

Amalgamation of Cyclic Bit Operation in SD-EI Image Encryption Method: An Advanced Version of SD-EI Method: SD-EI Ver-2

Somdip Dey
St. Xavier's College
[Autonomous]
Kolkata, India

E-mail:

somdipdey@ieee.org

somdipdey@acm.org

ABSTRACT

In this paper, the author presents an advanced version of image encryption technique, which is itself an upgraded version of SD-EI image encryption method. In this new method, SD-EI Ver-2, there are more bit wise manipulations compared to original SD-EI method. The proposed method consist of three stages: 1) First, a number is generated from the password and each pixel of the image is converted to its equivalent eight binary number, and in that eight bit number, the number of bits, which are equal to the length of the number generated from the password, are rotated and reversed; 2) In second stage, extended hill cipher technique is applied by using involutory matrix, which is generated by same password used in second stage of encryption to make it more secure; 3) In last stage, we perform modified Cyclic Bit manipulation. First, the pixel values are again converted to their 8 bit binary format. Then 8 consecutive pixels are chosen and a 8X8 matrix is formed out of these 8 bit 8 pixels. After that, matrix cyclic operation is performed randomized number of times, which is again dependent on the password provided for encryption. After the generation of new 8 bit value of pixels, they are again converted to their decimal format and the new value is written in place of the old pixel value. SD-EI Ver-2 has been tested on different image files and the results were very satisfactory.

KEYWORDS

SD-EI, SD-AEI, image encryption, bit reversal, bit manipulation, bit rotation, hill cipher, randomization.

1. INTRODUCTION

In modern world, security is a big issue and securing important data is very essential, so that the data can not be intercepted or misused for illegal purposes. For example we can assume the situation where a bank manager is instructing his subordinates to credit an account, but in the mean while a hacker interpret the message and he uses the information to debit the account instead of crediting it. Or we can assume the situation where a military commander is instructing his fellow comrades about an attack and the strategies used for the attack, but while the instructions are sent to the destination, the instructions get intercepted by enemy soldiers and they use the information for a counter-attack. This can be highly fatal and can cause too much destruction. So, different cryptographic methods are used by different organizations and government institutions to protect their data online. But, cryptography hackers are always trying to break the

cryptographic methods or retrieve keys by different means. For this reason cryptographers are always trying to invent different new cryptographic method to keep the data safe as far as possible.

Cryptography can be basically classified into two types:

- 1) Symmetric Key Cryptography
- 2) Public Key Cryptography

In Symmetric Key Cryptography [17][20], only one key is used for encryption purpose and the same key is used for decryption purpose as well. Whereas, in Public Key Cryptography [17][19], one key is used for encryption and another publicly generated key is used for the decryption purpose. In symmetric key, it is easier for the whole process because only one key is needed for both encryption and decryption. Although today, public key cryptography such as RSA [15] or Elliptical Curve Cryptography [16] is more popular because of its high security, but still these methods are also susceptible to attack like "brute force key search attack" [17][21]. The proposed method, SD-EI VER-2, is a type of symmetric key cryptographic method, which is itself a combination of four different encryption modules.

SD-EI VER-2 method is devised by Somdip Dey [5] [6] [9] [10] [11] [12] [13], and it is itself a successor and upgraded version of SD-EI [5] image encryption technique. The three different encryption modules, which make up SD-EI VER-2 Cryptographic methods, are as follows:

- 1) Modified Bits Rotation and Reversal Technique for Image Encryption
- 2) Extended Hill Cipher Technique for Image Encryption
- 3) Modified Cyclic Bit Manipulation

The aforementioned methods will be discussed in the next section, i.e. in The Methods in SD-EI VER-2. All the cryptographic modules, used in SD-EI VER-2 method, use the same password (key) for both encryption and decryption (as in case of symmetric key cryptography).

The differences between SD-EI [5] and SD-EI VER-2 methods are that the later one contains one extra encryption module, which is the modified Cyclic Bit manipulation, and the Bits rotation and Reversal Technique is modified to provide better security.

