International Journal of Current Trends in Engineering & Research (IJCTER)
e-ISSN 2455–1392 Volume 3 Issue 3, March 2017 pp. 1 – 7
Scientific Journal Impact Factor : 3.468
http://www.ijcter.com

An RGB Image Encryption using RSA Algorithm

Samson Chepuri

Department of Information Technology, MVSR Engineering College, Hyderabad

Abstract—Image encryption is an attractive area of research in the field of information security. Encrypting an image is different from that of text due to its features. It is difficult to deal with image encryption by using conventional encryption methods. This project is aimed at using RSA algorithm for encrypting images. The RSA algorithm modified suitable for an RGB image encryption. Experimental result shows that the proposed approach can successfully encrypt/decrypt various images, and the algorithm has good encryption effect. Cipher image developed by this method will be entirely different when compared to the original image. This approach provides better security and it will be suitable for secured transmission of images over the Internet.

Keywords—Information security**,** Cryptography**,** RSA Algorithm, Image encryption, image decryption, Public Key cryptosystem, Key Generation, Prime Numbers

I. INTRODUCTION

Information security has become a central issue in information storage and transmission. It often requires that data be kept safe from unauthorized access. The best line of defense is physical security. However, physical security is not always an option, due to cost and/or efficiency considerations. Instead, most computers are interconnected with each other openly, thereby exposing them and the communication channels that they use. Cryptography, defined as the science and study of secret writing concerns the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers and other methods, so that only certain people can see the real message.

With regard to confidentiality, cryptography is used to encrypt data residing on storage devices or travelling through communication channels to ensure that any illegal access is not successful. Also, cryptography is used to secure the process of authenticating different parties attempting any function on the system. Since a party wishing be granted a certain functionality on the system must present something that proves that they indeed who they say they are. That something is sometimes known as credentials and additional measures must be taken to ensure that these credentials are only used by their rightful owner. The most classic and obvious credential are passwords. Passwords are encrypted to protect against illegal usage. Security of internet banking account passwords, email accounts password etc. requires text protection in digital media.

Unlike text messages, the multimedia information including image data has some special characteristics like redundancy and high correlation among pixels. One of the main goals that must be achieved during the transmission of information over the network is security. This technique will make the information to be transmitted into an unintelligible form by encryption so that only authorized persons can correctly recover the information. Encryption is the process of transforming a piece of information, known as the plaintext, using an algorithm, known as the cipher, to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The output is known as the ciphertext. The reverse process of transforming cipher text to plaintext is known as decryption (sometimes called as decipherment).

As images are widely used in several processes including the Internet, the protection of image data from unauthorized access is very important. Image cryptography is a special kind of encryption techniques to hide data in an image for encryption and decryption of original message based on some key value. Very few algorithms, provides computational hardness and it makes difficult to break a key to find the original image. In the same way image transmission and storage during industrial and research processes requires image protection.

RSA is an encryption and authentication system, an algorithm developed in 1977 by Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman. RSA is a cryptosystem, which is also known as public-key cryptosystems. RSA is normally used for secure data transmission. This technique will make the information to be transmitted into an unintelligible form by encryption so that only authorized persons can correctly recover the information.

In the present paper, RSA algorithm is modified slightly to make it suitable for image encryption. The paper is organized as follows. Section II describes the related work carried out by various researchers. Section III discusses how RSA algorithm can be extended to RGB color image encryption. In Section IV, an illustration of encryption is presented. In Section V, computations are carried out and conclusions are drawn from the results obtained.

II. RELATED WORK

In 2005, Zhi-Hong Guan et al. [1] have presented a new image encryption scheme, in which shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher image and the plain image. In 2006, Mitra A et al. [2] have proposed a random combinational image encryption approach with bit, pixel and block permutations. The main idea behind their work is that an image can be viewed as an arrangement of bits, pixels and blocks. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. Komal D Patel, Sonal Belani, et. al [3] suggested the image encryption techniques are convert the original image to another image that is hard to understand, it is keep the image confidential between users. It is essential that nobody can't to get the information without a key for decryption. In 2012, Ahmad Abusukhon et al. [4] suggested that in cryptographic application, the data sent to a remote host are encrypted first at the source machine using an encryption key then the encrypted data are sent to the destination machine. This way the attacker will not have the encryption key which is required to get the original data and thus the hacker will be unable to do anything with the session. In 2012, Anal Paul et al. [5] suggest that some chaos based algorithms are working well and resists many type of crypto analysis attacks, but it takes lot of time for encryption and decryption. Some of chaos based algorithms are very fast but their strength to resist attack is questionable. So these have motivated us to design a crypto system which will take less amount of time for encryption and decryption and it should resist all type of crypto analysis attacks.

