Chapter 8

Security Toolkit and Methodologies

8.1. Overview

This chapter contains detailed description of the security toolkit along with its building blocks. The methodologies which have been developed during research and used to implement each of the building blocks are also being discussed in the later section of this chapter.

The objectives, structure of security toolkit and brief description of building blocks have been discussed in section 8.2. Section 8.3 includes detailed descriptions of the newly implemented methodologies used for the building blocks. A brief conclusion has been included in section 8.4.

8.2. Security Toolkit

The main objective of this research work is to develop an integrated ciphering system or a so called security toolkit. A set of newly implemented bit-level independent ciphering algorithms have been combined together in a cascaded manner to act as security toolkit as a whole. Each of the algorithms has acted as a building block for implemented security toolkit. Different standard parameters are used for measuring the performances of each of the building blocks.

In this current work, user authentication building blocks have been implemented based on CAPTCHA code generated from personal information and OTP formulated on a biometric image where generation time, the randomness of generated CAPTCHA or OTP and their security over different cryptographic attacks are considered for measuring their performances.

Special numbers, alphabetic group and cipher sequencing based text encryption schemes have been implemented for text encryption building blocks. The parameters like encryption and decryption time, Pearsonian chi-square value, the degree of freedom value are used for measuring the performance of text encryption building blocks.

Image Partitioning, digital enveloping based new image encryption building blocks have been introduced where PSNR, SSIM, CC, NCC, Q-INDEX, BER and encryption time are considered as parameters for measuring the performances.

Performances of each of the building blocks are measured based on all the mentioned parameters and the results are compared with standard algorithms. All the building blocks are combined in a cascaded manner as per schematic and operational characteristics. Satisfactory outcomes have been observed after implementing this security toolkit on a standalone system. That indicates successful completion of the chain of activities has reached to the end of work. Figure 8.1 represents system structure of 'security toolkit'.

