Modified Image Encryption Technique

Kirti Sapra [1], Swati Kapoor [2]

P.G. Student, Department of Electronics and Communications, R.P.I.I.T college, Haryana, India[1]

Assistant Professor, Department of Electronics and Communications, R.P.I.I.T college, Haryana, India[2]

ABSTRACT – *Protection to the data over the open network is very important. Encryption is one of the ways out to make your data safe and secure. In this paper, the main objective is to present a modified image encryption technique, which does not only makes the image very difficult to retrieve by any other person except the recipient but also reduces the time for encryption. This proposed encryption technique is the combined technique of various methods of encryption such as: RSA algorithm, Bit Rotation method, Ex-Hill Cipher method, Bit Reversal method and Randomization using Permutation. First the pixels value of an image is converted into eight bit binary format. RSA algorithm is chosen to generate the passwords, encrypting key and decrypting key. After this above mentioned methods are applied to encrypt the image. After the generation of new 8 bit value, the binary values are converted back to decimal format and the new pixels values replace the older one.*

Keywords

RSA, Ex- Hill Cipher, Permutation, Bit Rotation and Reversal.

1) INTRODUCTION

With the advent of technologies, the large numbers of users generate and exchange information in various fields such as in banking, defence, and financial institutions, e-shopping. The exchange of information requires a special security for the transmission of information over the insecure network and for the storage of information. For this method, encryption and decryption of data at respective sender and receiver side is applicable. Confidential data transmission requires a fast, secure and non reproductive exchange of information. Cryptography is the methods that allow the information to be sent in a secure form in such a way that only receiver able to retrieve the information. However the goal of cryptography is not only to provide confidential data but also it provides the solution to other problems such as authenticity, availability, integrity and non repudiation.In the modern era, cryptography has been categorised in two ways:

a) Symmetric Key Cryptography
b) Asymmetric Key Cryptography

In symmetric key cryptography same key is used for encryption and decryption purpose. If two people is communicating then only one key is required but with the increase in number of people, the number of keys are also increased. If n people are communicating then we require (n)(n-1)/2 keys. Therefore it is difficult to manage with large number of keys. Moreover, it is more susceptible to attacks, once the hacker able to crack the key. In Asymmetric Key Cryptography, two keys are generated. One key is used for encryption (public key) and other key is used for decryption (private key). Various algorithms has been using now-a-days such as RSA or Elliptic Curve Cryptography. These are very famous for their high security purpose. Also RSA is very time efficient in encrypting an image. RSA takes lesser time to encrypt the image than DES and Blowfish[16]. By the means of combining the public key cryptography, public key certification and secure hash function there are protocols that enable the digital signatures, authentication and integrity. In the proposed method RSA is used to generate the password and using this password further methods are used to encrypt the image.

There are many normal and combined encryption techniques for images. Bharti Ahuja and Rashmi Lodhi [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. 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.

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], [17] 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. SD-AEI, is basically a combined symmetric key cryptographic technique, which is basically based on three cryptographic methods Bits Rotation and Reversal, Extended Hill Cipher; Modified MSA Randomization.

The method proposed in this paper, is basically a combined asymmetric key cryptographic technique, which is basically based on various cryptographic methods: 1) Bits Rotation; 2) Extended Hill Cipher; 3) Bit Reversal 4) Randomization using permutation. But before these methods RSA algorithm is applied to generate the passwords to encrypt and decrypt the image.

The modified encryption technique, which is used to encrypt the image follows the following algorithm:

Step-1: RSA algorithm
Step-2: Image encryption technique by usingbits rotation method
Step-3: TheExtended Hill Cipher technique for ImageEncryption.
Step 4: Bit Reversal method
Step-5: Randomization using permutation.

2) THE COMBINED CRYPTOGRAPHIC METHOD

2.1.1 RSA

In this step, we generate two passwords, one used as a public key and other as a private key. The image is encrypted using public key and the decrypted using private key at sender and receiver respectively. Depending on length of password generated in RSA, the number of bits is used later for arrangements in randomization. Various steps of RSA are as follow:

- Take two large distinct primes p and q and then form the public modulus n= pq.
- Select a public exponent e to be co-prime to (p-1)(q-1), with 1< e <(p-1)(q-1)
- The pair (n, e) is a public key.
- The private key is the unique integer 1< d <(p - 1)(q – 1) such that ed = 1 mod(p-1)(q-1)
- The pair (n, d) is a private key.
- Encryption: split the message into sequence of blocks M1, M2, . . Mi, where each Mi satisfies 0< Mi < n then encrypt the blocks as $C = E(M) = M^e \pmod n$
- Decryption : with private key d and C (cipher text) , the decryption function is:
  $D(C)= C^d \pmod n$

Note that encryption does not increase the size of a message. The message text and the cipher text, both are integers in the range 0 to n – 1.
Each user creates his encryption key and makes it public, and also create the corresponding decryption key and use it privately.
Now by using receiver's public key, the sender sends the message and receiver retrieve the image using his decryption key.

