International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

FAST AND SECURE TRANSMISSION OF IMAGE BY USING BYTE ROTATION ALGORITHM IN NETWORK SECURITY

Miss A. P. Waghmare[1], Mr. S.S. Kemekar[2], Prof. P. R. Lakhe[3]

[1]*Student of Suresh Deshmukh College Of Engineering, Selukate, Wardha*
[2] *Instrumentation Engineer in Inox Air Product Ltd. Wardha*
[3] *Assistant Professor of Suresh Deshmukh College of Engineering Selukate Wardha*

Abstract - *In this paper, we have introduced some inventive advancement to the byte rotation encryption algorithm which is more secure and fast. There has been immense increase in the accumulation and communication of digital computer data in both the private and public sector. The main aim of this study is to increase security in communication by encryption the information using key that is created through using an image. Whatever we want to send file from one location to another location in the network, many unauthorized users are illegally access the information. There are different algorithms like blowfish, DES, AES, RC5 that achieve more security but increases the complexity of the algorithms and also takes more time for encryption and decryption of files. The benefits of this algorithm for security and also reduces time for process of file encryption and decryption.*

Key Words: **Byte Rotation Algorithm (BRA), Advanced Encryption Standard (AES), Network Security, Encryption, Decryption.**

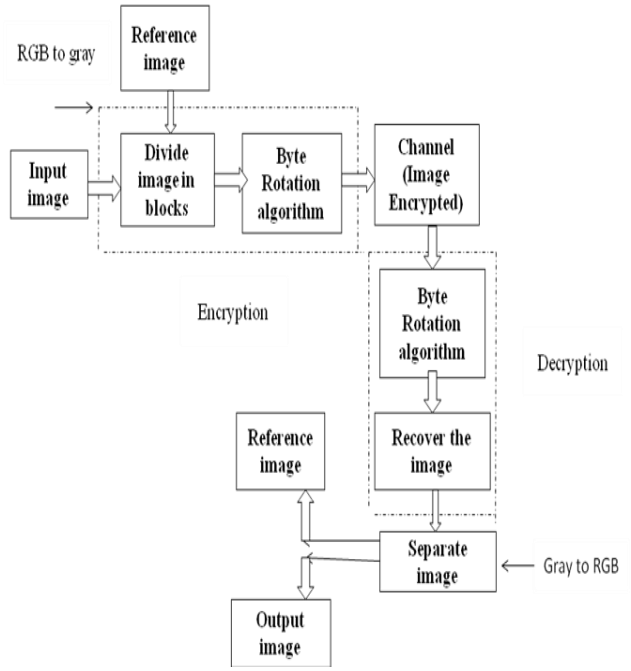
1.INTRODUCTION

In network security different types of attacker, ethical hacker unauthorized user access the secure data. All these types of hacker access illegal data. To provide security for the data authors implemented different algorithm for encryption and decryption of the data. In the present world as more and more information is generated and transferred through network system, the information being transmitted develops more and more important and security of this data becomes a greater issue. This data varies from text to multimedia data, multimedia data includes a major number of images, images are transferred for different applications that include medical image system, personal photographs, military images, and confidential documents that may contain some private or confidential information that is required to be protected from any unauthorized human. The commonly applied approaches are steganography and cryptography to implement image security. Cryptography is a technique that uses various encryption and decryption methods to hold the original message secret. As in cryptography the encrypted image is visual to user and is in unreadable form it attracts the attention of hacker. So to make the secret image more protected the idea of steganography is introduced that embed the secret message behind a carrier to make it viewless while communication. The two techniques differ from the fact that cryptography tries to keep the content of message secret whereas the steganography tries to keep the existence of message itself hidden. In steganography of Image, the presence of secret image is made hidden by hiding it behind another image. To provide security to data in network different algorithms are used but each and every algorithm having its own advantages and disadvantages. Secret key is used for encryption in DES algorithm. These algorithms face the problem when key transmission is done over the network. For encryption and decryption process RSA algorithm takes maximum time. AES, DES, Triple DES, RSA are useful algorithm for improve different parameter like security, encryption, and decryption process time and increase complexity. The author S. Bhati proposed Byte Rotation Algorithm (BRA). Using Byte Rotation Algorithm increase security and increase speed of encryption process.

1.1 Byte Rotation Algorithm

In digital computer programming, a bitwise operation operates on one or more bit patterns or binary numerals at the level of their individual bits. It is a fast, simple action directly supported by the processor, and is used to manipulate values for comparisons and calculations, typically, bitwise operations are substantially faster than division, several times faster than multiplication, and sometimes significantly faster than addition. While modern processors usually perform addition and multiplication just as fast as bitwise operations due to their longer instruction pipelines and other architectural design choices, bitwise operations do commonly use less power because of the reduced use of resources.

2. PROPOSED METHODOLOGY



Block diagram of Proposed method

In fig (1) block diagram, for encryption process, secret image is input image which divided into four blocks. By using byte rotation algorithm blocks are shuffle then the cover image is embedded on secret image. For decryption process the first byte rotation algorithm apply on embedded image. After extraction process, recovering and separating image is done. And get output image in RGB.