2. THE METHODS IN SD-EI VER-2

Before we discuss the four methods, which make the SD-EI VER-2 Encryption Technique, we need to generate a number from the password, which will be used to randomize the file structure using the modified MSA Randomization module.

2.1 Generation of a Number from the Key

In this step, we generate a number from the password (symmetric key) and use it later for the randomization method in modified Cyclic Bit manipulation, which is used to encrypt the image file. The number generated from the password is case sensitive and depends on each byte (character) of the password and is subject to change if there is a slightest change in the password.

If $[P_1P_2P_3P_4\dots P_{len}]$ be the password, where length of the password ranges from 1,2,3,4.....len and 'len' can be anything.

Then, we first multiply 2^i , where 'i' is the position of each byte (character) of the password, to the ASCII vale of the byte of the password at position 'i'. And keep on doing this until we have finished this method for all the characters present in the password. Then we add all the values, which is generated from the aforementioned step and denote this as N.

Now, if $N = [n_1n_2\dots n_j]$, then we add all the digits of that number to generate the code (number), i.e. we need to do: $n_1 + n_2 + n_3 + n_4 + \dots + n_j$ and get the unique number, which is essential for the encryption method of randomization. We denote this unique number as 'Code'.

For example: If the password is 'AbCd', then,

$$P_1 = A; P_2 = b; P_3 = C$$

$$N = 65*2^{(1)} + 98*2^{(2)} + 67*2^{(3)} + 100*2^{(4)} = 2658$$

$$\text{Code} = 2 + 6 + 5 + 8 = 21$$

2.2 Modified Bits Rotation and Reversal Technique

In this method, a password is given along with input image. Value of each pixel of input image is converted into equivalent eight bit binary number. Now we add the ASCII Value of each byte of the password and generate a number from the password. This number is used for the Bits Rotation and Reversal technique i.e., Number of bits to be rotated to left and reversed will be decided by the number generated by adding the ASCII Value of each byte of the password. This generated number will be then modular operated by 7 to produce the effective number (N_R), according to which the bits will be rotated and reversed. Let N be the number generated from the password and N_R (effective number) be the number of bits to be rotated to left and reversed. The relation between N and N_R is represented by equation (1).
 $N_R = N \bmod 7$ ----- eq. (1)

,where '7' is the number of iterations required to reverse entire input byte and $N = [n_1 + n_2 + n_3 + n_4 + \dots n_j]$, where $n_1, n_2, \dots n_j$ is the ASCII Value of each byte of the password.

For example, $P_{in}(i,j)$ is the value of a pixel of an input image. $[B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8]$ is equivalent eight bit binary representation of $P_{in}(i,j)$.

$$\text{i.e. } P_{in}(i,j) \longrightarrow [B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8]$$

If $N_R=5$, five bits of input byte are rotated left to generate resultant byte as $[B_6 B_7 B_8 B_1 B_2 B_3 B_4 B_5]$. After rotation, rotated five bits i.e. $B_1 B_2 B_3 B_4 B_5$, get reversed as $B_5 B_4 B_3 B_2 B_1$ and hence we get the resultant byte as $[B_6 B_7 B_8 B_5 B_4 B_3 B_2 B_1]$. This resultant byte is converted to equivalent decimal number $P_{out}(i,j)$.

$$\text{i.e. } [B_6 B_7 B_8 B_5 B_4 B_3 B_2 B_1] \longrightarrow P_{out}(i,j)$$

,where $P_{out}(i,j)$ is the value of output pixel of resultant image.

Since, the weight of each pixel is responsible for its colour, the change occurred in the weight of each pixel of input image due to modified *Bits Rotation & Reversal* generates the encrypted image.

Note: - If $N=7$ or multiple of 7, then $N_R=0$. In this condition, the whole byte of pixel gets reversed.

2.3 Extended Hill Cipher Technique

This is another method for encryption of images proposed in this paper. The basic idea of this method is derived from the work presented by Saroj Kumar Panigrahy et al [2] and Bibhudendra Acharya et al [3]. In this work, involutory matrix is generated by using the algorithm presented in [3].