2.1.2 BITS ROTATION TECHNIQUE

In this method, value of each pixel of input image is converted into equivalent eight bit binary number. Now the bits are rotated to one bit right.
For example, $X_{in}(i,j)$ is the value of a pixel of an input image. $[P_1P_2P_3P_5P_6P_7P_8]$ is equivalent eight bit binary representation of $X_{in}(i,j)$.
i.e.

$X_{in}(i,j)$ $[P_1P_2P_3P_4P_5P_6P_7P_8] \longrightarrow$
This resultant byte is converted toequivalent decimal number $X_{out}(i,j)$.i.e.

$[P_2P_3P_4P_5P_6P_7P_8P_1]$ $X_{out}(i,j) \longrightarrow$

where $X_{out}(i,j)$ is the value of output pixel of resultant image.
As, the weight of each pixel value of an image is responsible for its colour, therefore if any change occur in the weight of each pixel of input image due to Bits Rotation, it willmake the image as encrypted image.

2.1.3 EXTENDED HILLCIPHER TECHNIQUE

This new method for encryption of images proposed in the paper [17] by somdip dey. 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].

Extended Hill Cipher technique:

- An involutory matrix of dimensionsk×kisformed by using the input password.
- Index value of each row of input image is convertedinto *y*-bit binary number, where *y* is the number of bits present in binary equivalent of index value of last row of input image. The resultant *y*-bit binary number is rearranged in reverse order. This reversed-*y*-bit binary number is converted into its equivalent decimal number. Hence, 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-Reversal-Order. In

the same way, positions of all columns of input image are also rearranged in Bits-Reversed-Order.

- Hill Cipher algorithm is applied for thePositionalManipulated image generated from Step 2 to obtain the encrypted image.

2.1.4 BIT REVERSAL TECHNIQUE

In this method, the output of extended hill cipher method, the rows of the matrix are reversed. For example, $X_{in}(i,j)$ is the value of a pixel of an input image. $[P_1P_2P_3P_5P_6P_7P_8]$ is equivalent eight bit binary representation of $X_{in}(i,j)$.
i.e.

$X_{in}(i,j)$ $[P_1P_2P_3P_4P_5P_6P_7P_8]$
This resultant byte is converted toequivalent decimal number $X_{out}(i,j)$.i.e.

$[P_8P_7P_6P_5P_4P_3P_2P_1]$ $X_{out}(i,j)$

2.1.5 RANDOMIZATION USING PERMUTATION

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.
In SD-AEI, 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.
In the modified image encryption technique, randomization is done using permutation here two bits are rotated using password. That is a general permutation formula is used:
${}^{n}P_r$ = fact (n) / fact (n-r)
We are using 8*8 block matrix here, hence 8 bits are rotated and two bits move simultaneously.
Where, n = length of password and r = number of bits taken into considerations.
By adding this permutation block we got the variety of arrangement of pixel values of the image. Here value of r is taken as 2, that means two bits are rotated simultaneously and hence time to encrypt an image gets reduced.

3) PROPOSED TECHNIQUE

This image encryption method consists of various stages, among which first stage is Bits Rotation, second stage is Extended Hill Cipher stage and third stage isReversal stage and thenRandomization using permutation stage. For all the stages, onlyone alphanumeric password is neededwhich is generated using RSA algorithm. This RSA algorithm generate a password for encryption and the same password used in Ex Hill Cipher in the form of involutory matrix and also used in later steps of permutation. After the encryption of image using encrypting key, the binary value of the image is rotated left one time in each row. Thus change the bit value of the image and encrypt the image up to a certain level. Now after rotation of bits, the Ex hill cipher method is applied using the password. After hill cipher the reversal of bits method takes place. At last step, the randomization of bits using permutation takes place and thus final encrypted image is obtained. The flow diagram for the modified encryption algorithm is shown below in the figure 1

