Covert Communication using Mosaic Images

[1]PAVITHRA B.U, [2]DINESHA.P, [3]ARPITHA SHANKAR S.I

Department of Electronics & Communication,
[1,2]Dayananda Sagar College of Engineering, Bengaluru, India-560078
[3]Department of Telecommunication, GSSS institute of Engineering & Technology for Women, Mysore, India-570016

***Abstract*— Information security is turning out to be progressively essential 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. Several steganography techniques for transmitting information without raising suspicion are found in Literature. However, secret-fragment-visible mosaic images permit the user to securely transmit an image under the cover of another image of same size. This effectively accomplishes an embedding capacity of eight bit per pixel. In recent years, data hiding has been proposed as a likely technique for the motive of information privacy, authentication, fingerprint, protection, data mining, and copyright protection and etc. In this paper, a technique for secure image transmission is done by transforming a secret image into mosaic fragment visible images with the size almost the same and similar to the target image. Since the target image is selected randomly, Mosaic image should look similar to the target image, which will be used to hide the secret image. In this proposed paper, secret fragment visible mosaic image method is used, which is automatically created by composing small fragments of a given image and the target image, in order to achieve effect of embedding the given image visibly but secretly in the resulting mosaic image. For the resulting mosaic image, reversible color transmission is performed in order to reduce the distortion and also to recover the secret image exactly from the cover/input image. Good experimental results illustrate the feasibility and effectiveness of the proposed method.**

***Keywords*- Mosaic image, secret fragment visible mosaic image, reversible color transformation.**

I. INTRODUCTION

Images are very often used and are transferred through web, in such cases the security of the transmitted data through internet is quite important, and these transmitted images may comprise some personal and also some un-sharable documents. So it is essential to hide the data from the unauthorized users to avoid spillage of the data and hackers at the time of transmission process. In order to achieve this many data secure algorithms and methodologies have been presented which makes sure that the information being transmitted through internet is secure. In this massive changing network era, the data security for information transfer becomes very much necessary. In this prospective the sensitive data transformation along with security issue becomes very effective topic but for mass communication, the data which is being transformed from one media to another media should be secure enough for further process. In order to achieve this secure image transmission has to be adopted. Since there are several researches carried out on this topic by using the image processing technique at the most, and according to those researches, the methodology with the mosaic image formation for the secure data transmission process has been proposed in this paper.

In modern networking era, information security has become massive important and also many proposed methods have admitted the same regarding information security. Secure image transmission has the capacity for being adopted into mass communication of very sensitive data under the scrutiny of an adverse censoring authority. There are several steganography techniques that can be seen in the literature survey for information transmission without raising suspicion. So the method proposed here is that image which is formed from the secret image fragments i.e. mosaic image which permits the user to securely transmit an image under the security cover of another image of same size and properties. Way we using the architecture will provide us the very effective embedding capacity of eight bit per each pixel. For information privacy, data hiding, authentication, finger prints, there are several methodologies that are already deployed similar to the security issue during the data transmission using mosaic image.

The secret image which forms the fragmented mosaic image is a different variety of combination image. It consists of which includes tiny blocks which are created from the fragmentation is taught here. Staring at such a sort of mosaic photo, user may view entire segments of secret image, but segments will be so small in measurement and so random in function that user will not be able to work out what secret picture appears like. Hence, secret image could also be stated to be confidentially embedded in ensuing mosaic image, though segment portions are all seen to user. This is the basis why ensuing mosaic image is given another name as secret-fragment-image. This is an effect of haphazard reconstruction of image segments of secret photograph in cover of an extra image known as goal photo, growing precisely an impact of steganography, concern of securing a tremendous quantity of photo information at the back of a target image is resolved robotically by means of this form of mosaic image. Good experimental results demonstrate the feasibility and effectiveness of the proposed method.

II. RELATED WORK

Shilpa Gupta et al [1] has proposed a method for data transfer through internet with the help of mosaic image in a rapid development model and methods, by using this proposed method it is very much easy to transfer a data from one media

to another media without the hesitation of loosing data while transmission. In this methodology they make use of new algorithm for the steganography named as "Enhanced LSB Algorithm", when this algorithm is compared with the Least Significant Bit Algorithm it is having least distortion level in an methodology.

G. Di Blasi et al [2] has proposed a method for transforming raster input images into good quality mosaics, as there are many methods have been already proposed in the field of image processing and also it is very much massively spreading in computer graphic fields. It is in very different way of approaching the security of an data transmitting through internet because now a days it is very much important to secret the data which the end users willing to hide from unauthorized persons. This paper comprises of visual quality concepts and also computational complexity. By using effective method on the image processing it is necessary to identify the boundaries in a considered image and also generated mosaic image.

