International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 9 5653 - 5658

A Secured Technique for Transmission of an image/ video Via Mosaic image/video Creation.

Gija Susan Issac,PG scholar
Ece dept.
Ilahia college of engineering and technology
Ernakulam, India
gijasusan@gmail.com

Jobi Jose, Asst.Professor
Ece dept .
Ilahia college of engineering and technology
Ernakulam, India
jobijose03@yahoo.com

***Abstract*—** A new secured image/video transmission technique is proposed in paper. Here video is considered as a sequence of frames. The secret image is automatically transformed into a secret-fragment visible mosaic image. This image looks similar to a randomly selected target image. The target image is used to cover or hide the secret image. Also relevant information for reconstructing the secret image is embedded on the mosaic image by a loss less data hiding scheme using a key. The secret image is divided into cells and the color characteristics of each cell are transformed to that of the divided target blocks. In order to reconstruct the secret image losslessly skilful techniques are designed to conduct the color transformation process. Good experimental results and high signal to noise ratio shows the feasibility of the new technique for both image and video.

Keywords*-Mosaic image, steganography, color transformation*

*****

I. INTRODUCTION

In the present scenario, a number of images/video are sent through internet or other sources. These images may be highly confidential or private, that is it may include personal albums, medical images or military images. Internet is a global system, and everyone can have easy access to this network. Thus it is important to protect these confidential information from any kind of leakages or unauthorized access during transmission.

Recently , to overcome this situation of unauthorized access during transmission, a number of methods have been proposed. Out of the different methods present, steganography is one of the most appropriate method for secure image transmission. Steganography is the practice of concealing a file, message, image or video with in another file, image or video. The word steganography combines the Greek word ‘steganos’ meaning covered, concealed or protected and ‘graphein’ means ‘writing’.

The advantage of the steganography is that the image is hidden in cover object in such a manner that just by viewing the image or video, it is impossible to judge that there is any data hidden or not. It is mainly used for security communication. Here, a new secure image/video transmission technique is proposed, which is based on the steganographic approach. A graphical user interface system is provided to select whether an image or video is to be transmitted. If an image is to be transmitted it is hidden on a cover image, similarly a video is hidden in a cover video. The image which is highly confidential is considered as the secret image, and it is hidden on a arbitrarily selected cover image called the target image.

In this method the secret image is automatically transformed into the secret-fragment-mosaic image. The mosaic image looks similar to that of the target image. As the name suggests mosaic image is created by composing or mapping two images, that is the secret and the target image. For this the secret and the target images are divided into 4X4 cells. This resulting mosaic image is transmitted. Relevant information for recovering the secret image is embedded on the created mosaic image with a key.

II. REVIEW

Many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding. In Image Encryption[3] the encrypted image is a noise file so that no one can obtain the secret image unless he/she has the correct secret key. However, the encrypted image is a meaningless noise file, which cannot provide additional information before decryption and may arouse an attackers attention. An alternative to avoid this problem is data hiding[4][5]that hides a secret data into a cover image, so that no can realize the existence of the secret data. A main issue this method is to embed large amount of data into a single image.

Recently a new technique for secure image transmission, ie a new type of computer art image called secret fragment visible mosaic image is proposed by Lai and Tsai[2] . Mosaic which is created automatically by composing small fragments of a given image to become a target image in a mosaic form, achieving an effect of embedding the given image visibly but secretly in the resulting mosaic image. In this method the target image which is required to hide the secret image has to be preselected from a data base.

Requirement of a large database was obviously one of the weakness of this method. Thus the user was not allowed to select freely his/her favorite image as target image. Inorder to avoid this issue while keeping its merit a new method was proposed by Ya-Lin Lee and Tsai[1] ,it was aimed to design a new method that can transform a secret image into a secret fragment visible mosaic image of the same size that has a visual appearance of any freely selected target image without the need of a data base. But an obvious weakness of this method was that it divided the images into 8x8 cells, which resulted in for noise in the secret image after decrypting from the target image. The time required for processing was also high due to the presence of the calculation using Huffman table. Another limitation for this method was that only image transmission was possible, not video.

To overcome all this issues a new technique is introduced which can be used to transmit either image or video. A window is provided to select either video or image for transmission.

As an illustration figure(1)shows the result yielded by the proposed method. Specifically, after a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks, according to a similarity criterion based on color variations. Next, the color characteristic of each tile image is transformed to be that of the corresponding target block in the target image, resulting in a mosaic image which looks like the target image. Relevant schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image.

