

An Image Encryption Method: SD-Advanced Image Encryption Standard: SD-AIES

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

E-mail:

somdipdey@ieee.org
somdipdey@acm.org

ABSTRACT

The security of digital information in modern times is one of the most important factors to keep in mind. For this reason, in this paper, the author has proposed a new standard method of image encryption. The proposed method consists of 4 different 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 third stage, generalized modified Vernam Cipher with feedback mechanism is used on the file to create the next level of encryption; 4) Finally in fourth stage, the whole image file is randomized multiple number of times using modified MSA randomization encryption technique and the randomization is dependent on another number, which is generated from the password provided for encryption method. SD-AIES is an upgraded version of SD-AEI Image Encryption Technique. The proposed method, SD-AIES is tested on different image files and the results were far more than satisfactory.

KEYWORDS

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

1. INTRODUCTION

In today's world, keeping the digital information safe from being misused, is one of the most important criteria. This issue gave rise to a new branch in computer science, named Information Security. Although new methods are introduced every day to keep the data secure, but computer hackers and un-authorized persons are always trying to break those cryptographic methods or protocols to fetch the sensitive beneficial information from those data. For this reason, computer scientist and cryptographers are trying very hard to come up with permanent solutions to this problem.

Cryptography can be basically classified into two types:

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

In Symmetric Key Cryptography [16], only one key is used for encryption purpose and the same key is used for decryption purpose as well. Whereas, in Public Key Cryptography [16], 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 [14] or Elliptical Curve Cryptography [15] is more popular because of its high security, but still these methods are also susceptible to attack like "brute force key search attack" [16]. The proposed method, SD-AIES, is a type of symmetric key cryptographic method, which is itself a combination of four different encryption modules.

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

- 1) Modified Bits Rotation and Reversal Technique for Image Encryption
- 2) Extended Hill Cipher Technique for Image Encryption
- 3) Generalized Modified Vernam Cipher for File Encryption
- 4) Modified MSA Randomization for File Encryption

The aforementioned methods will be discussed in the next section, i.e. in The Methods in SD-AIES. All the cryptographic modules, used in SD-AIES method, use the same password (key) for both encryption and decryption (as in case of symmetric key cryptography). Although there is a rising issue of strong security in between symmetric key cryptography and public key cryptography, but SD-AIES is very strong cryptographic method indeed because of the use of modified Vernam Cipher with feedback mechanism. It has already been proved by scientists that the use of one-time padding Vernam Cipher is itself unbreakable if and only if the key chosen for encryption is truly random in nature. The combination of both bit and byte manipulation along with modified Vernam Cipher makes the SD-AIES method truly unique and strong.

The differences between SD-AEI [6] and SD-AIES methods are that the later one contains one extra encryption module, which is the modified Vernam Cipher with feedback

mechanism, and the Bits rotation and Reversal Technique is modified to provide better security.

2. THE METHODS IN SD-AIES

Before we discuss the four methods, which make the SD-AIES 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, 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).

$$N_R = N \bmod 7 \text{ ----- eq. (1)}$$

,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. Figure 1 (a, b) shows input and encrypted images respectively. For the encryption process given password is "SD13", whose $N_R=6$.

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

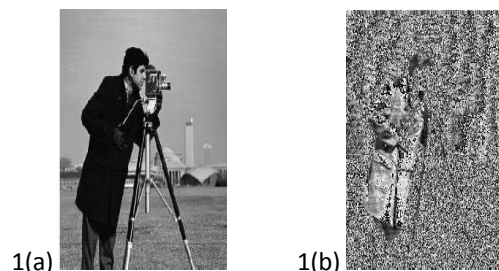


Figure 1: (a).Input Image. (b).Encrypted Image for password "SD13"

2.3 Extended Hill Cipher Technique

This is a new 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 Generalized Modified Vernam Cipher

The module of modified Vernam Cipher, which is used in this method is a concept proposed by Nath et al. [4][7]. Nath et al. in their cryptographic method, called TTJSA [7], has proposed an advanced form of generalized modified Vernam Cipher with feedback mechanism. For this reason, even if the data is slightly changed, the encrypted output generated is very different from the other outputs.