Algorithm of Extended Hill Cipher technique:

Step 1: An involutory matrix of dimensions $m \times m$ is constructed by using the input password.

Step 2: Index value of each row of input image is converted into x -bit binary number, where x is number of bits present in binary equivalent of index value of last row of input image. The resultant x -bit binary number is rearranged in reverse order. This reversed- x -bit binary number is converted into its equivalent decimal number. Therefore weight of index value of each row changes and hence position of all rows of input image changes. i.e., Positions of all the rows of input image are rearranged in *Bits-Reversed-Order*. Similarly, positions of all columns of input image are also rearranged in *Bits-Reversed-Order*.

Step 3: Hill Cipher technique is applied onto the *Positional Manipulated* image generated from Step 2 to obtain final encrypted image.

2.4 Modified Cyclic Bit Manipulation

This is a new encryption method, which is used in this paper. This method is proposed by Somdip Dey [5][6][8][9][10][11]. The basic algorithm for this method is as follows:

Step 1: Choose consecutive 8 pixels

Step 2: Convert each pixel value to their corresponding 8 bit binary value

Step 3: Form a 8X8 matrix with the 8 bit values of 8 pixels

Step 4: Perform multi-directional matrix Cyclic operation on that matrix “code” number of times

Step 5: Convert the modified 8 bit value of each pixel to their corresponding decimal value

Step 6: Put the newly generated value in place of the old value of that pixel

Step 7: Go to Step 1, and continue until and unless all the pixel values of the image are modified

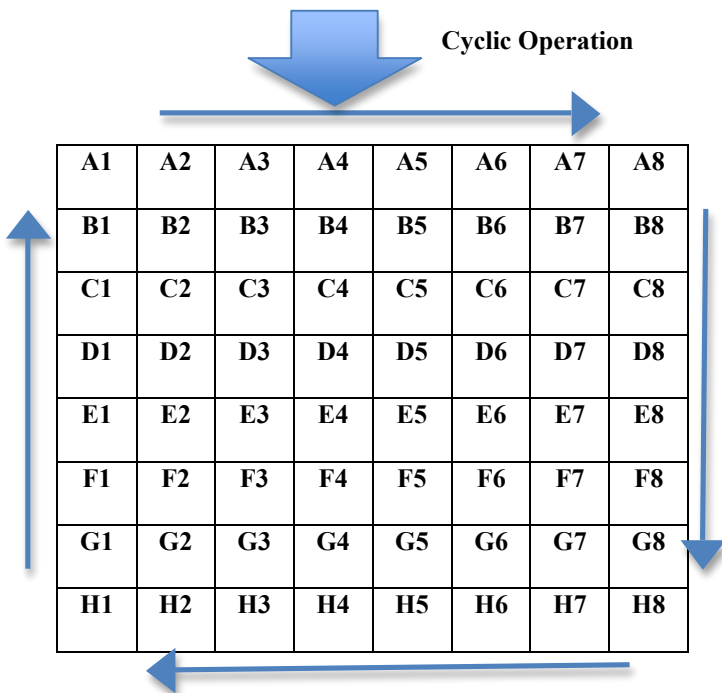
2.4.1 Diagrammatic Representation of Modified Cyclic Bit Manipulation

Let the following be the matrix comprising of 8 bit value of 8 pixel:

Note: A, B, C, D...H represent each pixel and 1,2,3...8

A1	A2	A3	A4	A5	A6	A7	A8
B1	B2	B3	B4	B5	B6	B7	B8
C1	C2	C3	C4	C5	C6	C7	C8
D1	D2	D3	D4	D5	D6	D7	D8
E1	E2	E3	E4	E5	E6	E7	E8
F1	F2	F3	F4	F5	F6	F7	F8
G1	G2	G3	G4	G5	G6	G7	G8
H1	H2	H3	H4	H5	H6	H7	H8

represent the 8 bit binary value of each pixel.



