Sunita, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 5, May- 2017, pg. 1-14 ISSN: 2321-8363
Impact Factor: 4.123

Image Encryption/Decryption Using RSA Algorithm

Sunita

Department of Electronics and Communication

Bhagat Phool Singh Mahila Vishwavidhalaya, Khanpur Kalan, Sonepat-131305, India

ABSTRACT: - Cryptography is a process used for sending information in secret way. Goal of this process is to provide protection for information but in different way. In this paper our motive to represent a new method for protection that is generated by combination of RSA and 2 bit rotation mechanism of cryptography. There are many algorithms exist for this process. For cryptography there are algorithms like RSA, IDEA, AES, and DES but here we are using only one algorithm from these that is RSA which is enough to implement combined process using 2 bit rotation. The encrypted image is used as input for network for further implementation.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.

Keywords: - Cryptography, RSA, hill cipher, 2 bit rotation, key etc.

1. INTRODUCTION

There is a process exist that are used for sending information in secret way. This process is known as cryptography [1]. The technique widely used for protection of information or data. Cryptography covert message in cipher text form so that it is not possible for unauthorized

party to understand it. In this paper we are going to develop a new system by using image is encrypted using two algorithms RSA and 2 bit rotation. 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 RSA technique with 2 bit rotation 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 [2].

2. Public Key Cryptosystem

In this cryptosystem, we have two different types of keys: one is the public key and second is the private key. Public key is publicly known and private key is kept secret[3]. The system is called asymmetric system. If data encrypted by the public key so it can only decrypted by the private key. In public key cryptosystem, no need to share the secret data between two parties. So there is less chance of data stolen & manipulation and data is more secure.

3. RSA Cryptosystem

RSA algorithm is the first practicable public-key cryptosystems and is widely used for secure data transmission. In cryptosystem, the encryption key is public and the decryption key is secret. In RSA, this asymmetry is based on the factoring the product of two large prime numbers that is called factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who is the founder of this algorithm and discovered in 1977[4].

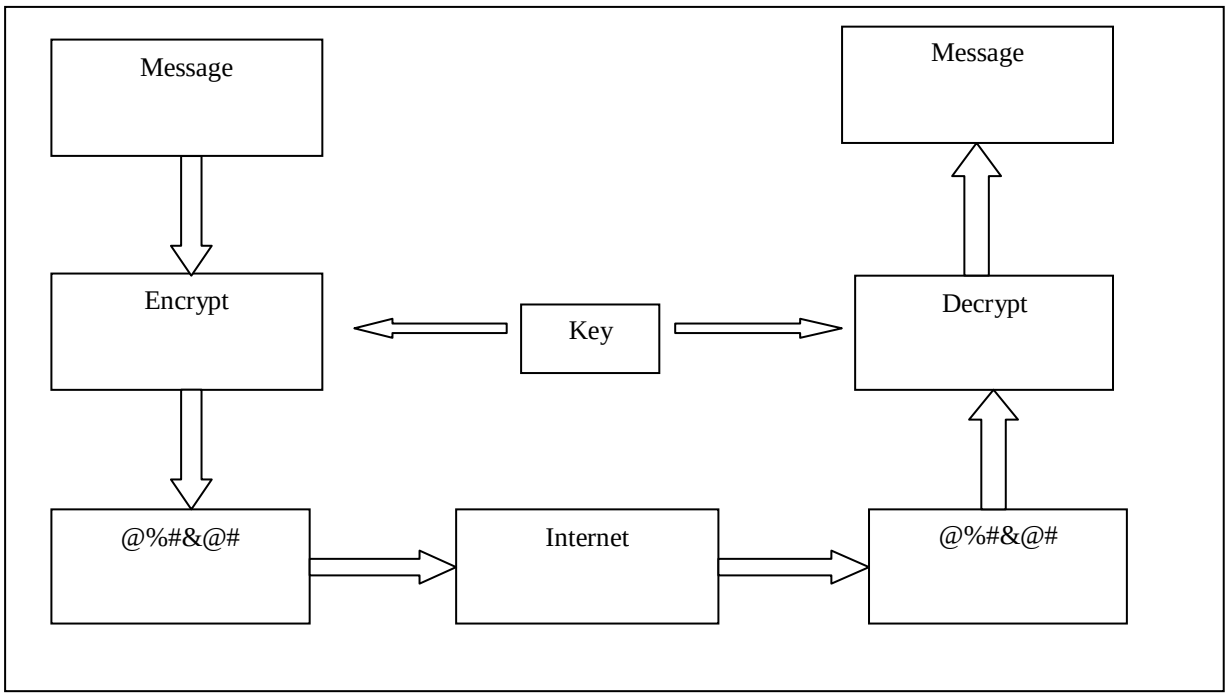

Fig: 1 RSA Cryptosystem

It involves three steps :