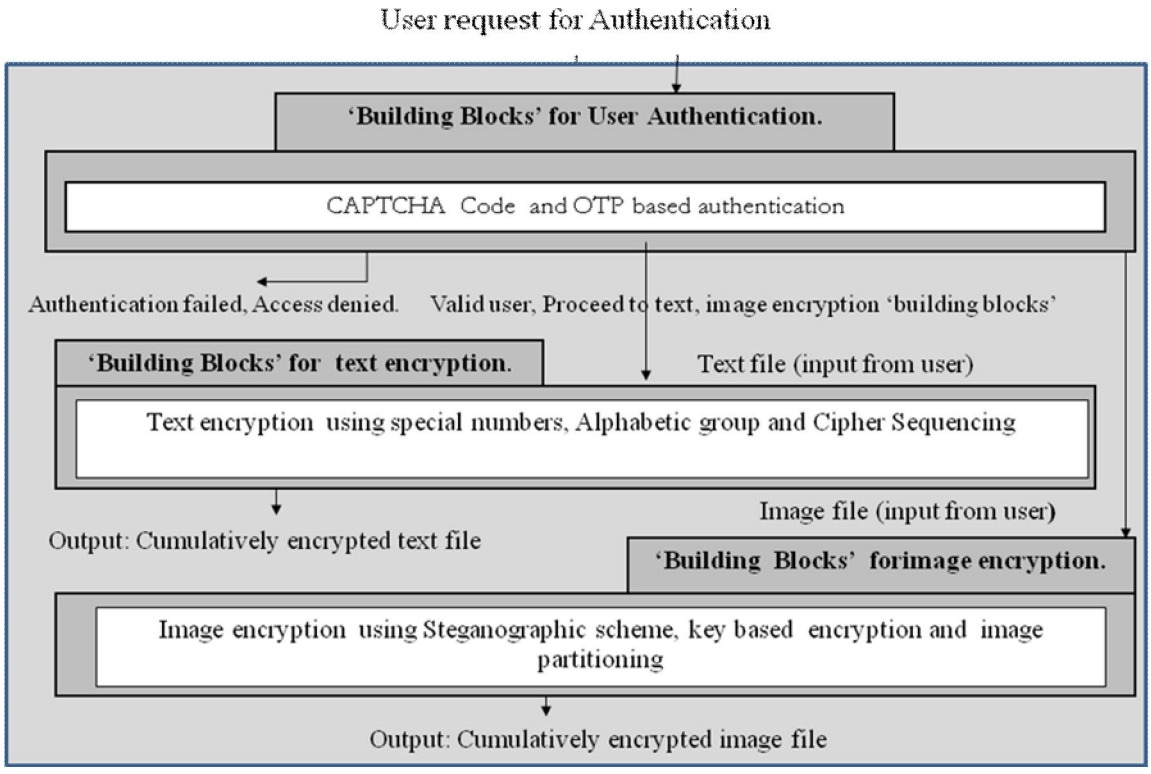

Figure 8.1: System Structure of 'Security Toolkit

8.2.1. Description of Building Blocks

User authentication building block deals with three newly implemented schemes namely they are CAPTCHA Code based on User Personal information and Likings (CCUPL), Secret Value based on Randomize One Time Password (SVROTP) and Numeric and biometric Image based One Time Password (NIOTP). Satisfactory performances of the schemes are observed by analyzing the protection over standard attacks.

Text encryption building block includes seven new schemes based on special numbers, alphabetic groups, operators and cipher sequencing. The schemes are Prime number with Alphabetic Group based text encryption (PAG), Palindrome number with Alphabetic Group and Operator based text encryption (PAGO), Amicable number with Cipher Sequencing based text encryption (ACS), Armstrong and Perfect number with Cipher Sequencing based text encryption (APCS), Multiple Operator and Even Odd position based text encryption (MOEO), Multiple Operator and ASCII Value based text encryption (MOAV) and Multiple Operator and number of Zeros and Ones based text encryption (MOZO). Appreciable performances are accessed for all the schemes as compared to standard algorithms like AES, Twofish, Serpent, Triple DES, and Blowfish algorithms.

Image encryption building block contains three newly introduced schemes. They are Even Odd block based Digital Enveloping scheme (EODE), Cumulative Image encryption using Steganographic scheme with Pixel repositioning (CISP) and Cumulative Image encryption using Digital Enveloping, Key based encryption with image Partitioning (CIDKP). These schemes produce satisfactory outcomes with better security and encryption ratio.

8.3. Bit-Wise Operation and Methodologies

The new operator & methodologies which are being implemented during the time of research have been used for the development of the building blocks. Methodologies have

been used for cipher block sequencing and pixel block sequencing where BWMAS Operation (Bit Wise Masking for Alternate Sequence) has been used between the bits of plain text and key value to generate the ciphertext rather than using the bitwise XOR operation. Those methodologies and operation have been discussed here.

8.3.1. Algorithm for BWMAS Operation (Bit Wise Masking for Alternate Sequence)

BWMAS operation has been performed between the binary representation of plain text and key value at the time of text based encryption. At the time of image based encryption, BWMAS operation has been carried out in between the binary representation of the original image and key or envelop image. The following rules are applied for this operation.

A. Rule for Even Bit Position

If the bit position is even and the bit position's value of envelope image or key is 0, the output is the bit value of the original image or plain text of that same bit position. If the bit position is even and the bit position's value of envelope image or key is 1, the output is the complement of the bit value of the original image or plain text of that same bit position.

B. Rule for Odd Bit Position

If the bit position is odd and the bit position's value of envelope image or key is 1, the output is the bit value of the original image or plain text of that same bit position. If the bit position is odd and the bit position's value of envelope image or key is 0, the output is the complement of the bit value of the original image or plain text of that same bit position. Table 8.1 represents the entire BWMAS operation as per even and odd bit position.

Table 8.1: Representation of BWMAS Operation as per Bit Position.

Bit Position	Bit Value of Original Image or Plain Text	Bit Value of Envelope Image or Key	Output of BWMAS Operation
1	0	0	1
2	1	0	1
3	0	1	0
4	1	1	0
5	0	1	0

8.3.2. Cipher and Pixel Block Sequencing Methodologies

Table 8.2 represents different cipher & pixel block sequencing methodologies with their brief algorithms.

