) and Fig. 6.5(a).	186
6.16	Statistical analysis between Fig. 6.5(h) and Fig. 6.5(a).	187
6.17	Statistical analysis between Fig. 6.10(d) and Fig. 6.4(a).	187
6.18	Entropy values for red, green and blue components of RGB image data Fig. 6.4.	188
6.19	Entropy values for red, green and blue components of RGB image data Fig. 6.5.	188
7.1	Error analysis of Fig. 7.3(b) with respect to Fig. 7.3(a).	219
7.2	Error analysis of Fig. 7.3(c) with respect to Fig. 7.3(a).	220
7.3	Error analysis of Fig. 7.3(d) with respect to Fig. 7.3(a).	220
7.4	Error analysis of Fig. 7.3(e) with respect to Fig. 7.3(a).	220
7.5	Error analysis of Fig. 7.4(b) with respect to Fig. 7.3(a).	220
7.6	Error analysis of Fig. 7.4(e) with respect to Fig. 7.3(a).	220
7.7	Entropy values of red, green and blue component of RGB image data Fig. 7.3.	221
7.8	Entropy values of red, green and blue component of RGB image data Fig. 7.4.	221

7.9	NPCR and UAIC results.	222
8.1	Analysis of Fig. 8.6(a) with respect to Fig. 8.4(a).	250
8.2	Analysis of Fig. 8.6(b) with respect to Fig. 8.4(b).	251
8.3	Analysis of Fig. 8.6(c) with respect to Fig. 8.4(c).	251
8.4	Analysis of Fig. 8.6(j) with respect to Fig. 8.4(j).	251
8.5	Analysis of Fig. 8.6(k) with respect to Fig. 8.4(k).	251
8.6	Analysis of Fig. 8.6(l) with respect to Fig. 8.4(l).	251
8.7	Analysis of Fig. 8.8(a) with respect to Fig. 8.4(a).	252
8.8	Analysis of between Fig. 8.8(b) with respect to Fig. 8.4(b).	252
8.9	Analysis of Fig. 8.8(c) with respect to Fig. 8.4(c).	252
8.10	Analysis of Fig. 8.8(j) with respect to Fig. 8.4(j).	252
8.11	Analysis of Fig. 8.8(k) with respect to Fig. 8.4(k).	252
8.12	Analysis of Fig. 8.8(l) with respect to Fig. 8.4(l).	253
8.13	Entropy values for red, green and blue components of Fig. 8.4.	254
8.14	Entropy values for red, green and blue components of Fig. 8.4.	254
8.15	Entropy values for red, green and blue components of Fig. 8.6.	254
8.16	Entropy values for red, green and blue components of Fig. 8.6.	255
8.17	Entropy values for red, green and blue components of Fig. 8.8.	255
8.18	Entropy values for red, green and blue components Fig. 8.8.	255
8.19	NPCR and UAIC results.	256