- **Key Generation**
- **Encryption**
- **Decryption**

3.1 Key Generation: In this, we need keys that are public and private. We will generate public and private key by using following steps. Public key is visible to both sender and receiver. But the private key is kept secret and not visible to end user[5]. Steps are:

1. Choose two distinct prime numbers p and q.
2. For security purposes, these prime numbers p and q should be chosen at random, and must be of similar bit-length.
3. Compute n = pq.

- n is used as the modulus for both the public and private keys. Its length is expressed in bits which is key length.

4. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p + q - 1)$, where φ is Euler's totient function.
5. Choose an integer e such that $1 < e < \varphi n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co-prime.
   - e is the public key exponent.
   - e is having a short bit-length and small Hamming weight results such as: $2^{16} + 1 = 65,537$. However, if the value of e is small. e.g:- e= 3 have been less secure.
6. Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$;i.e., d isthe multiplicative inverse of e (modulo $\varphi(n)$).

   - Solve d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$

3.2 Encryption:

$$c \equiv m^e \pmod{n}$$

3.3 Decryption

$$m \equiv c^d \pmod{n}$$

4. Hill Cipher Algorithm

Hill cipher is a polygraph substitution cipher based on linear algebra. It invented in 1929 by Lester S. Hill [8]. Each letter is represented by a number modulo 26 also we can assume A = 0, B = 1, ..., Z = 25. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, again modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

4.1 Data Encryption

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:

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

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:

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

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 diffuse fully across n symbols at once..

4.2 Data 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:

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

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

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

which gets us back to 'ACT', just as we hoped.

For our example key matrix:

$$\begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix} = 6(16.15-10.17)-24(13.15-10.20)+1(13.17-16.20)=441=25(\text{mod } 26)$$

So, modulo 26, the determinant is 25. Since this has no common factors with 26, this matrix can be used for the Hill cipher.

5. 2-bit Rotation Process

In 2-bit rotation, we rotate the random numbers or pixel values of the image with 2-bit. In this firstly, we select the size of the image, then generate the key by using pixel value of image. After that, convert the key value into binary format and then apply 2-bit rotation. In which we rotate or shift the 2- bit of the key. By apply this method our image will be more secure.

6. Practical Work: We implemented the code on MATLAB to showing the result of RSA algorithm. We applied RSA algorithm on the image and show the differences in output.