TTJSA method is a combination of 3 distinct cryptographic methods, namely, (i) Generalized Modified Vernam Cipher Method, (ii) MSA method and (iii) NJJSA method. To begin the method a user has to enter a text-key, which may be at most 16 characters in length. From the text-key, the randomization number and the encryption number is calculated using a method proposed by Nath et al. A minor change in the text-key will change the randomization number and the encryption number quite a lot. The method have also been tested on various types of known text files and have been found that, even if there is repetition in the input file, the encrypted file contains no repetition of patterns.

In SD-AIES Image Encryption method we have only used the modified Vernam Cipher module of TTJSA by Nath et al. Here, 'Code' represents the randomization number and 'N' represents the encryption number. All the data in the file are converted to their equivalent 16 bit binary format and broken down into blocks.

Algorithm for Modified Vernam Cipher with feedback mechanism is as follows:

2.4.1 Algorithm of $vernamenc(f1, f2)$:

Step 1: Start $vernamenc()$ function

Step 2: The matrix $mat[16][16]$ is initialized with numbers 0-255 in row major wise order

Step 3: call function $randomization()$ to

$randomize$ the contents of $mat[16][16]$.

Step 4: Copy the elements of random matrix

$mat[16][16]$ into $key[256]$ (row major wise)

Step 5: $pass=1, times3=1, ch1=0$

Step 6: Read a block from the input file $f1$ where number of characters in the block 256 characters

Step 7: If block size < 256 then goto Step 15

Step 8: copy all the characters of the block into an array $str[256]$

Step 9: call function encryption where $str[]$ is passed as parameter along with the size of the current block

Step 10: if $pass=1$ then

$times=(times+times3*11)\%64$

$pass=pass+1$

else if $pass=2$ then

$times=(times+times3*3)\%64$

$pass=pass+1$

else if $pass=3$ then

$times=(times+times3*7)\%64$

$pass=pass+1$

else if $pass=4$ then

$times=(times+times3*13)\%64$

$pass=pass+1$

else if $pass=5$ then

$times=(times+times3*times3)\%64$

$pass=pass+1$

else if $pass=6$ then

$times=(times+times3*times3*times3)\%64$

$pass=1$

Step 11: call function $randomization()$ with

current value of $times$

Step 12: copy the elements of $mat[16][16]$ into

$key[256]$

Step 13: read the next block

Step 14: goto Step 7

Step 15: copy the last block (residual character if any) into $str[]$

Step 16: call function $encryption()$ using $str[]$ and the no. of residual characters

Step 17: Return

2.4.2 Algorithm of function encryption($str[],n$):

Step 1: Start encryption() function

Step2: $ch1=0$

Step 3: calculate $ch=(str[0]+key[0]+ch1)\%256$

Step 4: write ch into output file

Step 5: $ch1=ch$

Step 6: $i=i+1$

Step 7: if $i=n$ then goto Step 13

Step 8: $ch=(str[i]+key[i]+ch1)\%256$

Step 9: write ch into the output file

Step 10: $ch1=ch$

Step 11: $i=i+1$

Step 12: goto Step 7

Step 13: Return

2.4.3 Algorithm for function randomization():

The randomization of key matrix is done using the following function calls:

Step-1: call Function cycling()

Step-2: call Function upshift()

Step-3: call Function downshift()

Step-4: call Function leftshift()

Step-5: call Function rightshift()

Note: Cycling, upshift, downshift, leftshift, rightshift are matrix operations performed (applied) on the matrix, formed from the key. The aforementioned methods are the steps followed in MSA algorithm [2] proposed by Nath et al.

After the execution of modified Vernam Cipher, each block is written down into the file and further processed by next steps of the cipher method.

2.5 Modified MSA Randomization

Nath et al. [4][7] proposed a symmetric key method, where they have used a random key generator for generating the initial key and that key is used for encrypting the given source file. MSA method [4] is basically a substitution method where we take 2 characters from any input file and then search the corresponding characters from the random key matrix and store the encrypted data in another file. MSA method provides us multiple encryptions and multiple

decryptions. The key matrix (16x16) is formed from all characters (ASCII code 0 to 255) in a random order.

The randomization of key matrix is done using the following function calls:

Step-1: Function cycling()

Step-2: Function upshift()

Step-3: Function rightshift()

Step-4: Function downshift()

Step-5: Function leftshift()

N.B: Cycling, upshift, downshift, leftshift, rightshift are matrix operations performed (applied) on the matrix, formed from the key. The detailed description of the above methods is given in MSA [4] algorithm.

The above randomization process we apply for $n1$ times and in each time we change the sequence of operations to make the system more random. Once the randomization is complete we write one complete block in the output key file.

