Image/Video Transmission with Secret Fragment Visible Mosaic Image Technique

Sankara Rao Palla[1], S.Venkata Anand[2]

[1]Asst.professor, [2]Asst.professor,

[12]Dept.of E.C.E,

[1]Raghu Engineering College Visakhapatnam,

[2] S.V.P.Engineering College Visakhapatnam,

Abstract* - The main aim of the paper is to analyze about security in image transfer through the network. Secret-fragment-visible mosaic image is proposed for combining small tiles of secret image to form a target in the sense of mosaic. When this artwork is viewed at close, the observer can view smaller elements, yet when viewed at a distance the collection of tiles blend together to yield the overall picture. When the mosaic generating process starts, original image is divided into many tiles. Before splitting the image, compare the image for mosaic creation. Mosaic image is created automatically by composing small fragments of a given image in to target image, achieving an effect of embedding the given source image secretly in the resulting mosaic image. To create the mosaic image, first find the similar target image for selected source image. Finding the best fit tile for embedding in the target image blocks. The information of placing the tile image fitting sequence in target image is embedding into random selected pixel in created mosaic image. The embedded information act as a text key file. The key file contains the tile image fitting sequence. Without this key receiver can't retrieve the secret image. It is implemented by MATLAB software.

Keywords: Target blocks, Tile images, Image hiding, Mosaic image, Color Transformation, Image encryption, PSNR.

I. INTRODUCTION

Recently, many methods have been used for securing image Transmission. The two common approaches are image encryption and data hiding. Image encryption is a technique that uses the natural property of an image, like high redundancy and strong spatial correlation, to get an encrypted image based on Shannon's confusion as well as diffusion properties.

The encrypted image is a noise image so none can obtain the secret image from it unless he/she has the correct key. However, the encrypted image is a useless file, which can't provide any additional information before decryption and may arouse an attacker's mind during transmission due to the randomness in form. An alternative for this problem is data hiding, which hides a secret message into a cover image due to that no one can think the existence of the secret data, in which the data type of the secret message learnt in this paper, is an image. In this paper, a new technique for secure image transmission 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 lossless from the mosaic image.

The proposed method is inspired by Lai and Tsai [1] 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 [1] 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. 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.

II. PROPOSED WORK

The block diagram of the proposed method is as shown in figure1. In Proposed System Secrete image is preprocessed before caring out mosaic image process, in preprocessing both secretes and target images are resized to a standard image resolution, It will avoid the dimensionality error during the processes. The Images are divided into blocks or tiles; from each block standard deviation is calculated and stored it in a ascending order. Using sorted information first tile of secrete mage is fit to particular first block of Target similarly all the image tiles are fit in Target image and resulting image looks like Selected Target. Then Color Transformation is done to Mosaic Image, image tiles are rotated using RMSE value to get final Mosaic Image. In the above block diagram fig.1 Shows the creating of mosaic image using secrete and target image. Steps involved in generating secret fragment visible Mosaic image are given in this section:

A. Selection of cover and payload images:

In this step user has to select their secret image and any random image of his/her choice as cover image user can select any image as target image of any size in contrast to

Lai and Tsai method that requires cover image should be double in size and should satisfy some similarity, measure criteria to be used s cover image. But in order to avoid to suspicion it is advised that target image is to be selected, which is of some field or of same background as that of secret image.

B. Resize the secret image:

Here in this proposed method to create secret fragment visible Mosaic of the same size as that of cover image, after the payload image and cover image are selected, we have to check whether the cover image and payload image are of same size or not, if they are not of same size then we have to resize the payload image to make it of same size as that of cover image.

C. Divide both the payload and cover images into tiles:

Next step is to split the source image into small pieces called as tiles. In proposed algorithm in order to create the secret fragment visible mosaic image there is requirement that the number of blocks of target image should be same in size. So the cover and payload images are to be split by using splitting technique.

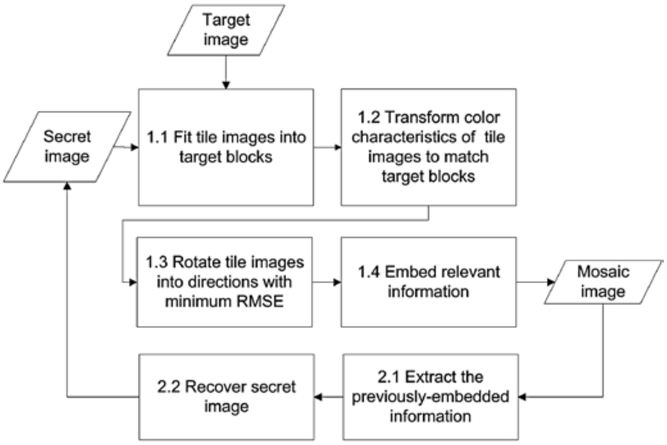

Target image
Secret image
1.1 Fit tile images into target blocks
1.2 Transform color characteristics of tile images to match target blocks
1.3 Rotate tile images into directions with minimum RMSE
1.4 Embed relevant information
Mosaic image
2.2 Recover secret image
2.1 Extract the previously-embedded information

FIGURE1: Block Diagram of the Proposed Method

III.ALGORITHMS OF THE PROPOSED METHOD

Algorithm 1: 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.

Steps:

Stage 1: fitting the tile images into the target blocks.

