Review on Fast and Secure Transmission of Image in Network Security

Ms. Apurva P. Waghmare[1] , Mr. S. S. Kemekar[2], Prof. P. R. Lakhe[3]
[1]*(Student of Suresh Deshmukh College of Engineering Selukate Wardha)*
(apurva.waghmare679@gmail.com)
[2]*(Instrumentation Engineer in Inox Air Product Ltd. Wardha)*
(kemekar.shailesh@gmail.com)
[3]*(Assistant Professor of Suresh Deshmukh College of Engineering Selukate Wardha)*
(pravinlakhe@rediffmail.com)

Abstract **-** Transmission of data from one user to another user securely in network is important issue in network security. Encryption and Decryption method used for transmission of data. Various type of encryption algorithm used for transmission data securely over network like Data Encryption Standard(DES), Triple DES Advance Encryption Standard (AES), etc. In this paper I have introduce Byte rotation algorithm (BRA) for encryption and decryption within minimum delay. This algorithm helps the security and reduces time for process of file encryption and decryption.

BRA is more secure and fast method for transmission data. User can set time and frequency during data transmission. When these conditions are satisfied file and key used for encryption will be deleted. BRA is not only hiding the some contents of data but also hides all data by another data due to that security level is increased, and data is more secure in network transmission.

Keywords- *Byte Rotation Algorithm (BRA), Encryption Standard (AES), Network Security.*

*****

1. INTRODUCTION

In network security different types of attacker, ethical hacker illegal user access the secure data all these types of hacker access illegal data. To provide security for the data authors implemented different algorithm like AES, DES, Triple DES and RSA for encryption and decryption of the data. Using these algorithm increase the speed of encryption and decryption process. Modified RSA is used for better encryption and decryption within minimum delay. 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 information 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. There are different approaches that are in use to implement image security, the commonly applied approaches are steganography and cryptography. 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 noise or unreadable form it attracts the attention of hacker or eavesdroppers. 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 Image steganography 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. DES algorithm used secret key is used for encryption. These algorithms face the problem when key transmission is done over the network. RSA algorithm takes maximum time for encryption and decryption process. AES, DES, Triple DES, RSA are very useful for improve different parameter like security, encryption, and decryption process time and increase complexity. The author S. Bhati proposed Byte Rotation Algorithm(BRA). Using BRA increase security and increase speed of encryption process.

2. RELATED WORK

[1] Secure file transmission from one android user to another android user is important issue in network security. 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] When Images are transmitted through network it may happens that any third person or any unauthorized user may try to read the contents of the secret image. 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. Now a day's a new concept of mosaic image is used in the field of data hiding for secure image transmission. 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] In this paper, a new technique for secure image transmission is proposed, which transforms a secret image into a meaningful mosaic image with the same size and looking like a preselected target image. The transformation process is controlled by a secret key, and only with the key can a person recover the secret image nearly lossless from the mosaic image. The proposed method is inspired by Lai and Tsai, in which a new type of computer art image, called secret-fragment-visible mosaic image, was proposed. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the target image preselected from a database.

3. OBJECTIVE

1. Implementing rotational algorithm for fast and secure transmission image.
2. Security of image hiding quality increases.
3. Compatibility of transmission of image in any media.

4. PROPOSED METHODOLOGY

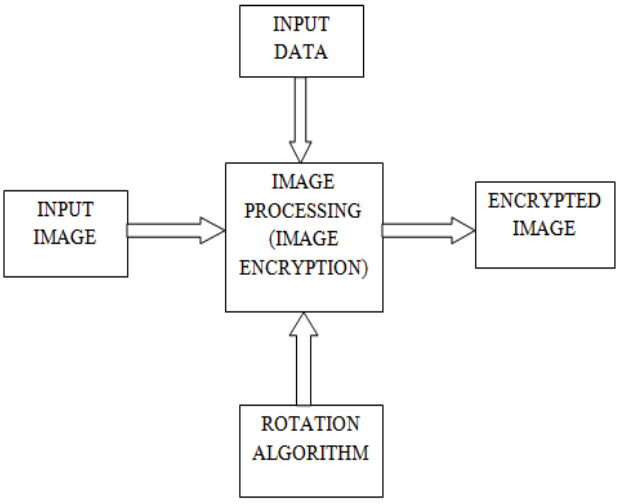

Fig. 1. Flow diagram of the proposed method.

The proposed method includes following steps:

1. First taking input image which contain secret data.
2. Image encryption process by using Image processing.
3. Load the original image and resize the image to a size M*N so that divide resized image into four sub-images.
4. The sub-images have the size (M/2)*(N/2).
5. 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.
6. 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 ofblocks, the image can be scrambled.
7. 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.
8. The correlation between the blocks of the image is decreased so as to provide a good level of encryption of the image.
9. At the receiver side, original image can be retrieved by an inverse rotation of the blocks.

The rotation algorithm is presented below. It creates a rotation table that will be utilized to build a newly encrypted image.

4.1 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

4.2 MODES OF SECURE FILE TRANSMISSION SYSTEM ARCHITECTURE

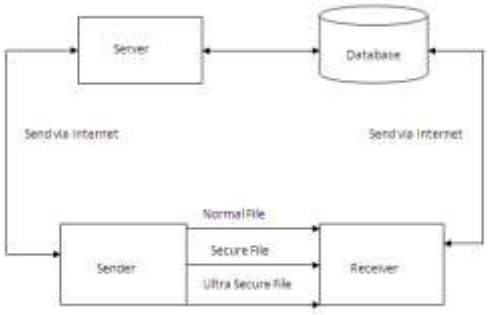

Fig 2. Modes of secure file transmission System Architecture.

Secure file transmission using three different files by sender to receiver in shown figure 1. Normal file, secure file and ultra secure file are three modes of secure file transmission in network. File can be send without any key in normal file transmission. Server can provide the key for file encryption in secure file transmission mode. Multiple securities for file can be provided by only in ultra secure file transmission mode. All encrypted data by sender is stored in server side database. So chances of data loss should be reduce.

5. CONCLUSION

In our Byte Rotation Algorithm system proposed a good strategy of most out of advantage eliminates the limitations. The develop for the system in any network services for the network security. In this algorithm security will be high compare with others. The concept of byte rotation algorithm using AES enhances the speed of encryption system.

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] 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.
[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] Tsang-Yean Lee,Huey-Ming Lee,Homer Wu,Jin-Shieh Su. , "Data Transmission Encryption and Decryption Algorithm in Network Security." ICSMO, pp.22-24, September-2006.