Secured Secret Image Transmission by using Fragment Visble Mosaic Image Technique

Ashalatha H M, M.D Anitha Devi,Dr. K.B Shivakumar, Dr. M. Z Kurian
Dept. of ECE,Sri Siddhartha Institute of Technology ,Tumkuru Karnataka, India
Ashalatha401@gmail.com ,anumdssit@gmail.com, shivakumarkb@ssit,edu.in, mzkurianvc@yahoo.com

ABSTRACT : In recent years as many of our daily tasks are related to internet, the security of information being transmitted over the internet is an important issue. Many applications or fields require transmitting secret image over the internet that may contain private and confidential information that is needed to be protected from hacker or from unintended users. Many techniques and methods have been proposed to ensure security, out of them most commonly used techniques are encryption and data hiding. Encryption ensures security but the problem with encryption algorithm is that the resultant noise image attracts the attention of hacker so it may be possible after many trials they can be decrypted by hacker. Another method is data hiding in which pieces of secret information is hidden behind a carrier that may be anything a text file, video, audio or an image. Now a day's, for secure image transmission a new concept that is of mosaic image is used in the field of data hiding. A new type of mosaic image that is called as secret fragment visible mosaic is formed to hide the existence of secret image by using a carrier image. In this project a new technique for creating a secret fragment visible mosaic image is proposed.

Keywords – Mosaic image, secret fragment visible mosaic image, reversible color transformation, data hiding and steganography algorithm.

I. INTRODUCTION

In recent years the secret information is hided in the images from various sources and are transmitted through the internet in many applications. Medical and military imaging systems and databases are examples of such applications. These images consist of some private or confidential data which is to be Kept confidential and protected from leakage process while transmitting. Many techniques are available to provide security for image transmission operations. There are two general methods they are image encryption approach and data hiding technique.

The image encryption uses images which have a neutral property like high redundancy and strong correlation. There is a possibility that the image which is created using image encryption technique may be attracted by the third party because of its randomness in nature while transmission. By using these properties of the image researchers worked on authenticating the image. Image Encryption algorithms make use of these natural properties of the image to authenticate the image. Another method of authenticating the color image is data hiding where we use two types of entities to transmit the image secretly. One is an image which we required to transmit secretly called as secret image and another one is an image which is used to hide the secret image called as a cover image.

These encryption and decryption process is controlled by key at transmitter and receiver end. Without the key we cannot decrypt the image at receiver end. Several data hiding techniques have been proposed in the literature includes LSB Substitution [1], histogram Shifting [2], difference expansion [3], prediction error expansion [4]. In this paper we have implemented an authentication system for an image which transforms a secret image into meaningful mosaic image which looks like a preselected carrier image. We are using a simple LSB Substitution to hide the data required for recovering secret image at receiver end. The method implemented in this paper is inspired by Lai and Tsai [5] and Lee and Tsai [6]. The mosaic image is the result of rearrangement of the fragments of a secret image in disguise of another image called the carrier image preselected from a preselected database. Specifically, a secret image and a carrier image first divided into rectangular fragments and then the secret image blocks is fit into carrier image P a g e blocks according to a similarity criterion based on color variations. Next, the color characteristic of each secret image block is transformed to be that of the corresponding carrier block in the carrier image, resulting in a mosaic image which looks like the carrier image. The relevant information required for recovering the original image id hide into the created mosaic image. The image encryption algorithms yield a mosaic image which is meaningless. The data hiding method must be hide data in highly compressed manner into a disguising mosaic image without compression.

II. RELATED WORK

The authorsYa-Lin Lee ; Nat. Chiao Tung Univ., Hsinchu, Taiwan; Wen-Hsiang Tsai, proposed a paper titled as –A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations‖. It is a new secure image transmission technique, in which the given selected large volume secret image is transformed into a mosaic image called as secret-fragment-visible mosaic image of the same size as that of secret and target image. The created mosaic image looks similar to a selected target image and it may be used as a disguise of the secret image, which is constructed by dividing the secret image into small fragments and by color transforming those fragments color characteristics to be those of the corresponding blocks of the selected target image. There are various color transforming techniques which are designed skillfully to conduct the color transformation process by doing this the secret image may be recovered lossless. In this paper the author proposed a new scheme of handling the overflows/underflows. The information which is needed to recover the secret image is embedded into the created mosaic image by a lossless data hiding technique with a secret key.

The author Merlin et all. Proposed a new method for secured communication in the paper titled as –Covert Image Transmission Technique Using Mosaic Image‖. This is a novel method for secret communication which involves transmission of secret images. The color image which is to be transmitted secretly is disguised into a cover image of the same size which produces a mosaic image. The mosaic image looks as mirror image of the cover image and is visually indistinguishable from it. The creation of mosaic image involves block by block processing of both secret and cover images. In the proposedmethod the Gaussian noise is added to the secret Image to ensure positive variance of intensities within image blocks. Image blocks are matched according to the standard deviation of the intensities. Color transformation technique is applied to transform the secret image blocks into theblocks of mosaic image. The information required which is required to retrieve the secret image from mosaic image is compressed and embedded in the mosaic image by using a LSB embedding technique. The RMSE and PSNR ratios are considered to analyze the performance of the method.