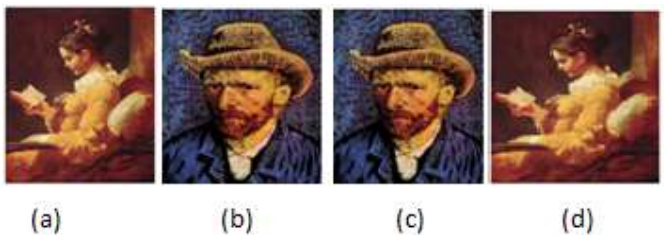

Figure1: (a) secret image.(b) target image.(c) target mosaic image created.(d) recovered secret image.

An easy comparison between the already existing method[1] and the new technique can be made clear through the basic block diagrams in figure (2) and figure(3), where figure(2) represents the existing method whereas figure(3) represents the new technique.

The remainder of this paper, the basic idea of the proposed method is described in section III. Section III is subdivided into two A: For secret image transmission, B: For secret video transmission. Detailed algorithm for secret image transmission is provided at section IV and algorithm for video transmission is provided in section V, experimental results are presented to show the feasibility of the proposed method in section VI, Security issues are considered in section VII, followed by conclusion in section VIII.

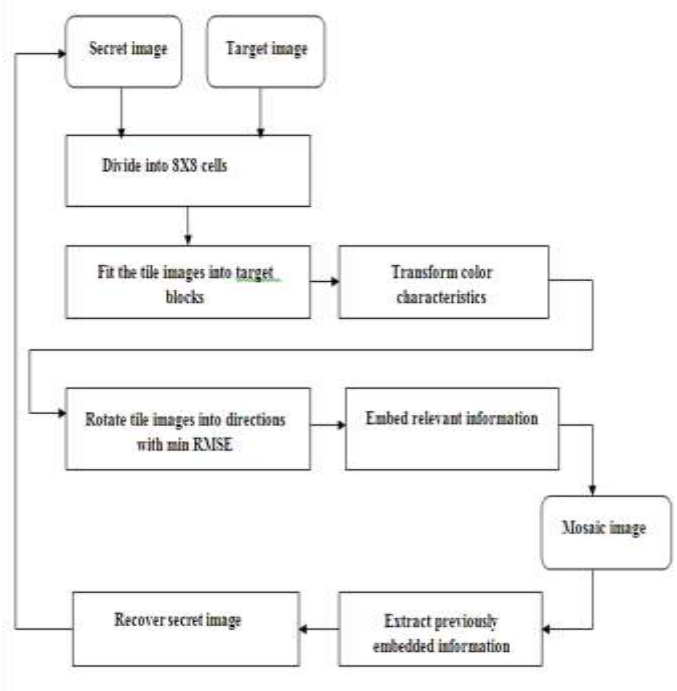

Figure 2. Basic block diagram of the existing technique

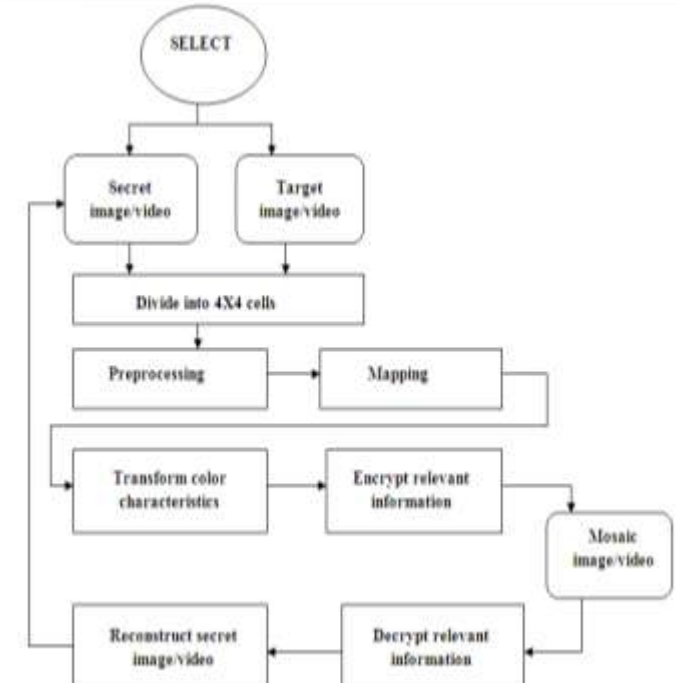

Figure3 .Basic block diagram of the new technique.

