Image Encryption using Different Techniques for High Security Transmission over a Network

Mohammad Sajid Qamruddin Khizrai [1], Prof. S.T.Bodkhe[2]

[1]Research Scholar (PG), Priyadarshini Institute of Engineering & Technology, Dept. Computer Science and Engg, Nagpur, India

[2]Professor, Priyadarshini Institute of Engineering & Technology, Dept. Computer Science and Engg, Nagpur, India

E-mail- IDsajid4u0023@gmail.com

1. ABSTRACT

Digital image is a collection of the pixel with different intensity values, and each image is in the form of n*m, no of pixel (where n,m is no of Rows and Column) when we transfer a digital image from source to destination through a network, it need to be encrypted at the source side and decrypted at the destination side. Encryption is process of hiding the information, when the information is transferred through a network and decryption is the process of extracting the information from an encrypted information. For this encryption and decryption, we need some encryption and decryption algorithm.

Security of a data or information is very important now a day in this world. And everybody want a secure network, for transmission of his information, being a well secure network there is also a chance of hacking a data, most of the banks and other organization where data security in important are well secured but there is also a online fraudulent is there. So we need a more secure data with high security environment. Generally, we do high secure working environment and data is also secure with a encryption and decryption method or technique, but that techniques uses only one encryption and decryption keys.

Keywords— Image encryption with high security, Image security, high security encryption decryption

2. INTRODUCTION

As the world changes technology is also changing rapidly. In advancement of network technology domain, large amount of multimedia information is transmitted over the Internet conveniently. Various confidential data such as Government, Military, Banking and other secured data, space and geographical images taken from satellite and commercial important document are transmitted over the Internet. While using secret information we need more secure information hiding techniques.

In our new method, we are securing information sixteen (16) times or we can increase 2^n no of times (where “n” is a “no” of splitted part) instead of one in a single information transmission, more “no” of splitted blocks means more secure information.

3. RELATED WORKS.

The information security is used from old ages, different person using different technique to secure their data .

Following are some techniques that uses for security of images from ancient age to till date

A. Steganography
B. Water Marking Technique
C. Visual Cryptography
D. Without sharing Keys Techniques

A) Steganography

The steganography word comes from the Greek word Steganos, which is used to covered or secret and a graphy is used for writing or drawing. Therefore, steganography is, literally, covered writing. The main idea for covering the information or steganography is used for secure communication in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data [4]. During the transmission process, characteristics of these methods are to change in the structure and features so as not to be identifiable by human eye. Digital videos, images, sound files, and other files of computer that contain perceptually important information can be used as "covers" or carriers to hide secret messages. After embedding a message into the cover-image, a so-called " stego image" is obtained.

In [2] Security, Capacity and robustness are three different aspects which is affecting steganography and its usefulness. Capacity is used to the amount of information that can be hidden in the cover medium. Security relates to an eavesdropper's inability to detect hidden information and robustness is the amount of modification the stego medium can withstand before an adversary can destroy the hidden information. The concept of the mosaic images in [1] was created perfectly and it has been widely used. Four types of mosaic images namely crystallization mosaic, ancient mosaic, photo mosaic and puzzle image mosaic are proposed in [2]. In the first two types, the source image is split into tile image and then it is reconstructed by painting the tiles and they are named as tile images. The next two types include obtaining target image and with the help of database, cover image has been obtained. They may be called as multi-picture mosaics.

B) Water Marking Technique

Water Marking is also one of the technique used to hide the digital image, Digital watermarking is a process of embedding (hiding) marks which are typically invisible and that can be extracted only by owner's of the authentication. This is the technology which is used in [15] with the image that cannot be misused by any other unauthorized miss users. This technology allows anyone to do without any distortion and keeping much better quality of stegno-image, also in a secured and reliable manner guaranteeing efficient and retrievals of secret file. Digital watermarking finds wide application in security, authentication, copyright protection and all walks of internet applications. There has been effective growth in developing techniques to discourage the unauthorized duplication of applications and data . The watermarking technique is one, which is feasible and design to protect the applications and data related. The term' cover' is used to describe the original message in which it will hide our secret message, data file or image file. Invisible watermarking and visible watermarking are the two important types of the above said technology. The main objective of this package is to reduce the unauthorized duplication of applications and data, provide copyright protections , security, and authentication, to all walks of internet applications.

C) Visual Cryptography

Visual Cryptography is used to hide information in images, a special encryption technique in such a way that encrypted image can be decrypted by the human eyes, if the correct key image is used. The technique was propose by Naor and Shamir in 1994[1]. It is uses two transparent images. One image contains image contains the secret information and the other random pixels.. It is not possible to get the secret information from any one of the images. Both layers or transparent images are required to get the actual information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

D) Without sharing Keys Techniques

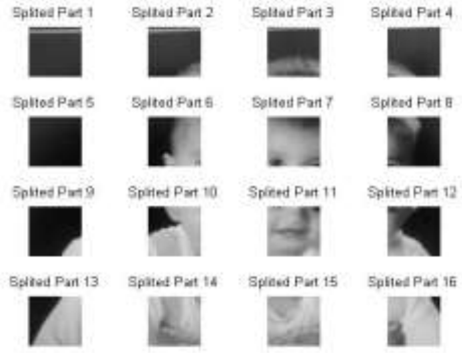
The author at [11] is securing image for transmission without sharing his encrypted key, but it needs two transmission for a single image transmission, In [11]the image is encrypted with private key and is sent without sharing key to the receiver, after receiving the encrypted image receiver again encrypted the image by its own keys, and send it to the first sender, first sender removed the first encrypted key and again send to opponent, The opponent already had it's keys then with this key the image is finally decrypted. Thus different person applying different-different techniques for securing his information.

