International Journal of Advanced Research in Engineering Technology & Sciences ISSN: 2394-2819

June-2016 Volume 3, Issue-6

Email:editor@ijarets.org www.ijarets.org

IMPROVEMENT PROTECTION IN RSA ALGORITHM USING 2 BIT ROTATIONS

Monika Suhag
M. Tech Scholar
Department CSE
GITM, Kablana, Jhajjar

Dr. Neetu Sharma
Assistant Professor
Department CSE
GITM, Kablana, Jhajjar

ABSTRACT: - RSA is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA encrypt image with 1 bit rotation. In 1 bit rotation only 1 bit is shifted and at decrypt side shifted bit are reversed. But to make it more secure we are going to perform 2 bit rotation due to which it is more secure as compared to existing algorithm. After applying the 2 bit rotation we perform the permutation of that image that will give us encrypted image.

KEYWORD*:* Cryptography, RSA, Hill Cipher, Bit Rotation

I. INTRODUCTION

There is a process exist that are used for sending information in secret way. This process is known as cryptography [1]. This technique widely used for protection of information or data. Stenography is art of that technique in which information hides on the way of communication between two nodes. Cryptography covert message in cipher text form so that it is not possible for unauthorized party to understand it. So the information hidden by stenography technique cannot see by any other person that is not authorized for it. In this paper we are going to develop a new system by using both processes stenography and cryptography. New system developed for better protection and confidently. Now days in market we have a cryptography technique - RSA very secure technique. After that we use custom neural network technique for applying second encryption technique to make more secure. Even we can apply these both techniques alone but any attacker can get original message by decrypt separately. So we apply both techniques at same time so any intruder cannot decrypt it or not as easy as single encryption technique can. This paper will highlight a new method that is developed for more security where image can be encrypted by using cryptography and stenography. We know how these processes can process as like:

- It is more secure if we send data in hidden form as compared to send it encrypted or visible to others.
- Main benefit of hidden data is that attention of intruder cannot notice.
- By chance if data extracted then it may be in encrypted form.

So there can any way to crack the encrypted image but the algorithm proposed by us has some well features with different way to implement as following:

- At place of hiding complete text in image we firstly segments according to 32*32 segmentation plan.
- To merge ASCII encoded bits into the base image using public or private keys.
- Original message is accessible to that who knows about this with the help of keys that are used for encryption. Reverse process is applied to get original message.

Finally our object is to develop a method which is more secure and if anyone trying to access it from steno image [2] then it became waste for that intruder.

II. RSA ALGORITHM

RSA based on a public key system that is generated by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978 [5]. Three basic steps are required to complete the process of RSA operations that are; key generation, encryption and decryption. First, messages are converted to numbers (integers), and then the numbers are manipulated according to the prescribed encryption scheme. Here is the description of the RSA cryptosystem. For the implementation of RSA we have to follow following steps [6]:

Step 1 Firstly Choose two prime number p and q.
Step 2 Then compute value of n= p x q.
Step 3 Chooses e with (e, (p − 1)(q − 1)) = 1 and computes d with de ≡ 1(mod(p − 1)(q − 1)).
Step 4 Makes n and e public and keeps p, q, and d secret.
Step 5 Sender encrypts m as c ≡ me (modn) and sends c to Receiver
Step 6 Bob decrypts by computing m ≡ cd (modn).

III. HILL CIPHER

Hill cipher is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once.

OPERATION

Each letter is represented by a number modulo 26. (Often the simple scheme A = 0, B = 1, ..., Z = 25 is used, but this is not an essential feature of the cipher.) To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × nmatrix, again modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26). The cipher can, of course, be adapted to an alphabet with any number of letters; all arithmetic just needs to be done modulo the number of letters instead of modulo 26.

Consider the message 'ACT', and the key below (or GYBNQKURP in letters):

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector:

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Thus the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

Which corresponds to a cipher text of ‘POH’ Now, suppose that our message is instead 'CAT', or:

$$\begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix}$$

This time, the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \pmod{26}$$

Which corresponds to a cipher text of 'FIN'? Every letter has changed. The Hill cipher has achieved Shannon's diffusion, and an n-dimensional Hill cipher can diffuse fully across n symbols at once.

DECRYPTION

In order to decrypt, we turn the cipher text back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters). (There are standard methods to calculate the inverse matrix; see matrix inversion for details.) We find that, modulo 26, the inverse of the matrix used in the previous example is:

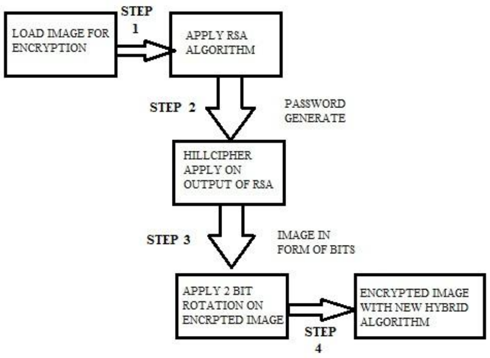
$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \pmod{26}$$

Taking the previous example cipher text of 'POH', we get:

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26}$$

Which gets us back to 'ACT', just as we hoped?

