International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-3
International Conference on Research and Recent Trends in Engineering and Technology. (ICRRTET)
Held on 27th January 2016 organized by **Sai Polytechnic College,** Kinhi Jawade, Yavatmal, Maharastra, India.

Robust Image Mosaic Scheme

Shireen Sheikh[1*]; Chetana Nimje[2*]& Vaishali Bhagat[3*]
[1, 2] Students, Information Technology, SRMCEW, Nagpur, India.
[3] Assistant Professor Department of Information Technology, SRMCEW, Nagpur, India.
[*]Email: shireensheikh1726@gmail.com, chetananimje@rediffmail.com, bhagat.vaishali14@yahoo.in

Abstract—

In this paper, we propose the crypto-stego technique which is combination of image steganography and cryptography as a tool for authentication. Steganography is the method of hiding any text, password, image or file behind and original cover media. Cryptography is an art of protecting information by encrypting it into unreadable format called cipher text only those who possess a secret key can decrypt message into plain text. A new approach for the secure transmission is proposed, which hide multiple secret image into a so-called mosaic image. The mosaic image, looks similar to a randomly selected secret images and may be use as a cover for secret images. Here, we are using 3-LSB bit substitution technique for image steganography and Bit Plane slicing algorithm is used to slice the mosaic image which is used as cover image. Advance cryptographic algorithm like Blowfish is used for encryption and decryption of data and images on both sender and receiver side.

***Keywords*:** Steganography; Image Steganography; Cryptography; LSB; Encryption; Decryption; PSNR ratio; Mosaic Image; Cover Media; Slicing.

1.Introduction

As the increasing use of digital documents, digital document image processing becomes more and more useful. Data-hiding in document images have received much attention recently. The internet is always vulnerable to interception by unauthorized people over the world. The importance of reducing a chance of the information being detected during the transmission is being an issue now days. Some solution to overcome these issue are steganography and cryptography, but once it is decrypted the information secrecy will not exist any more. Hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media.

Steganography means the practice of hiding message, so that the presence of the message itself hidden, often by writing them in places where they may not be found. It is an art and science of hiding secret information imperceptibly in a cover media such that only sender and receiver can detect the existence of secret information. The main aim of steganography is to hide the existence of the message in the cover medium. It is a technique that facilitates hiding of message that is to be kept secret inside other messages. The purpose of steganography is to communicate information secretly so that others who respect the objects being exchanged cannot notice the existence of extra information hidden in the objects.

Cryptography involves converting a message text into an unreadable cipher. It is an art of codifying messages, so that they become unreadable. It is a method of storing and transmitting data in a particular from so that those for whom it is intended can read and process. The main aim of cryptography is scramble a message to make it meaningless and unintelligible unless the decryption key is available. It encrypts the content of information using some mathematical computation and then the decryption is done to revert back onto the original image and it requires the use of a secret key.

An image steganography, the convert embedding of data into digital pictures, represents a threat to the safeguarding of sensitive information and the gathering of intelligence. It is one kind of steganography systems, where the secret message is hidden in a digital image with some hiding method. Someone can then use a proper embedding procedure to recover the hidden message from the image. The original image is called a cover image in steganograhy, and the message-embedded image is called a stego-image. The main aim of image steganography is hiding the fact that communication is taking place, by hiding a secret message in an image.

Mosaic image is a result of arranging of the block of secret image fragments of a secret image in a way to create the other image called the target image or it can be a composite picture made from overlapping photograph. Mosaic makes image or representation by arranging or attaching small pieces in various colors on the rough outline. Mosaicing is one of the technique of image processing which is useful for tiling digital images. It is blending together of several arbitrarily shaped images to form one large radio metrically balanced image so that the boundaries between the original images are not seen.

2. EXISTING SYSTEM

Present day transmission of data over the network is considered to be "un-trusted" in terms of security, i.e. they are relatively easy to be hacked. Only single level of security is present in the existing systems.

In traditional data hiding technique, we seen that how images can be embedded behind cover image. Embedding upto seven images using bit plane slicing technique had been developed. We notice that embedding more than one images in cover image, loses its resolution. Hence the attacker can easily recover the data from cover media. To overcome this problem we increase the PSNR ratio of the cover image and also increase the data hiding capacity of cover image.