I-Jen Lai and Wen-Hsiang Tsai, Senior Member, IEEE proposed a novel method for secure communication in the paper titled as –Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding‖. It is a new type of computer art image which is called as secret-fragment-visible mosaic image, so called mosaic image can be created by dividing the selected secret image into a small fragments and embedding them in to a cover image to form a mosaic image of a given image to become a target image in a mosaic form, this achieves an effect of embedding the secret image visibly but secretly in the resulting mosaic image. This method of hiding a secret image is useful for covert communication or secure keeping of secret images. The author proposed a method for transforming the 3-D color space to 1-D color scale to transfer the secret image and to create a mosaic image and a new image similarity measure is proposed for the selection of target image from the database, based on which a new image similarity measure is proposed for selecting from a database. A fast greedy search algorithm is proposed to select a secret image tile to fit into corresponding block in target image. The information regarding the tile image fitting sequence is embedded into randomly-selected pixels in the mosaic image using a lossless LSB replacement technique with the secret key. Good experimental results show the feasibility of the proposed method.

III. PROPOSED WORK

The block diagram of the proposed method is as shown in figure 1 In Proposed System Secrete image is pre-processed before caring out mosaic image process, in pre-processing both secretes and target images are resized to a standard image resolution, It will avoid the dimensionality error during the processes. The Images are divided into blocks or tiles; from each block standard deviation is calculated and stored it in a ascending order. Using sorted information first tile of secrete mage is fit to particular first block of Target similarly all the image tiles are fit in Target image and resulting image looks like Selected Target. Then Color Transformation is done to Mosaic Image, image tiles are rotated using RMSE value to get final Mosaic Image. In the above block diagram fig.1 Shows the creating of mosaic image using secrete and target image.

Steps involved in generating secret fragment visible Mosaic image are given in this section:

A. Selection of cover and payload images:

In this step user has to select their secret image and any random image of his/her choice as cover image user can select any image as target image of any size in contrast to Lai and Tsai method that requires cover image should be double in size and should satisfy some similarity, measure criteria to be used s cover image. But in order to avoid to suspicion it is advised that target image is to be selected, which is of some field or of same background as that of secret image.

B. Resize the secret image:

Here in this proposed method to create secret fragment visible Mosaic of the same size as that of cover image, after the payload image and cover image are selected, we have to check whether the cover image and payload image are of same size or not, if they are not of same size then we have to resize the payload image to make it of same size as that of cover image.

C. Divide both the payload and cover images into tiles:

Next step is to split the source image into small pieces called as tiles. In proposed algorithm in order to create the secret fragment visible mosaic image there is requirement that the number of blocks of target image should be same in size. So the cover and payload images are to be split by using splitting technique.

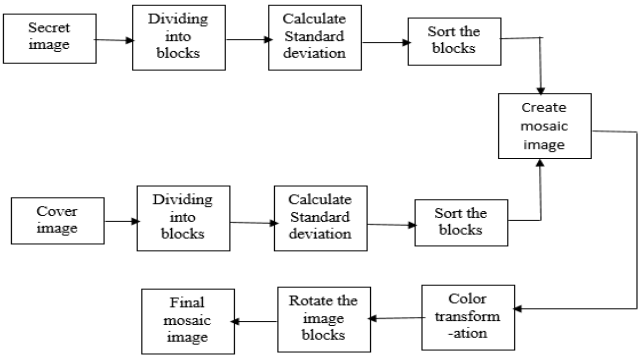

Fig 1: proposed system.

D. Calculate standard deviation and arrange them in ascending order:

Here how to choose an appropriate block B of target image for each of the tile T of secret image is the main issue. For this the standard deviation of the pixels of each block is to be calculated as a similarly measure value to select of the tile T of payload image .Then the tile image is found by arranging the tiles in ascending order to form the sequence stile and all the blocks to form sequence target that is in

ascending order with respect to their standard deviation value.

E. Creation of Mosaic image:

To create the Mosaic image, the used sorted sequence of standard deviation to form resultant image. First we fit the first tile in sequence stile into the first block in sequence target, and accordingly fit the second tile in stile to second block in target and so on. In this way resultant Mosaic image is formed which will look somewhat similar to the selected cover image.