S. Battiato et.al [3] has proposed a method for transforming raster input images into good quality mosaics, as there are many methods have been already proposed in the field of image processing and also it is very much massively spreading in computer graphic fields. It is in very different way of approaching the security of an data transmitting through internet because now a days it is very much important to secret the data which the end users willing to hide from unauthorized persons. This paper comprises of visual quality concepts and also computational complexity.

Nitin kumar Agarwal et.al [4] has proposed an algorithm for the mosaic photography in a steganography in which the snapshots of the mosaic images are considered as the input image for getting the effective proper output with different styles of mosaic images. Mosaic image is obtained by the generation of the tiles in considered images which can form the mosaic image which contains the parameter which makes the input image perfect. This proposes of hiding secret image by using mosaic image can be very much useful in large number of data hiding and also it is very much useful in color transmission of an image from which we can hide the data without any authentication problem. The authors describe the effective way of utilizing the adapted methodology for hiding data and new photography method by using mosaic image.

Vathelil Subair et al. [5] has proposed 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.

III. PROPOSED SYSTEM

Figure1 represents the proposed architecture. In this section the method for the creation of secret fragment visible mosaic image is given; the detailed system architecture of creating mosaic image is shown in figure 1(a). Firstly user has to select the secret image and any random image of their choice as target image, in order to avoid suspicion it is advised to select target image of same field or background as that of secret image. Next, resize the secret and target image by apply pre-processing to both the secret and target image in order to check whether target and secret image is of same size.

The next step is to divide the source image into small pieces known as tiles. For creating secret fragment visible mosaic image by proposed algorithm there is requirement that the number of blocks of target image should be same in size and number to that of secret image. So we divide both the target image and secret image by using same splitting technique. The main problem in the splitting technique is how to choose a appropriate divided blocks of target image for each of the tile of secret image, in order to make it easy will calculate the mean of standard deviation of the pixels of the block as a similarity measure value to select most appropriate block B for each of the tiles T of secret image.

Next, in order to create the mosaic image, sorted sequence of standard deviation is used to form the resultant image. That is we fit the first tile in sequence Stile into the first block in sequence Starget, and accordingly fit the second tile in Stile to second block in Starget and process continues. In this way will keeps on fitting each of the tile T of secret image to form resultant mosaic image. It will look somewhat similar to the selected target image. Thus, noise free mosaic image is obtained, which is used to recover the secret image.

Figure 1(b) represents the proposed architecture for recovery of secret image. As the color characteristics of target image and secret image are different from one another it may happen that the resultant mosaic image may contain some distortion due to its color differentiations. So to reduce this distortion, reversible color transformation is proposed so that the resultant mosaic image should look identical to that of target image. After transforming color characteristics of target and secret image, in order to enable better fitting of tile block to that of target block , we have to rotate resulting mosaic image with minimum RMSE i.e. (root mean square error) value with respect to target image. Finally, we can recover the secret image in better efficient way.

