ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Secret Image Transforming into Meaningful Mosaic Image for Secure Image Transmission

Kirti. R. Joge

M.E Student, Dept. of Electronics & Telecommunication Engg., JCET Yavatmal, Maharashtra, India

ABSTRACT: A new method is proposed for securing image by transforming into secret fragment mosaic image. Now a day, images are transmitted through internet for various purposes. Among these some image can be confidential. So it needs to keep safe from unauthorized receptor, hence security of image is one of the main issues in internet world. In this proposed method ,secure image transmission is achieved by transforming image into mosaic image of same size as that of randomly chose target image. Mosaic image form by combining tile fragments of secret image. A color transformation process is used for securing secret image. A data hiding is used to embedded key in mosaic image for recovery of secret image on receiver side

KEYWORDS: Color transformation, data hiding, secret fragment mosaic image, secure image transmission, target image.

I. INTRODUCTION

Image sharing is one of the most convenientway to share the information. Internet media is most popular for transmitting image from one to other. But in some application fields such as military, private enterprises achieversetc, images usually contain private or confidential information. These information need not to be leak. so the issue of security of secret image is growing all over. Most of techniques are proposed for secure image transmission two of them are most popular: Cryptography and image steganography.

Cryptography is a science for protecting information from unauthorized receptors by changing its form. It provide four services confidential, integrity, non-repudiation, authentication. But it came with some drawbacks such as high availability, delay in time, high cost. Second method is steganography, it is a science of hiding secret image in cover media so that no one can find the secret image. Issues in this method are size and protection[1-6].

The proposed work overcomesthese drawbacks by transferring image into meaningful mosaic image. Obtained mosaic image look similar in shape and size as that of selected target image. The mosaic tile image is outcome of the tile fragment of secret image is concealed in another image called target image which is selected from database. A key is embedded in mosaic image using data hiding technique. Using the same key secret image can be extracted from mosaic image. Hence the authorized key holder himself can get secret image.

II. RELATED WORK

According to the I.J. Lai and W.H.Tsai the secure image transmission can be acquired by creating secret fragment mosaic image which looks similar to target image. It will become an computer art to create this image. But drawbacks of this method is the requirement of large image data base. Secondly, there is restriction on selecting target image. User have to select target image exactly same size of secret image[7].

X. Li, B. Yang &T. Zeng are proposing a novel technique to improve the embedding capacity i.e. reversible watermarking using an adaptive prediction error expansion & pixel selection. This work is an improvement in conventional PEE by adding two new techniques adaptive embedding & pixel selection. Instead of uniform embedding

,they adaptively embed one or two bits into the expandable pixels as per the regional complexity. Drawbacks of this method ,image pixel values affected by the embedded data and Obliterating information within altered pixels in a way that cannot be reversed[8].

III. IMPLEMENTATION

The proposed work is consisting ofvariousstages which are shown in the Fig. 1. There are mainly six stages: Input image, pre-processing, embedded image encryption, and decryption.

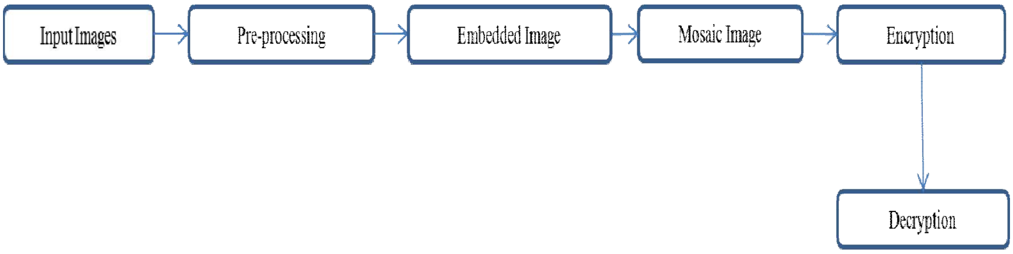


Fig. 1: Block Diagram of proposed work

1. Input Image
In the first stage the secret image is taken as one of the input image. Other image is target image . This image can be any randomly chosen image from database. There is no restriction for selecting target image one can use any image as target image . Fig. 2 shows the target image and secret image

(a) Target Image (b) Secret Image

Fig. 2: Two Input Images

2. Pre-processing
Image can undergo with various process asenhancing, smoothing, filtering, etc. This is important stage as noise is filtered out from images.The pre-processing is a series of operations performed on scanned input image. It essentially enhances the image rendering it suitable for segmentation. The role of pre-processing is to segment the interesting pattern from the background. Generally, noise filtering, smoothing and normalization should be done in this step.