Fig 1 Sender Window

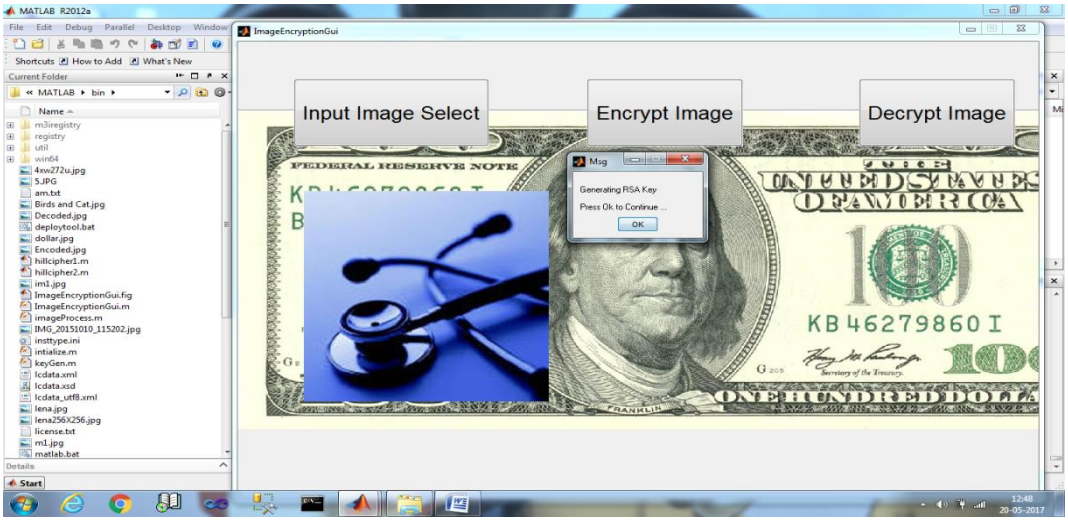

Fig: 2 Original Image at Sender Window

The second tab is used for load the image which is used to implement for encryption process. The selected image is shown in snapshot. The image is selected in pixel form.

Now, there RSA algorithm is applied on selected image as shown in Fig 3

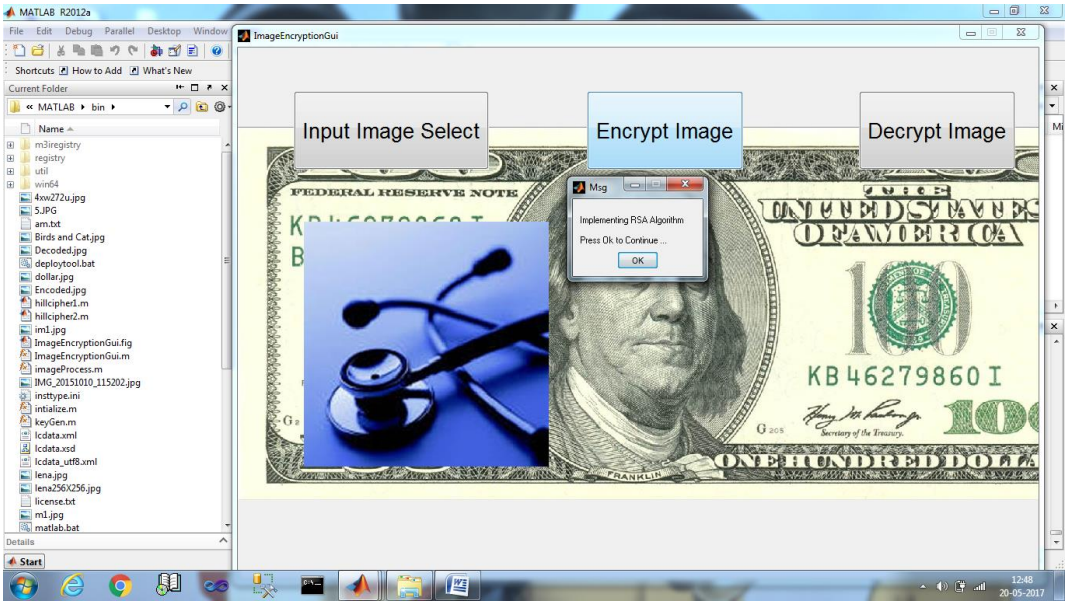

Fig :3 Implement RSA Algorithm on Selected image

Now, we apply 2-bit rotation on encrypted image.

