IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

New Secure Image Transmission Technique Using Mosaic Image By RCT

Prof. Ulhas V. Patil[1], Miss. Shital R. Khande[2]

Associate Professor & Head, Department of E&TC Engg, PREC, Loni[1]

ME Student, Department of E&TC Engg, PREC, Loni[2]

Abstract: A new secure image transmission technique which changes naturally a given enormous volume secret image into a secret-fragment-visible image is called mosaic image of the exactly similar size. The mosaic image, which looks to be like an discretionarily choose target image and it may be used as a disguise of the secret image, is yielded by separating the secret image in sections and changing their shading attributes to those of the comparing pieces of the target image. Skillful techniques are invented to lead the shading change process so that recovered secret image may be almost losslessly. A scheme for handling overflows/underflows in the converted pixels shading values by recording the shading contrast in the untransformed shading space is proposed in addition. The data needed for improving the secret image is embedded in the created mosaic image by a lossless information concealing plan using a key.

Keywords: mosaic image,image encryption, data hiding , secure image transmission.

I. INTRODUCTION

Currently, images from different sources are frequently used and are transmitted through the web for different applications, such as online personal photograph albums, private enterprise archives, restorative imaging framework, medical imaging system, military picture databases. These images generally contain secure or confidential data so that they ought to be protected from leakages during transmissions. Recently so many techniques have been proposed for secure image transmission, for which two basic techniques are data hiding and image encryption.

Image encryption is a method that makes use of characteristic property of an image, such as strong spatial correlation and high redundancy, to get scrambled image. The scrambled image is a noise image i.e it is a useless document, which can't give extra data before unscrambling and this may stir an assailant's attention during transmission because of its irregularity in structure. An alternative method for secure image transmission is the data hiding that hide secret message in a cover image so that one cannot recognize the presence of the secret image. But the important issue of this method is that if anyone wants to hide secret image in a cover image with the identical size, the secret image must be exceptionally compacted ahead of time. However for many applications, such as transmitting medical images, legal documents, and military images etc. that contains private information, in such cases data compression operations results in a loss of important information.

In this paper, we proposed an approach for secure image transmission, which transmitted secret image into significant mosaic image of the exact same size and which look like a preselected target image. The transformation method is measured by a secret key and with the secret key person can recover the secret image nearly losslessly from the mosaic image. The mosaic image is the result of arrangement of the fragments of a secret image in disguise of another image called the target image which is preselected from the database.

A mosaic image is the process of generating pictures or decorative arrangements. They are created by cementing together insignificant pieces of glass, stone and other hard materials of various colors. Mosaic contains more number of small picture called tile images. Mosaic image can be created by dividing the original image into many tiles and for every tile, find another image with similar content from an image database. Finally we have to build the mosaic image by exchanging all tiles by their similar images.

Firstly the given secret image is divided into rectangular fragments called tile images, then which are fit into exact same blocks in the target image, called as target blocks, according to a homogeneous condition based on color variations. Next, the color characteristic of every tile image is changed in to that of the corresponding target block in the target image, which result in a mosaic image which look like the target image. The proposed method is new so in that a meaningful mosaic image is created, in contrast with the image encryption method that creates meaningless noise images.

Also, this method can transform a secret image in a significant mosaic image without compression, and data hiding method must hide a highly compressed version of the secret image into a cover image when the cover image and the secret image have the same data volume.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

II. RELEATD WORK

1. "A New Secure Image Transmission Technique via Secret-fragment-Visible Mosaic Images by Nearly RCT"
In this paper, Ya-Lin Lee shows a method for the transmission of the secret image securely and lossless. This technique transforms the secret image in a mosaic tile image having the same size like that of the target image which is previously selected from a database. This color transformation is controlled and the secret image is recovered lossless from the mosaic tile image with the help of the extracted applicable information generated for the recovery of the image.[1]

2. "Secret-fragment-visible mosaic image -A new computer art and its application to information hiding", I. J. Lai and Tsai, proposed, a new technique of computer art image is called secret-fragment-visible mosaic image proposed which is created automatically by setting small pieces of a given image in a mosaic form, and then embedding secret image in the resulting mosaic image. This type of data hiding is helpful for covert communication and secure keeping of secret images.