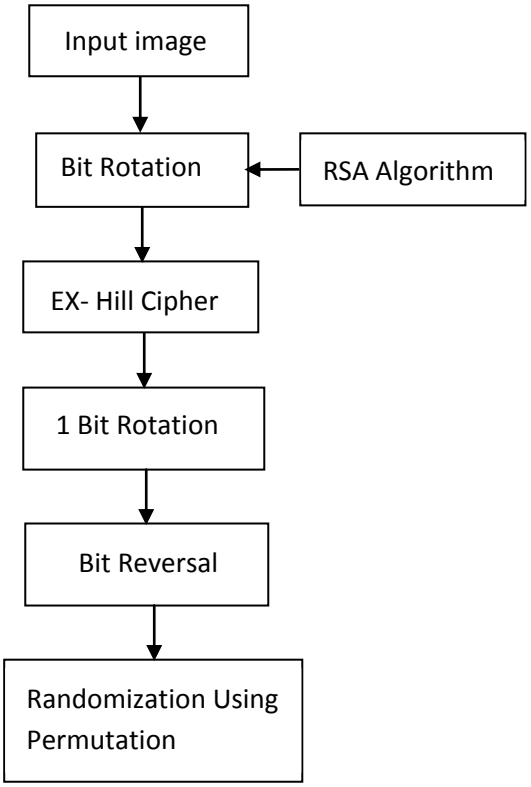


Figure 1: Block Diagram representation of Proposed image encryption technique

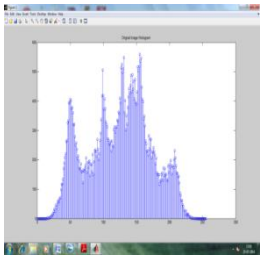
4) RESULTS AND DISCUSSIONS

Here, the aforementioned technique is implemented for different images and the encrypted image is shown for all stages. Also the histogram of the original image and the final permuted image is also shown. it can be observed that the histogram of encrypted image is altered as compared to histogram of original image. Here the encrypted image is shown after every step, as the different methods are applied the level of encryption is increasing and making the original image more

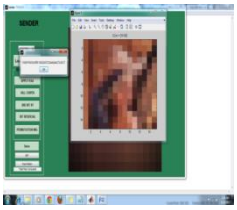
complex even harder for the brute force attack. In the last step randomization is done using permutation, therefore two bits are rotated simultaneously for different arrangements and this reduces the total time taken for encryption.

5) EXPERIMENTAL RESULTS:

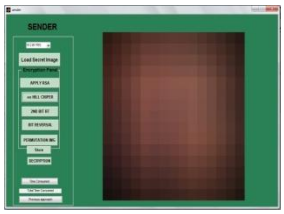
Original Image



Histogram of Original Image

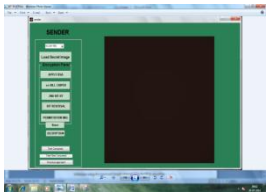


Step 1: RSA

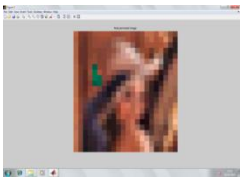


Step 2: Bit Rotation& Hill Cipher

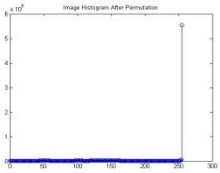
Step 3: Bit Rotation



Step 4: Bit Reversal



Step 5: Permutation



Histogram of Final Image

The proposed technique has been applied to images of variable size and on the basis of the size of an image time calculation has been done. The above table shows the time taken by the images of variable sizes.

TIME TAKEN FOR ENCRYPTION/DECRYPTION

Image Size	Total Time consumption for Encryption (in sec)
512 bytes	1.2
1024 bytes	2.10
2048 bytes	2.38
4096 bytes	3.65

Table 1: Time taken to Encrypt/ Decrypt an Image

6) CONCLUSION AND FUTURE SCOPE

In this paper, the author proposes a technique, where the encryption has four stages. In first three stages the image is encrypted using visual distortion and in the final stage the whole file structure is altered in a totally random fashion using permutation, so that the time taken for encryption reduced to encrypt an image. Thus, modified image encryption technique can be used to encrypt secret images and that too in less time. We can also hide secret messages or password in an image and then encrypt it using proposed technique, and then forward it to anyone more securely. The technique can be further extended by adding bit manipulation to this technique, so that the encryption algorithm becomes much strong. Also the normalized correlation coefficient (NCC) can also be calculated to compare the similarity among two images. The effect of NCC in gray level and colour images and its effect can be used to for defect detection.

REFERNCES:

[1]. Bharti Ahuja, Rashmi Lodhi, "*Differentalgorithm used in Image encryption :A review*", International Journal of computer sciences and engineering Technology, ISSN 2229-3345, Volume 4, No. 7, July 2013.

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

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

[4]. Panduranga H T, Naveenkumar S K, "*An image encryption approachusing 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-InvertibleMatrix for Hill Cipher Algorithm*", International Journal of Security, Vol1, Issue 1, 2007, pp.14-21.

[6]. Saroj Kumar Panigrahy, Bibhudendra Acharya, Debasish Jena, "*ImageEncryption 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 CipherAlgorithm*", 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 ofComputer Applications* 46(20): 46-53, May 2012. Published byFoundation of Computer Science, New York, USA.

[16]. Ali E. Taki El Deen, El-Sayed A. EL-Badawy and Sameh N. Gobran, "Digital Image Encryption Based on RSA algorithm" , IOSR journal of Electronics and Communications (IOSR-JECE) e-ISSN: 2278-2834, p-ISSN: 2278-8735. Volume 9, Issue 1, Ver. IV(Jan 2014), PP 69-73.

[17]. Somdip Dey, " SD-AEI: Advanced encryption techniques forthe images" , 2012 IEEE Second International Conference onDigital Information Processings and Communications(ICDIPC),pp. 69-74