SD-AEI: An Advanced Encryption Technique For Images

An Advanced Combined Encryption Technique For Encrypting Images Using Randomized Byte Manipulation

Somdip Dey, Student Member IEEE
St. Xavier's College [Autonomous]
Kolkata, India.
Email: somdipdey@acm.org

***Abstract*—In this paper, the author propose a method, SD-AEI, for image encryption, which is an upgraded module for SD-EI combined image encryption technique and basically has three stages: 1) In first stage, each pixel of image is converted to its equivalent eight bit binary number and in that eight bit number, the number of bits, which are equal to the length of password are rotated and then 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, the whole image file is randomized multiple number of times using Modified MSA Randomization encryption technique and the randomization is dependent on an unique number, which is generated from the password provided for encryption. This proposed technique, SD-AEI, is very effective in encrypting any type of images and the results were very satisfactory. SD-AEI method is also compared with various other image encryption techniques and it was found that SD-AEI cryptographic method takes optimal amount of time when compared to other encryption techniques, for encrypting and decrypting an image file. This method can be used to encrypt any type of image file, especially secret images, where steganography has been applied, so that the contents in the image file can be kept more secure.**

Keywords-Cryptography; Image Encryption; Extended Hill Cipher; Randomization; SD-EI;

I. INTRODUCTION

Due to tremendous growth in communication technology now the security of data is a really a big issue. In banking system the data must be fully secured. Under no circumstances the authentic data should go to hacker. In defense the security of data is much more prominent. The leakage of data in defense system can be highly fatal and can cause too much destruction. Due to this security issue, different cryptographic methods are used by different organizations and government institutions to protect their data. 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 produce different new cryptographic method to keep the data safe as far as possible.

The cryptographic methods can be basically divided into two types: (i) symmetric key cryptography, where the same key is used for encryption and for decryption purpose. (ii) Public key cryptography, where we use one key for encryption and one key for decryption purpose.

Symmetric key algorithms are well accepted in the modern communication network. The main advantage of symmetric key cryptography is that the key management is very simple. Only one key is used for both encryption as well as for decryption purpose. There are many methods of implementing symmetric key. In case of symmetric key method, the key should never be revealed / disclosed to the outside world or to other user and should be kept secure. The key should be known to sender and the receiver only and no one else.

There are many normal and combined encryption techniques for images. Komal D Patel and Sonal Belani [1] have presented a survey on existing work, which has used different techniques for image encryption as subject matter and also given a general introduction about cryptography. There are several methods for image encryption with some advantages and disadvantages. Ismet Ozturk and Ibrahim Sogukpinaar [2] have discussed the analysis and comparison of image encryption algorithms. And they classified the image encryption methods into three major types: (i) position permutation, (ii) value transformation and (iii) visual transformation. Nath et al [8],[9],[10],[12] have proposed many combined cryptographic techniques for securing digital data using both encryption and steganography. Nath et al. have also developed an encryption technique using randomization method in form of MSA [10]. Panduranga H T and Naveenkumar S K [4] have proposed an approach using bit reversal method. Bibhudendra Acharya et al [5] have proposed several methods of generating self-invertible matrix, which can be used in Exended Hill Cipher algorithm. Saroj Kumar Panigrahy et al [6] have implemented image encryption using Self-Invertible key matrix of Hill Cipher algorithm.

978-1-4673-1107-6/12/$31.00 ©2012 IEEE

Bibhudendra Acharya et al [7] have proposed a novel Advanced Hill Cipher encryption technique, which uses Involutory key matrix. Somdip Dey [11],[13],[14],[15] has proposed a technique of combining both the bits rotation and reversal technique and the extended hill cypher method to encrypt images in SD-EI [11] Image Encryption method.

The method proposed in this paper, SD-AEI, is basically a combined symmetric key cryptographic technique, which is basically based on three cryptographic methods: 1) Bits Rotation and Reversal; 2) Extended Hill Cipher; 3) Modified MSA Randomization. But, to achieve this combined technique, first an unique number (code) is generated from the password (symmetric key), which is provided for the encryption/decryption method.