The proposed method includes following steps:

1. First taking input image which contain secret data to a size M*N so that divide resized image into four sub-images.
2. The sub-images have the size (M/2)*(N/2).
3. Load four sub-images and divide into a number of pixels. The image is decomposed into blocks with the same number of pixels. The Image is decomposed into blocks, each one containing a specific number of pixels.
4. The main idea is that an image can be encrypted by rotating the rows and columns of the faces of sub-images and not to change the positions of the blocks. By rotating the rows a number of times depending on the rotation table, and then same number of times for the columns for an arrangement of blocks, the image can be scrambled.
5. With a small block size, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors.
6. The correlation between the blocks of the image is decreased so as to provide a good level of encryption of the image.
7. At the receiver side, original image can be retrieved by an inverse rotation of the blocks.

3. SIMULATION RESULT

Fig 1(a)

Fig 1(b)

Fig 1(c)

Fig 1(d)

Here first resolution of both inputted file that is of both cover image and data image is checked. Cover image and data image are of resolution 300*168 and 512*512 respectively shows in fig 1(a) and fig 1(b). In next step data images is pixel divided into four blocks. Each block size is of 16 bytes. Subimages divided into number of pixels. Cover image is embedded with data image. Fig.1 (c) shows embedded image of resolution 64*64. At last AES encryption algorithm is implemented to transfer the recovery information along with embedded image for exact recovery of data image. The embedded image is compressed by using lossless JPEG compression to reduce size for fast transmission. At the receiver end the image is first decompressed and then data image is recovered from embedded image. The output image is data image shown in fig 1(d).

Fig 2(a)

Fig 2(b)

Fig 2(c)

Fig 2(d)

Fig. 2 Experimental result (a) cover image. (b) Data image. (c) Embedded image (d) Extracted image.

Fig 3(a)

Fig 3(b)

Fig 3(c)

Fig 3(d)

Fig. 3 Experimental result: (a) Cover image (b) Data image (c) Embedded image (d) Extracted image.

3.1 PEAK SIGNALTO NOISE RATIO

The high value of MSE and low value of PSNR causes the resulting encrypted image more randomness. MSE is calculated using equation (1).

$$MSE = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - I'(x,y)]^2 \quad \text{..... (1)}$$

PSNR = 10 * log10 (255 / sqrt(MSE)) ..... (2)
where I(x,y) is the original image, I'(x,y) is the approximated version (which is actually the decompressed image) and M,N are the dimensions of the images. Calculated results of MSE and PSNR are tabulated in the following table.

Input Images (Original Vs. Encrypted image)	PSNR	NC
Fig 1(a) & Fig.1(c)	59.9406	0.9262
Fig 2(a) & Fig.2(c)	67.1402	0.8811
Fig 3(a) & Fig.3(c)	66.8443	0.9110

Table 1

4. CONCLUSION

In this paper, A new secure image transmission method has been proposed, which not only improve the image quality of recover image in but also increase PSNR ratio. Also, the original secret images can be recovered nearly lossless from the embedded image. Good experimental results have shown the feasibility of the proposed method. Future studies may be directed to applying the proposed method to images of colour models other than the RGB.

ACKNOWLEDGEMENT

My thanks goes to my guide who have guided me for development of this project.

REFERENCES

[1] Punam V. Maitri Rekha V. Sarawade "Secure File Transmission using Byte Rotation Algorithm in Network Security" International Conference for Convergence of Technology – 2014.
[2] Deepali G. Singhavi, P. N. Chatur, PhD, "A Fast and Secure Transmission of Image by using Mosaic" International Journal of Computer Applications (0975 – 8887) International Conference on Quality Up-gradation in Engineering, Science and Technology (ICQUEST2015).
[3] Prabir Kr. Naskar1, Ayan Chaudhuri2, Atal Chaudhuri3" A Secure Symmetric Image Encryption Based on Linear Geometry" 2014IEEE.
[4] Kalyani V. Gulhane,"A Review on Low Latency for File Encryption and Decryption Using BRA Algorithm for Secure Transmission of Data",IJARECE vol-5,Issue 1,ISSN 2278-909X January 2016.
[5] S. Bhat, A. Bhati, S. K. Sharma,"A New Approach towards Encryption schemes: Byte Rotation Encryption Algorithm." World CECS, Vol-2, pp.24-26, 2012.
[6] Nidhi Gouttam,"Implementation Of Simulation Of Byte Rotation Encryption Algorithm,"IJTEEE, vol-2,Issue 6 ,ISSN 2347-4289,2014.
[7] Ya-Lin Lee." A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations,"IEEE Trans on crts and sys for video Tech, vol.24, no.4, April 2014.
[8] Sonalina Chowdhury, "A New Combinational Approach Using Different Encryption Technique", IJARCSSE, vol-3, Issue-8, ISSN 2777-128X PP.1022-1026, August 2013.
[9] Mahendran R "Byte rotation with CBC encryption algorithm" IJMCE vol-1,Issue 1 August 2014.
[10] Naveen Kumar S K, Sharath Kumar H S, Panduranga H T, "Encryption Approach for Images Using Bits Rotation Reversal and Extended Hill Cipher Techniques" International Journal of Computer Applications Vol-59, No. 16,December 2012.