In this paper, database is used to choose the target image. After selection, secret image and target image are preprocessed and splitting into tiles and blocks. Secret image tiles are made to fit into the target blocks and create mosaic image. The drawback of this technique is the use of database for target image selection, that requires extra memory to store mosaic image and mosaic image can be similar to selected target image.[2]

3. C. K. Chan and L. M. Cheng, proposed a "Hiding data in image by simple LSB substitution [3]", it is a method of hiding the secret message in a cover image so that unauthorized person will not realize the presence of hidden message.

This paper shows, 8-bit grayscale images are chosen as cover media and are called cover images. LSB is one of the common data hiding method, which replaces the LSB's of cover image with message bits.

Experimental results show that with extra computation complexity we can get the enhanced image quality.
The drawback here, is when the size of storing message is increased, image quality of the cover image is degraded.

4. Y. Hu, proposed a "Difference expansion based reversible data hiding using two embedding direction [4]", recent difference expansion embedding method performs only one layered embedding in a difference image due to which there will be degradation in the image. So in this paper proposed a new difference expansion embedding algorithm based on Harr wavelet transform, which make use of two embedding directions horizontal and vertical difference image for data hiding which specify the algorithm and makes it flexible to different types of images.

The proposed algorithm does'nt has the original layer embedding capacity limit. It can perform well at different embedding rates.

III. PROPOSED SYSTEM

The proposed method has two main phases shown by the block diagram of Fig.1
1. Mosaic image creation
2. Secret image recovery

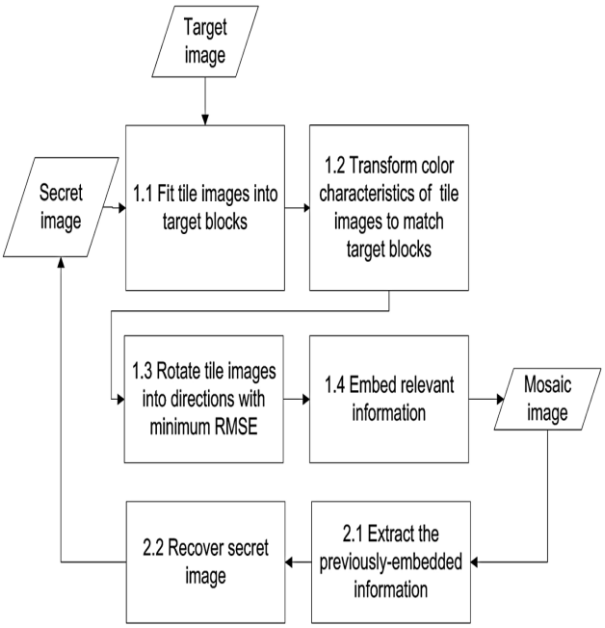

Fig.1 block diagram of proposed system

In the first phase, a mosaic image is gained, which comprises of fragments of input secret image with color corrections as per similarity criterion based on color variations.[1]

The phase have four stages: 1) fitting the tile images of the secret image in the target blocks of a previously selected target image; 2) By changing characteristic of color of every tile image in the secret image to turn that of corresponding target block in the target image; 3) rotating every tile image into a direction with the minimum RMSE value with respect to its corresponding target block; 4) implanting required data into the created mosaic image for future recuperation of the secret image.

In the second phase, the embedded data is extracted to recuperate the secret image nearly losslessly from the created mosaic image. The phase has two stages: 1) extracting the implanted information from the mosaic image for regaining the secret image, and 2) regain the secret image using the extracted information.