The technique, SD-AEI, which is used to encrypt the images follows the following algorithm:

Step-1: ***Generation of Unique Number*** from the Key

Step-2: Image encryption technique by using ***bits rotation and reversal*** method based on password

Step-3: The ***Extended Hill Cipher technique for Image Encryption***.

Step-4: ***Modified MSA Randomization***

II. THE COMBINED CRYPTOGRAPHIC METHOD

1) GENERATION OF UNIQUE NUMBER FROM THE KEY

In this step, we generate an unique 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 unique because it 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 $[P_1P_2P_3P_4\ldots..P_{len}]$ 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 above mentioned step and denote this as N.

Now, if $N = [n_1n_2\ldots\ldots n_j]$, then we add all the digits of that number to generate the unique code (number), i.e. we need to do: $n_1 + n_2 + n_3 + n_4 + \ldots.. + n_j$ 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 'AbC', then,

P_1 = A; P_2 = b; P_3 = C

$N = 65*2^{(1)} + 98\ 2^{(2)} + 67*2^{(3)} = 1058$

Code = 1 + 0 + 5 + 8 = 14

2) BITS ROTATION AND REVERAL TECHNIQUE FOR IMAGE ENCRYPTION

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 length of password is considered for bit rotation and reversal. i.e., Number of bits to be rotated to left and reversed will be decided by the length of password. Let L be the length of the password and L_R be the number of bits to be rotated to left and reversed (i.e. L_R is the effective length of password). The relation between L and L_R is represented by equation (1).

$L_R = L \bmod 7$ ------ eq. (1)

where '7' is the number of iterations required to reverse entire input byte.

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

i.e. $P_{in}(i,j) \longrightarrow [B_1B_2B_3B_4B_5B_6B_7B_8]$

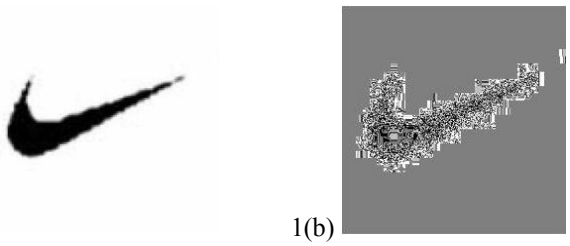
If L_R=5, five bits of input byte are rotated left to generate resultant byte as $[B_6\ B_7\ B_8\ B_1\ B_2\ B_3\ B_4\ B_5]$. After rotation, rotated five bits i.e. $B_1\ B_2\ B_3\ B_4\ B_5$, get reversed as $B_5\ B_4\ B_3\ B_2\ B_1$ and hence we get the resultant byte as $[B_6\ B_7\ B_8\ B_5\ B_4\ B_3\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

i.e. $[B_6B_7B_8B_5B_4B_3B_2B_1] \longrightarrow P_{out}(i,j)$

,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 *Bits Rotation & Reversal* generates the encrypted image. Figure 1 (a, b) shows input and encrypted images respectively. For the encryption process given password is "SYS2012", whose effective length (L_R) = 7.

Note: - If L=7, then L_R=0. In this condition, the whole byte of pixel gets reversed.



1(a) 1(b)

Figure 1. (a).Input Image. (b).Encrypted Image for password "SYS2012".

978-1-4673-1107-6/12/$31.00 ©2012 IEEE

3) EXTENDED HILLCIPHER 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 [6] and Bibhudendra Acharya et al [7]. In this work, involutory matrix is generated by using the algorithm presented in [7].

Algorithm of Extended Hill Cipher technique:

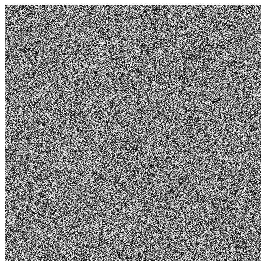
Step 1: An involutory matrix of dimensions $m \times m$ is constructed by using the input password.

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.

TABLE 1 shows various input and encrypted image respectively, where the encryption process is carried out by using *Extended Hill Cipher* technique. The password given to generate involutory matrix is "sandi".

