ISSN: 2321-8169
3595 - 3598

Secure Image Transmission with Secret Fragment Visible Mosaic Images

Miss. Nayan A. Ardak[1], Prof. Nitin A. Shelke[2],
[1] M.E. final year CSE, GHRCEM,
Amravati, India
nayan.ardak@gmail.com
[2]Dept. of comp. science and Engg. Asst. Professor of GHRCEM,
Amravati, India

Abstract: Mosaic means picture or decorative design made by setting small colour pieces, also mosaic is a composite picture made of overlapping images, photos etc. Reshuffle of the fragments of a one image in another image form a new image called mosaic image. To create a mosaic image, secret image is first divided into rectangular shaped fragments, called tile images, which are fitted into a target image called secret fragment visible mosaic image of same size. The mosaic image looks similar to preselected target image, is yield by dividing input image into fragments and transforming their colour into another colour. Greedy heuristic algorithm is proposed to find a related tile image of the secret image to fit into each block in the target image. The information related to the recovery of image is embedding inside target block with the help of lossless substitution scheme. The proposed method, designed for dealing with mosaic images which are useful for hiding secret images. To enhance the security of embed data proposed system also work.

Keywords- *Colour transformation, image encryption, mosaic image, secures image transmission.*

*****

1. INTRODUCTION

Today 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 such as image encryption and data hiding. Image encryption is a technique that uses to encrypt image into noise form, using high redundancy and strong spatial correlation. The encrypted image is a meaningless file and before encryption additional information is not provided. Data hiding is alternative for image encryption that hide secret image into a cover image so that no one can realize the existence of the secret data. Large number of data is not hide into a single is the main issue of data hiding. Specifically, if one wants to hide a secret image into a cover image with the same size, the secret image must be highly compressed in advance. A new technique for secret image transmission is proposed with the help of secret image and target image.

Select three images secret image, target image, and mosaic image. After selecting the target image, the given secret image is first divided into number of rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks, according to a comparison of colour transformation. Next, the color characteristic of each tile image is transformed into the other colour, resulting in a mosaic image which looks like the target image. Appropriate schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image [1].

2. PROPOSED METHOD

In the mosaic image creation firstly select the one secret image and target image both having same size, secrete image is divided into number of fragments called the tiles of images. Then target image it again divided into same number of tiles as that of secrete image then apply the colour transformation on it the fit that tiles of secret image into target block and form a mosaic image.

2.1 Mosaic Image Creation

In this module after creating the mosaic image, upload the mosaic image on web page for secure transmission with the key then receiver get this mosaic image and key. Key on receiver side is in encrypted form by using private key receiver decrypt this key, download the mosaic image and recover the secret image with the help of decrypted key.

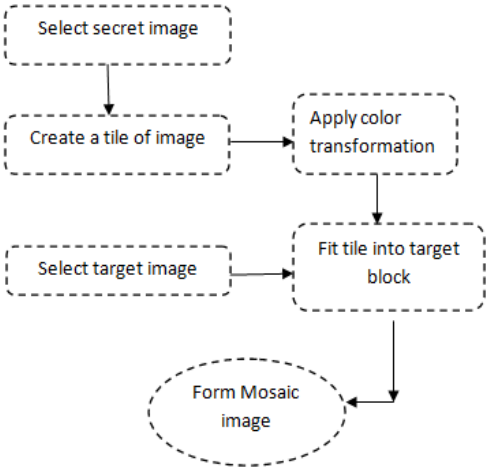

Figure 2.1 Mosaic Image creation

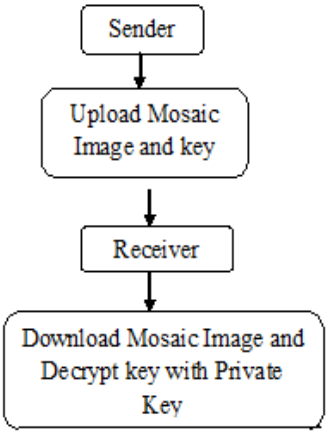

Figure 2.2 Transmission of image

 ISSN: 2321-8169
3595 - 3598

Above figure 2.2 shows transmission of mosaic image, for recovery of secret image sender uploads mosaic image and key on web. In receiver side key is in encrypted format using MD 5, receiver decrypt the key with the help private key. MD 5 is used for hash key generation.

2.2 Recovery of Image

In the recovery of secret image module firstly take mosaic image then extract embedded information from it and recover the information and secret image. The module includes two stages:

- Extracting the embedded information for secret image recovery from the mosaic image.
- Recovering the secret image using the extracted information.

Recover one by one in a raster-scan order the tile images Ti, i = 1 through n, of the desired secret image S by the following steps:

1) Rotate in the reverse direction the block indexed by ji, namely Bji, in F through the optimal angle θ° and fit the resulting block content into Ti to form an initial tile image Ti
2) Use the extracted means and related standard deviation quotients to recover the original pixel values in Ti.
3) Use the extracted means, standard deviation quotients, and to compute the two parameters cS and cL.
4) Scan Ti to find out pixels with values 255 or 0 which indicate that overflows or underflows respectively have occurred there.