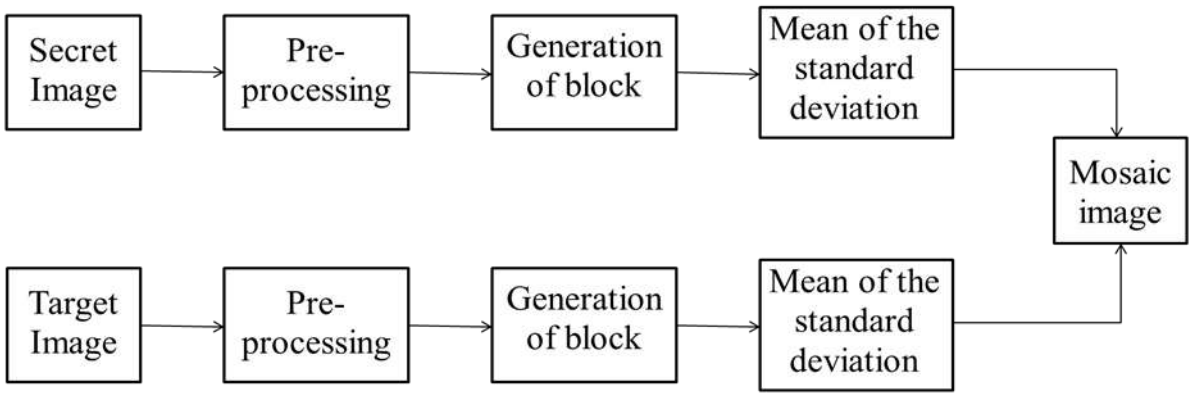


Figure 1(a): Block diagram of proposed architecture for creating Mosaic image

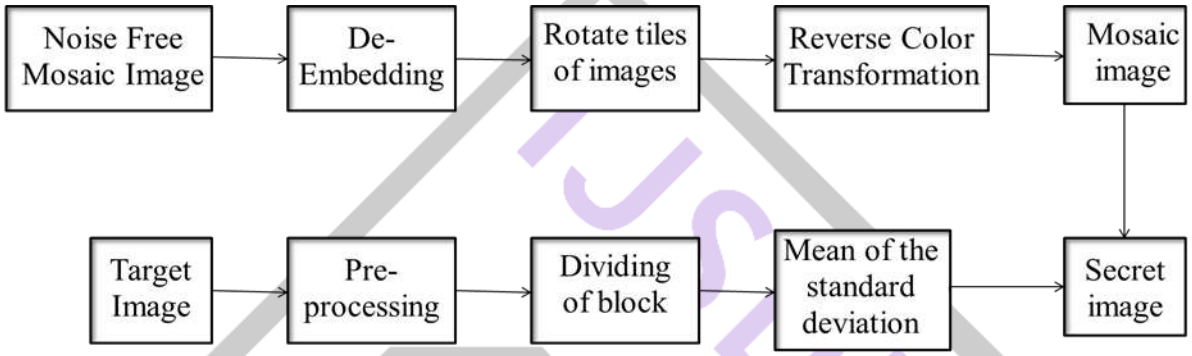


Figure 1(b): Block diagram of proposed architecture for recovery of secret image

Figure 1: Block diagram of proposed work

A. *Creation of Mosaic Image*

Pre-processed secret and target image is divided into small pieces called tiles. This steps plays very important role in our proposed methodology, because the secret image which we are going for hiding will be in normal form, so that it is very much easy to identify by the end user in order to overcome this disadvantage we are adapting the method which is creating mosaic image for both the target and secret image, due to un related blocks at unrelated place it is very difficult to identify the secret image from the mosaic image, this process will achieve high level data security. As we have to divide both considered image into same blocks we are going for same splitting techniques for both target and secret image. The main challenge in the splitting technique is for each of the tile of secret image selection a appropriate divided blocks of target image, in order to make this challenge in easy way we are going for calculating the mean of standard deviation of each of pixels in an image also will go for selecting the blocks B for the next levels from the secret and target image. As the final stage of first phase of methodology will go for generating mosaic image by considering the tiles created from the considered images, in order for better fitting of frames will make use of rotating tile according to the size and dimension by applying sequence of rotation of tiles, So that it will appear as similar to selected target image, thus will get the noise free mosaic image, which can be used to recover the secret image. From the resultant image we are making use of the properties in order to create the efficient mosaic image for data hiding by deploying standard deviation sorted sequence method. As the generated tile has to be fit in an frame in order to form mosaic image, in this way first tile is fitted as straget in the first block and similarly fit tile which is at second place is fitted in Stile to second block in Starget the explained procedure will continue until we get all the tiles fitted in an frame to create mosaic image in very efficient manner.

B. *Reverse Color Transformation*

Reverse color transformation is applied to remove extra noise and distortion present in an considered target and secret image, since both of the considered images might be having the different color characterizations and also a different size, this may cause lots of difference in generation of mosaic image and also in creation of mosaic image, so in order to avoid these problem with the color characters the method to be selected is reversible color transmission which can convert and make both the image into similar color characteristics. In this method we are adopting this reverse color transmission to improve the accuracy of hiding the secret image which is generated in mosaic image and advantage of this method is both the target

and secret image appears same for the end users, from this authentication problem is cleared.

For color transformation, let us consider T and B as two pixel sets described by $\{P_1, P_2, P_3 \dots \dots \dots P_n\}$ and $\{P_1, P_2, P_3 \dots \dots \dots P_n\}$ respectively, where T is used to represent secret image block and B is used to represent target image block. Let us further consider that each pixel P_i is represented by color (r_i, g_i, b_i) and each pixel P_i' is represented by color (r_i, g_i, b_i). Next we have to compute mean and standard deviation of T and B respectively by using formula given below.

