Image Encryption Using Advanced Techniques

Gurpreet Singh[1], Amandeep Kaur[2]

[1]STUDENT M.TECH ECE PUNJABI UNIVERSITY PATIALA

[2]ASSISTANT PROFESSOR DEPARTMENT OF ECE PUNJABI UNIVERSITY PATIALA

ABSTRACT

In this era of technology, security is a big issue and securing important data is very essential, , and encryption is one of the way to ensure security so that the data can not be intercepted or misused for illegal purpose. Different techniques are proposed to make encryption stronger. In this paper, we survey on existing work which is used different techniques for image encryption and discussed the most advanced technique which is a combination of four stages for higher security: 1. Modified Bits Rotation and Reversal Technique for Image Encryption 2. Extended Hill Cipher Technique for Image Encryption 3. Modified Cyclic Bit Manipulation 4. Bit Reversal Technique.

Keywords - Image Encryption, Bit Reversal, Bit Manipulation, Bit Rotation, Hill Cipher, Randomization.

I. INTRODUCTION

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. 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 crypto-graphic methods [13] 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 there 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 [1][2], only one key is used for encryption purpose and the same key is used for decryption purpose. Public key cryptography, also called asymmetric key cryptography, uses a pair of keys for encryption and decryption. In public key cryptography, keys work in pairs of matched public and private keys.

2. DIFFERENT TECHNIQUES

1) SD-EI: A Cryptographic Technique to Encrypt images.

SD-EI, for image encryption, which basically has two 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 involuntary matrix, which is generated by same password used in second stage of encryption to make it more secure.

2) SD-AEI: An advanced combined encryption technique for encrypting images using randomized byte manipulation. 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 involuntary 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**.**

3) SD-IES: An Advanced Image Encryption Standard an advanced version of image encryption technique, which is itself an upgraded version of SD-EI image encryption method. In this new method, SD-IES, there are more bit wise manipulations compared to original SD-EI method. The proposed method consist of four 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 the third 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; 4) In the last stage of encryption, the pixels are again converted to their 8 bit pattern and the total bit pattern is reversed to achieve the last encryption phase.

This method discussed in this paper is a type of symmetric key cryptographic method, which is itself a combination of four different encryption modules. The four different encryption modules, which make up this 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
4. Bit Reversal Technique.

3.THE METHODS

Before we discuss the four methods, which make the SD-IES 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**.**

A) 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 $[P1P2P3P4....P_{len}]$ 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_1,n_2……nj], then we add all the digits of that number to generate the unique code (number), i.e. we need to do: n1 + n2 + n3 + n4 + ….. + nj 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,

P1 = A; P2 = b; P3 = C

N = 65*2(1) + 98 2(2) + 67*2(3) = 1058

Code = 1 + 0 + 5 + 8 = 14.

B) MODIFED 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 mod 7 ... (1)

where '7' is the number of iterations required to reverse entire input byte and N = [$n_1 + n_2 + n_3 + n_4$ + ... nj], where n_1,n_2 ...... nj is the ASCII Value of each byte of the password. For example, Pin(i,j) is the value of a pixel of an input image. [B_1 B_2 B_3 B_4 B_5 $B_6B_7B_8$] is equivalent eight bit binary representation of Pin(I,j).

i.e. P_{in}(i,j) - [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_4B_5, get reversed as B_5 B_4 $B_3B_2B_1$, and hence we get the resultant byte as [B6 B_7 B_8 B_5 $B_4B_3B_2B_1$]. This resultant byte is converted to equivalent decimal number 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, thenN_R=O. In this condition, the whole byte of pixel gets reversed,

C. EXTENDED HILL CIPHER TECHNIQUE

Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda [3] have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption.

Algorithm of Extended Hill Cipher technique

Step 1: An involutory matrix of dimensions m x 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 presentation 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[3].