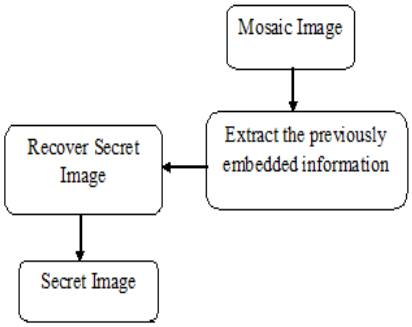

Figure 2.3 Recovery of secret image

5) Add respectively the values cS or cL to the corresponding residual values of the found pixels.
6) Take the results as the final pixel values, resulting in a final tile image Ti.

In recovery of secret image first select the mosaic image from its saved location then enter the decrypted key and click on get original button to get the recovered image with smallest rmse value than original one in the second phase, the embedded information is extracted to recover nearly losslessly the secret image from the generated mosaic image.

3. PERFORMANCE ANALYSIS

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.

The Root Mean Square Error (RMSE) (also called the root mean square deviation, RMSD) is a used to measure the error between recover image and original image. These calculated difference is also called residuals, and the RMSE serves to aggregate them into a single measure of predictive power. The RMSE of a model prediction with respect to the estimated variable Xmodel is defined as the square root of the mean squared error:

$$\text{RMSE} = \sqrt{\sum_{i=1}^{n} \frac{1}{n} (\text{Xobs} - \text{Xmodel})^2}$$

Table 3.1 Time for embedding and recovery of secret image

Input Images	Time to fit the tiles of secret image into target image (ms)	Time to recover the secret image from mosaic image (ms)
Koala	191.25	56.02
Desert	201.84	102.02
Lighthouse	243.23	142.26
Jellyfish	205.23	126.09
Flower	186.25	146.23

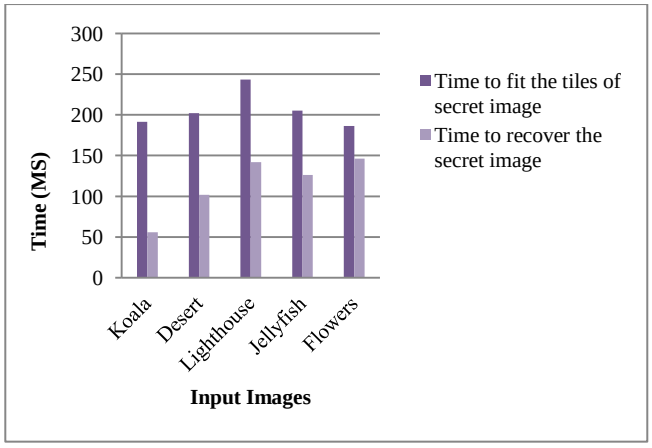

Figure 3.1 Time for embedding and recovery of secret image

Above 3.1 shows time for embedding tile and time for recovery of the secret image from the mosaic images using sample images. Both calculated time are in MS.

ISSN: 2321-8169
3595 - 3598

Table 3.2 Time for colour transformation

Input Images	Time for colour transformation(millisecond)
Desert	1903.2
Lighthouse	1196.8
Flowers	2028.01
Jellyfish	1887.6
Image (1)	1998.06
Koala	1965.6
Image (2)	1526.23
Penguins	1823.03

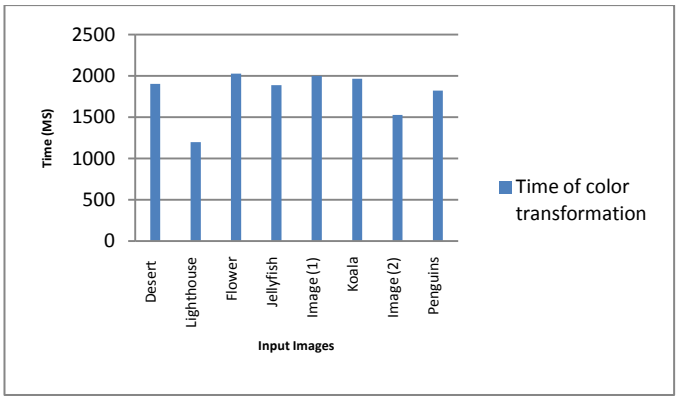

Figure 3.2 Time for colour transformation

Above 3.2 shows time for embedding and time recovery of secrete image for above sample images, dark colour column for time of fit the tiles of secret image light colour column is for time of recovery of secret image.