4. Proposed Research Methodology

4.1) Encryption Process

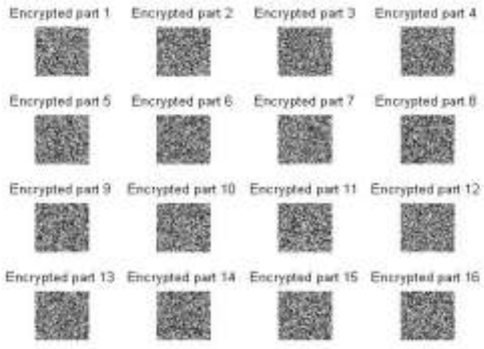
Process of Encryption Methodology of this research, we will read a image (A) fig (a) by using some command OR algorithm we will divide the image in to J*J parts i.e. (2*2, 4*4) parts. Each parts of the image will be treated as a single image, we can say that Splitted Image1, Splitted Image2, Splitted Image3,Splitted Image4, Splitted Image5,………………Splitted ImageJ,

Fig(a) (Original Image)



Fig(b) (Splitted Image)

The output of the above i.e. fib(b) Splitted Image1, Splitted Image2, Splitted Image3, Splitted Image4, Splitted Image5,…………Splitted Image J, and each parts of the image is treated as a single image. And using different-different encryption algorithm, we will encrypt each image, and we can say that each encrypted images (Encrypted images = Encrypted Part1, Encrypted Part2, Encrypted Part3, Encrypted Part4, Encrypted Part5,………,Encrypted Part J), Shown in fig (c).



Fig(c) (Splitted & Encrypted Image)

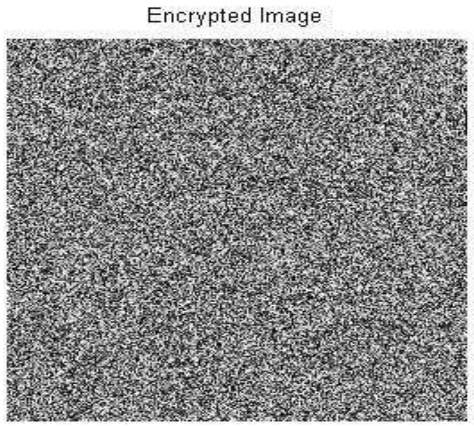


Fig (d) (Combined Encrypted Image)

After that we have two options

I. Now We will transfer all sub encrypted images (Encrypted images= Encrypted Part1, Encrypted Part2, Encrypted Part3, Encrypted Part4, Encrypted Part5,…….. Encrypted Part J), which is shown in Fig(c) to the receiver side.

OR

II. We can Merges (Combine) all encrypted images (Encrypted images= Encrypted Part1, Encrypted Part2, Encrypted Part3, Encrypted Part4, Encrypted Part5,…….. Encrypted Part J) and make a single encrypted image i.e. Fig (d) we can say image (A1), for transfer.

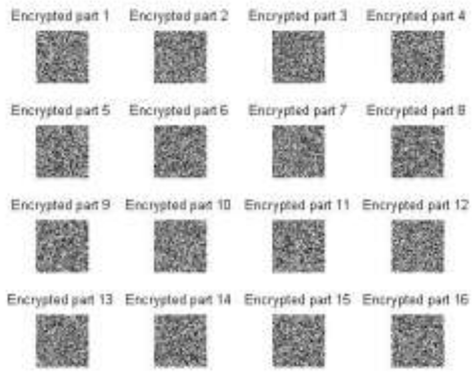
Now we will transfer the image (A1) from one location (source) to another location (destination).

4.2) Decryption Process

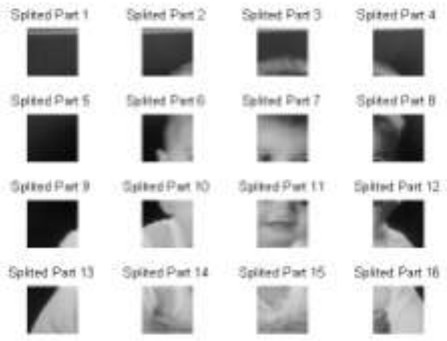
Here we will receive the encrypted image from source side through option (I) and decrypt the each part of image which is shown in fig(f) construct a single image shown in fig (g).