In existing system, a method was proposed for secured transmission, user first have to create mosaic image and embed the secret image into mosaic image with the same size of data for camouflaging the secret image. This was made by the use of proper color transformations, pixel by pixel in mosaic tile image with maximum color similarities. The original secret image retrieved from mosaic image at the other end loose some of its resolution.

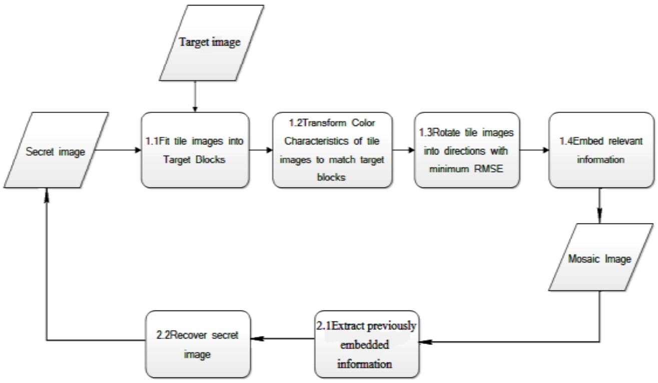
Target image
Secret image
1.1Fit tile images into Target Blocks
1.2Transform Color Characteristics of tile images to match target blocks
1.3Rotate tile images into directions with minimum RMSE
1.4Embed relevant information
Mosaic Image
2.1Extract previously embedded information
2.2Recover secret image

Fig 1:-Flow diagram of existing system

3. PROBLEM DEFINITION

The aim of achieving the security while transmitting the images was not properly achieved due to poor visual quality of cover media. When more images were embedded in the cover media, the cover media become transparent and its quality degrades with loss in its resolution. The cover media where secret images are hidden is degraded too much, so attacker can easily recover the hidden message by repeating process. The quality of the stego image is too poor and requires large complex computational to reconstruct the image at receiver’s side.

In traditional technique, limited amount of secret data can embedded in cover media. In a single cover image only upto seven secret images were hidden. By taking this problem into consideration, we have designed a technique “Robust Image Mosaic Scheme” which prevents the user from any kind of hacking data. In this paper we presented we are trying to hide more than seven image in cover image . In proposed system, we are using a 3-LSB alorithm for data hiding and and BLOWFISH algorithm is used for encrypting and decrypting the secret images which is the strongest symmetric key cryptographic algorithm .

4.RESEARCH METHODOLOGY

Blowfish Algorithm

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. It is a fast, simple, secure & compact i.e execute in less than 5KB of memory. It is suitable for applications where the key does not change often, like coomunication link or an automatic file encryptor making it both flexible and secure.

Working of blowifsh algorithm is divided into two parts i.e key-expansion and data encryption. The subkey generation process convert key upto 448 bits long to sub-keys totalling 4168 bits. These sub-keys are stored in array $K_{1,}$ K_{2},……,K_{14} and size of each sub- key is 32-bits. There is also a P-array and S-boxes which consist of 18 sub-keys each of 32-bits in P-array and 256 32-bit entries in S-boxes. After that, do bit-wise XORing of P_1 with K_1, P_2 with K_2 untill P_{18} and store the result in P_1, P_2, P_3,…., $P_{14.}$But for 4168 bit there is only 14 sub-keys so their will be 4 remaining key in P-array P_{15}, $P_{16,}$ P_{17} and P_{18}, so we reusse first four key K_1, K_2, K_3 and K_4 again and XOR it with P_{15}, P_{16}, P_{17} & P_{18}, all the key get exhausted.

Data encryption process divide the original message into number of 64-bit block i and that 64-bit i.e X is again divided into two parts 32-bit each i.e XL(left block) and XR(right block). In blowfish all the operations perform on XL. The sub-keys store in P_1, P_2,…, P_{18} is XOR with XL and the output is store in XL and the output is given to the funtion.