TABLE 1

Input Image	Encrypted Image
	

4) MODIFIED MSA RANDOMIZATION

Nath et al. [8],[9],[10],[12] 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 [10] 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 detail description of the above methods are given in MSA [10] 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, 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-AEI 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()

Now, we describe the meaning of all above functions by implementing each function on a 4x4 matrix as shown below:

TABLE I : ORIGINAL TABLE

AA	AB	AC	AD
BA	BB	BC	BD
CA	CB	CC	CD
DA	DB	DC	DD

TABLE II: CALLED CYCLING( )

BA	AA	AB	AC
CA	BC	CC	AD
DA	BB	CB	BD
DB	DC	DD	CD

978-1-4673-1107-6/12/$31.00 ©2012 IEEE

TABLE III: CALLED UPSHIFT()

CA	BC	CC	AD
DA	BB	CB	BD
DB	DC	DD	CD
BA	AA	AB	AC

TABLE IV: CALLED RIGHTSHIFT()

AD	CA	BD	CC
BD	DA	BB	CB
CD	DB	DC	DD
AC	BA	AA	AB

.

TABLE V: CALLED LEFT_DIAGONAL_RANDOMIZATION()

DA	CA	BD	CC
BD	DC	BB	CB
CD	DB	AB	DD
AC	BA	AA	AD

TABLE VI: CALLED DOWNSHIFT()

AC	BA	AA	AD
DA	CA	BD	CC
BD	DC	BB	CB
CD	DB	AB	DD

TABLE VII: CALLED LEFTSHIFT()

BA	AA	AD	AC
CA	BD	CC	DA
DC	BB	CB	BD
DB	AB	DD	CD

TABLE VIII: CALLED RIGHT_DIAGONAL_RANDOMIZATION()

BA	AA	AD	DB
CA	BD	CC	AA
DC	CC	CB	BD
BB	AB	DD	CD

The functions shown above are to demonstrate the functionality of each called methods. The use of cycling function multiple times ("code", which is the unique number generated from the password, number of times) in the middle of all other functions makes the encryption technique totally random and more powerful from cryptanalysis attacks.

III. PROPOSED TECHNIQUE

This image encryption method consists of three stages, among which first stage is *Bits Rotation Reversal* stage, second stage is *Extended Hill Cipher* stage and third stage is *Modified MSA Randomization* stage. For all the stages, only one alphanumeric password is needed.

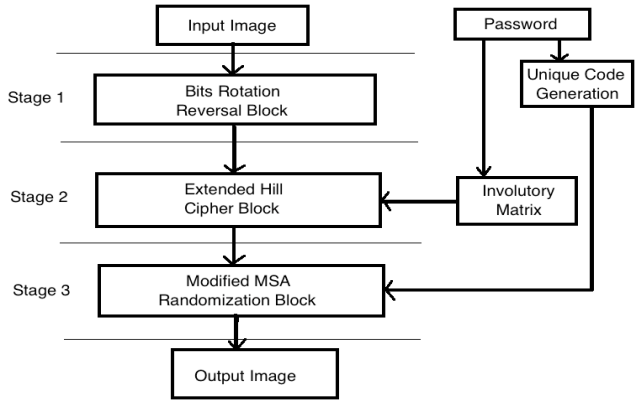


Figure 2. Block Diagram representation of proposed image encryption technique

In first stage, input image of first stage is given along with an *alphanumeric password*. Unique Code, which is an unique number, is generated from the given password and is explained in Section 1 of II. The encryption process is carried out as explained in Section 2 of II. But the encrypted image generated in first stage can be decrypted by other passwords of same length as original password. To avoid this inconvenience second stage of encryption has been designed. In second stage, an *Involutory Matrix* is generated by using the *alphanumeric password* given in first stage. By using password generated Involutory Matrix, *Extended-Hill-Cipher* technique is applied on encrypted image generated from first stage to obtain more secured encrypted image. To generate an Involutory Matrix, minimum length of alphanumeric password should be four. And finally in Third stage, the whole structure of the image file is messed up using randomization technique, where the randomization is totally dependent on the password provided in first stage. If the password is changed a little bit, then, the whole encryption process of the final stage (third stage) will be different. Figure 2 shows block diagram representation of Proposed Image Encryption Technique.