OR

We will receive the image from option (II) and we will divide the image into a sixteen part (Encrypted images= Encrypted Part1, Encrypted Part2, Encrypted Part3, Encrypted Part4, Encrypted Part5,………. Encrypted Part J) which will also in a encrypted form which is also shown in a figure shown in fig (e). Now we will apply decryption algorithm on each encrypted sixteen part (Encrypted images= Encrypted Part1, Encrypted Part2, Encrypted Part3, Encrypted Part4, Encrypted Part5,……Encrypted Part J). Now will say that decrypted part (Decrypted images= Decrypted Part1, Decrypted Part2, Decrypted Part3, Decrypted Part4, Decrypted Part5… Decrypted Part J) shown in fig(f).



Fig(e) (Splitted & Encrypted Image)



Fig(f) (Splitted & decrypted Image)

Now we will combine each of the decrypted part in to a single image which is shown in fig(g) i.e original image.

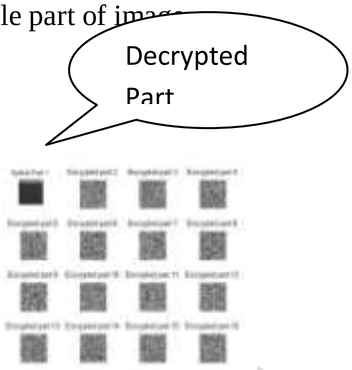
Fig(g) (Original Image)

5. DIFFERENCE BETWEEN

i) Existing Encryption Method and

ii) Proposed Encryption Method

Existing Encryption Method	Proposed Encryption Method
1) It is encrypted using single key.	1) It is encrypted using sixteen no of keys.
2) It is less secure as, it is encrypted by single key	2) It is more secure as, It is sixteen time encrypted than any other encryption algorithm.
3) It takes less time for encryption and decryption.	3) It takes more time for encryption and decryption. But more secure.

4) If it is hacked, after 'N' no of iteration using different keys(if key is success) he is able to view hole image. 	4) If it is hacked, after 'N' no of iteration using different keys (if key is success) he is able to view only single part of image. 

6 ACKNOWLEDGMENT

I acknowledge the sincere and long lasting support of my project guide Prof. S.T Bodkhe and other Professor's of Computer Science Department, who gave me healthy suggestion and had helpful discussion.

7 CONCLUSION

Thus we have increased the security of an image for transmission over a network up to sixteen (16) times or we can increase 2^n number of times (where "n" is a no of splitted part) instead of one in a single information transmission, more number of splitted blocks means more secure information.

8 FUTURE SCOPE

Our future work will mainly focus on to study and analysis of more security, and security can be increased by splitting the images into more "no" of parts and different algorithm can be applied in a single image. If we apply more algorithms it will take more time for encryption and decryption but it will be more secure than this methods, but one problem would come, if we apply different algorithms than different key sizes can cause the problem.

REFERENCES:

[1] Silver and M. Hawley, "Photo mosaics". New York: Henry Holt, 1997.

[2] Battiato, G. M. farinella, and G. Gallo, "Digital mosaic framework: An overview," Eurograph.– Comput. Graph.Forum,Vol.26, no. 4, pp. 794 – 812, Dec.2007.

[3] Y. Dobashi, T. Haga, H. Johan, and T. Nishita, "A method for creating mosaic image using voronoi diagrams,"

[4] John Blesswin, Rema, Jenifer Josel 978-1-4244-9799-71111$26.00 ©20 11 IEEE , in Proc. Eurographics, Saarbrucken, Germany, Sep. 2002, pp. 341-348.

[5] Visual Cryptography Moni Naor and Adi Shamir EUROCRYPT -1994

[6] Resolution Variant Visual Cryptography for Street View of Google Maps Jonathan WeirWeiQi YanQueen's University Belfast Belfast, BT7 1NN

[7] Koo Kang in IEEE transactions on image processing, vol. 20, no. 1, January 2011

[8] Jayanta Kumar Pal1, J. K. Mandal2 and Kousik Dasgupta3 in (IJNSA), Vol.2, No.4, October 2010

[9] Debasish Jena1, Sanjay Kumar Jena2 in 978-0-7695-3516-6/08 $25.00 © 2008 IEEE DOI 10.1109/ICACC.2009.109

[10] Zhi Zhou IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 8, AUGUST 2006 2441 Halftone Visual Cryptography

[11] Abdul Razzaque and Narendra Thakur International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July - 2012 ISSN: 2278-0181

[12] N. Madhumidha and Dr.S. Chandramathi Bonfring International Journal of Advances in Image Processing, Vol. 2, Special Issue 1, Part 2, February 2012 63 ISSN

[13] E. Myodo, S. Sakazawa, and Y. Takishima, "Visual cryptography based on void-and-cluster halftoning technique," in Proc. IEEE Int. Conf. Image Process., 2006, pp. 97–100.

[14] Tsung-Yuan Liu and Wen-Hsiang Tsai, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 19, NO. 5, MAY 2010

[15] Ahmad Salameh Abusukhon, "Block Cipher Encryption For Text-To-Image Algorithm",International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 3,2013, pp. 50 - 59, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375