3. Embedded image
The created same size target image use as a camouflage of the secret image. By improving its visibility the secret image can completely marge into target image.

4. Mosaic Image
After Filtering out the secret image is divided into fragments called as tile image and target image is divided in to blocks. These tile image get fixed into target blocks according to their similar color variation. The color characteristic of each tile image is transformed into corresponding target blocks. In this way secret fragment visible mosaic image is obtained which look similar to target image[9]

5. Encryption
In an encryption process, a key is embedded using data hiding technique. This is very important step as it provides security to the confidential image. The secure image transmission is confirmed in this stage. Key can be private key or generated key[10-13].The private key is given by users and the generated key based on that size of the image.

6. Decryption
This process is come on receiver side. The key which was embedded in encryption process is used to decrypt the image. The image can be extracted only if one can use the same key. In this process the security of image is obtained. Hence if someone or unauthorized receiver can able to find created mosaics image then also he will not be able to get the confidential data as he don’t have the correct key.

IV. ALGORITHM

Stage 1: Pre-processing
I. The input to this stage are two images, secret image and target image. Both the images may be of different size, so first change target image size same as secret image.
II. The presence of uneven pixel loss in the image is known as noise. In this process the noise gets filter out. Noise generally comes as red and white dots. By removing noise we get filtered image. Preprocessing stage output is shown in fig. 3

Stage 2: Embedded image
The figure 4 shows that the message is embedded in the image. This stage is important as it provide robustness, perceptibility. It helps in improving the proposed method and to get proper result with less distortion. There are two type of embedding techniques as visible embedding and Invisible embedding. Here, in this proposed work invisible embedding is used. (Note- In fig. 4 visibility of output is increases to understand output of this stage. It is not compulsory.)