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} C_i \quad ,\mu'_c = \frac{1}{n}\sum_{i=1}^{n} C'_i \tag{1}$$

$$\sigma_c = \sqrt{\left(\frac{1}{n}\sum_{i=1}^{n}(C_i - \mu_c)^2\right)}$$

$$\sigma'_c = \sqrt{\left(\frac{1}{n}\sum_{i=1}^{n}(C'_i - \mu'_c)^2\right)} \tag{2}$$

Where in this equations $C_i$and C'_idenotes C channel values of each pixel $P_i$and P'_i respectively, with c= r, g, or b and C= R, G, or B. In next step we have to compute new color (r''_i, g''_i, b''_i) for each P_i in T by using formula given below

$$C''_i = q_c\,(C_i - \mu_c) + \mu'_c \tag{3}$$

Where qc is the standard deviation coefficient calculated by using$\left(q_c = \frac{\sigma'_c}{\sigma_c}\right)$ and c = r, g, or b. Now to compute original color value that is (r_i, g_i, b_i) of P_i we have to use inverse of (3) which is given by

$$C_i = \left(\frac{1}{q_c}\right)(C'_i - \mu'_c) + \mu_c \tag{4}$$

After performing color transformation by using formula given in above section it may be possible that new tile T' obtained after color transformation contain some pixels that might have overflow/underflow values. We have to deal this overflow/underflow values for that we have to convert all the pixel values above than 255 to 255 and pixel values less than zero to zero. To recover the color of original tile block T we have to record residual value that is the difference between original pixel values and converted one and record them as well.

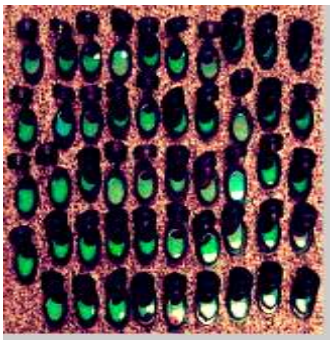
C. Rotating Blocks to Allow it to Fit Better

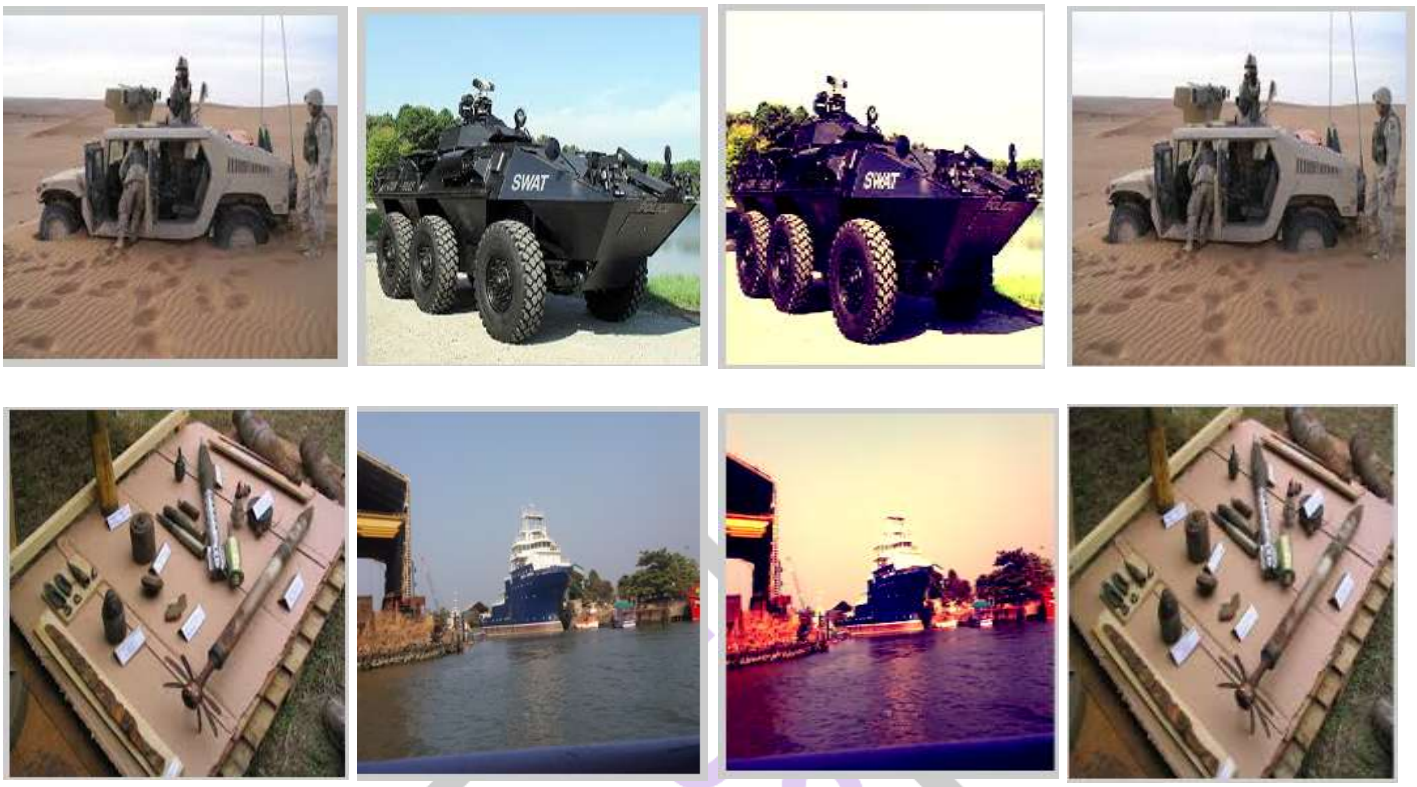
As the target and secret image color characteristics are slightly different from one another, color transmission process is applied on the considered images since they might have contained some sort of noise and distortion in them because of color differentiations properties of images. Once we done with the color transformation of the generated mosaic image of the considered secret image by using the equation explained above, it might be occur in some cases color characteristic of secret image blocks created from secret image and the tile created from the target mage are considered for better experimental results of further process, which may help in better fitting of tiles in an mosaic images. In order to do this, there is a lot of scope for rotating tiles in many directions i.e. 0°, 90°, 180°, 270° and then compute the RMSE values Rotate tile with the smallest calculated RMSE values.

