International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 5, May 2016

A New Approach for Mosaic Image Creation for Hiding Secret Image/video for Secure image Transmission

[1]Shamna E.P, [2]Sabna I
[1][2] Department of Electronics and Communication Engineering,
KMCT College of Engineering, Calicut, India,
[1]shamna4innu@gmail.com,[2]sabnahaniz@gmail.com

***Abstract*: Information security is becoming increasingly important in the modern networked age. Secure Image Transmission has the potential of being adopted for mass communication of sensitive data under the scrutiny of an adverse censoring authority. Images from various sources are often used and are transmitted through the internet for various purposes, such as confidential enterprise archives, document storage systems, medical imaging systems, and military image databases. These images may contain secret or confidential information since it should be protected from leakage during transmissions. A new type of computer art image called secret-fragment-visible mosaic image is proposed, 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. This effect of information hiding is useful for covert communication or secure keeping of secret images. receiver recover the secret image with a high precision. The root mean square error and peak signal to noise ratio are used as quality measures.**

***Index Terms* — Color Transformation, data hiding, image encryption, secure image transmission, mosaic image.**

I. INTRODUCTION

Nowadays, images from various sources are often used and are transmitted through the internet for various applications, such as confidential enterprise archives, document storage systems, medical imaging systems, and military image databases. These images usually contain private or confidential information so that they should be protected from leakages during transmissions. Recently, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding.

Encryption of image is a technique that make use of the natural property of an image, such as high redundancy and strong spatial correlation, to get an encrypted image. The encrypted image is meaningless and this may arouse the third parties attention due to its randomness in form during transmission. Another method for secure image transmission is data hiding that hides a secret entity into a cover image so that a third party cannot found the presence of the secret entity. The problem of data hiding is the difficulty in embedding large volume of secret entity into a single image. If anyone wants to hide a secret entity into a cover image, the secret entity must be highly compressed earlier. During retrieval this will cause distortion of the secret entity.

In this project, propose an approach for secure image transmission is needed, which is to transform a secret image into a meaningful Secret Fragment Mosaic image with size almost same and looking similar to the preselected target image. The mosaic image is the outcome of arranging of the block fragments of a secret image in a way so as to disguise the other image called the target image. The mosaic image, which looks similar to a randomly selected target image, which is used for hiding of the secret image by color transforming their characteristics similar to the blocks of the target image. Such technique is necessary so for the lossless recovery of the transmitted secret image. The appropriate information is embedded into the mosaic image for the recovery of the transmitted secret image.

II. RELATED WORKS

A Steganography is the science of hiding secret messages into cover media so that no one can realize the existence of the secret data. Existing steganography techniques may be classified into three categories – image, video, and text steganographies, and image steganography aims to embed a secret message into a cover image with the yielded stego-image looking like the original cover image. Many image steganography techniques have been proposed, and some of them try to hide secret images behind other images. The main issue in these techniques is the difficulty

to hide a huge amount of image data into the cover image without causing intolerable distortions in the stego-image.

[1] Least significant bit (LSB) is the best method for data protection. LSB method is very simple and a commonly used approach for developing Steganography system because the amount of space that an image can provide for hiding data will be more comparing with another other method LSB technique is the easiest way of hiding information in an image and yet it is effective.

[2] JPEG: Still Image Data Compression Standard Here, W. B. Pennebaker tries to explain that the main obstacle in many applications is the quantity of data required to represent a digital image. For this we would need an image compression standard to maintain the quality of the images after compression. To meet all the needs the JPEG standard for image compression includes two basic methods having different operation modes: A DCT method for "lossy" compression and a predictive method for "lossless" compression.

[3] A Keyless Approach to Image Encryption, by Indian Institute of Technology Roorkee This paper shows a keyless approach to encryption methods which are used to encrypt images. We make the use of this paper to apply the keyless approach in the proposed method. This is done by generating relevant information with the help of some RMSE value which help to rotate the tile images to a certain angle.

[4] 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. But an obvious weakness of Lai and Tsai is the requirement of a large image database so that the generated mosaic image can be sufficiently similar to the selected target image. Using their method, the user is not allowed to select freely his/her favorite image for use as the target image.

Based on literature survey, it has been found that the previous methods have its own drawback. It is therefore desired in this study to remove this weakness of the method while keeping its merit, that is, it is 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 the visual appearance of any freely selected target image without the need of a database.