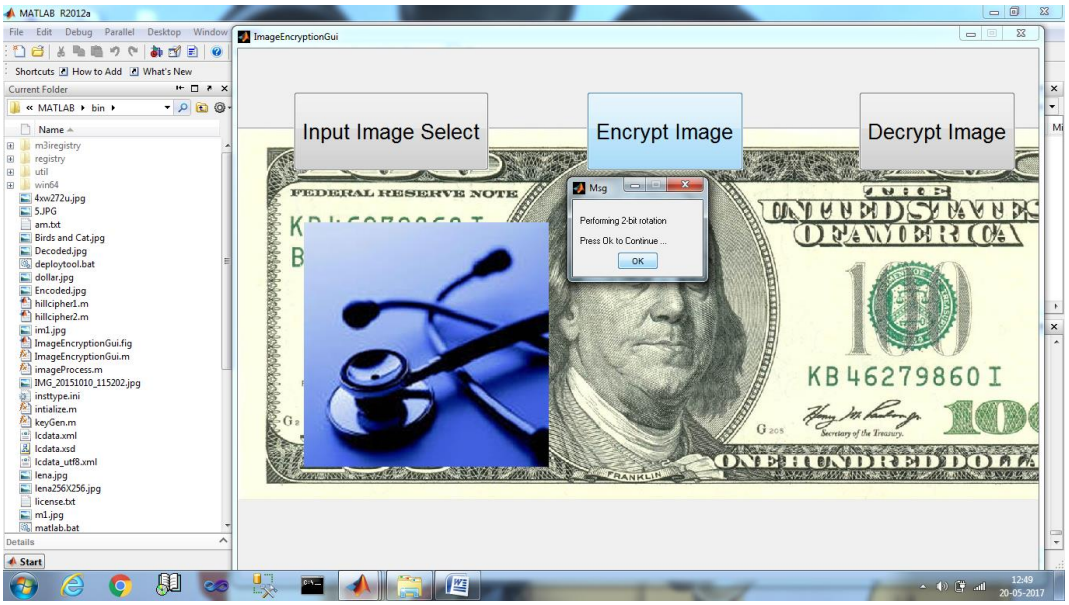

Fig: 4 Implement 2-bit rotation on the image

Then, apply Hill Cipher algorithm as shown in Fig 5 to encrypt the image.

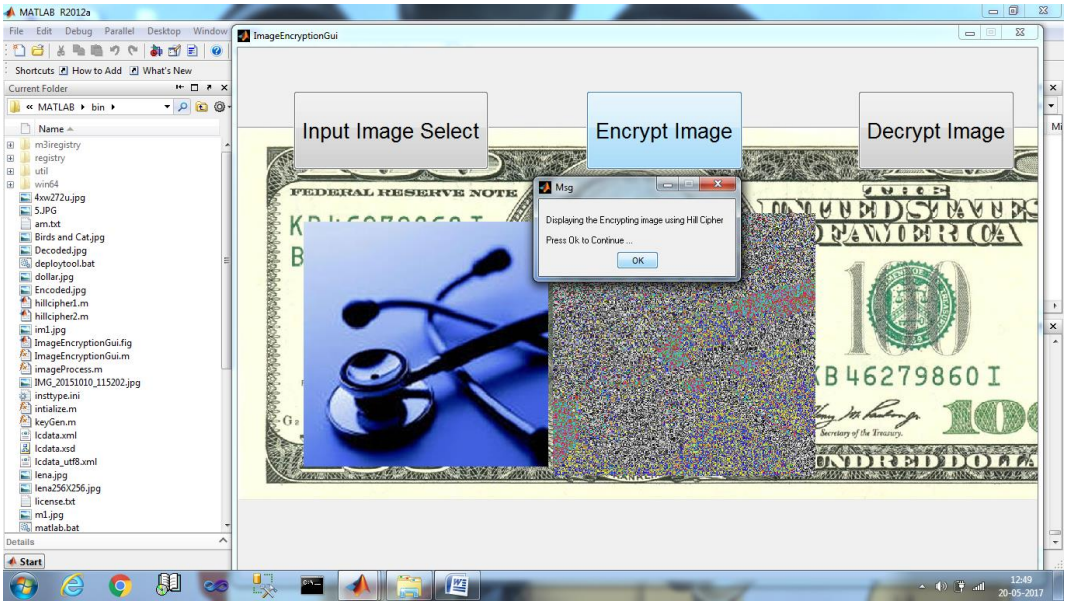

Fig: 5 Apply Hill Cipher Algorithm on image

Now, encrypted image is shown below after apply these three procedures and it is more secure and nobody can access it when we send through transmission medium.