III. BASIC IDEA OF PROPOSED METHOD

A. For Secret Image Transmission:

A flow diagram of the proposed method is shown in fig(4),which includes two main phases:

Phase 1: Mosaic Image creation
Phase 2: Secret Image recovery

The first phase includes Mosaic image creation. As the flow chart represents, the secret and the target image is selected. Target image is used to cover the secret image.

1.Preprocessing:

The size of the target image and the secret image is set to a unique size, so that both are identical; then divide the target and secret images into cells, with each cell of size 4*4.

2. Mapping:

For mapping the secret image blocks to target blocks, first compute the mean and standard deviation of each tile image 'g1i' of the target block and g2i of the secret image. Sort the standard deviation values and then sort the tile images in the set g1 & set g2.Then map each secret tile images to that of the target tile images based on the calculated standard deviation. Mapping of the secret tile images with minimum standard deviation to that of the target tile images with minimum standard deviation provide be the correlation between the tile images.

3. Transform Color Characteristics between blocks

Each tile image in the given secret image is to fit into a target block in a preselected target image.Since the color characteristic of the secret and target images are different, it is required to perform certain color transform techniques.

Let the target & the secret images represented by two pixel sets { T1,T2……Tn} & {T1', T2'….} respectively; Let the color of each Ti be denoted by (ri,gi,bi) and that of each Ti' by (ri',gi',bi'). At first, we compute the mean & standard deviation of the secret & target cells in each of the three color channels r,g,and b. Next compute new color values (ri",gi",bi") for each Ti in T[1] by

$$c_i''=q_c(c_i-\mu_c)+\mu_c' \quad (1)$$

In which $q_c[1]$ is obtained by dividing the standard deviation of the target image by mosaic image.

4. Encrypting Relevant Information:

In order to recover the secret image from the mosaic image, it is required to embed relevant recovery information into the mosaic image. For this, a LSB replacement method proposed by Chi-Kwong Chan[4]is used. The classical LSB replacement which substitute LSB's of target image with message bits directly. LSB substitute provide less chance for image degradation& also provide more hiding capacity.

After embedding the relevant information on the LSB of the target image we get the Target Mosaic Image.

5.Decrypting Relevant Information & Reconstructing the Secret image

In order to reconstruct the secret images it is first necessary to decrypt, the relevant information. The information required for reconstruction is obtained from the LSB of the Target Mosaic Image, which is transmitted. For recovering the secret image, it is required to perform the reverse operation to obtain the original cell value.

That is to compute the original color values (ri,gi,bi) of Ti from new ones (ri", gi",bi"), the following formula which is the inverse of (1) ie used[1]:

$$c_i=1/(q_c)(c_i''-\mu_c')+\mu_c \quad (2)$$

All these values required are obtained from the LSB of the target mosaic image . Finally the secret image is reconstructed with minimum distortion.

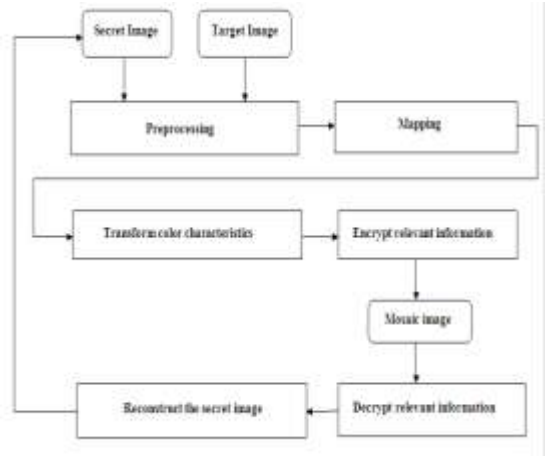

Figure.4.Processes for Mosaic Image creation and Secret Image recovery.

IV. ALGORITHM-I

The algorithm consist of Mosaic Image creation& Secret Image Recovery. The first phase Mosaic Image Creation can be divided into 4 stages.

Stage 1: *Fixing the secret tile images into target blocks*.

Step1: Resize both the Target & Secret image. Divide both the images into cells of size 4X4.

Step 2: Compute the mean (mn1) & (mn2) & standard deviation (Sd1 & Sd2) for the 3 color channels & sort the average standard deviation values.

Step 3: Sort the secret tile images according to the computed average standard deviation value of the target blocks; Map in order the sorted tile images to the sorted target block in 1-1 manner

Step 4: Create a mosaic image 'g' by fitting the tile images into the corresponding target blocks according to the mapping sequence.