III. PROPOSED METHOD

In this project, 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 losslessly from the mosaic image. In more detail, as illustrated by Fig. 1, a given secret image is first "chopped" into tiny rectangular fragments, a target image is selected arbitrarily, Then, the fragments are arranged in a random fashion controlled by a key to fit into the blocks of the target image, yielding a stego-image with a mosaic appearance.

Fig 2 shows a result yielded by the proposed method. Specifically, after a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments

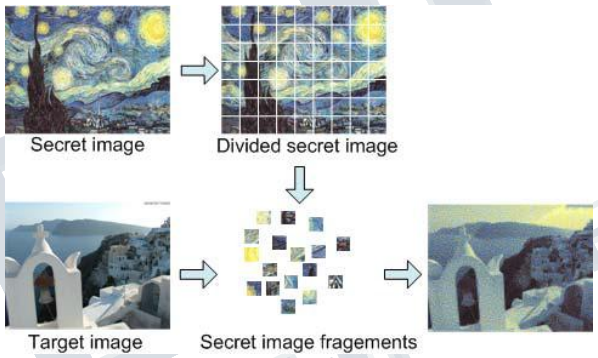


Fig 1: creation of secret-fragment-visible mosaic image.

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.

The proposed method is new in that a meaningful mosaic image is created, in contrast with the image encryption method that only creates meaningless noise images. Also, the proposed method can transform a secret image into a disguising mosaic image without compression, while a data hiding method must hide a highly compressed version of the secret image into a cover image when the secret image and the cover image have the same data volume.

Fig 2: A result yielded by proposed method. (a) Secret image. (b) Target image. (c) Secret-fragment-visible mosaic image created from (a) and (b)

IV. IDEAS OF PROPOSED METHOD

The proposed method includes two main phases as shown by the flow diagram of Fig. 3: 1) mosaic image creation and 2) secret image recovery.

In the first phase, a mosaic image is yielded, which consists of the fragments of an input secret image with color corrections according to a similarity criterion based on color variations. The phase includes four stages: 1) fitting the tile images of the secret image into the target blocks of a pre selected target image; 2) transforming the color characteristic of each tile image in the secret image to become that of the corresponding target block in the target image; 3) rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block; and 4) embedding relevant information into the created mosaic image for future recovery of the secret image.

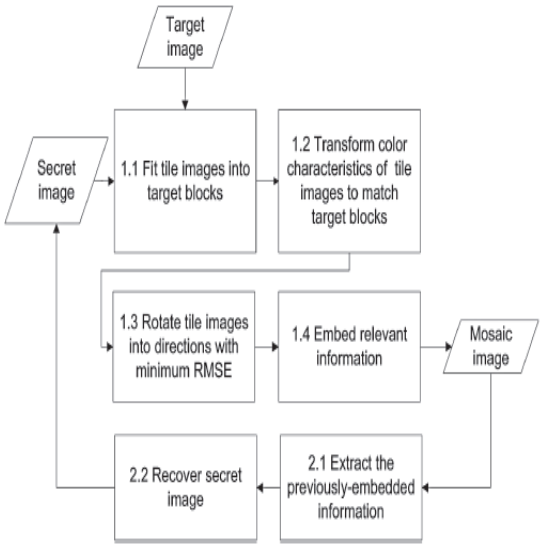


Fig 3 flow diagram of a proposed method

In the second phase, the embedded information is extracted to recover nearly losslessly the secret image from the generated mosaic image. The phase includes two stages: 1) extracting the embedded information for secret image recovery from the mosaic image, and 2) recovering the secret image using the extracted information.

V. IDEAS OF MOSAIC IMAGE GENERATION

The problems encountered in generating mosaic images by the proposed method are discussed in this section, and the proposed solutions to them are also presented.

A. Color Transformations between Blocks

Suppose that in the first phase of the proposed method, a tile image T in a given secret image is to be fit into a target block B in a pre-selected target image. Since the color characteristics of T and B are different from each other, how to change their color distributions to make them look alike is the main issue here. This idea is an answer to the issue and is adopted in this study. But instead of conducting color conversion in the lαβ color space, we do it in the RGB space to reduce the volume of the generated information which should be embedded in the created mosaic image for later recovery of the original secret image. More specifically, let T and B be described as two pixel sets {p1, p2, …, pn} and {p1′, p2′, …, pn′}, respectively, assuming that both blocks are of the same dimensions with size n. Let the color of pixel pi in the RGB color space be denoted by (ri, gi, bi) and that of pi′ by (ri′, gi′, bi′). First, we compute the means and standard deviations of T and B, respectively, in each of the three color channels R, G, and B by the following formulas:

$$\mu_c = 1/n \sum_{i=1}^{n} ci\,,\ \mu_c' = 1/n \sum_{i=1}^{n} ci' \quad \text{.....(1)}$$

$$\sigma_c = \sqrt{1/n \sum_{i=1}^{n} (ci - \mu_c)^2} \quad \text{.....(2)}$$

$$\sigma_c' = \sqrt{1/n \sum_{i=1}^{n} (ci - \mu_c')^2} \quad \text{.....(3)}$$

where ci and ci′ denote the C-channel values of pixels pi and pj′, respectively, with c denoting r, g, b. Next, we compute new color values (ri″, gi″, bi″) for each pi in T by:

$$ci'' = \frac{\sigma_c'}{\sigma_c} (ci - \mu_c)^2 + \mu_c' \quad \text{.....(4)}$$

This results in a new tile image T′ with a new color characteristic similar to that of target block B. Also, we use the following formula, which is the inverse of Eq. (4), to compute the original color values (ri, gi, bi) of pi from the new ones (ri″, gi″, bi″):

$$ci = \sigma_c / \sigma_c'(ci'' - \mu_c')^2 + \mu_c \quad \text{.....(5)}$$

Furthermore, we have to embed into the created mosaic image sufficient information about the transformed tile image T′ for use in later recovery of the original secret

image. For this, theoretically we can use Eq. (5) to compute the original pixel value of pi. But the mean and standard deviation values are all real numbers, and it is not practical to embed real numbers, each with many digits, in the generated mosaic image. Therefore, we limit the numbers of bits used to represent a mean or a standard deviation. Specifically, for each color channel we allow each of the means of T and B to have 8 bits with values 0 ~ 255, and the standard deviation quotient $q_c = \sigma'_c/\sigma_c$ to have 7 bits with values 0.1 ~ 12.8. We do not allow qc to be 0 because otherwise the original pixel value cannot be recovered back by Eq. (5) for the reason that $\frac{\sigma_c}{\sigma'_c} = 1/q_c$ in Eq. (5) is not defined when qc = 0, where c = r, g, b.

B. *Choosing Appropriate Target Blocks and Rotating Blocks to Fit Better*

In transforming the color characteristic of a tile image T to be that of a corresponding target block B as described above, how to choose an appropriate B for each T (i.e., how to fit each T to a proper B) is an issue. If two blocks are more similar in color distributions originally, a better transformation effect will result. For this, we use the standard deviation of block colors as a measure to select the most similar target block B for each tile image T. First, we compute the standard deviations of every tile image and target block for each color channel. Then, we sort all the tile images to form a sequence, S_{tile}, and all the target blocks to form another, S_{target}, according to the mean of the standard deviation values of the three colors. Finally, we fit the first tile image in S_{tile} to the first target block in S_{target}; fit the second in Stile to the second in S_{target}, etc.
Additionally, after a target block B is chosen for fitting a tile image T and after the color characteristic of T is transformed to be that of B as described above, we conduct a further improvement on the color similarity between the transformed T (denoted as T′) and B by rotating T′ into one of the four directions 0^o, 90^o, 180^0 and 270^o, which yields a rotated version T″ of T′ with the minimum RMSE value with respect to B among the four directions for final use to fit T into B.

C. *Handling Overflows/Underflows in Color Transformation*

After the color transformation process between a tile image T and a target block B is conducted as described before, some pixel values in the transformed block T′ might have overflows or underflows. To deal with this problem, we convert such values to be non-overflow/non-underflow ones and record the value differences as residuals for use in later recovery of the exact pixel values. Specifically, we convert all the transformed pixel values in T′ not smaller than 255 to be 255, and all of those not larger than 0 to be 0. Next, we compute the differences between the original pixel values and the converted ones, 255 or 0, as the residuals and record them as information associated with T′.