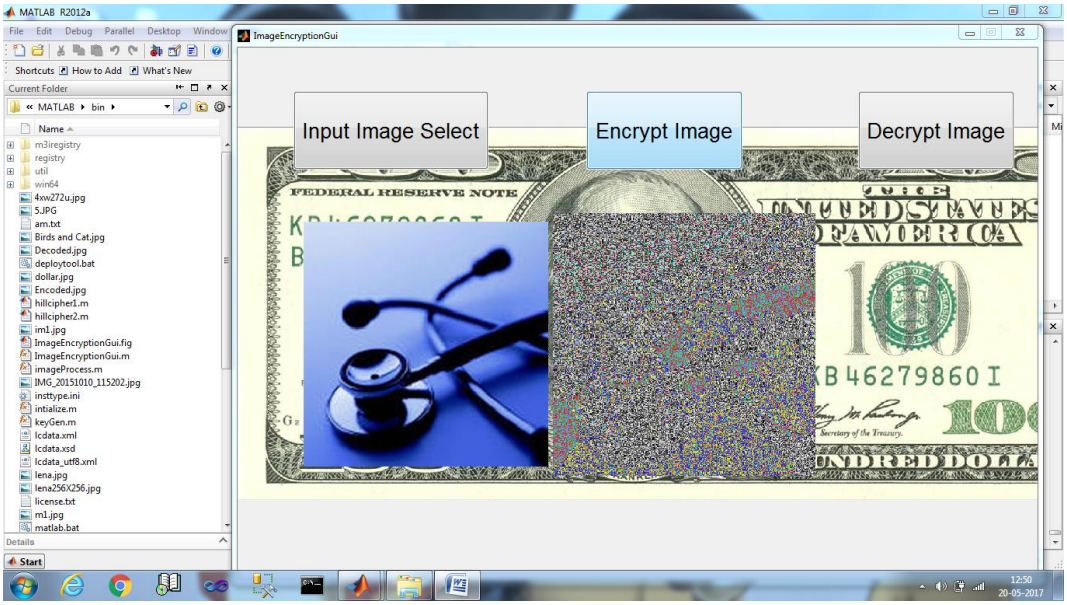

Fig: 6 Encrypted Image

As the process of encryption is completed then the key generate and used in decryption process. In decryption process reverse process will apply.

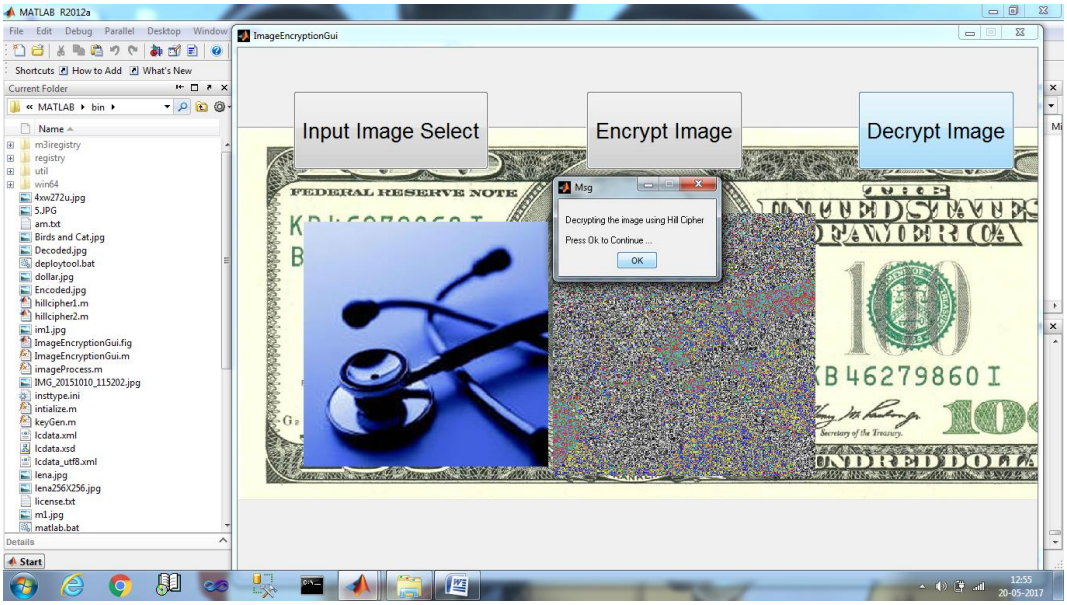

Fig: 7 Decrypting Image by Hill Cipher

Then, apply 2-bit Rotation on an image.