IV. RESULTS AND DISCUSSIONS

Here, the aforementioned technique is implemented for different images and also histograms are plotted for all stages. From the histograms, it can be observed that the histogram of encrypted image due to *Bits Rotation Reversal* technique is altered as compared to histogram of original image, and also the histogram of encrypted image due to *Extended Hill Cipher* technique is altered as compared to histograms of encrypted images of previous stages. But, it was seen that the histogram of the *Modified MSA Randomization* technique did not change as compared to Extended Hill Cipher technique, but the whole structure of the final encrypted image file is altered and there is no visible pattern to predict the cipher algorithm. Results of the encryption process for different images along with their histogram are tabulated in TABLE 2 & 3.

TABLE 2

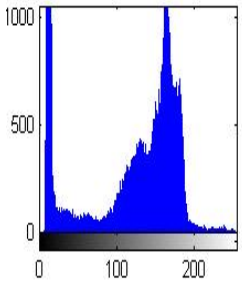
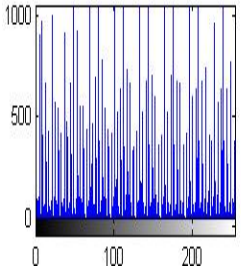
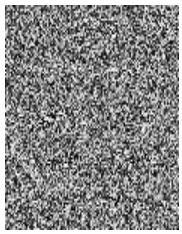
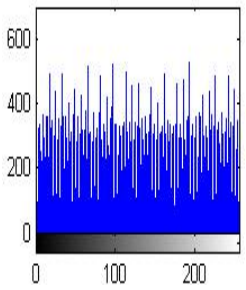
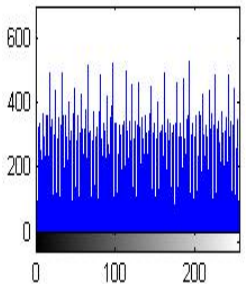
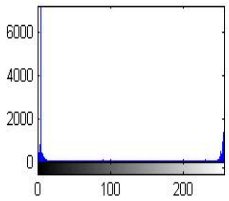
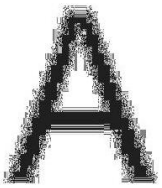
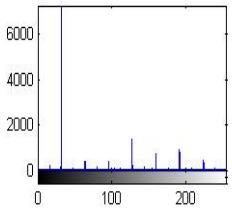
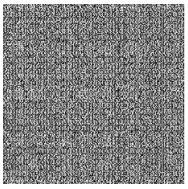
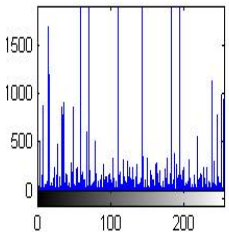
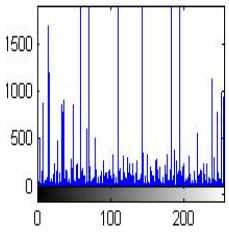
Password	sandi	
Input Image		
Encryption Stage 1 (using Bits Rotation Reversal technique)		
Encryption Stage 2 (Using Extended Hill Cipher technique)		
Encryption Stage 3 (Using Modified MSA Randomization technique)	**No Preview**	

TABLE 3

Password	SOMDIP DEY

Input Image		
Encryption Stage 1 (using Bits Rotation Reversal technique)		
Encryption Stage 2 (Using Extended Hill Cipher technique)		
Encryption Stage 3 (Using Modified MSA Randomization technique)	**No Preview**	

V. COMPARISON WITH OTHER ENCRYPTION TECHNIQUES

The method, SD-AEI, proposed in this paper, is compared with other encryption techniques like SD-EI [12], MSA [11] and TTJSA [13].

TABLE 4 shows the difference between SD-AEI encryption technique and other encryption techniques on the basis of time taken to encrypt/decrypt and the encryption processes were executed using "sandi" as password.

TABLE 4: Time Taken To Encrypt/Decrypt in seconds (secs)

Image Size	SD-EI	SD-AEI	MSA	TTJSA
512 B	2	2	1	2
1 KB	2	3	2	3
512 KB	4	5	3	4
1 MB	6	6	5	7

978-1-4673-1107-6/12/$31.00 ©2012 IEEE

Thus, from the table it can be seen that time taken to encrypt/decrypt for SD-AEI is optimal in comparison to other encryption techniques. Figure 3 shows the difference in graphical representation.