D. *Embedding Secret Image Recovery Information*

In order to recover the secret image from the mosaic image, we have to embed relevant recovery information into the mosaic image. For this, we adopt a technique of reversible contrast mapping proposed by Coltuc and Chassery [7], which is applied to the least significant bits of the pixels in the created mosaic image to hide data. The information required to recover a tile image T which is mapped to a target block B includes: (1) the index of B; (2) the optimal rotation angle of T; (3) the means of T and B and the related standard deviation quotients of all color channels; and (4) the overflow/underflow residuals. These data are coded by binary strings respectively as t1t2…tm, r1r2, m1m2…m48, q1q2…q21, and r1…rk, which together with the binary strings for encoding the values m and k are concatenated into a bit stream M for tile image T. Then, such bit streams of all the tile images are concatenated in order further into a total bit stream Mt for the entire secret image. Moreover, in order to protect Mt from being attacked, we encrypt it with a secret key to obtain an encrypted bit stream Mt′, which finally is embedded into pixel pairs in the mosaic image using the method proposed in [7].

After embedding the bit stream Mt′ into the mosaic image, we can recover the secret image back. But some loss will be incurred in the recovered secret image (i.e,the recovered image is not all identical to the original one). The loss occurs in the color transformation process using Eq. (4) where each pixel's color value ci is multiplied by the standard deviation quotient $q_c = \sigma'_c/\sigma_c$ and the resulting real value ci″ is truncated to be an integer in the range of 0 through 255. However, because each truncated part is smaller than the value of 1 when no overflow or underflow occurs, the recovered value of ci using Eq. (5) is still precise enough. Even when overflows/underflows occur at some pixels in the color transformation process, we record their residual values as described previously and after using Eq. (5) to recover the pixel value ci, we can add the residual values back to the computed pixel values ci to get the original exact pixel data, yielding a nearly-lossless recovered secret image.

VI. MOSAIC IMAGE CREATION AND SECRET IMAGE RECOVERY ALGORITHMS

ALGORITHAM 1: Mosaic Image Generation
Input: a secret image S, a target image T, and a secret key K
Output: a secret-fragment-visible mosaic image F.
Steps:
Step 1: Take the input s are secret image, target image and key.

Step 2: Generate the tile blocks for secret image and target blocks for target image.
Step 3: Calculate the mean and standard deviation for each tile block and target block.

$$\mu_c = 1/n\sum_{i=1}^{n} ci \quad , \quad \mu'_c = 1/n\sum_{i=1}^{n} ci' \quad \text{..................(1)}$$

$$\sigma_{c}=\sqrt{1/n\sum_{i=1}^{n}(ci-\mu_c)^2} \quad \text{.................................(2)}$$

$$\sigma'_c = \sqrt{1/n\sum_{i=1}^{n}(ci-\mu'_c)^2} \quad \text{.................................(3)}$$

Step 4: Calculate the average standard deviation for each block and sort them.

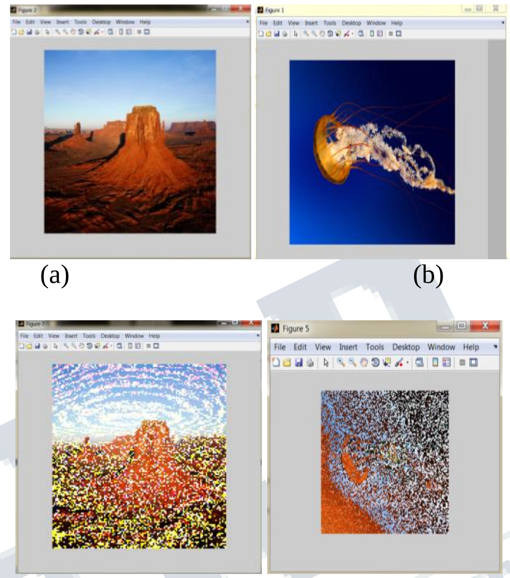
$$ci'' = \frac{\sigma'_c}{\sigma_c}(ci-\mu_c)^2+\mu'_c \quad \text{..................................(4)}$$

Step 5: Sort the tile blocks and target blocks as per sorted average standard deviations respectively.
Step 6: Map sorted tile blocks with the sorted target blocks.
Step 7: Create mosaic image fitting tile box as per the mapped target blocks.
Step 8: Transform the color of all the pixel of each tile image using means and standard deviations.
Step 9: Rotate each transformed tile to 90,180 and 270 degrees and calculate root mean square error.
Step 10: Retain the rotation with minimum RMSE.
Step 11: Convert the mean and standard deviations for each tile block and mapped target block to binary.
Step 12: Convert tile rotation performed into binary.
Step 13: Concatenate the bit stream and compress into data to be embedded into the corresponding tile box of the mosaic image.
Step 14: Will finally get the output of mosaic image.

