Contents

Contents	Page No.
List of Abbreviations	VII
List of Symbols	IX
List of Notations	X
List of Figures	XI
List of Tables	XVIII
List of Algorithms	XXII
Chapter 1: Introduction	
1.1.Overview	1
1.2. CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart)	2
1.2.1. Text CAPTCHA	3
1.2.2. Audio CAPTCHA	3
1.2.3. Image CAPTCHA	3
1.2.4. Mathematical CAPTCHA	3
1.2.5. 3d CAPTCHA	3
1.2.6. Ad Injected CAPTCHA	4
1.2.7. Drag and Drop CAPTCHA	4
1.3. OTP (One Time Password)	4
1.4. Cryptography	5
1.4.1. Private Key Cryptography	7
1.4.2. Public Key Cryptography	7
1.4.3. Hash Functions	8
1.5. Different Number Types	8
1.5.1. Prime Numbers	8
1.5.2. Palindrome Numbers	9
1.5.3. Armstrong Number	9
1.5.4. Amicable Number	9
1.5.5. Perfect Number	10
1.6. Color Management and Pixel Structure of Digital Image	10
1.6.1. Color Models	10
1.6.2. Pixel Structure	11

1.7. Digital Watermarking	12
1.7.1. Visible Watermarking	13
1.7.2. Invisible Watermarking	13
1.8. Steganography	13
1.8.1. Applications and Comparison with Cryptography and Watermarking	14
1.8.2. Steganography Approaches on Data Set	14
1.8.3. Steganography Attacks	15
1.9. Problem Domain	15
1.10. Thesis Objective	16
1.11. Contributions of Thesis	16
1.12. Thesis Organization	18
1.13. Conclusion	21
Chapter 2: Early Work related to Current Research in User Authentication and Data Encryption	
2.1. Overview	22
2.2. Data Encryption	22
2.3. CAPTCHA based User Authentication	24
2.4. OTP based User Authentication	29
2.5. Text Encryption	35
2.6. Image Encryption	40
2.7. Steganography	44
2.8. Conclusion	50
Chapter 3: Performance Assessment Metrics	
3.1. Overview	51
3.2. Performance Assessment Matrices	51
3.2.1. Different Cryptographic Attacks	52
3.2.2. CrypTool	54
3.2.3. Triple DES	54
3.2.4. Advanced Encryption Standard	55
3.2.5. Serpent Algorithm	56
3.2.6. Blowfish Algorithm	57
3.2.7. Twofish Algorithm	57
3.2.8. Chi-Square Test	58
3.2.9. Degree of Freedom	59

3.2.10. Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE)	59
3.2.11. Structural Similarity Index Metric (SSIM)	60
3.2.12. Universal Image Quality Index	61
3.2.13. Bit Error Rate (BER)	62
3.2.14. Correlation Coefficient (CC)	63
3.2.15. Normalized Cross-Correlation (NCC)	64
3.3. Conclusion	64
Chapter 4: User Authentication Building Blocks	
4.1. Overview	65
4.2. CAPTCHA Code based on User Personal information and Likings (CCUPL)	66
4.2.1. Process of CAPTCHA Generation	68
4.2.2. Process of User Authentication	70
4.2.3. Implementation with Experiment Results	70
4.2.4. Security Analysis for CAPTCHA Code based on User Personal information and Likings (CCUPL)	77
4.3. User authentication scheme using Secret Value based on Randomize One Time Password (SVROTP)	81
4.3.1. Server Side OTP Formation	83
4.3.2. Final OTP Distribution	86
4.3.3. Generation of Secret Value and User Authentication	86
4.3.4. Implementation with Experiment Results	86
4.3.5. Security Analysis for SVROTP Scheme	93
4.4. User authentication scheme using Numeric and biometric Image based One Time Password (NIOTP)	95
4.4.1. Server Side OTP Generation	96
4.4.2. Numeric OTP and Image OTP Distribution	99
4.4.3. User End OTP Extraction and Authentication	99
4.4.4. Implementation with Experiment Results	99
4.4.5. Security Analysis for NIOTP Scheme	106
4.5. Measurement of Security over Cryptographic Attacks by SVROTP and NIOTP Schemes	107
4.6. Conclusion	110