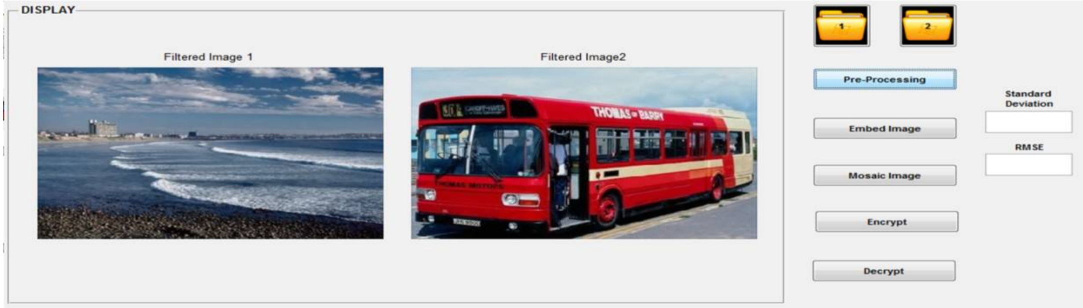


Fig.3: Pre- processing on images

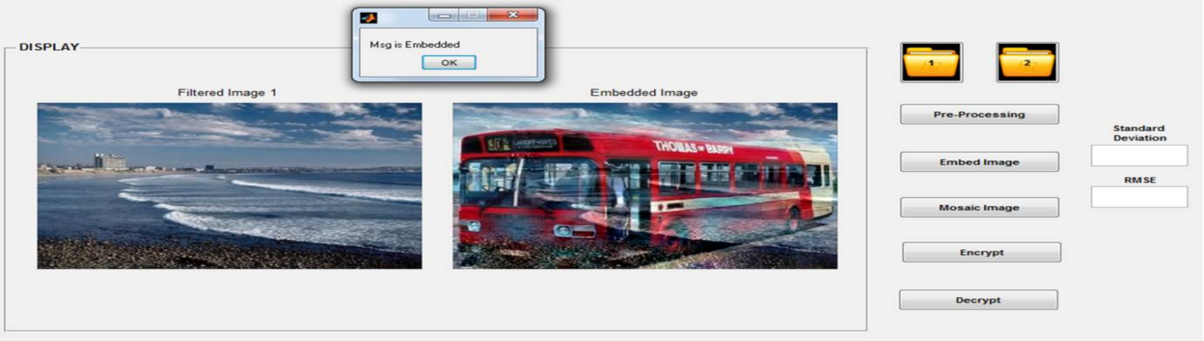

Msg is Embedded

Fig. 4: Output of embedded image process

Stage 2: Creation of mosaic image

I. Divide the secret image into tile images and target image into block images. Shown in fig 5

II. Calculate the standard deviation and RMSE value using formulas

Standard deviation:

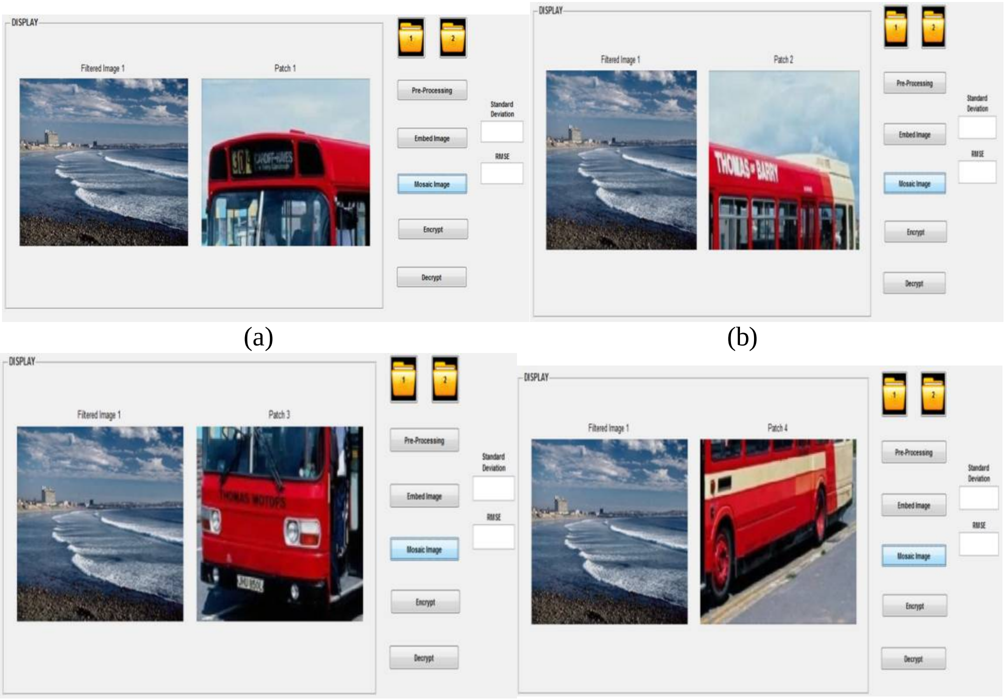
Mean value $\mu = \frac{1}{n}\sum_{i=1}^{n} P_i(1)$

Hence $\sigma^2 = \frac{1}{n}\sum_{i=1}^{n}(P_i - \mu)^2(2)$

Root Mean Square Algorithm:

RMSE $=\sqrt{\frac{\sum_{i=1}^{n}(P_M - P_T)^2}{n}}(3)$

Where,i is the number of tile images. P_M stand for the pixels of created mosaic image and P_T is pixel of target image. Pi is the pixel of formed image.