Table 8.2: Different Cipher & Pixel Block Sequencing Methodologies

Sl No.	Name of Sequencing Method	Applied Domain	Brief Algorithm of Sequencing Method
1	PRONE (Positional Reverse Odd Normal Even)	Cipher & pixel block sequencing	Characters of odd numbered blocks are reversed. Characters of even numbered blocks remain unchanged.
2	PRENO (Positional Reverse Even Normal Odd)	Cipher & pixel block sequencing	Characters of even numbered blocks are reversed. Characters of odd numbered blocks remain unchanged.
3	CRONE (Continuously Reverse Odd Normal Even)	Cipher & pixel block sequencing	Characters of odd numbered blocks are reversed and odd numbered blocks are stored together. Characters of even numbered blocks remain unchanged.

4	CRENO (Continuously Reverse Even Normal Odd)	Cipher & pixel block sequencing	Characters of even numbered blocks are reversed and even numbered blocks are stored together. Characters of odd numbered blocks remain unchanged.
5	EEFR (Exchange Even From Right)	Cipher block sequencing	Characters of even numbered blocks are exchanged starting from the right end. Characters of odd numbered blocks remain unchanged.
6	EEFL (Exchange Even From Left)	Cipher block sequencing	Characters of even numbered blocks are exchanged starting from the left end. Characters of odd numbered blocks remain unchanged.
7	EOFR (Exchange Odd From Right)	Cipher block sequencing	Characters of odd numbered blocks are exchanged starting from the right end. Characters of even numbered blocks remain unchanged.
8	EOFL (Exchange Odd From Left)	Cipher block sequencing	Characters of odd numbered blocks are exchanged starting from the left end. Characters of even numbered blocks remain unchanged.
9	PRPNNP (Positional Reverse Prime Normal Non-Prime)	Cipher block sequencing	Reverse the characters or numbers in order which are present in the prime positions of storing array Z[]. Characters or numbers present in non-prime positions of storing array Z[] remain unchanged.
10	PRNPNP (Positional Reverse Non-Prime Normal Prime)	Cipher block sequencing	Reverse the characters or numbers in order which are present in the non-prime positions of storing array Z[].

			Characters or numbers present in prime positions of storing array Z[] remain unchanged.
11	CRPNNP (Continuous Reverse Prime Normal Non-Prime)	Cipher block sequencing	Reverse the characters or numbers in order which are present in prime positions of storing array Z[] and those characters or numbersare stored together. Characters or numbers present in non-prime positions of storing array Z[] remain unchanged.
12	CRNPNP (Continuous Reverse Non-Prime Normal Prime)	Cipher block sequencing	Reverse the characters or numbers in order which are present in non-prime positions of storing array Z[] and those characters or numbers are stored together. Characters or numbers present in prime positions of storing array Z[] remain unchanged.

Each block contains 4 numbers of characters as the block size is fixed to 32-bits. All the characters of the plain text file are divided into blocks before sequencing algorithms are applied Figure 8.2 represents PRONE, PRENO, CRONE and CRENO sequencing methods.