Algorithm for Mosaic image creation:
Input: a secret image S, a target image T, and a secret key K.
Output: a secret-fragment-visible mosaic image F.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

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 of target image.
Step 3: Calculate the mean and standard deviation for each tile block and target block.

$$\mu c = 1/n \sum_{i=1}^{n} Ci$$

Where Ci - pixel value of c-channels such as red, green and blue.
n- No of pixels

$$\sigma c = \sqrt{1/n \sum_{i=1}^{n} (Ci' - \mu c')2}$$

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

$$Ci' = q_c(Ci - \mu c) + \mu c'$$

Where - standard deviation quotient
Step 5: Sort the tile blocks and target blocks according to sorted average standard deviations respectively.
Step 6: Map sorted tile blocks with the sorted target blocks. Step 7: Generate mosaic image fitting tile box as per the mapped target blocks.
Step 8: Transform the color of all the pixel of every tile image using means and standard deviations.
Step 9: Rotate each transformed tile to 90,180 and 270 degrees and then calculate root mean square error.
Step 10: Retain the rotation with minimum RMSE.
Step 11: Modify the mean and standard deviations for every tile block and mapped target block to binary.
Step 12: Transform tile rotation performed in 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.

Algorithm for Secret image recovery:
Input: a mosaic image F with secret key k and n tile images.

Output: the secret image S.
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 recuperate the original pixel values.
Step 5: Gain the results as the final pixel values, result into a final tile image.
Step 6: Combine all the final tile images to form the desired secret image S as output.