(a) (b)

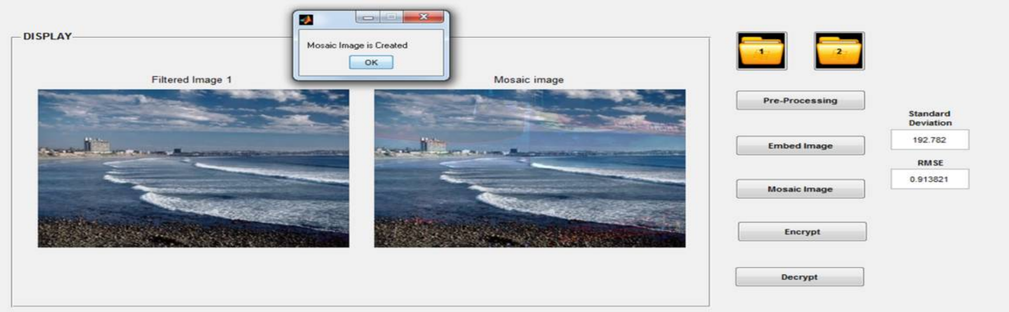
(c) (d)

Fig. 5: Image is divided into four patches

III. Sort the tile image and block image as per the values of standard deviation. Map them in order of sorted block images and record mapping according to indices of tile images.

IV.The RMSE value of transformed tile image is calculated at each directions θ = 0o, 90o, 180o, 270o while fitting into a target block. The tile image gets set at the direction which has smallest RMSE value.

V. Create mosaic image by fitting tile image into corresponding target blocks as per the formed sequence obtained from above steps.



Mosaic Image is Created

Standard Deviation: 192.782

RMSE: 0.913821

Fig. 6: Creation of mosaic image

Stage 3: Encryption

In this step the key is embedded in formed mosaic image. A key is generate key type. It is formed by using Data Hiding. LSB Data hiding technique is use in this proposed work[10-11]. The LSB technique is used for data hiding, achieves both invisibility and reasonably high storage payload. The advantages of LSB based data hiding method is that it is simple to embed the bits of the message directly into the LSB plane of image and many techniques use these methods. The LSB modification does not result in image distortion and thus the resulting secret image will look identical to the cover-image. Fig.7 Shows the encrypted image.

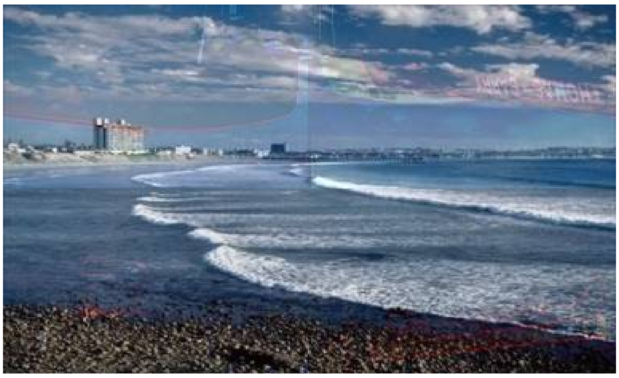


Fig. 7: Encrypted Image

Stage 4: Decryption

By using the same key, secret image is extracted from the encrypted image. In this stage two separated secret image and target image is obtained.

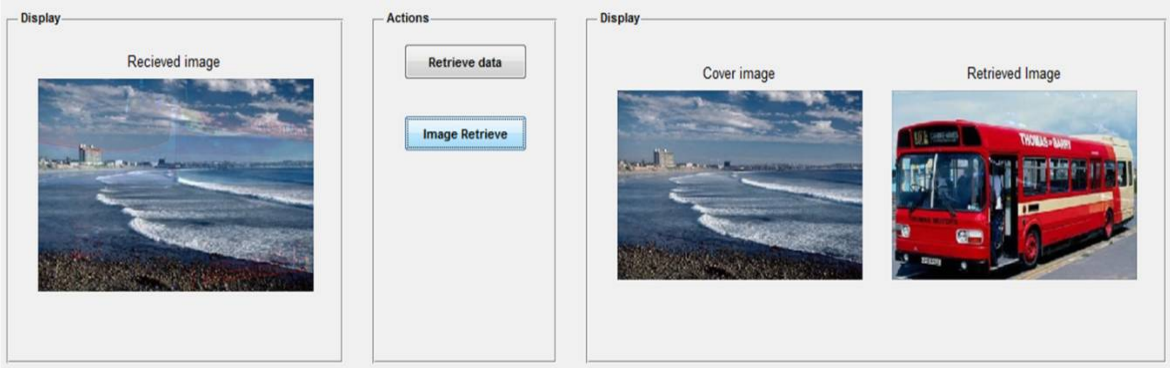
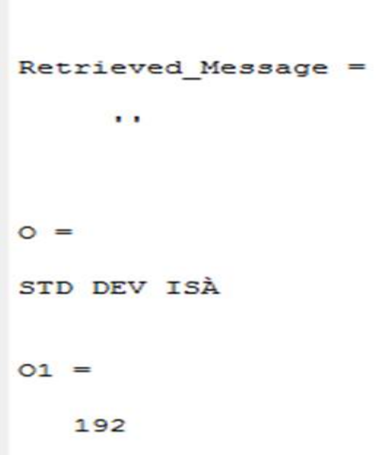