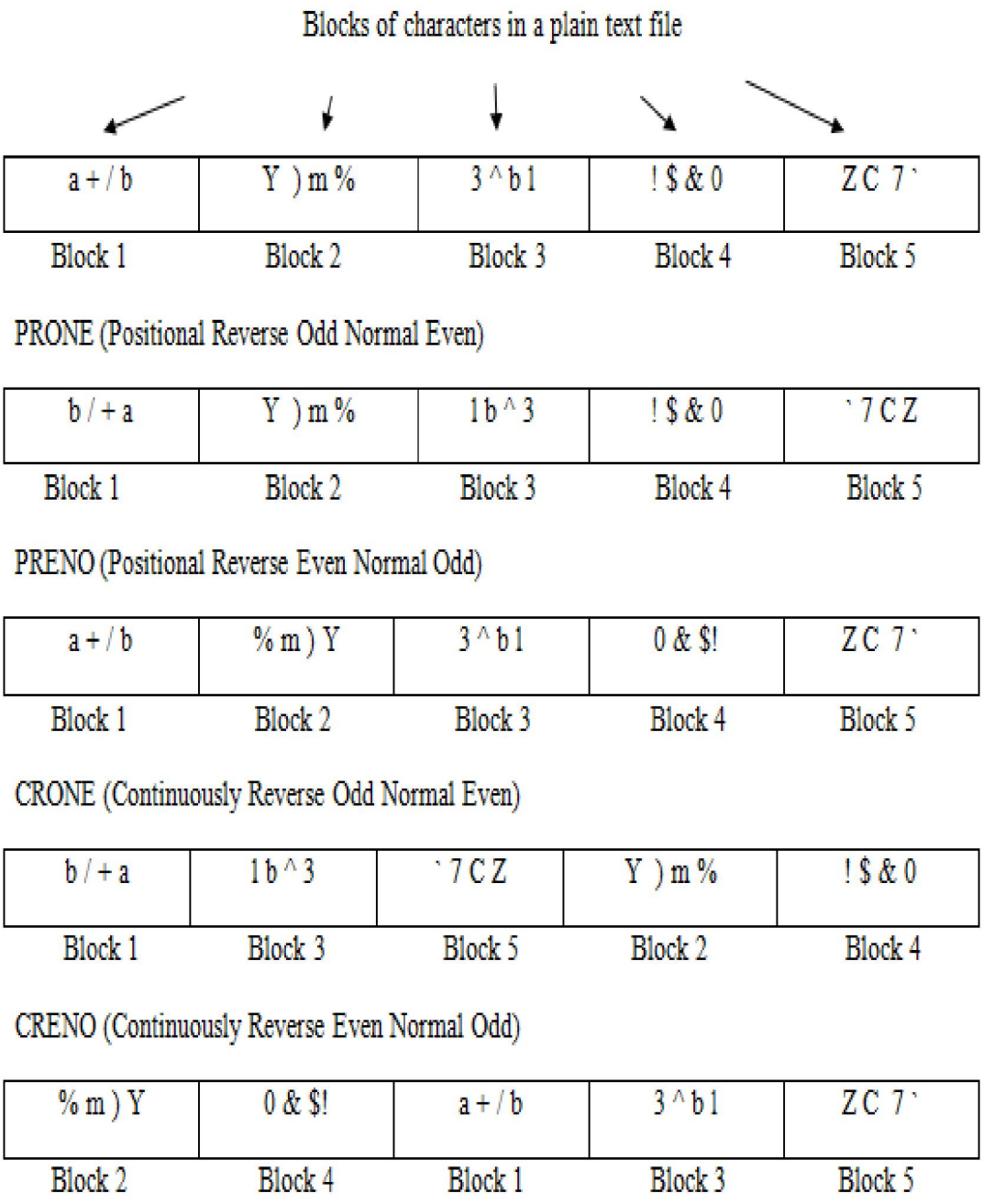

Figure 8.2: Diagrammatic Representation of PRONE, PRENO, CRONE and CRENO Sequencing Methods.

Each block contains 4 numbers of characters as the block size is fixed to 32-bits. Figure 8.3 represents EEFR, EEFL, EOFR, and EOFL sequencing methods.