Stage2: Performing color conversions between the tile images and the target blocks.

Stage 3: Rotating the tile images.

Stage4: Embedding the secret image recovery information.

Algorithm 2: Secret image recovery

Input: A mosaic image F with n tile images {T1, T2… Tn} and the secret key K.

Output: The secret image S.

Steps:

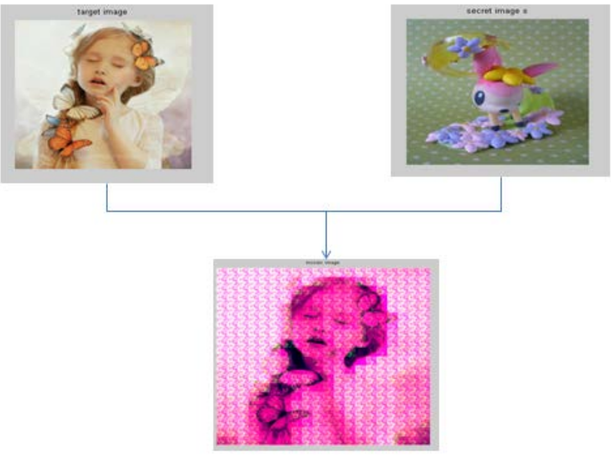
Stage 1: Extracting the secret image recovery information.

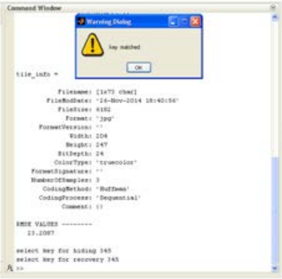
Stage 2: Recovering the secret image

IV. SECURITY CONSIDERATIONS

In order to increase the security of the proposed method, the embedded information for later recovery is encrypted with a secret key as seen in Algorithm 1. Only the receiver who has the key can decode the secret image. However, an eavesdropper who does not have the key may still try all possible permutations of the tile images in the mosaic image to get the secret image back. Fortunately, the number of all possible permutations here is *n*!, and so the probability for him/her to correctly guess the permutation is *p*=1/*n*! which is very small in value. For example, for the typical case in which we divide a secret image of size 1024×768 into tile images with block size 8×8, the value *n* is (1024×768)/(8×8) = 12,288. So the probability to guess the permutation correctly without the key is 1/*n*! = 1/(12,288!). So breaking the system by this way of guessing is computationally infeasible.

V.RESULTS





```
tile_info =

           Filename: [1x73 char]
        FileModDate: '26-Nov-2014 18:40:56'
           FileSize: 6182
             Format: 'jpg'
      FormatVersion: ''
              Width: 204
             Height: 247
           BitDepth: 24
          ColorType: 'truecolor'
    FormatSignature: ''
    NumberOfSamples: 3
       CodingMethod: 'Huffman'
      CodingProcess: 'Sequential'
            Comment: {}

RMSE VALUES --------
   23.2087

select key for hiding 345
select key for recovery 345
>>
```

Recovered image

VI.CONCLUSION

In this generation nothing is secure. A Secure image Steganography technique is proposed, where secret images are embed into an image and encrypted with a key to transmit. Mosaic image is formed with secret tile image and target image for the lossless data hiding and recovery. Experimental results are shown the feasibility of secure transmission of image in the proposed method is good. Future studies may be directed to applying proposed method to video, where video frames are used as target image.

REFERENCES:

[1]. Ya-Lin Lee and Wen-Hsiang Tsai, "**A New Secure Image Transmission Technique via Secret-fragment- Visible Mosaic Images by Nearly Reversible Color Transformations**," IEEE Transactions on Circuits and systems for video Technology, vol. 24, no. 4, April 2014

[2]. 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. Secur, vol. 6, no. 3, pp. 936–945, Sep. 2011.

[3]. Chin chenChang , MinShian Hwang and Tung Shou Chen," **A new image encryption algorithm for image cryptosystems**", the journal of system and software 58(2001).

[4]. W. B. Pennebaker and J. L. Mitchell, "**JPEG: Still Image Data Compression Standard**", New York, NY, USA: Van Nostrand Reinhold, pp. 34–38, 1993.

[5]. Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su," **Reversible Data Hiding**", IEEE transactions on circuits and system for vedio technology, vol. 16, no. 3, march 2006.

[6]. C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "**Reversible hiding in DCT-based compressed images**," Inf. Sci., vol. 177, no. 13, pp. 2768–2786, 2007.

[7]. E. Reinhard, M. Ashikhmin, B. Gooch, and P. Shirley, "**Color transfer between images**," IEEE Comput.Graph. Appl., vol. 21, no. 5, pp. 34–41, Sep.–Oct. 2001.

AUTHOR BIOGRAPH:

Mr.SANKARA RAO PALLA has completed his M.Tech (VLSI system design) in AITAM college of Engineering, srikakulam. He is currently working as an Assistant Professor in Raghu Engineering College, visakhaptanm.His area of research includes Image Processing and digital signal processing.

Mr.S.VENKATA ANAND has completed his M.Tech (Electronics instrumentation) in Andhra University, Visakhapatnam. He is currently working as an Assistant Professor in Sanketika Vidya Parishad Engineering College, visakhaptanm.His area of research includes microstrip Antenna Design and fabrication.