B1	A1	A2	A3	A4	A5	A6	A7
C1	B3	B4	B5	B6	B7	C7	A8
D1	B2	D3	C3	C4	C5	D7	B8
E1	C2	E3	D5	E5	C6	E7	C8
F1	D2	F3	D4	E4	D6	F7	D8
G1	E2	F4	F5	F6	E6	G7	E8
H1	F2	G2	G3	G4	G5	G6	F8
H2	H3	H4	H5	H6	H7	H8	G8

Thus, the new pixel values are:

Pixel 1: B1 A1 A2 A3 A4 A5 A6 A7,

Pixel 2: C1 B2 B4 B5 B6 B7 C7 A8,

Pixel 3: D1 B2 D3 C3 C4 C5 D7 B8,

And so on.

3. BLOCK DIAGRAM OF SD-EI VER-2 METHOD

In this section, we provide the block diagram of SD-EI VER-2 method.

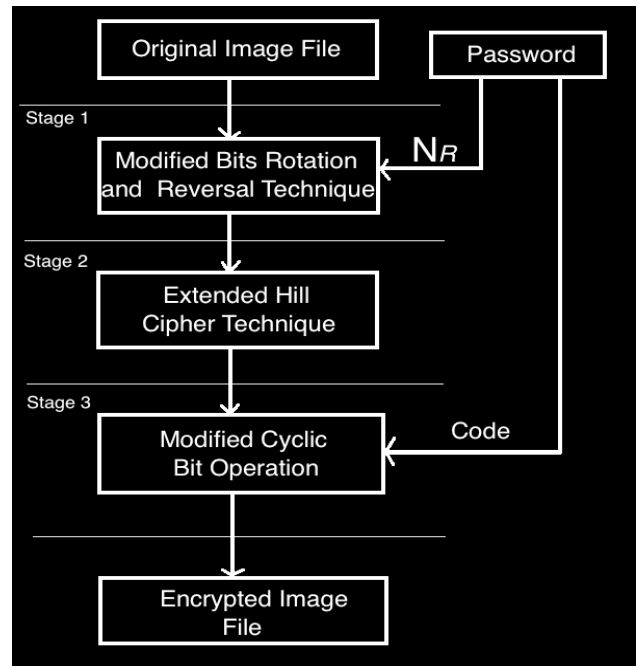


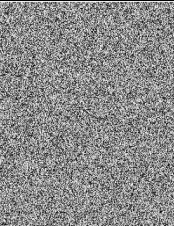

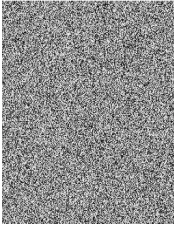


Fig 1: Block Diagram of SD-EI VER-2 Method

4. RESULTS AND DISCUSSIONS

We provided few results of the proposed SD-EI VER-2 method in the following table.

TABLE 1: Results of SD-EI VER-2

Original File	Encrypted File
	
	
	

From the results section it is not possible to know the effectiveness of the SD-EI VER-2 method because the end result of both SD-EI and SD-EI VER-2 are almost same if viewed with naked eyes. But, if we compare the two methods then we can see that SD-EI VER-2 method is more secure than SD-EI encryption method.

5. CONCLUSION AND FUTURE SCOPE

In this paper, the author proposed a standard method of image encryption, which tampers the image in a very effective way. SD-EI VER-2 method is very successful to encrypt the image perfectly to maintain its security and authentication. The inclusion of modified bits rotation and reversal technique, and modified Cyclic Bit Manipulation, made the system even stronger than it used to be before. In future, the security of method can be further enhanced by adding more secure bit and byte manipulation techniques to the system. And the author has already started to work on that.

6. ACKNOWLEDGMENTS

Somdip Dey would like to thank the fellow students and his professors for constant enthusiasm and support. He would also like to thank Dr. Asoke Nath, founder of Department of Computer Science, St. Xavier's College [Autonomous], Kolkata, India, for providing his feedback on the method and help with the preparation of the project. Somdip Dey would also like to thank his parents, Sudip Dey and Soma Dey, for their blessings and constant support, without which the completion of the project would have not been possible.

