ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

*Website: www.ijircce.com*

Vol. 5, Issue 6, June 2017

# Fast Image Transmission by Using Byte Rotation Algorithm in Network Security

Apurva P. Waghmare [1] , Prof. P. R. Lakhe [2]

M.Tech Student, Dept. of Electronics and comm. Engineering, Suresh Deshmukh College of Engineering, Wardha Nagpur University, Maharashtra, India [1]

Assistant Professor, M.Tech, Dept. of Electronics and comm. Engineering, Suresh Deshmukh college of Engineering, Wardha, Nagpur University, Maharashtra, India[2]

**ABSTRACT**: – In this paper, we have introduced some inventive advancement to the byte rotation encryption algorithm which is more 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.

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

## I. 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.

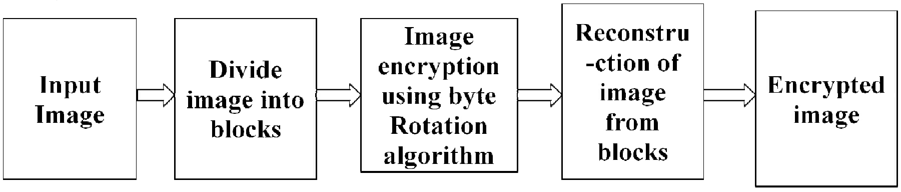
## II. RELATED WORK

[1] In this paper author introduced BRA for file encryption and decryption within minimum delay. These algorithms improves the security and reduce time for process of file encryption and decryption. To provide security for different types of file like image, text, audio and video using BRA. Results are taken using Net Bean java complier for AES and BRA. Compare result for various parameters like BRA and AES encryption time as well as decryption time.
[2] To prevent Image containing private and confidential information from leakage some security is needed. The commonly used methods for image security are Encryption and data hiding. Among them data hiding is seen to be most commonly used method for information security. In this paper for secure image transmission a new type of mosaic image is created called as secret fragment visible mosaic image by dividing secret image into small tiles and then arranging these tiles in a puzzled format with the help of another image called as carrier image. To enable resultant mosaic image to look exactly similar to selected target image reversible color transformation is proposed.
[3] Transmission of image as secret over unreliable communication media is the demanding need of the day. But some intrinsic features like bulk data size, correlation among pixels are not image. To enable resultant mosaic image to look exactly similar to selected target image reversible color transformation is proposed. The information required for recovering the secret image is embedded into the mosaic image by using enhanced LSB algorithm. Further to allow fast transmission of image lossless compression is performed on resultant mosaic image.
[4] Their algorithm proposes a method for low latency encryption decryption algorithm that will take smallest amount of time for file encryption and decryption and provide more security. This algorithm can be applied on different types of files. In Byte Rotation Algorithm a random key generation technique is used. They proposed architecture diagram of BRA. In architecture diagram shows sender side in which the image file is divided into small number of blocks and BRA encryption technique applied on small block of data to get encrypted image. This encrypted image is decrypted using BRA decryption algorithm and combines the divided blocks into image. At receiver side we get decrypted image i.e. recovered image.
[5] Presented a new approach towards Encryption Schemes: Byte – Rotation Encryption Algorithm. The BREA is applied on different blocks of plain text and executes in parallel manner through multithreading concept of single processor system. BREA which is a block cipher and used with Block Wise Parallel Encryption Model. The model has been written into two steps. In the first step, the plaintext has been broken into number of blocks. Each block size is of 16 bytes. So the number of blocks depends on the total input bytes of plain text. Each block is represented by 2D array. These arrays of blocks are passed into BREA in parallel manner to execute simultaneously by using multithreading concept. The concept will allows all the blocks to process parallel in CPU. Because of parallel execution, the processing speed of the system will enhance.

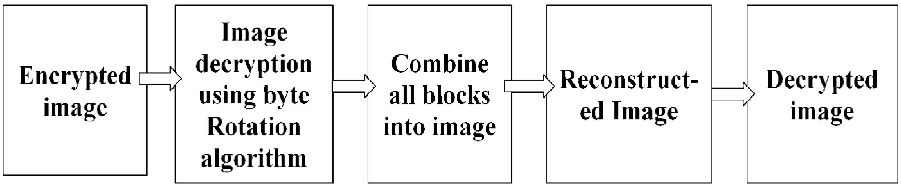
## III. PROPOSED ALGORITHM

In this system we will implement Byte Rotation Algorithm which gives higher quality result in parameters like encryption time and decryption time as compared to others.

At sender side,


Input Image
Divide image into blocks
Image encryption using byte Rotation algorithm
Reconstru -ction of image from blocks
Encrypted image

At receiver side,


Encrypted image
Image decryption using byte Rotation algorithm
Combine all blocks into image
Reconstruct-ed Image
Decrypted image

Block diagram of BRA

In architecture diagram shows sender side in which the image file is divided into small number of blocks and BRA encryption technique applied on small block of data to get encrypted image. This encrypted image is decrypted using BRA decryption algorithm and combines the divided blocks into image. At receiver side we get decrypted image i.e. recovered image.

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 neighbours.
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.

*Algorithm create rotation table:*

```
1: Load Original Image
2: Input Secure Key
3: Divide the Original Image into 4 sub-images
4: Calculate Width and Height of the sub-Images
5:
5.1: N_Horizontal = Width /2 (each block contain 3 pixels * 3 pixels)
5.2: N_Column = Height /2 (each block contain 3 pixels * 3 pixels)
6:
6.1: N_Column_Rotation Table (Index Of Columns in Rotation Table) = 128
6.2: If (N_Horizontal ≥ N_Column) then N_Horizontal_RotationTable (Index of Rows in Rotation Table) =
     N_Horizontal Else N_Column_Rotation Table (Index of Rows in Rotation Table) = N_Column
7:
   For I = 0 to N_Column_Rotation
   For J = 0 to N_Horizontal_Rotation Position Value = Hash Function
```

```
  (Index (I), Index (J), Secure Key)
   Position Value to Assign location I and J in the Rotation Table Next J Next I End Create_Rotation_Table
8: Output: Rotation table
```

## IV. Simulation Results

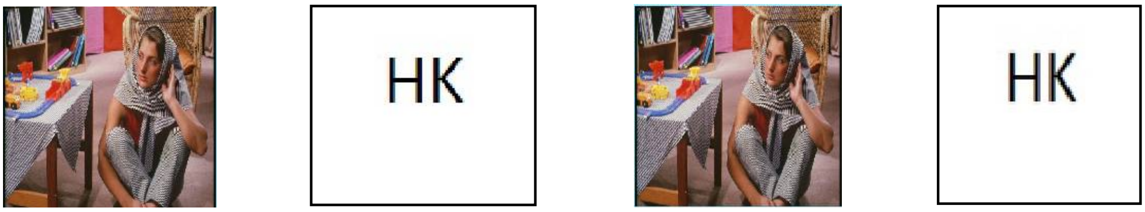


Fig 1(a) Fig 1(b) Fig 1(c) Fig 1(d)

Fig 1 Image file Encryption and Decryption

Fig 1(a) and fig (b) shows cover image (512*512) and data image (111*98) respectively. Data image is secret image which embedded with cover image shows in fig 1(c). The embedded image is compressed by using lossless jpeg compression to reduce size to 64*64 for fast transmission. At receiver side the image is first decompressed and then data image is recovered from embedded image. The final output i.e. data image is shown in fig 1(d).

## V. Conclusion and Future Work

In this paper, A new fast image transmission method has been proposed, which not only improve the image quality of recover image in but also transmitted secret image fast. 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 colour images.

## 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.