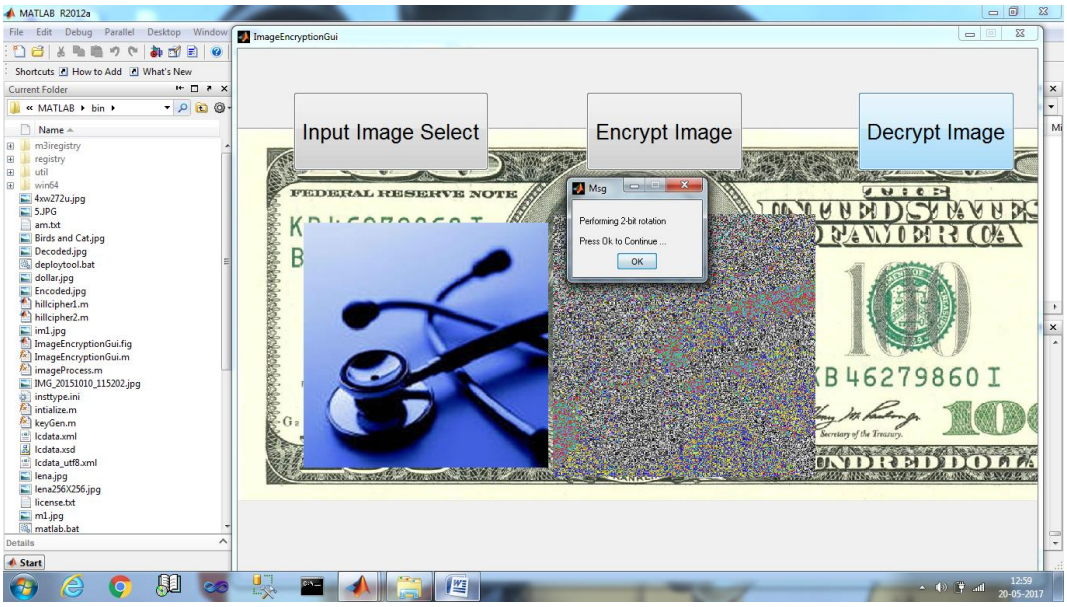

Fig:8 Performing 2-bit Rotation on an image

After apply Hill Cipher & 2-bit Rotation on an image for decryption, we apply RSA Algorithm for final result.

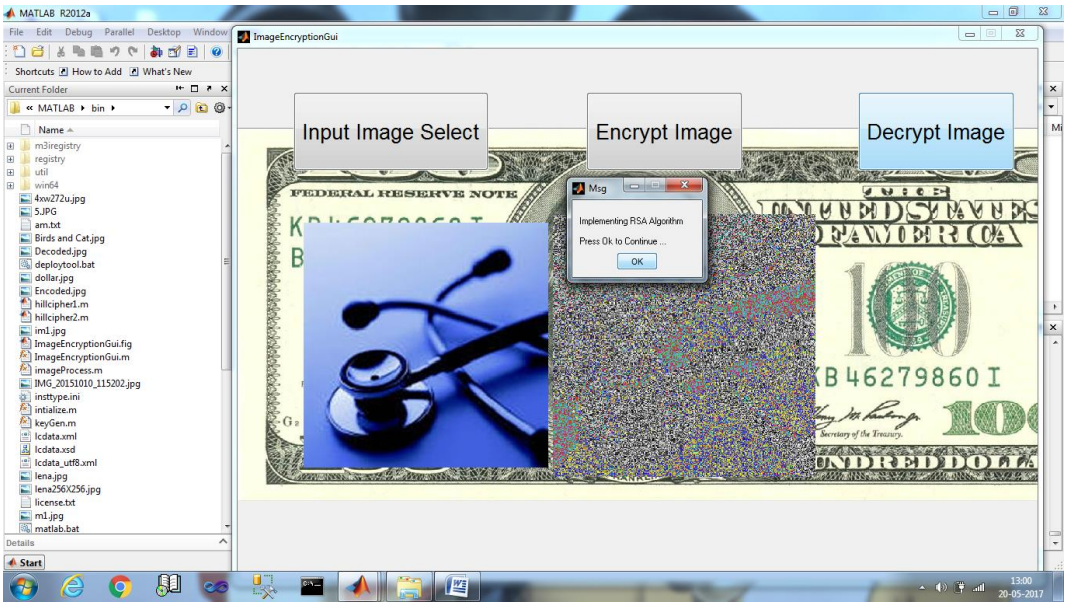

Fig:9 Apply RSA algorithm

Now, image is shown in its original form after apply the above procedure. The original iamge is shown in Fig. 10.