Table 3.3 RMSE value of recovery of secret image

Input images	RMSE value of existing system for recovery [9]	RMSE value of proposed system for recovery
Image (1)	0.94	0.936
Image (2)	1	0.98
Image (3)	1.2	0.995
Image (4)	1.5	1.1
Image (5)	2.1	1.8

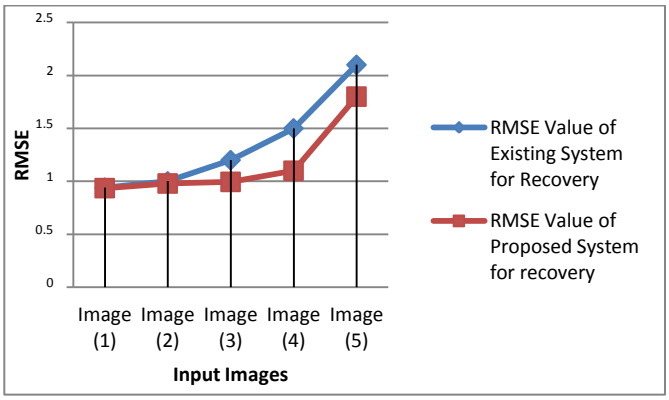

Figure 3.3 RMSE value of recovery of secret image

In the above table and figure 3.3 calculate the RMSE value for recovery of secret image for taking the value of existing system and the proposed system, from the five different images of same size.

Table 3.4 RMSE value of mosaic image

Name of image	Image(3)	Lighthouse	Images(4)	Koala
Penguins	77	55	63	87
Rocks	68	43	59	76
Hydrangeas	63	68	63	73
Images(6)	65	57	69	71

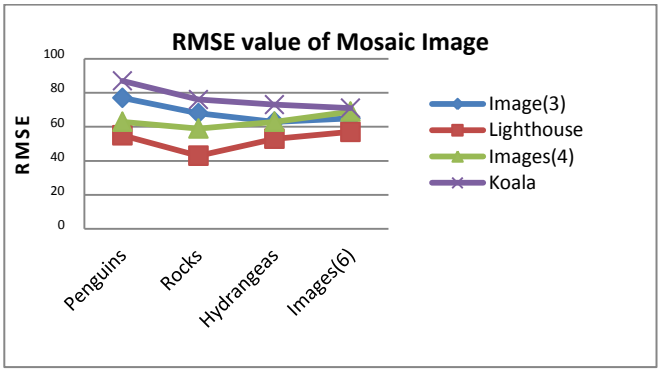

Figure 3.4 RMSE value of mosaic image

Following table is for calculating the RMSE value of the mosaic image for one secret image with number of target images show in table 7.4 and figure 7.6

4. Conclusions

In this proposed work tile image fitting information for secret image recovery is embedded into randomly selected tile images in the resulting mosaic image controlled by a secret key. An additional security enhancement measure was also use, with the help of key additional security is provided to the system. This

proposed system is better than existing system because additional security is provide in proposed system and freely choose the secret image and target image.

REFERENCES

[1] J. Kim and F. Pellacini, "Jigsaw image mosaics," Proc. of 2002 Int'l Conf. on Computer Graphics & Interactive Techniques (SIGGRAPH 02), San Antonio, USA, July 2002, pp. 657-664.

[2] Y. Dobashi, T. Haga, H. Johan and T. Nishita, "A method for creating mosaic image using voronoi diagrams," Proc. of 2002 European Association for Computer Graphics (Eurographics 02), Saarbrucken, Germany, Sept. 2002, pp. 341-348.

[3] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, Vol. 13, No. 8, Aug. 2003, pp. 890–896.

[4] Ming-Shing Su, Wen-Liang Hwang, and Kuo-Young Cheng "Analysis on Multi resolution Mosaic Images" *IEEE transactions on image processing*, Vol. 13, No. 7, July 2004, pp. 952-959.

[5] Lukac and Plataniotis "digital image indexing using secret sharing schemes: a unified framework for single-sensor consumer electronics" *IEEE transactions on consumer electronics*, Vol. 51, No. 3, August 2005, pp. 908-917.

[6] S. Battiato, G. Di Blasi, G.M. Farinella and G. Gallo, "Digital mosaic framework: an overview," Euro graphics – Computer Graphic Forum, Vol. 26, No. 4, Dec. 2007, pp. 794-812.

[7] 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, Sep. 2011, pp. 936–945.

[8] LI Jing "Remote Viewing Image Mosaic based on Fuzzy Cellular Automata Corner Detection in Substation" *International Journal of Security and Its Applications* Vol.7, No.6 (2013), pp.55-66.

[9] Hae-Yeoun Lee "Generation of Photo-Mosaic Images through Block Matching and Color Adjustment" *International Journal of Computer, Information, Systems and Control Engineering* Vol.: 8 No:3, 2014, pp. 426-430.

[10] Ya-lin lee and Tsai *IEEE transactions on circuits and systems for video technology*, Vol. 24, No. 4, April 2014, pp. 695-704.

AUTHOR BIOGRAPH

Miss Nayan A. Ardak has completed her B.E. in computer science and engineering from Sant Gadge Baba University Amravati. She is currently pursuing the M.E. degree at GHRCEM College Amravat.

Prof. N. A. Shelke has completed his M.Tech in Computer Science and Engineering from Government College of Engineering Amravati. He is currently working as an Assistant Professor in GHRCEM Amravati. His area of research includes Image Processing, Artificial Neural Network, Pattern Recognition and Genetic Algorithm.