© 2015 IJSRSET | Volume 1 | Issue 6 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Study and Modified Key Based Image Encryption using RSA Algorithm

Devashish Vaghela*, Rajyalakshmi Jaiswal
Department of Computer Science and Engineering, L. D. Engineering College, Ahmedabad, Gujarat, India

ABSTRACT

Now a day's data security is one of key issue in information security whether it is image, audio, text etc. We are sharing image files for many causes like identity information, medical diagnosis, and study on space related issues so while we do transfer images there should be some defensive security mechanism in order to stand against vulnerably attacks on image data. There exist various techniques in cryptography for encryption of images. In this paper we studied various image encryption methods and proposed a more secured Encryption with incorporating RSA algorithm in Password key generation and we have passed same key in consecutive steps of bit rotation, extended hill cipher, modified vernam cipher, modified MSA algorithm in order to improve security of password key as well as Image encryption method.

Keywords: Cryptography, Image encryption, RSA, Extended Hill Cipher

I. INTRODUCTION

Now a day's world is going towards digital media. So in general thinking it is good there will be less human efforts and more time and work potential utilization but digitalization comes with big security and vulnerability threats. In present scenario we transfer many confidential image files through digital gadgets. There can be possibility that our data will be intercepted by any unwanted personal to whom we don't want to share our valuable data. So to avoid such circumstance encryption of image or any data file is required before sharing Security of data is an important aspect in communication and storage. Image data security can be ensured by applying encryption to the images or by using various types of image watermarking techniques. Image encryption techniques convert original digital image to encrypted image that is difficult to understand and to keeps the image confidential between users. It is important that without key no one can access the content. Image encryption has applications in online shopping, Medical diagnostics and space applications. However, the traditional cryptosystems used for text encryption is not suitable for following reasons. Digital images are usually larger in size than that of text. Therefore, the traditional system takes more time for encrypting the digital image data. Other is decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Many techniques under cryptography is there to encrypt data and get back to original format. There are some terms widely used in cryptography area like cryptanalysis, cryptology and cipher data. Cryptanalysis means to decode message from non-readable to readable format. Encoded message is refer to as a cipher data.
Cryptography can be broadly classified in two terms.

1. Symmetric key cryptography
2. Asymmetric key cryptography

In Symmetric key cryptography also known as private key cryptography one key is used for both purpose encryption and decryption and in asymmetric key cryptography also known as public key cryptography have two different keys for encryption and decryption respectively. In asymmetric key decryption key is private and encryption key is publically defined. So asymmetric Key cryptography is more secure compare to symmetric key cryptography. There are various techniques exist in symmetric and asymmetric cryptography for image data encryption.

IJSRSET151641 | Received: 06 December 2015 | Accepted: 09 December 2015 | November-December 2015 [(1)6: 185-189]

Key cryptography is more secure compare to symmetric key cryptography. There are various techniques exist in symmetric and asymmetric cryptography for image data encryption.

II. METHODS AND MATERIAL

2.1 Image Encryption

There are many ways for image encryption like position permutation, value transformation, and visual transformation etc. In permutation, transformation and randomization we use random bit manipulation on image pixels.

In our study we consider various techniques in order to do bit manipulation in image encryption like RSA algorithm in order to generate encryption key, advance hill cipher algorithm, bit rotation and randomization, matrix transformation. Firstly Image is converted into block of bit values. Block size is decided initially. Then we will generate two public and private key using RSA algorithms. After that with help of bit rotation we shuffled bit values and we will apply involutory Matrix generated using key apply to that blocks. Next Step we will apply modify vernam cipher. Next step will be applying cyclic bit randomization and rotation. So at end we will get encrypted form of image.

2.2 Methods Use in Image Encryption

A. RSA Algorithm.[1]

We do 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.

Steps:

- 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 (i.e. no two factor should be same except 1) to (p-1) (q-1), with 1< e < (p-1) (q-1)
- The pair (e, n) is a public key.
- The private key is the unique integer
- 1< d < (p -1) (q – 1) such that e*d = 1 mod (p-1) (q-1). The pair (d ,n) 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) = Me (mod n)
- Decryption :
  With private key d and C (ciphertext), the decryption function is:
  D(C) = Cd (mod n)

Here while we do encryption size of message remains same no matter it is plain data or cipher data. So if image is divided into n block of pixels then size of image would be 0….n-1.