F. Perform Color Transformation:

The Mosaic image created above contains some noise which willdegrade the picture quality of the Mosaic image so to make the Mosaic image to look very similar to the cover image color transformation has to be applied to the Mosaic image. Calculate the RMSE value for each block by rotating the each blocks to the angles of 0^o, 90^0, 180^0, 270^0 and the blocks are rotated to the angle with the least RMSE value. The Mosaic image created after the color transformation will look same as that of cover image.

G. Reconstruction of Secret image with the Mosaic image :

Reconstruct the secret image with the Mosaic image by carrying de-embedding process.

IV. RESULTS AND ANALYSIS

Secret Fragment Visible Mosaic image creation involves following steps:

A. Selection of cover and payload images

B. Resize the secret and cover images

C. Divide both the payload and cover images into tiles

D. Calculate standard deviation and arrange them in ascending order

E. Creation of Mosaic image

F. Perform Color Transformation.

The Mosaic image created with the above steps is as shown in fig. 2 and fig. 3 it looks very similar to the selected target image.Inputs to the Mosaic image creation are target image and secret image. Simulation results of mosaic image creation are shown below. Mosaic image which is created with the target and secret images and the reconstrucred secret image from Mosaic image are shown in fig. 2 Secret iamge is retreived back without any loss of information.

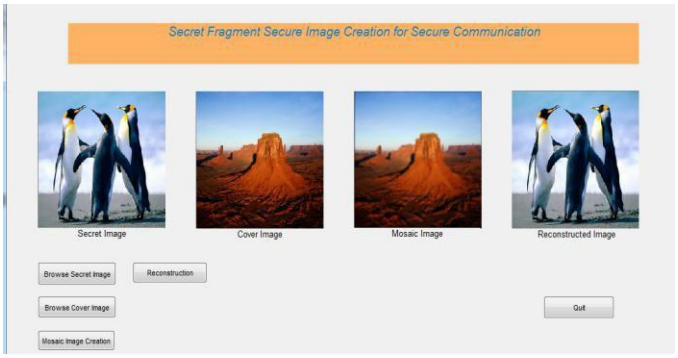

Fig 2: simulation results of Mosaic image constructed with selected target andsecret image and secret image retrieved from the Mosaic image.

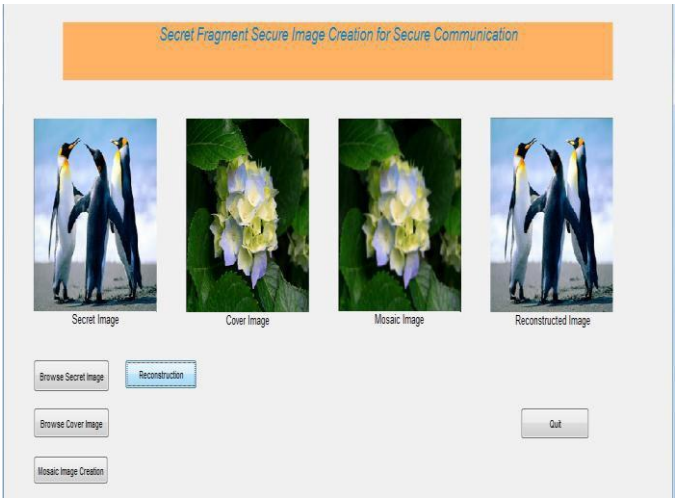

Fig 3: simulation results of Mosaic image constructed with different target and same secret image and secret image retrieved from the Mosaic image.

V. CONCLUSION

In this paper a new method for creation of secret fragment visible Mosaic image has been proposed. This method allows user to select any cover image of their choice to create Mosaic image and also user can select payload image and cover image of any size to create Mosaic image. The resultant Mosaic image can be used for secret communication and the secret image is retrieved from the Mosaic image (Fig. 2 and 3) without any loss. This method of creation of mosaic image has the advantage of strong secret data embedding capacity so the unintended user cannot decrypt the secret data.

REFERENCES:

[1] C. K. Chan and L. M. Cheng, Hiding data in images by simple LSB substitution,‖ Pattern Recognition..,vol. 37, pp. 469474, Mar. 2004.

[2] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, Reversible data hiding,‖ IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354362, Mar. 2006.

[3] J. Tian, ―Reversible data embedding using a difference expansion,‖ IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890896, Aug. 2003.

[4] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, Reversible water- marking algorithm using sorting and

prediction,‖ IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989-999, Jul. 2009.
[5] I. J. Lai and W. H. Tsai, Secret-fragment-visible mosaic image—A new computer art and its application to information hiding,‖ IEEE Trans. Inf. Forens. Secure.,vol. 6, no. 3, pp. 936–945, Sep. 2011.
[6] Ya-Lin Lee and Wen-Hsiang Tsai, A New Secure Image Transmission Technique via Secret-Fragment Visible Mosaic Images by Nearly Reversible Color Transformations,‖ IEEE Trans. Circuits and systems for video technology., volume:24 , Issue: 4 ,pp. 695 – 703, April 2014.