Fig. 8: Decrypted image

V. EXPREMENTAL RESULTS

1. To show that created mosaic image is look similar to preselected target image, RMSE is utilized, which defines the difference between the pixel values of two images. The mosaic image created by small tile image has smaller value of RMSE. The smaller value shows the better result. Here the value of RMSE is 0.19.
2. The key generated according to the size of images. Here it provide key as - " (single double quotation symbol). This key use to retrieve the secret image. Value is obtained during process shown in fig. 9.



```
Retrieved_Message =

      ''



O =

STD DEV ISÀ


O1 =

    192
```

Fig. 9: Generated key and Standard deviation value

VI. CONCLUSION

A secure image transmission method has been proposed. It creates the mosaic image which contain secret image in it. The mosaic image looks similar to selected target image. By the use of proper color transformation secret fragment mosaic image is created with high visibility. And also original secret image can be recovered without any loss. Good experimental result shows the feasibility of this work.

REFERENCES

1.Chang, Chin-Chen, Min-Shian Hwang, and Tung-Shou Chen. "A new encryption algorithm for image cryptosystems." Journal of Systems and Software vol 58, no.2, pp 83-91, 2001
2. R. J. Anderson, F.A.P Petitcolas, "On the limits of steganography" IEEE Journal on Selected Areas in Comm., vol. 16(4), pp 474-481,1998.
3. I. Avciabs, N. Memon and B.Sankur, "Steganalysis using image quality metrics," IEEE Trans. Image Processing, vol. 12, no.2, pp. 221-229, 2003.
4. Neil F. Johson, SushilJajodia,"Exploring steganography: Seeing the unseen," computer,vol. 31, no.2, pp. 26-34, 2003.
5. N. Provos, P. Honeyman,"Hide and seek: an introduction to steganography,"IEEE security and privacy, vol. 1, no. 3 pp. 32-44, 2003.
6.A. D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE signal processing letters, vol. 12, no.6, pp. 441-444, 2005.
7.I.J. Lai, W.H. Tsai, "Secret-fragment mosaic image- A new computer art and its application," IEEE Trans. Inf. Forens. Secure., vol. 6, no.3, pp. 936-945, 2011.
8. X. Li, B. Yang & T. Zeng," Efficient reversible watermarking based on adaptive prediction error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12,pp. 3524-3533, Dec. 2011
9.W. Bender, D Gruhl, n. Morimoto, a. Lu, "Techniques of data hiding," IBM system journal. vol. 35, no.3.4,pp. 313-336, 1996.
10. C.K. Chan, L. M. Cheng, "Hiding data in image by simple LSB substitution," Pattern Recognit.,vol. 37, pp.469-474, 2004.
11. Z. Ni, Y. Q. Shi, N. Ansari, W.su, "Reversible data hiding," IEEE Trans. Circuits System Video Technology, vol. 16, no.3, pp. 354-362, 2006.
12. Anitha Devi M. D, K. B. ShivKumar, "Protection of confidential color image information based on reversible data hiding technique," CoCoNet, pg. 742-747.2015.