Chapter 5: Text Encryption Building Blocks using Special Numbers with Alphabetic Group or Cipher Sequencing	
5.1.Overview	112
5.2. Prime number with Alphabetic Group based text encryption scheme (PAG)	113
5.2.1. Encryption Process	114
5.2.2. Decryption Process	116
5.2.3. Implementation with Experiment Results	116
5.2.4. Security analysis of Prime number with Alphabetic Group based text encryption scheme (PAG)	118
5.3. Palindrome number with Alphabetic Group and Operator based text encryption scheme (PAGO)	122
5.3.1. Encryption Process	123
5.3.2. Decryption Process	125
5.3.3. Implementation with Experiment Results	126
5.3.4. Security analysis for Palindrome number with Alphabetic Group and Operator based text encryption scheme (PAGO)	128
5.4. Armstrong and Perfect number with Cipher Sequencing based text encryption scheme (APCS)	132
5.4.1. Special Number Types	133
5.4.2. Encryption Process	134
5.4.3. Decryption Process	136
5.4.4. Experiment Results and Discussion	137
5.4.5. Security analysis of Armstrong and Perfect number with Cipher Sequencing based text encryption scheme (APCS)	139
5.5. Amicable number with Cipher Sequencing based text encryption scheme (ACS)	143
5.5.1. Different Terminology	144
5.5.2. Encryption Process	145
5.5.3. Decryption Process	147
5.5.4. Experiment Result and Discussions	148
5.5.5. Security Analysis of Amicable number with Cipher Sequencing based text encryption scheme (ACS)	150
5.6. Conclusion	154
Chapter 6: Text Encryption Building Blocks using Operators and Position of Bits in Plain Text	
6.1. Overview	155

6.2. Multiple Operator and Even Odd position based text encryption scheme (MOEO)	156
6.2.1. Encryption Process	157
6.2.2. Decryption Process	160
6.2.3. Implementations with Experimental Results	161
6.2.4. Security analysis of Multiple Operator and Even Odd position based text encryption scheme (MOEO)	163
6.3. Multiple Operator and ASCII Value based text encryption scheme (MOAV)	166
6.3.1. Encryption Process	167
6.3.2. Decryption Process	169
6.3.3 Experimental Results and Discussions	170
6.3.4. Security Analysis of Multiple Operator and ASCII Value based text encryption scheme (MOAV)	172
6.4. Multiple Operator and number of Zeros and Ones based text encryption scheme (MOZO)	175
6.4.1. Encryption Process	176
6.4.2. Decryption Process	179
6.4.3. Experimental Results and Discussions	179
6.4.4. Security Analysis of Multiple Operator and number of Zeros and Ones based text encryption scheme (MOZO**)**	181
6.5. Conclusion	184
Chapter 7: Image Encryption Building Blocks	
7.1. Overview	185
7.2. Even Odd block based Digital Enveloping scheme (EODE)	186
7.2.1. Encryption Process	189
7.2.2. Decryption Process	190
7.2.3. Experiment Results and Discussions	190
7.2.4. Security Analysis for Even Odd block based Digital Enveloping scheme (EODE)	193
7.3. Cumulative Image encryption scheme using Digital enveloping, Key based encryption with image Partitioning (CIDKP)	199
7.3.1. Encryption Process	201
7.3.2. Decryption Process	204
7.3.3. Implementations with Experimental Results	205
7.3.4. Security Analysis of Cumulative Image encryption scheme using Digital enveloping, Key based encryption with image	212

Partitioning (CIDKP)	
7.4. Cumulative Image encryption approach using Steganographic scheme with Pixel repositioning (CISP)	219
7.4.1. Different Terminology	221
7.4.2. Encryption Process	222
7.4.3. Decryption Process	224
7.4.4. Experiment Result and Discussions	224
7.4.5. Security Analysis for Cumulative Image encryption approach using Steganographic scheme with Pixel repositioning (CISP)	230
7.5. Conclusion	236
Chapter 8: Security Toolkit and Methodologies	
8.1. Overview	238
8.2. Security Toolkit	238
8.2.1. Description of Building Blocks	240
8.3. Bit-Wise Operation and Methodologies	240
8.3.1. Algorithm for BWMAS Operation (Bit Wise Masking for Alternate Sequence)	241
8.3.2.Cipher and Pixel Block Sequencing Methodologies	242
8.4. Conclusion	247
Chapter 9: Performance Analysis, Conclusion and Future Scope	
9.1. Overview	248
9.2. Performance Analysis of Building Blocks	248
9.3. Summary of Research	267
9.4. Future Scope of Work	269
Bibliography	271