The Rivest-Shamir-Adleman (RSA) algorithms is one of the most popular and secure public-key encryption methods [6]**.** Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, et. al. [7] explained about an image cryptography it may use the traditional cryptosystems to encrypt images. But it having two problems. The first problem is that the image size is always much greater than text. So the cryptosystems is need much time to encrypt the image. The second problem is the decrypted data should be equal to the original data. Due to the Characteristic of human perception, a decrypted image containing small distortion is usually acceptable. Gunasekaran G. and Bimal Kumar Ray, et.al. [8] proceeded the technique which is used for securing data is known as encryption. The encrypted data is transfer through the network. And the encrypted data is decrypt using provided algorithm which is known as decryption. The secret information is hide within an image and it is

transfer with the secret key. In past times for secure the information using by wax tablets and invisible ink, but now it is a modern society so the security is totally changed. Now a day's images, pictures, videos and voices are carrying the message in transferring from one place to another place with the help of network communication.

Ambika Oad, Himanshu Yadav, Anurag Jain, et. al. [9] recommended the image encryption is a technique which is convert the original image into another format that is difficult to understand. So, without knowing the decryption key no one can access the information. The image encryption has applications in corporate world, health care, military operations, and multimedia systems. Encryption is the process which is encoding the plain text into cipher text, and the reverse process of converting cipher text into the plain text is decryption. The cryptography consists of encryption and decryption techniques.

III. RSA FOR IMAGE ENCRYPTION

RSA algorithm is basically meant for text encryption. As there is a significant need for providing security on image transmission, this paper is extending the RSA algorithm to perform image encryption and decryption. Initially, two prime integers p and q are taken which are used for calculating keys (private key and public key) and selecting the input image for encrypting. 'e' and d are selected in such a way that $e \times d \bmod \Phi(n)$.=1. The selected image is encrypted by using the formula $C \equiv P^e \bmod n$. P is the input image we are encrypting. 'e' is the public key which is used for encrypting. Φ(n) is the product of (p-1) and (q-1) such that gcd(e,Φ(n)) =1 i.e. e and Φ(n) are coprime. C is the cipher image produced after encryption is done. We are decrypt the encrypted image using the formula $P \equiv C^d \bmod n$. C is the cipher image after it has been encrypted. 'd' is the private key which is used to decrypt the cipher image. 'n' is the product of (p-1) and (q-1) such that $d \equiv e^{-1} \pmod{\Phi(n)}$. This is more clearly stated as $d.e \equiv 1 \pmod{\Phi(n)}$.

Algorithm for Encryption and Decryption

1. Read the input RGB color image, S

2. First choose the two distinct prime numbers p and q.

3. Calculate the value, n = pq.

4. Compute φ(n) = φ(p)φ(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 < φ(n) and gcd (e, φ(n)) = 1; i.e., e and φ(n) are co-prime.

   e is the released as the public key.

6. Determine d as d ≡ e −1 (mod φ(n)); i.e., d is the modular multiplicative inverse of e (modulo φ(n)).

   Solve the d given d·e ≡ 1 (mod φ(n)).

7. Obtain the encrypted image, $C = S^e \bmod \varphi(n)$.

8. C = C mod 256, as gray level values of an image lie in the range [0,255].

9. Recover decrypted image, $S = C^d \bmod 256$.

10. The original input (recovered) image, R = S mod φ(n).

IV. ILLUSTRATION OF ENCRYPTION

Let us illustrate the process of encryption by considering any one of the sub images of the original input image, given in Fig 4.1. To carry out this one, we focus our attention on the first sub image (top most left corner of the image S). This is given by

$$S = \begin{bmatrix} 40 & 40 & 39 & 38 & 39 & 41 & 44 & 45 \\ 43 & 42 & 41 & 40 & 40 & 42 & 43 & 45 \\ 43 & 42 & 41 & 40 & 40 & 41 & 42 & 43 \\ 40 & 39 & 39 & 38 & 39 & 40 & 41 & 41 \\ 37 & 37 & 38 & 39 & 40 & 42 & 43 & 43 \\ 38 & 39 & 40 & 42 & 43 & 45 & 46 & 47 \\ 40 & 40 & 42 & 43 & 45 & 46 & 46 & 46 \\ 40 & 41 & 42 & 43 & 44 & 44 & 44 & 44 \end{bmatrix} \quad (4.1)$$

Two distinct prime numbers p and q chosen are 37 and 43 respectively. The value of n is 1591, which is obtained by multiplying p with q. The value φ(n) calculated is 1512. 53 is chosen as the value of e and d is determined as 485. The enciphered image, E, is obtained by using $E = S^e \bmod \varphi(n)$, which is shown below in 4.2.

$$E = \begin{bmatrix} 99 & 99 & 647 & 482 & 647 & 102 & 904 & 1059 \\ 43 & 429 & 102 & 99 & 99 & 429 & 43 & 1059 \\ 43 & 429 & 102 & 99 & 99 & 102 & 429 & 43 \\ 99 & 647 & 647 & 482 & 647 & 99 & 102 & 102 \\ 222 & 222 & 482 & 647 & 99 & 429 & 43 & 43 \\ 482 & 647 & 99 & 429 & 43 & 1059 & 847 & 729 \\ 99 & 99 & 429 & 43 & 1059 & 847 & 847 & 847 \\ 99 & 102 & 429 & 43 & 904 & 904 & 904 & 904 \end{bmatrix} \quad (4.2)$$