IV. RESULTS

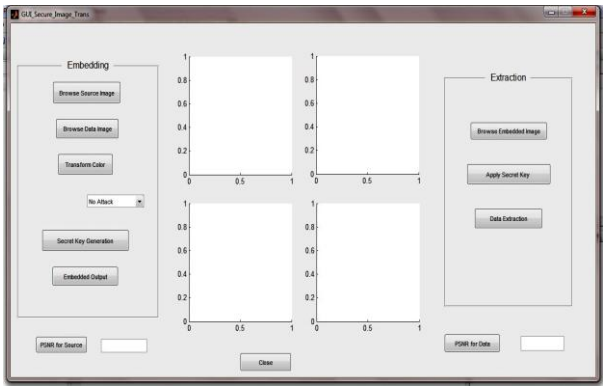

Fig.2 GUI Screen

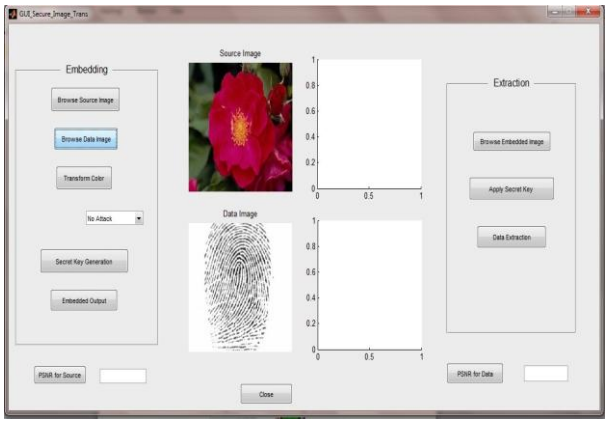

Fig.3 Source and data image selected

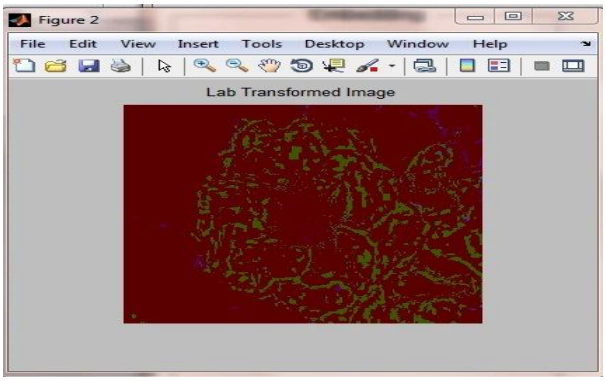

Fig.4 Color transform of source image

Fig.5 Secret key Encryption

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

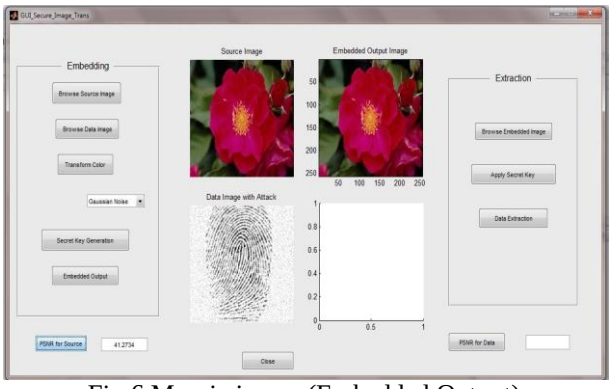

Fig.6 Mosaic image (Embedded Output)