B. Image Block Creation[10]

In order to disturb the correlation among pixels and increase the entropy value, we divide the images into the horizontal row wise blocks and perform XOR of these blocks before passing the image to the encryption algorithm.

In this step, an image to be encrypted and a key is provided. The key provided consists of alphanumeric characters. In this method we will find total of ASCII Key value of key value provided then we finds sum of each ASCII value. Then we iteratively find sum of digit we get while adding until we get single digit value.

After dividing the images into sum of rows, and keeping first horizontal block as it is, and all other horizontal blocks are replaced with the result of XOR of the corresponding horizontal block with first horizontal block. i.e. each horizontal block is XOR with first horizontal block. Here first horizontal block acts as a key for XOR operation. Original image blocks can be recovered by XOR the result block again with first horizontal block.

C. Extended Hill Cipher.[9]

Generally for normal and grey scale images hill cipher and advance hill cipher is used. In Hill Cipher we requires key matrix should be inversible.so due to this we will use involutory key matrix because involutory key matrix is self inversible.

A is called an involutory matrix if A = A^{-1}.

Algorithm

Step 1: An involutory matrix of dimensions p x p is Constructed by using the input key generated by RSA algorithm.

Step 2: Index value of each row of input image is converted into n-bit binary number, where n is number of bits present in binary equivalent of index value of last row of input image. The resultant n-bit binary number will be reversed. This reversed-n-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 reversed Order. Similarly, positions of all columns of input image are also rearranged in Reversed-Order.

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

D. Bit rotation and reversal technique.

We generate 8 bit equivalent bit binary number from image provided for encryption. Now we add the ASCII Value of each byte of the key generated using RSA algorithm. This number is used for the Bits Rotation and Reversal technique i.e., Number of bits to be rotated to left or right 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 (NR), according to which the bits will be rotated and reversed.

Let N be the number generated from the key using RSA algorithm 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 3 ... (1)

Where '3' is the number of iterations required to reverse entire input byte and N = [$n_l + n_2 + n_3 + n_4 + \ldots\ldots n_j$], where $n_{1,}$ n_2,… n_j is the ASCII Value of each byte of the password.

For example, $P_{in(ij)}$ 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 $P_{in(ij)}$.

Example:

$P_{in(i,j)}$ → [B_1, $B_{2,}$ B_3, B_4 ,B_5 $B_{6,}B_{7,}$ B_8]

If NR= 5, five bits of input byte are rotated left to generate resultant byte as

[B_6 B_7, B_8, B_1, B_2, B3, B4 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, B8, B_5, B_4, B3 B_2 B_1].

This resultant byte is converted to equivalent decimal number $P_{out(i,j).}$

i.e. [B_6, B_7, B8, B_5, B_4, B3 B_2 B_1] → Pout (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 modify Bits Rotation & Reversal generates the encrypted image.

Note: - If N= 3 or multiple of 3, then N_R=0. In this condition, the whole byte of pixel gets reversed. After this we apply MSA randomization.

E. Modified MSA Randomization[9]

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 detailed description of the method is given in MSA [4] algorithm.

F. Modified Vernam Cipher[9]

In this 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. [4][7]. 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.

G. Proposed modified key based Image Encryption algorithm using RSA.

Based on Literature study we have found password key was vulnerable to brute force attack. So we have proposed to secure password key encryption using RSA algorithm. In existing system secret key was used to share image password. We have proposed encryption of password using RSA algorithm in order to add more security in password key sharing. RSA generated password key will be used in bit rotation, Involutory key matrix and Vernam cipher algorithm. It overall improves security to brute force attack.