Stage 2: Perform color conversion between the secret image &target blocks

Step 5 : For each pixel Ti in each tile image 'gi'of mosaic image with color value C_i where c= r, g or b, transform c_i into new value c_i" by (1).

Stage 3: Embedding the secret image recovery information.

Step 6 : The value of 'q' & the mean of the two images which are required for secret image recovery are encrypted to the target mosaic image using a key.

Step 7: The values are encrypted using LSB substitution method, thus the values are stored to end & end-1 position

Stage 4: Secret image recovery.

Step 8: Decrypt the embedded information by using the correct key

Step 9: Perform the reverse of the equation (1) ie equation (2) to obtain the original cell value c_i for 3 color channels.

Step 10: Compose all the final tile images to form the required secret image as the output.

B. For Secret Video Transmission

The flow diagram of the proposed method is shown in figure(5).

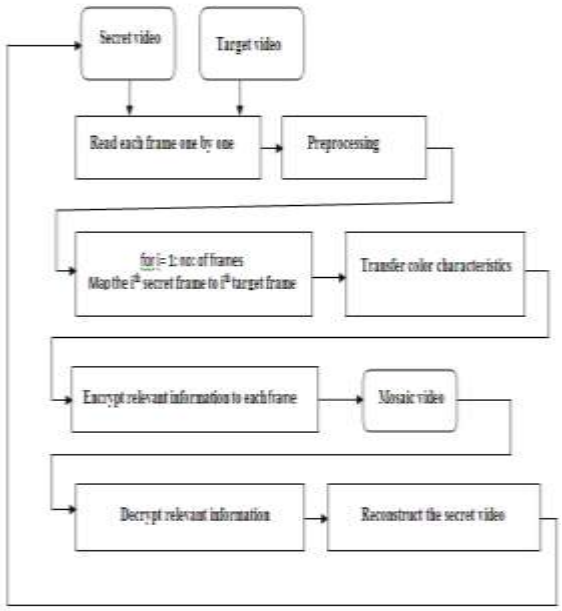

Figure.5 Processes for Mosaic Video creation and recovery

V. ALGORITHM-II

The algorithm consist of mosaic video creation and secret video recovery. Algorithm consist of 5 stages.

Stage 1 : Read the secret and the target video

Step 1: for i= 1: no: of frames selected
Read both the secret and the target video frames one by one.

Stage 2: Fixing the secret tile frames into the target frames.

Step 2: Resize each target and secret frame to a fixed size.

Step 3: Compute the mean (mn1) & (mn2) & standard deviation (Sd1 & Sd2) for the 3 color channels & sort the average standard deviation values.

Step 4: Sort the secret tile frame according to the computed average standard deviation value of the target blocks; map in order the sorted tile images to the sorted target blocks in one by one manner.

Step 5: for i= 1: no: of frames selected,
Map the i th frame of the secret video to the i th frame of the target video. Thus creating the Mosaic video.

Stage 3: Perform color conversion between the secret &target frames

Step 6 : For each pixel Ti in each tile image 'gi'of mosaic image with color value C_i where c= r, g or b, transform c_i into new value c_i" by (1).

Stage 4: Embedding the secret image recovery information.

Step 7 : The value of 'q' & the mean of the two images which are required for secret image recovery are encrypted to the target mosaic image using a key.

Step 8: The values are encrypted using LSB substitution method, thus the values are stored to end & end-1 position

Stage 5: Secret image recovery.

Step 9: Decrypt the embedded information by using the correct key

Step 10: Perform the reverse of the equation (1) ie equation (2) to obtain the original cell value c_i for 3 color channels.

Step 11: Compose all the final tile images to form the required secret image as the output.

VI. EXPERIMENTAL RESULTS

A series of experiments have been conducted to test the proposed method using many secret and target images. An example of the experimental result is shown in fig.6;fig.6(a) shows the secret image, fig.6(b) shows the target image; fig. 6(c) shows the mosaic image created. The tile image size is 4X4.The reconstructed secret image using the correct key is as shown in fig. 6(d) which looks nearly identical to that of the secret image fig. 6(a).

Fig .7(a) and fig 7 (b) gives a comparison of the output, between the images obtained by considering the existing method ie by dividing the tile images into 8X8 cells and the new technique in which the tile images are divided into 4X4 cells.