D) 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 i: 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

BLOCK DIAGRAM

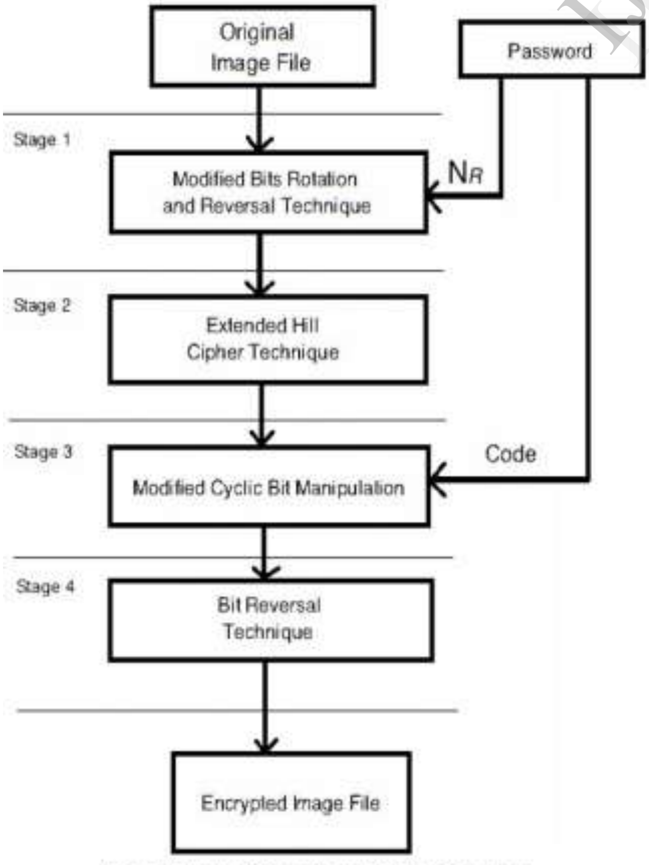

FIG 1: BLOCK DIAGRAM OF SD-IES METHOD

IV. DECRYPTION PROCESS

The Decryption process is a reverse process of encryption process, i.e. it is just the opposite to the process of the encryption method.

4.CONCLUSION

In this paper different techniques to encryept the image are discussed . SD-IES method is very successful to encrypt the image perfectly to maintain its security and authentication. The inclusion of modified bits rotation and reversal technique ,modified Cyclic Bit Manipulation and Bit Reversal technique in last stages, made the system even stronger than it used to be before.In future, the security of this method can be further enhanced by adding more secure bit and byte level cryptographic techniques to the system.

5.References

[1] Cryptography & Network Security, Behrouz A. Forouzan, Tata McGraw Hill Book Company.
[2] http://en.wikipedia.orglwiki/Symmetric-key_algorithm
[ONLINE]
[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.
[4] Somdip Dey, Joyshree Nath, Asoke Nath,"An Integrated Symmetric Key Cryptographic Method - Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit
[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 (lCDIPC), pp. 69-74.
[7] Asoke Nath, Trisha Chatterjee, Tamodeep Das, Joyshree
Nath, Shayan Dey, "Symmetric key cryptosystem using combined cryptographic algorithms -

Generalized modified Vern am Cipher method, MSA method and NJJSAA method: TTJSA algorithm", Proceedings of "WICT, 2011 " held at Mumbai, 11 th - 14th Dec, 2011, Pages: 1175-1180

[8] Somdip Dey, "SD-REE: A Cryptographic Method To Exclude Repetition From a Message", Proceedings of TheInternational 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. absI1205.4279, 2012.

[10] 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.

[II]http://en.wikipedia.orglwiki/RSA_(algorithm)[ONLINE]

[12]http://en.wikipedia.orglwikilElliptic_curve_cryptography [ONLINE]

[13] Cryptography & Network Security, Behrouz A. Forouzan,v Tata McGraw Hill Book Company.

[14]http://en.wikipedia.orglwikilPublic-key_cryptography [ONLINE]