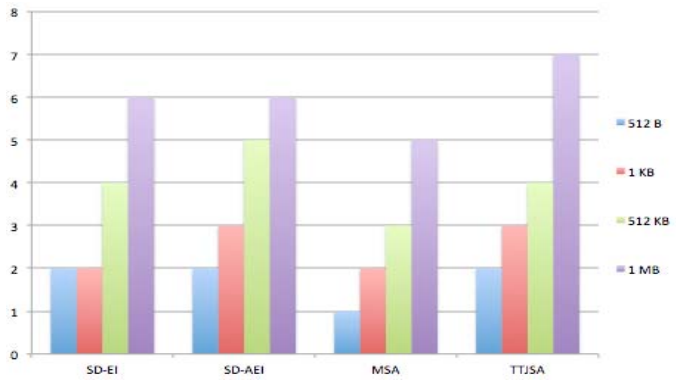


Figure 3. Difference between SD-AEI and other encryption techniques

Although from Figure 3, the least amount of time is taken by the MSA algorithm, but that encryption technique is not only for encrypting images but is a generalized version of encryption cipher, and MSA algorithm also has few flaws. TTJSA takes little more time to encrypt/decrypt large image files, but like MSA also it is for encrypting any type of files. SD-EI takes almost same time as SD-AEI to encrypt/decrypt, but in SD-AEI due to additional randomization encryption technique the encryption method used in SD-AEI is much stronger than SD-EI encryption technique.

VI. CONCLUSION AND FUTURE SCOPE

In this paper, the author proposes a technique, where the encryption has three stages. In first two stages the mage is encrypted using visual distortion and in the final stage the whole file structure is altered in a totally random fashion, so that there can be no preview of the image without knowing the exact cipher algorithm and the authentication password. SD-AEI technique can be used to encrypt secret images. We can also hide secret messages or password in an image and then encrypt it using SD-AEI technique, and then forward it to anyone more securely. The technique, SD-AEI, can be further extended by adding bit manipulation to this technique, so that the encryption algorithm becomes much more strong. And the author has already started working on that.

ACKNOWLEDGEMENT

Somdip Dey (SD) expresses his gratitude to all his fellow students and faculty members of the Computer Science Department of St. Xavier's College [Autonomous], Kolkata, India, for their support and enthusiasm. He also thanks Dr. Asoke Nath, professor and founder of Computer Science Department of St. Xavier's College (Autonomous), Kolkata, for his constant support and helping out with the preparation of this paper.

REFERENCES

[1]. Komal D Patel, Sonal Belani, "*Image encryption using different techniques:A review*", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 1, November 2011

[2]. Ismet Ozturk and Ibrahim Sogukpinaar, "*Analysis and Comparison of Image Encryption Algorithms*", Transaction on engineering, Computer and Technology, 2004, vol.3, pp.38-42.

[3]. Mitra et. el., "*A New Image Encryption Approach using Combinational Permutation Techniques*," IJCS, 2006, vol. 1, No 2, pp.127-131.

[4]. Panduranga H T, Naveenkumar S K, "*An image encryption approach using bit-reversal method* ", NCIMP 2010, pp.181-183.

[5]. Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy. 2007. "*Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm*", International Journal of Security, Vol 1, Issue 1, 2007, pp.14-21.

[6]. 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.

[7]. 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.

[8]. Joyshree Nath and Asoke Nath,"Advanced Steganography Algorithm using encrypted secret message", International Journal of Computer Science and Applications, Vol-2, No. 3, p. 19- 24, Mar (2010).

[9]. Joyshree Nath, Meheboob Alam Mallik, Saima Ghosh and Asoke Nath, "New Steganography algorithm using encrypted secret message", Proceedings of Worldcomp 2011 held at Las Vegas (USA), 18-21 Jul, 2011.

[10]. 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).

[11]. 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.

[12]. 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 "Information and Communication Technologies (WICT), 2011 " held at Mumbai, 11th – 14th Dec, 2011, Pages:1175-1180.

[13]. 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.

[14]. 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.

[15]. 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.

978-1-4673-1107-6/12/$31.00 ©2012 IEEE