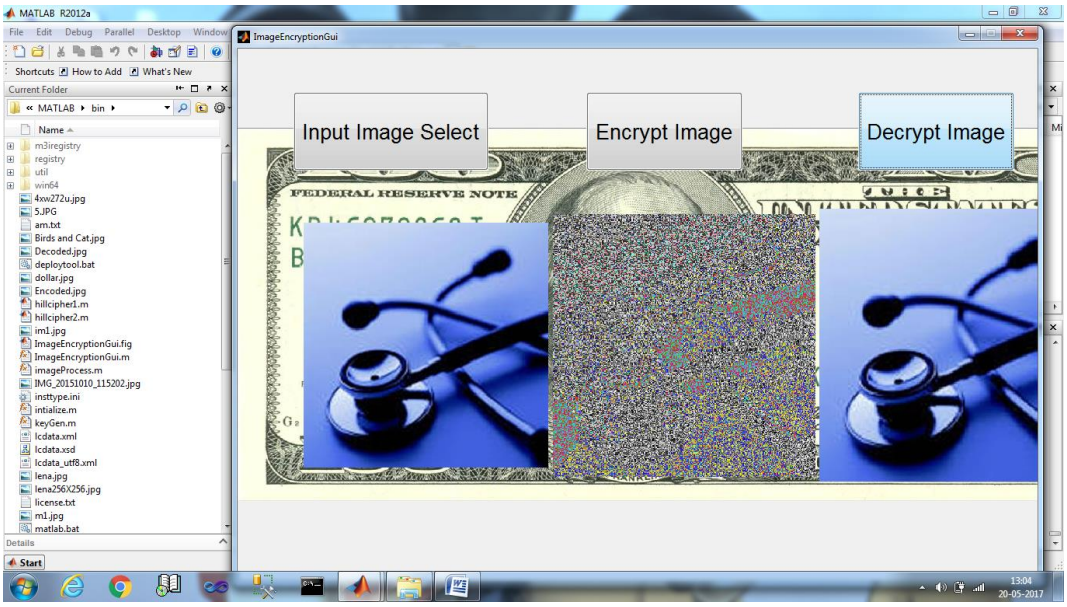

Fig:10 Original Image at Receiver side

7. **Result and Conclusions:** With the implementation of RSA algorithm using 2 bit rotation, we reach a conclusion that for better security of any text or image. In this work there choose an image and apply RSA algorithm on it. Then we got encrypted image and applies the 2 bit rotation algorithm on encrypted image and after that we apply Hill Cipher algorithm for better security. Then got an encrypted image which is very difficult to decrypt by any other person. So, the conclusion is that the, image is more secure.

References

[1] Kalyan Chakraborty**, "Introduction to Basic Cryptography",** CIMPA School of Number Theory in Cryptography and Its Applications School of Science, Kathmandu University, Dhulikhel, Nepal July 20, 2010.

[2] Vishwagupta, Gajendra Singh ,Ravindra Gupta**," Advance cryptography algorithm for improving data security",** International Journal of Advanced Research in

Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[3] Shikha Kuchhal, Ishank Kuchhal," **Data Security Using RSA Algorithm In Matlab",** International Journal of Innovative Research & Development, Volume 2,Issue 7, July 2013 ISSN:2278-0211(ONLINE).

[4] W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd edition, Prentice Hall, NJ, 2003.

[5] K.Sony , Desowja Shaik, B.Divya Sri , G.Anitha**," Improvised Asymmetric Key Encryption Algorithm Using MATLAB",** IOSR Journal of Electronics and Communication Engineering (IOSR-JECE),Volume 10,Issue 2, (Mar - Apr.2015), e-ISSN: 2278-2834,p- ISSN: 2278-8735.

[6] Vishwagupta, Gajendra Singh ,Ravindra Gupta**," Advance cryptography algorithm for improving data security",** International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[7] Mohammed AbuTaha, Mousa Farajallah, Radwan Tahboub, Mohammad Odeh**," Survey Paper: Cryptography Is The Science Of Information Security",** International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (3) : 2011.

[8] Thai Duong, Juliano Rizzo**," Cryptography in the Web: The Case of Cryptographic Design Flaws in ASP.NET",** Unrecognized Copyright Information DOI 10.1109/SP.2011.42.

[9] Sonal sharma, Jjitendrasinghyadav, Parshantsharma**," Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm"** International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012 ISSN: 2277 128X.

[10] Rajinder Kaur, Er. Kanwalprit Singh," **Image Encryption Techniques: A Selected Review**" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013), PP 80-83.

[11] Www. Google.com/INTERNET Source