By limiting the gray level values of the basic enciphered image to lie in the range [0,255], encrypted image is obtained which given in 4.3.

$$C = \begin{bmatrix} 99 & 99 & 135 & 226 & 135 & 102 & 136 & 35 \\ 43 & 173 & 102 & 99 & 99 & 173 & 43 & 35 \\ 43 & 173 & 102 & 99 & 99 & 102 & 173 & 43 \\ 99 & 135 & 135 & 226 & 135 & 99 & 102 & 102 \\ 222 & 222 & 226 & 135 & 99 & 173 & 43 & 43 \\ 226 & 135 & 99 & 173 & 43 & 35 & 79 & 217 \\ 99 & 99 & 173 & 43 & 35 & 79 & 79 & 79 \\ 99 & 102 & 173 & 43 & 136 & 136 & 136 & 136 \end{bmatrix} \quad (4.3)$$

By applying the reverse procedure of encryption, the original input is recovered without any loss of data.This ensures the validity of the procedure.

Elapsed time= 12.367247

V. COMPUTATIONS AND CONCLUSIONS

Consider an RGB color image of Sachin Tendulkar shown in Fig. 1. On carrying out the process of encryption of the color image, by adopting the modified RSA algorithm discussed in Section III, the basic encrypted (enciphered) form of input image is obtained, which is shown in Fig 2.

Fig 1. Original input image

It is observed that some features of the original input image are visible in Fig 2. Hence we need to limit the gray level values of the image to lie in the range [0,255].

Fig 2. Basic enciphered image

Therefore, step 8 is applied on the basic enciphered image and final encrypted (cipher) image is obtained which is shown in Fig 3.

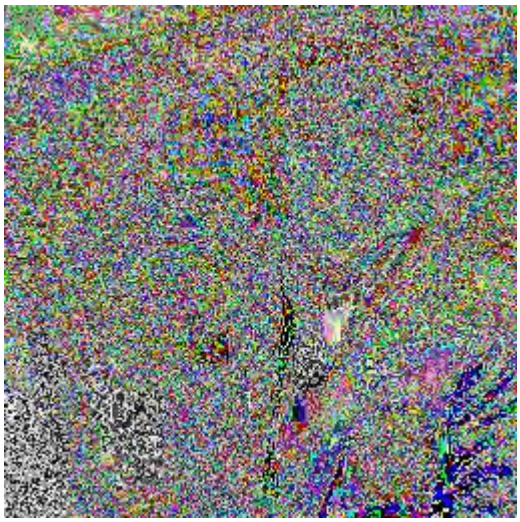

Fig 3. Encrypted(cipher) image

In this encrypted color image, we find several red, green and blue pixels placed together. This reflects the color of the original image, but all the features of the original image are totally hidden in Fig 3. By applying steps 9 and 10 of the algorithm, decrypted image is obtained. The recovered image so obtained, is a replica of the original input image, shown in Fig 4. The time taken for both encryption and decryption together is 12.36 seconds which is less compared to existing methods.

Fig 4. Decrypted(recovered) image

In this paper, all computations including image encryption and decryption are carried out by using MATLAB [10].

Image security has become more important in today's world as the communication has increased rapidly. All the techniques are in a real-time image encryption could only find a low level of security. In this paper, RSA algorithm is modified for color image encryption. Here, the image encryption and decryption approaches are highly securable and with less computational time. The results of the simulation prove that this approach is an efficient cryptosystem for image encryption and it is suitable for secured transmission of images over the Internet.

REFERENCES

[1] G. Zhi-Hong, H. Fangjun, and G. Wenie "Chaos - based image encryption algorithm",Department of Electrical and computer Engineering, University of Waterloo, ON N2L 3G1, Canada. Published by: Elsevier, 2005, pp. 153-157.

[2] A. Mitra, Y V. Subba Rao, and S. R. M. Prasanna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, Vol. 1, No. 1, p.127, 2006.

[3] Komal D Patel , Sonal Belani, Image Encryption Using Different Techniques: A Review International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 1, November 2011.

[4] Ahmad Abusukhon and Mohammad Talib, "A Novel Network Security Algorithm Based on Private Key Encryption", IEEE 2012.

[5] Anal Paul, Nibaran Das and Agyan Kumar Prusty, "An Advanced Gray Image Encryption Scheme by Using Discrete Logarithm with Logistic and HEH64 Chaotic Functions", IEEE 2012.

[6] Rivest, R.L., Shamir, A., and Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol 21, No. 2, February 1978, p. 120-26.

[7] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm), ISSN 2249-6343 International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3.

[8] Gunasekaran G. and Bimal Kumar Ray, Encrypting And Decrypting Image Using Computer Visualization Techniques, Journal of Engineering and Applied Sciences VOL. 9, NO. 5, ISSN 1819-6608, MAY 2014.

[9] Ambika Oad, Himanshu Yadav, Anurag Jain, *A Review: Image Encryption Techniques and its Terminologies*, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014.

[10] Alasdair Mcandrew,—Digital Image processing with MatLab, Cengage learning 2004.