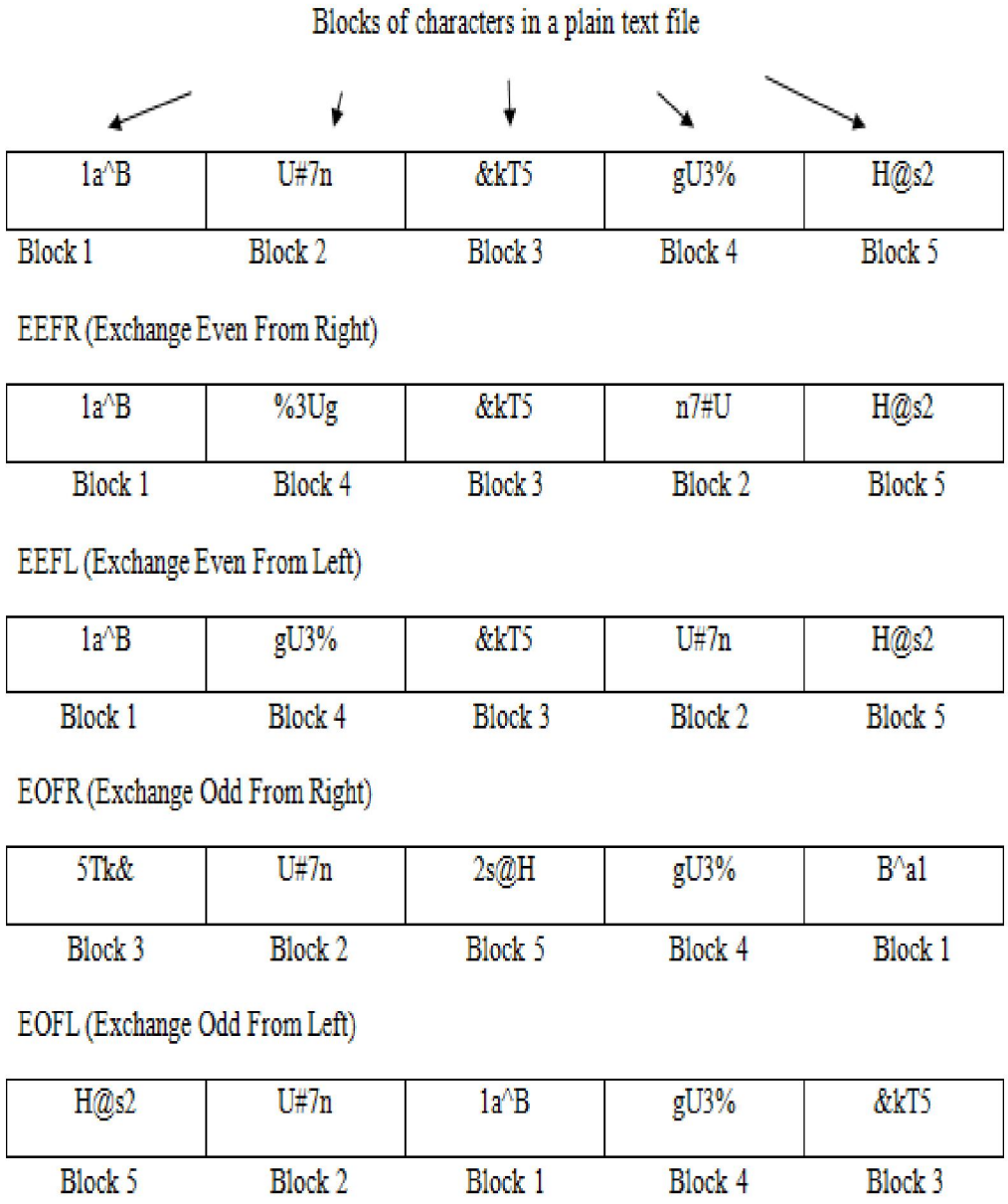

Figure 8.3: Diagrammatic Representation of EEFR, EEFL, EOFR, and EOFL Sequencing Methods.

Table 8.3 represents PRPNNP, PRNPNP, CRPNNP and CRNPNP sequencing methods.

Table 8.3: Representation of PRPNNP, PRNPNP, CRPNNP and CRNPNP Sequencing Methods.

Position of Digits in Storing Array	Inputted Values	PRPNNP (Output)	PRNPNP (Output)	CRPNNP (Output)	CRNPNP (Output)
1	9	3	9	3	6
2	1	7	1	7	6
3	4	4	4	4	0
4	6	6	6	3	1
5	3	3	3	4	6
6	7	7	6	1	7
7	4	4	4	9	7
8	7	7	0	6	6
9	6	6	1	7	9
10	1	1	6	7	1
11	7	1	7	6	4
12	0	0	7	1	3
13	3	9	3	0	4
14	6	6	7	6	7
15	6	6	6	6	3

8.4. Conclusion

Mathematical tricks, especially the concept of combinatorics to a great extent has been applied in an intelligent manner in developing fresh ciphering protocols, which has become the building blocks for the security toolkit. After measuring satisfactory performances of the building blocks, they are being combined in a cascaded manner to form the security toolkit. The satisfactory outcome has been experienced for the security toolkit implemented on a standalone system which leads to the ultimate goal. The methodologies which are being designed and implemented during research work have been used for the building blocks only after observing appreciable outcomes compared with other standard existing protocols. A lot of scopes still exist for further improvement of each of these protocols and methodologies.