ALGORITHAM 2: Secret image recovery
Input: a mosaic image F with n tile images and secret key k. **Output**: the secret image S.
Steps: *Step 1*: Extract the bit stream from mosaic image F by performing reverse operation.
Step 2: Decrypt the bit stream by using secret key K.
Step 3: Recover the desired secret image S by rotating the tile images in a reverse direction.
Step 4: Use the extracted mean and standard deviation quotients to recover the original pixel values.
Step 5: Take the results as the final pixel values, resulting in a final tile image.
Step 6: Compose all the final tile images to form the desired secret image S as output

VII. EXPERIMENTAL RESULTS

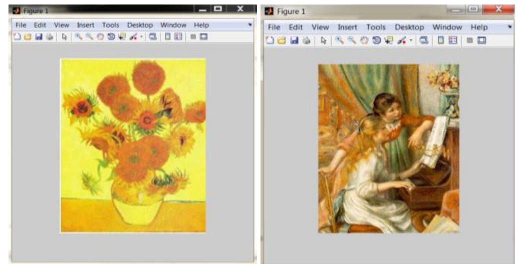
Result is shown in Fig. 4, where 4(c) shows the created mosaic image using Fig. 4(a) of size 1024×1024 as the secret image and Fig. 4(b) of the same size as the target image. The tile image size is 8×8 The recovered secret image using a correct key is shown in Fig. 4(d) which is quite similar to the original secret image shown in Fig. 4(a). It has PSNR = 30.2816 and RMSE = 8.1679 with respect to the secret image.



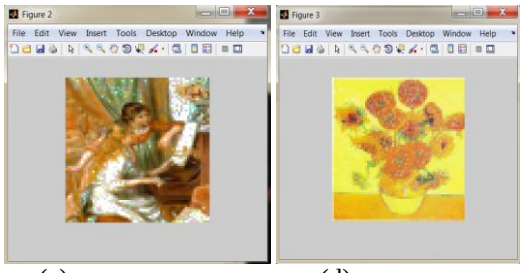
(a) (b) (c) (d)

Fig. 4. Experimental result of mosaic image creation. (a) Secret image. (b) Target image. (c) Mosaic image created with tile image size 8×8. (d) Recovered secret image using a correct key

Result is shown in Fig. 5, where 5(c) shows the created mosaic image using Fig. 5(a) of size 256×256 as the secret image and Fig. 5(b) of the same size as the target image. The tile image size is 4×4 The recovered secret image using a correct key is shown in Fig. 5(d) which is quite similar to the original secret image shown in Fig. 5(a). It has PSNR = 34.7962 and RMSE = 4.6741 with respect to the secret image.



(a) (b)



(c) (d)

Fig. 5. Experimental result of mosaic image creation. (a) Secret image. (b) Target image. (c) Mosaic image created with tile image size 4x4. (d) Recovered secret image using a correct key

VIII. CONCLUSION

A new secure image transmission technique creates a meaningful mosaic image and can also transform the secret image into a secret-fragment-visible mosaic image of the same size and has the same visual appearance as the target image which is preselected from the database. With this technique user can select his/her favourite image to be used as a target image without the need of large database. Also the original secret image can be recovered nearly losslessly from the created mosaic image.

ACKNOWLEDGMENT

I would like to thank my project guide Ms. Sabna I and Head of the Department Ms. Nishida for their guidance and support and also grateful to all the staff members of the Department of Electronics and Communication Engineering of KMCT College of Engineering and Technology, Calicut for their support and for providing all the important facilities like internet access and books, which were essential to carry out the survey. Last but not the least, I would like to thank my family and friends for their whole hearted support and co operation .

REFERENCES

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

[2] Reversible Data Hiding in Images by Reserving Room Before Encryption, Kede Ma, Weiming Zhang Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li. IEEE Transactions on Information Forensics and Security, vol. 8, no. 3, march 2013.

[3] Fast estimation of optimal marked-signal distribution for reversible data hiding, X. Hu, W. Zhang, X. Hu, N. Yu, X. Zhao, and F. Li. IEEE Transactions on Information Forensics and Security, vol. 8,no. 5, pp. 187–193, May 2013.

[4] A probabilistic image jigsaw puzzle solver, T. S. Cho, S. Avidan, and W. T. Freeman, in Proc. IEEE CVPR, 2010.