In this first of all image is divided into set of block consisting binary bit numbers. Then we do apply modified rotation and reversal technique in order to initial shuffling of bits. Then we will apply extended hill cipher method. Here we are using involutory matrix that is generated by key we have produced using RSA algorithm. After that we will apply Vernam Cipher method. In Modified vernam Cipher random number we are passing would be key generated using RSA algorithm. And lastly we follow Modified MSA algorithm. Here also random number will be passed from RSA algorithm generated password. The resultant image gives encrypted image of original image. As we know that it is not necessary that encrypted image data should be same as original as text data should be same. The resultant image would give encrypted form and as we have used Modified vernam cipher and MSA algorithm it is very difficult to decrypt image. Following figure shows general flow diagram.

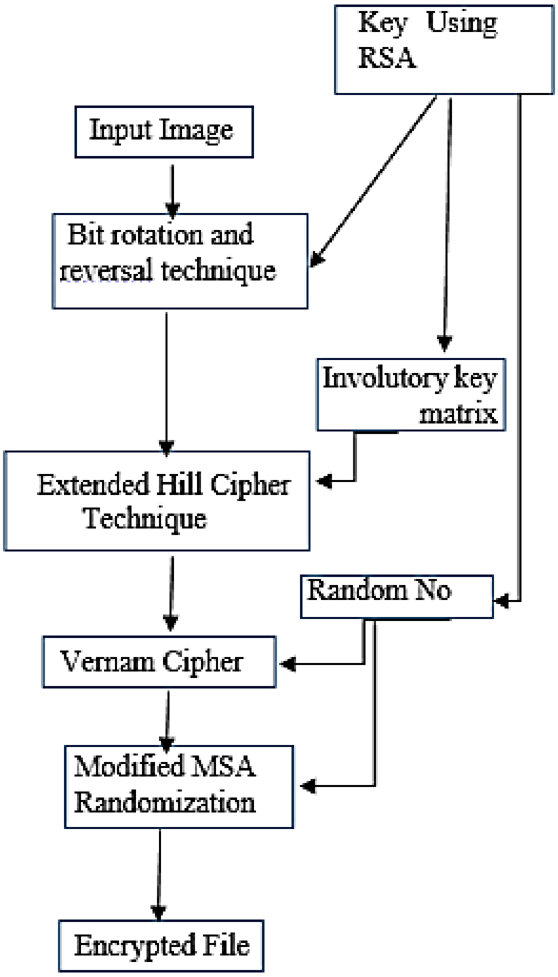
Key Using RSA
Input Image
Bit rotation and reversal technique
Involutory key matrix
Extended Hill Cipher Technique
Random No
Vernam Cipher
Modified MSA Randomization
Encrypted File

Figure 1: Image Encryption algorithm

III. CONCLUSION

Based on study of image encryption techniques we found that using bit rotation, reversal, mathematical models and matrix manipulation techniques we can encrypt images. These techniques can be very useful in medical imaging, space applications, and social media application. In existing methods we found there can be vulnerable attacks on password secret key that we are using for bit rotation and reversal, extended hill cipher. In order to improve security of image data encryption we proposed algorithm that uses password generated using RSA algorithm. So due to this modification security of password key will be increased to brute force attack. We will measure performance using parameters Normalized correlation coefficient (NCC) and correlation index.

IV. REFERENCES

[1] Kirti Sapra, Swati Kapoor, "MODIFIED IMAGE ENCRYPTION TECHNIQUE", (SSRG-IJECE) – August 2014

[2] B Acharya, S Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", ACEEE, Vol 1, No. 1, Jan 2010

[3] Somdip Dey, Sriram S. Ayyar, S.B. Subin, P .K. Abdul Asis,"SD-IES: An Advanced Image Encryption Standard Application of Different Cryptographic Modules in a New Image Encryption System"

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

[6] S 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.

[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] S Dey, "SD-AEI: An advanced encryption technique for images", 2012 IEEE Second International Conference on Digital Information Processing and Communications (lCDIPC), pp. 69-74.

[9] S Dey, "An Image Encryption Method: SD-Advanced Image Encryption Standard: SD-AIES", (IJCSDF) 1(2): 82-88, (ISSN: 2305-0012)

[10] Rajput Y, Gulve A, "An Improved Cryptographic Technique to Encrypt Images using Extended Hill Cipher", International Journal of Computer Applications (0975 – 8887) Volume 83 – No 13, December 2013