7. REFERENCES

- [1]. Mitra et. al., "A New Image Encryption Approach using Combinational Permutation Techniques," IJCS, 2006, vol. 1, No 2, pp.127-131.
- [2]. Saroj Kumar Panigrahy, Bibhudendra Acharya, Debasish Jena, "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm", 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.
- [3]. Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009, pp. 663-667.
- [4]. Asoke Nath, Saima Ghosh, Meheboob Alam Mallik, "Symmetric Key Cryptography using Random Key generator", "Proceedings of International conference on security and management (SAM'10) held at Las Vegas, USA Jull 12-15, 2010), P-Vol-2, pp. 239-244 (2010).
- [5]. Somdip Dey, "SD-EI: A Cryptographic Technique To Encrypt Images", Proceedings of "The International Conference on Cyber Security, CyberWarfare and Digital Forensic (CyberSec 2012)", held at Kuala Lumpur, Malaysia, 2012, pp. 28-32.
- [6]. Somdip Dey, "SD-AEI: An advanced encryption technique for images", 2012 IEEE Second International Conference on Digital Information Processing and Communications (ICDIPC), pp. 69-74.
- [7]. Asoke Nath, Trisha Chatterjee, Tamodeep Das, Joyshree Nath, Shayan Dey, "Symmetric key cryptosystem using combined cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSA method: TTJSA algorithm", Proceedings of "WICT, 2011 " held at Mumbai, 11th - 14th Dec, 2011, Pages:1175-1180.
- [8]. Somdip Dey, "SD-REE: A Cryptographic Method To Exclude Repetition From a Message", Proceedings of The International Conference on Informatics & Applications (ICIA 2012), Malaysia, pp. 182 - 189.
- [9]. Somdip Dey, "SD-AREE: A New Modified Caesar Cipher Cryptographic Method Along with Bit- Manipulation to Exclude Repetition from a Message to be Encrypted", Journal: Computing Research Repository - CoRR, vol. abs/1205.4279, 2012.
- [10]. Somdip Dey, Joyshree Nath and Asoke Nath. Article: An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation, Bit Reversal, Modified Caesar Cipher (SD-REE), DJSA method, TTJSA method: SJA-I Algorithm. *International Journal of Computer Applications* 46(20): 46-53, May 2012. Published by Foundation of Computer Science, New York, USA.
- [11]. Somdip Dey, Joyshree Nath, Asoke Nath, "An Integrated Symmetric Key Cryptographic Method - Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm", IJMECS, vol.4, no.5, pp.1-9, 2012.
- [12]. Somdip Dey, Kalyan Mondal, Joyshree Nath, Asoke Nath, "Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QR Algorithm", IJMECS, vol.4, no.6, pp.59-67, 2012.
- [13]. Somdip Dey, Joyshree Nath, Asoke Nath, "Modified Caesar Cipher method applied on Generalized Modified Vernam Cipher method with feedback, MSA method and NJJSA method: STJA Algorithm" Proceedings of FCS'12, Las Vegas, USA.
- [14]. Somdip Dey, "An Image Encryption Method: SD-Advanced Image Encryption Standard: SD-AIES", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(2), pp. 82-88.
- [15]. http://en.wikipedia.org/wiki/RSA_algorithm [ONLINE]
- [16]. http://en.wikipedia.org/wiki/Elliptic_curve_cryptography [ONLINE]
- [17]. Cryptography & Network Security, Behrouz A. Forouzan, Tata McGraw Hill Book Company.
- [18]. Somdip Dey, "Amalgamation of Cyclic Bit Operation in SD-EI Image Encryption Method: An Advanced Version of SD-EI

Method: SD-EI Ver-2”, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3), pp. 238-242.

- [19]. http://en.wikipedia.org/wiki/Public-key_cryptography [ONLINE]
- [20]. http://en.wikipedia.org/wiki/Symmetric-key_algorithm [ONLINE]
- [21]. http://en.wikipedia.org/wiki/Brute-force_search [ONLINE]