Function will divide the output into four 8-bits block and that first 8-bit block is given as input to first S-box, second 8-bit block to second block, same for third & fourth 8-bit block. The S-box make that 8-bit block into 32-bit block. The output of first S-box is XOR with second S-box and the output of this is XOR with third S-box and so on. The final result is store in the XL i.e 32-bit block and that 32-bit block is XOR with XR and the result is store in XR, now swap XL and XR. In this algorithm, swapping is perform for each round i.e 16, after 16 round again swap XL and XR or undo last swap. At last, XOR XL with P_{18} and store the result in XL, combine XL and XR back into X i.e 64-bit block.

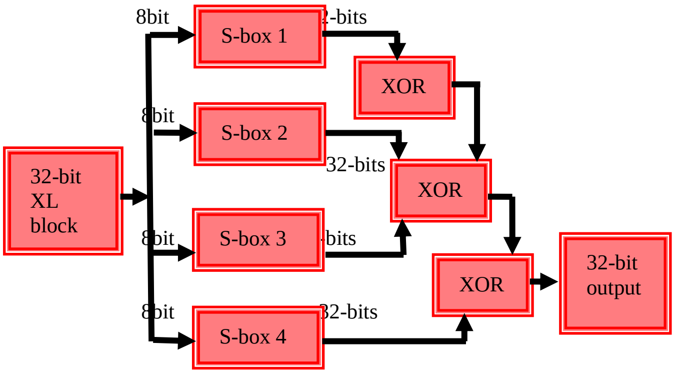

Fig 2:- Function F in Blowfish

5. PROPOSED SYSTEM

Sender side:

Firstly, secret images and mosaic image are selected. After that the secret images are encrypted by using Blowfish algorithm key which generate a secret key K1 and produce encrypted secret images. Now the cover image is nothing but a mosaic image is slice as per the size of encrypted secret images by

using Bit Plane Slicing algorithm. The encrypted secret images are randomly hided inside the mosaic image using 3-LSB substitution technique and henced stego mosaic image is generated. As shown in figure(3) given below.

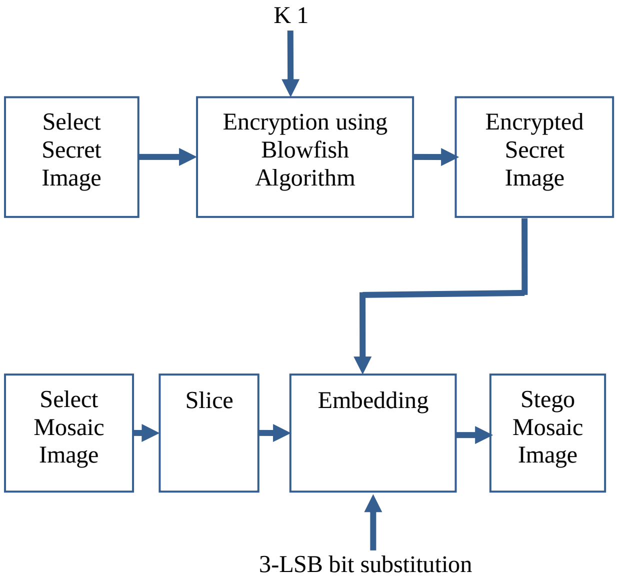

Fig 3:- Block diagram at sender side

Receiver Side:

The receiver received the stego mosaic image which contain more than seven encrypted images. And they extract the encrypted secret images from the stego mosaic image using reverse 3-LSB substitution technique. The key K1 is used to decrypt the encrypted secret images henced the original secret images are obtained. As shown in figure(4) given below.

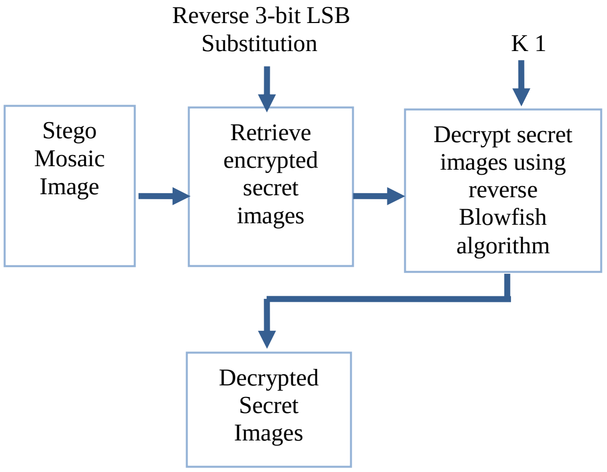
Reverse 3-bit LSB Substitution
K 1
Stego Mosaic Image
Retrieve encrypted secret images
Decrypt secret images using reverse Blowfish algorithm
Decrypted Secret Images