In our method SD-AEI [6] and SD-AIES, we have used the same concept of randomization but instead of doing the randomization on the key matrix, we applied the randomization technique on the whole file after picking up each block from the image file. Basically, the whole file is broken up into number of blocks of data and then randomization technique is applied on each block of data of the image file, then after the completion of randomization method, each block is written down in the output file as the final encrypted image file.

Modified Randomization method algorithm, which is followed in this SD-AIES method is:

Step-1: Function cycling()

Step-2: Function upshift()

Step-3: Function rightshift()

Step-4: Function left_diagonal_randomization()

Step-5: Function cycling() for "code" number of times

Step-6: Function downshift()

Step-7: Function leftshift()

Step-8: Function right_diagonal_randomization()

3. IMPORTANT FEATURES

In this section we discuss about few special features of the SD-AIES method, which is as follows:

3.1 Effectiveness of Generalized Modified Vernam Cipher

The use of modified Vernam Cipher is an important thing in this method. The feedback mechanism in the modified Vernam Cipher is the game changing method and it makes the entire cipher system very secure. Even if there is a slight change in the original file, the entire content of the final encrypted file will be totally different from the encrypted file in previous state.

For example, we chose two test cases to show the effectiveness of modified Vernam Cipher by analyzing the frequency of the characters of the encrypted file i.e. by studying the spectral analysis of the encrypted file. The following table shows the test cases:

TABLE 1: Test Cases for Modified Vernam Cipher

Serial No.	Test Case
1	File containing 2048 bytes of A (AAAAAAAAAAAAAAAAAAAA.....AAAAAAAAAAAA)
2	File Containing 2047 bytes of A and 1 byte of B (AAAAAAAAAAAAAAAAAAAA AAAAAA.....AAAAAA AAAAAAB)

Fig 2.1 shows the spectral analysis of the test case 1 and Fig 2.2 shows the spectral analysis of the encrypted file of test case 2.

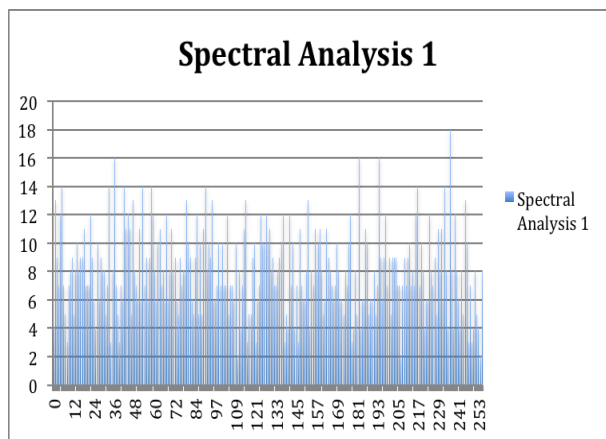


Fig 2.1: Spectral Analysis of Test Case 1

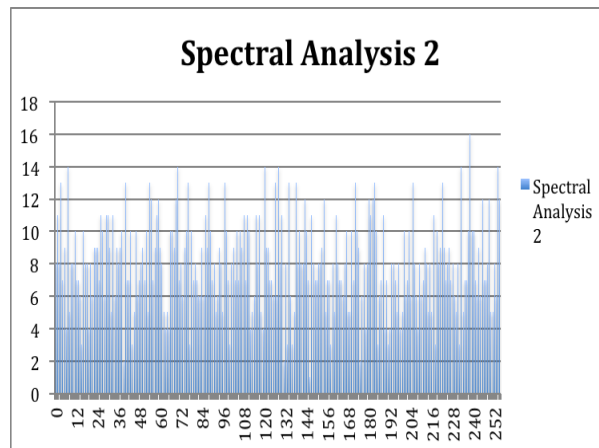


Fig 2.2: Spectral Analysis of Test Case 2

Thus from the spectral analysis it is evident that there is no pattern match in between the two test cases and the peaks are totally different. For this reason, it proved that even if there is slight change in the original file, the final encrypted file will be totally different.