IV. ARCHITECTURE OF PROPOSED METHODOLOGY

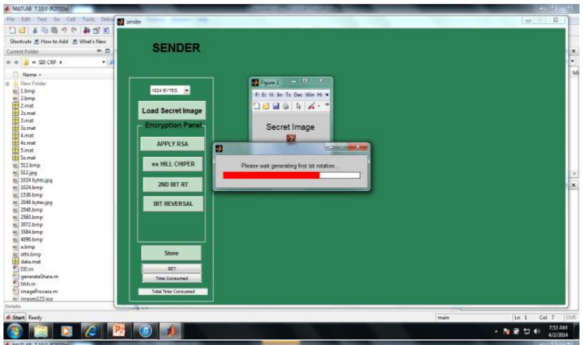

LOAD IMAGE FOR ENCRYPTION
STEP 1
APPLY RSA ALGORITHM
STEP 2
PASSWORD GENERATE
HILLCIPHER APPLY ON OUTPUT OF RSA
STEP 3
IMAGE IN FORM OF BITS
APPLY 2 BIT ROTATION ON ENCRPTED IMAGE
STEP 4
ENCRYPTED IMAGE WITH NEW HYBRID ALGORITHM

ENCRYPTION PROCESS FOR PROPOSED ALGORITHM

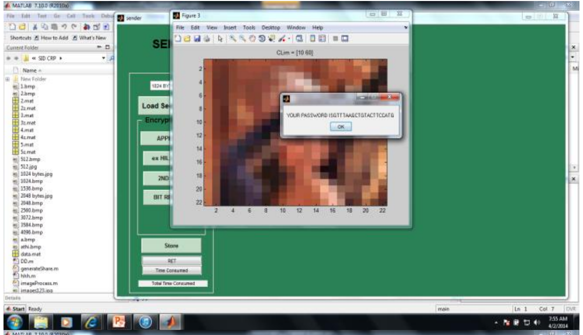
V. OBJECTIVES OF RESEARCH WORK

1. We have to study basic concept of cryptography.
2. After study concept, we need to choose algorithm which use in work like RSA, hill cipher.
3. Choose an image to start implementation, firstly apply rsa algorithm on this image to get encrypted image.
4. Use output of RSA as input for hill cipher algorithm. Implement hill cipher.
5. Now our purposed algorithm applied on encrypted image that is 2-bit rotation.
6. Permutation for encrypt image by 2 bit rotation is find out in this object.
7. In our last object we check some parameter like ret and store encrypted image.

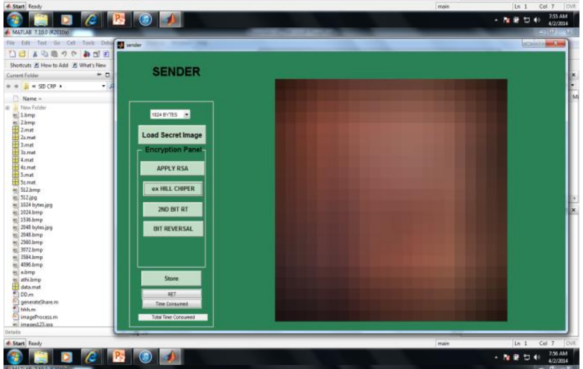
VI. RESULTS

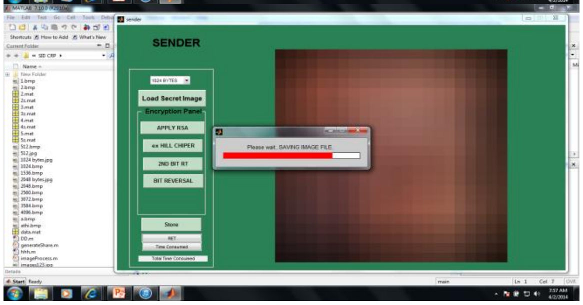


Please wait generating first bit rotation...



YOUR PASSWORD ISGTTTAAGCTGTACTTCCATG





Please wait..SAVING IMAGE FILE

VII. CONCLUSION

With the implementation of RSA algorithm using 2 bit rotation, a conclusion is achieved that for better secureness of any text or image we can apply any two techniques one by one on each other that make it more secure. For an illusion designing of this work we chose an image and apply RSA algorithm on it with hill cipher process. We got some encrypted image and after that apply the 2 bit rotation algorithm on encrypted image and further got an encrypted image that is very difficult to any other person to decrypt it. This is achievement in our conclusion that makes an image more secure.

REFERENCES

1. Domenico Daniele Bloisi, Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1, pp. 127-134.
2. Kharrazi, M., Sencar, H. T., and Memon, N. Image Steganography: Concepts and practice. In WSPC Lecture Notes Series (2004).
3. DiaaSalama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept
4. SimarPreet Singh, and Raman Maini "COMPARISON OF DATA ENCRYPTION ALGORITHMS" International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127
5. C. Kaufman, R. Perlman, M. Speciner, Network Security, Private Communication in a Public World, Prentice Hall, 1995.
6. Paul Brittan, Shelley Petzer, "Mobile Medical Records", Link: people.cs.uct.ac.za /~spetzer/mobile Med Records/results_shelley.html