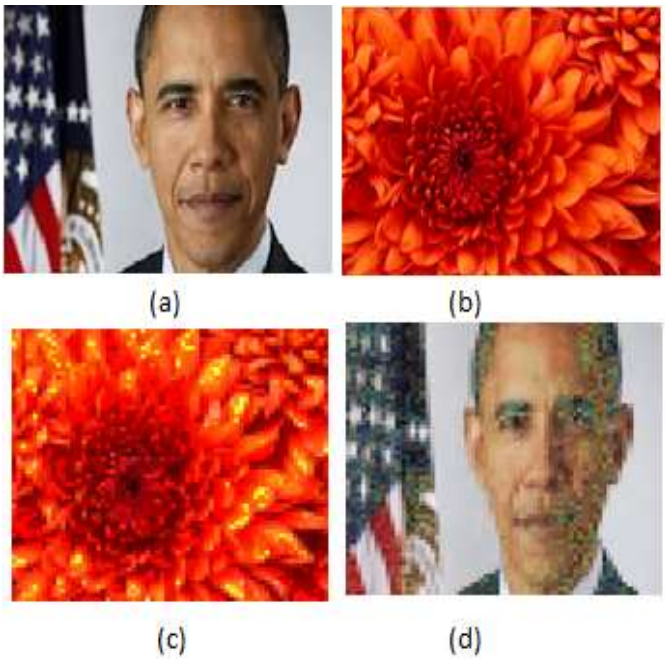

Figure. 6. (a) secret image,(b)target image, (c)mosaic image, created by dividing the tile images into4X4(d)reconstructed

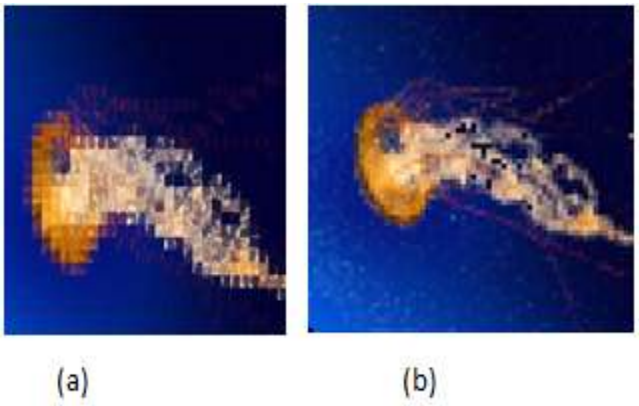

Figure 7. (a) image decrypted by dividing the tile images into 8X8 blocks.(b) image decrypted by dividing the tile images into 4X4 blocks

Table I Peak Signal to Noise Ratio Calculated

Method	Division of tile	PSNR
Existing Method	8X8	27.174
New technique	4X4	34.7618

VII.SECURITY CONSIDERATIONS

In order to increase the security of the proposed method, the encrypted information for later use is embeded using a secret key as shown in the algorithm. Only the reciever who have the proper key can decode the secret image or video. Figure 8, shows the advantage of using a secret key. Figure 8.(c) shows the image decrypted using wrong keep, whereas figure 8.(d) shows the secret image recovered successfully.

Figure 8: (a)secret image,(b) target image,(c) secret image tried to obtained using a wrong key,(d)secret image using correct key.

VIII. CONCLUSION

A new secure image/video transmission technique was proposed, which create meaning full mosaic image/video to cover the secret data to me transmitted. The proposed system does not require a data base for target image. Thus the user can select any image on his/her wish as the target image. Also the original secret image / video can be recovered nearly lossessly. Good experimental result have shown feasibility of the proposed method. Future studies may be directed to apply the proposed method to video with audio.

ACKNOWLEDGMENT

The authors gratefully acknowledge the contributions of Ya-Lin Lee and Wen-Hsiang Tsai for their work on the original version of this document.

REFERENCES

[1] Ya-Lin Lee and W.H. Tsai," A new secure image transmission technique via secret-fragment –visible mosaic image by nearly reversible color transformations.", IEEE Trans, circuits and systems for video technology, vol.24,no.4,april 2014'

[2] 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. Secur., vol. 6, no. 3, pp. 936–945, Sep. 2011.

[3] J. Fridrich, "Symmetric ciphers based on two-dimensional chaoticmaps," Int. J. Bifurcat. Chaos, vol. 8, no. 6, pp. 1259–1284, 1998

[4] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit.., vol. 37, pp. 469–474, Mar. 2004

[5] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEETrans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.