3.2 The Difference between Bits Rotation and Reversal Method Vs Modified Bits Rotation and Reversal Method

In the Bits Rotation and Reversal Method, which is used in SD-EI and SD-AEI Image Encryption techniques, was dependent on the length of the password and thus the bits were rotated and reversed according to the effective length of the password. For example, the password is “Somdip”, then L_R (effective length of password)= 6 (according to Bits Rotation And Reversal technique), and thus 6 bits of every pixel are rotated and then reversed. Now, majority of the passwords can be of same length and the resultant of this method will be the same for all those password. For example, if the password is “123456” or “DeYSYS”, the effective length (L_R) is still 6, and the result of Bits Rotation and Reversal Technique will be same for the same password.

So to make the method more effective and secure, we add all the ASCII Values of each byte in the password to generate the N and thus find the effective number (N_R) instead of effective length (L_R), which will instead be used for Bits Rotation and Reversal Technique. For example, if the password are “Somdip”, “123456” and “DeySYS”, then the effective numbers are 4, 1 and 6 respectively. Thus, the resultant of Bits Rotation and Reversal technique will be different for all the three passwords. But still, even in modified Bits Rotation and Reversal Technique, two passwords are likely to produce the same effective number (N_R) because the range of the effectiveness is in between 0-6 i.e. (because the data range is in between 1-7), and the summation of ASCII Value may also lead to same sum. For example, if a password is “DeY” or “DYe”, both will generate same effective number (N_R). Thus, this is a drawback of the system, but still this method is better than the normal Bits Rotation and Reversal Method.

4. BLOCK DIAGRAM OF SD-AIES METHOD

In this section, we provide the block diagram of SD-AIES method.

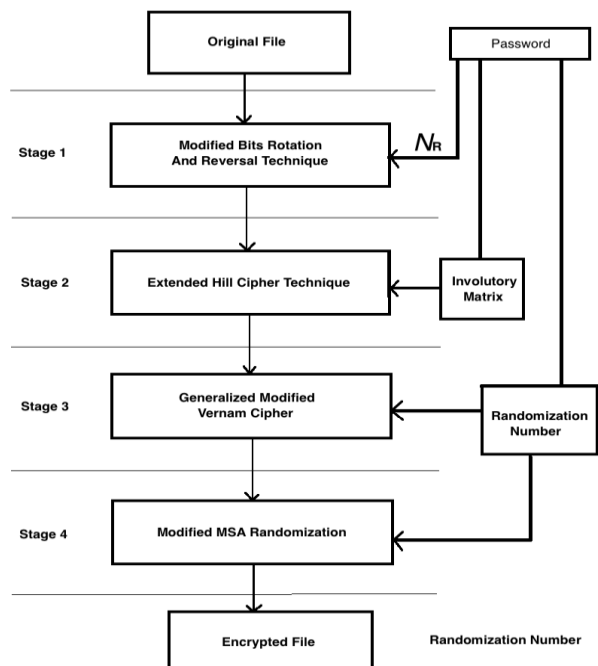




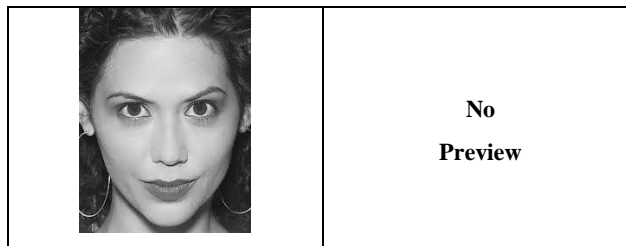
Fig 3: Block Diagram of SD-AIES Method

5. RESULTS AND DISCUSSIONS

We provided few results of the proposed SD-AIES method in the following table.

TABLE 2: Results of SD-AIES

Original File	Encrypted File
	No Preview
	No Preview



From the results section it is not possible to know the effectiveness of the SD-AIES method because the end result of both SD-AEI and SD-AIES are same i.e. there will be no preview of the encrypted file, because the internal structure of the file is already messed up due to encryption methods.

6. CONCLUSION AND FUTURE SCOPE

In this paper, the author proposes a standard method of image encryption, which first tampers the image and then disrupts the file structure of the image file. SD-AIES 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 Vernam Cipher along with feedback mechanism, 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.

7. 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.

8. 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 Jul 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 NJJSAA 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]. [http://en.wikipedia.org/wiki/RSA_\(algorithm\)](http://en.wikipedia.org/wiki/RSA_(algorithm)) [ONLINE]
- [15]. http://en.wikipedia.org/wiki/Elliptic_curve_cryptography [ONLINE]
- [16]. Cryptography & Network Security, Behrouz A. Forouzan, Tata McGraw Hill Book Company.