IV. EXPERIMENTAL RESULTS

Below figures show the experimental results of our proposed work. Fig.2 (a) indicates the secret image, fig.2 (b) represent the cover image both considered as input mages, after pre-processing, generation of blocks and calculation of standard mean values the resulting image is shown in fig(c) is the mosaic image shown in fig.2 (d) represent the extracted secret image by using reverse color transformation. So from proposed algorithm most accurate results are obtained and we have achieved the best PSNR value as 2971.90 when compared with other conventional methods.





(a) Secret Image (b) Cover Image (c) Mosaic Image (d) Extracted Secret Image

Figure 2: Results of proposed Work

V. CONCLUSION

The very effective methodology for the secure data transmission of the secret image by the creation of mosaic image has been proposed in this project. This methodology allows the customers to opt the input image of their selection for the generation of mosaic image and also end users can select the target image also for the next process to be carried out and also to generate the mosaic image. The generated mosaic image is used to hide the important data which is meant for transmission without any authentication issues. The application of reverse color transmission made the system to be in very effective way in color transformation. In order to achieve best results we used rotating tiles to fit it into the generated mosaic image frame. The fashioned secret snapshot will also be recovered almost lossless from the created Mosaic graphics.

REFERENCES

[1] Shilpa.Guptal, “Mosaic Image Creation in Videos for Secure Image Transmission”,Vol. 4, Issue 3, 2015.

[2] G.Di Blasi “Image Steganography via Secret Visible Mosaic Image”, EngineeringVol.3, Issue 3, pp. 2320-9798, 2011.

[3] S.Battiato, “A Fast and Secure Transmission of Image by using Mosaic”. Aleja.Hansuer, “Mosaic Image Creation in Videos for Secure Image Transmission”, Vol. 4, Issue 3, 2015.

[4] Nitin kumar, Neeraj Panday, ”A Survey Report on Visual Cryptography and Secret Fragment Visible Mosaic Images”, Vol 3, Issue 10, 2014.

[5] Shabana Vathelil Subair1, Timna P Elizabeth, “Secret Fragment Mosaic Images: A Secure Method for Image Transmission”, International Journal of Science and Research (IJSR).

[6] K.Naga Jyothi and J.S.S.Rama Raju, “An Algorithm Based on Secret-Fragment-Visible Mosaic Images for Secure Image Transmission using Pixel Color Transformations”, International Journal of Professional Engineering Studies, Vol. 3, Issue 3, 2015.

[7] Deepak.A.B.C, P.S.Shilpashree, “An Authentication System For An Image Secret Mosaic Imaging And Lsb Substitution”, IJEEE, Vol. 07, Issue 01, 2015.

[8] I. 1. Lai and W. H. Tsai, “Secret-fragment-visible mosaic image -A new computer art and its application to information hiding” IEEE Trans. vol. 6, no. 3, pp. 936-945, 2011.

[9] S. Gupta, G. Guj ral and N. Aggrawal, "Enhanced Least Significant Bit algorithm For Image Steganography," IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4,pp. 40-42, July 2012.

[10] S.Pragatheeswari, Maram Reddy Srija, Mannuru Tejaswini and M.S.Vinmathi M, “Mosaic Image Creation in Videos for Secure Image Transmission”, IEEE Trans, Vol. 4, Issue 3, 2015.