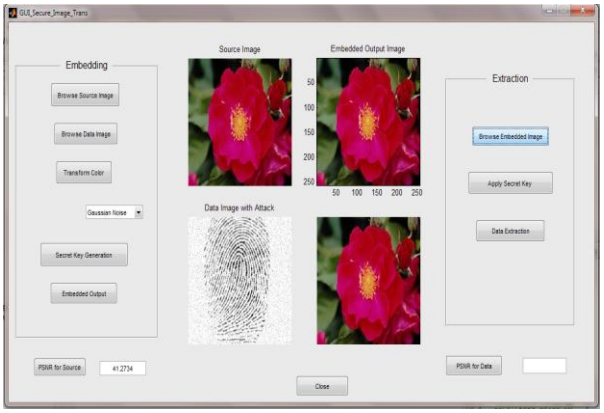

Fig.7 Browse embedded Image

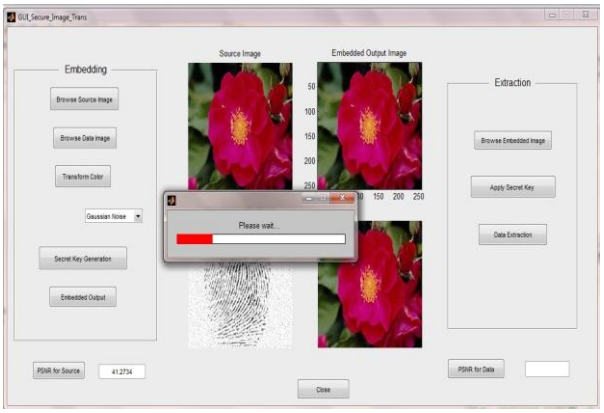

Fig. 8 Data Extraction from embedded image

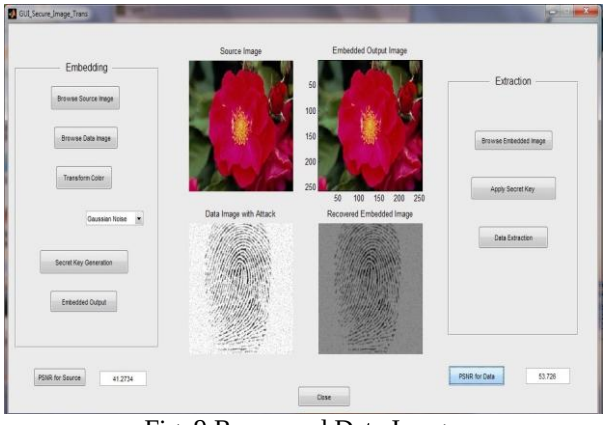

Fig. 9 Recovered Data Image

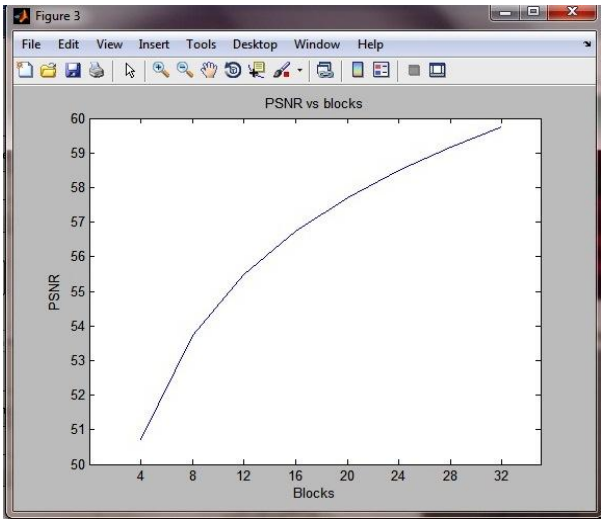

Fig. 10 Graph for PSNR vs Blocks

V. RESULTS AND DISCUSSION

A series of experiments have been conducted to test the proposed method using many secret and target images. To show that the created mosaic image looks like the preselected target image, the quality metric of root mean square error (RMSE) and PSNR (Peak Signal To Noise Ratio) is utilized, which is defined as the square root of the mean square difference between the pixel values of the two images

It can also be seen that the blackness effect is observable when the image is magnified to be large; but if the image is observed as a whole, it still looks like a mosaic image with its appearance similar to the target image

A mosaic image created with smaller tile images has a smaller RMSE value with respect to the target image

VI. CONCLUSION AND FUTURE SCOPE

A new secure image transmission technique creates a meaningful mosaic image and can also transform the secret image in secret-fragment-visible mosaic image of the similar size and has the same visual appearance as the target image which is pre-selected 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.

As this method is only limited to RGB color. So, the future studies may be directed to applying the proposed method to images of the color models other than RGB In the future, the visual quality of the mosaic image could be enhanced further using more parameters of color transformation

REFERENCES

[1] Ya-Lin Lee. "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations", IEEE Trans. on Crts.and Ya-Lin Lee. Sys for Video Tech., vol. 24, no.4, April 2014.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

[2] I. J. Lai, "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] C. K. Chan, "Hiding data in images by simple LSB substitution," Pattern Recognit.., vol. 37, pp. 469–474, Mar. 2004.
[4] Y. Hu, H.-K. Lee, "Difference expansion based reversible data hiding using two embedding directions," IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1500–1512, Dec. 2008.
[5] V. Sachnev, H. J. Kim, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.
[6] X. Li, B. Yang, and 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.
[7] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Trans. Inf. Forens. Secur., vol. 2, no. 3, pp. 321–330, Sep. 2007.
[8] W.-H. Lin, S.-J. Horng, and Y. Pan, "An efficient watermarking method based on significant difference of wavelet coefficient quantization," IEEE Trans. Multimedia, vol. 10, no. 5, pp. 746–757, Aug. 2008.
[9] W. Zhang, X. Hu, "Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. Image Process., vol. 22, no. 7, pp. 2775–2785, Jul. 2013.
[10] C. C. Chang, C. C. Lin, "Reversible hiding in DCT-based compressed images," Inf. Sci., vol. 177, no. 13, pp. 2768–2786, 2007.
[11] X. Hu, W. Zhang, and F. Li, "Fast estimation of optimal marked-signal distribution for reversible data hiding," IEEE Trans. Inf. Forens. Secur., vol. 8, no. 5, pp. 187–193, May 2013.
[12] E. Reinhard, "Color transfer between images," IEEE Comput. Graph. Appl., vol. 21, no. 5, pp. 34–41, Sep.–Oct. 2001.
[13] Shital R. Khande, Ulhas V. Patil "Secure Image Transmission Using Secret Fragment Visible Mosaic Image" International Journal of Informative & Futuristic Research , IJIFR/V3/ E10/ 056,pg. 3867-3875