Fig 4: Block diagram at receiver side

6 CONCLUSION

Protecting the secret images by encrypting the secret images and embedding these encrypted secret image behind the mosaic image. We can conclude that the proposed system is more effective for secret communication over the network channel.So if a confidential message is expected to send, then it should provide more security and it should make the hacker to consume his/her maximum amount of time to hack the content.

7 REFERENCES

[1]H. Faheem Ahmed, U. Rizwan,“ Embedding Multiple Images in an Image Using Bit Plane Slicing ” , International Journal of Advance Research in Computer Science and Software Engineering, Volume 3,Issue 1, January 2013, Page(s):327-335.

[2]Pye Pye Aung and Tun Min naing,”A novel Secure Combination Techniques of Stegnography and Cryptography,” International Journal of Information Technology Modeling and computing (IJTMC)vol.2, No.1 February 2014.

[3]R.Nivedhita, Dr.T.Meyyappan, “Image Security Using Steganography And Cryptography Techniques”, International Journal of Engineering Trends and Technology, Volume 3, Issue 3, Publication Year: 2012, Page(s):366-371.

[4]Priyanka P. Palsaniya,Pravin D. Soni “CryptoSetganography: Security Enhancement by using Efficient Data Hiding Techniques” International Journal of Application or Innovation in Engineering and Management (IJAIEM), Volume 3,Issue 2, February 2014.

The receiver extract the encrypted secret images from th

[5]Masud karim,Rahman,Hossain,”A new approach for LSB based image Steganography using secrete key”,14th International Conference on Computer and Information(ICCI)Pages 286-291,year:2011.

[6]Pradeep Kumar Mallick, Narendra Kumar Kamila “Crypto Steganography Using Linear Algebraic Equation” International Journal of Computer & communication Technology, Volume 2, Issue VIII, Publication Year: 2011.

[7]Mr. Vikas Tyagi, “Data Hiding in Image Using Least significant Bit with Cryptography” , International Journal of Advance Research in Computer Science and Software Engineering, Volume 2, Issue 4,April 2004.

[8]Dipti Kapoor Sarmha, Neha Bajpai “Proposed System for Data Hiding using Cryptography and Steganography” Proc. International Journal of Computer Application, Volume 9, Issue 2, Publication Year: 2010.

[9]Rahul Jain,Naresh Kumar “Efficient Data Hiding Scheme Using Lossless Data Compression and Image Steganography” International Journal of Engineering Science and Technology(IJEST), Volume 4, 08 August 2012.

[10]Namrata A. Khodke, Prof. Dr. Siddhart A. Ladhake “ A New Approach to Secure Image Transmission via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformation” International Journal of Advance Research in Computer Science and Software Engineering, Volume 5, Issue 4, April 2015.

[11]Harshita K M, Dr. P. A. Vijaya “Secure Data Hiding Algorithm Using Encrypted Secret Message”

International Journal of Scientific and Research Publication, Volume 2, Issue 6, June 2012.

ABOUT THE AUTHOR

Shireen Sheikh is pursing B.E in Information Technology from RTMNU Maharashtra, India. Her area of interest is computer system security and networking .

Chetana Nimje is pursing B.E in Information Technology from RTMNU Maharashtra, India. Her area of interest is computer system security and hardware networking.

Vaishali Bhagat has received B.E degree in Information Technology from RTMNU Maharashtra, India in 2008 and pursuing M.Tech in CSE from RTMNU Maharashtra, India .She is working as a assistant professor in department of Information Technology SRMCEW Nagpur, Maharashtra, India Her area of interest is computer system security and visual cryptography. She has publish 10 research paper and is member of IAENG, STE, Academia.edu, review of premierl publication.