Secure Image Transmission Technique Based On Mosaic Image and Pixel Color Transformation

[1]Manjunatha N, [2]Mrs. Reshma M

[1]M. Tech Student, [2]Assistant Professor
Department of Digital Electronics & Communication System,
Visvesvaraya Technological University, Chikkaballapur, India

Abstract - *Concealing the information in computerized pictures has been territory of enthusiasm for the advanced picture preparing space. Albeit so much work has been done in the writing to determine the issues like expanding the information limit, making the mystery picture alike of target picture however a large portion of the works neglects to meet the commonsense necessities. This paper introduces an approach that can change a mystery picture into a mystery part unmistakable mosaic picture of a similar size that has the visual appearance of any uninhibitedly chose target picture without need of a database. Where, this mosaic picture era has done by separating the mystery picture into parts and changing their separate shading qualities into relating squares of the objective picture. Utilization of the Pixel shading changes yields the lossless recuperated picture in view of the untransformed shading space values. Era of the key assumes a vital part to recoup the information from the mystery picture in lossless way. Along these lines, just with the key, a man can recover the mystery picture almost lossless, from the mosaic image. Good exploratory outcomes demonstrate the plausibility of the proposed strategy.*

Keywords: *Color Transformation, data hiding, image encryption, secure image transmission, mosaic image.*

I. INTRODUCTION

The quick development of web use over high data transmission and minimal effort PC equipment has pushed the touchy development of Covert correspondence utilizing pictures. In the present year, secure and concealed correspondence is the chief necessity of the general population. In this manner undercover correspondence is picking up fascination by individuals because of the security issues over web. Ordinarily, pictures from different sources are oftentimes utilized and transmitted through the web for various applications, for example, online individual photo collections, barrier association mystery information dissemination, classified endeavor chronicles, record stockpiling frameworks, therapeutic pictures, quiet points of interest are inserted inside picture demonstrating insurance to data, and military imaging databases. As these pictures contain private and classified data, they ought to be shielded from spillages amid transmissions. Along these lines, there is need of secure picture transmission system.

There are numerous strategies have been proposed for securing picture transmission, in that, two basic methodologies are picture encryption and information stowing away. Picture encryption makes utilization of the regular property of a picture, for example, high repetition and solid spatial relationship, to get an encoded picture in view of Shannon's disarray and dissemination properties [2]-[3]. The scrambled picture is a clamor picture so that nobody can get the mystery picture from it unless he/she has the right key. In any case, the scrambled picture is a clamor picture so pulls in an aggressor's consideration amid transmission. An option is information concealing [4]-[5], that shrouds a mystery message into a cover picture so that nobody can understand the presence of the mystery information, in which the information sort in this paper is a picture. Existing information concealing strategies basically use the methods of LSB substitution, histogram moving, distinction development, forecast blunder extension, recursive histogram change, and discrete cosine/wavelet changes [1].

A principle issue of the techniques for concealing information/picture in picture is to install an expansive size or same size picture into a picture. In particular, on the off chance that one needs to conceal implies, it needs that picture must be exceedingly packed ahead of time. Be that as it may, for some applications, where installed pictures short data is likewise so important, there must not be the stipend of genuine twists, in such picture applications, pressure operations are generally unrealistic. This paper show another method for secure picture transmission, which changes a mystery picture into an important mosaic picture with a similar size and resembling a preselected target picture. The proposed technique is new in that a significant mosaic picture is made, conversely with the picture encryption and information stowing away. Era of the key assumes an essential part to recuperate the information from the mystery picture in lossless way. Fitting data is inserted into the mosaic picture for the recuperation of the transmitted mystery picture [1] [2].

II.METHODOLOGY

To get secure pictures regardless of spillages, we should be build up a framework for clandestine correspondence and this is to be created by taking after planned system which is based on mosaic picture and pixel shading change.

The proposed strategy incorporates two fundamental stages:

1) Mosaic image creation
2) Secret image recovery

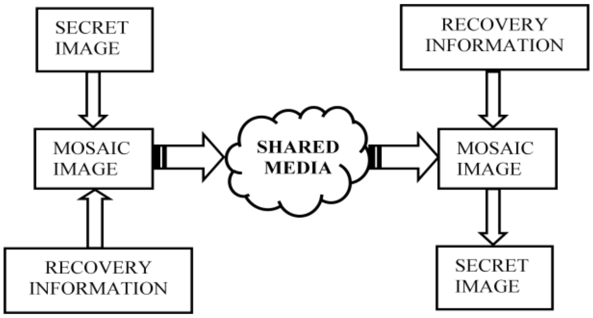

Fig. 1. Flow diagram of proposed method.

In the first phase, a mosaic image is obtained, which comprises of the fragments of an input secret image with color corrections according to a similarity criterion based on color variations.

The phase incorporates four stages: 1) fitting the tile images of the secret image into the target blocks of a preselected target image; 2) changing the color characteristic of every tile image in the secret image to turn that of the corresponding target block in the target image; 3) pivoting every tile image into a direction with the minimum RMSE value with respect to its corresponding target block; and 4) implanting required information into the created mosaic image for future recuperation of the secret image. In the second phase, the implanted information is extracted to recuperate the secret image nearly losslessly from the generated mosaic image. The phase incorporates two stages: 1) extracting the implanted information from the mosaic image for recovery of the secret image, and 2) recuperating the secret image using the extracted information.

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

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i$$

Where ci – pixel value of C channels such as red, green and blue. n – number of pixels.

$$\sigma_c = \sqrt{\frac{1}{n}\sum\nolimits_{i=1}^{n} (c_i' - \mu_c')^2}$$

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

$$c_i'' = q_c\left(c_i - \mu_c\right) + \mu_c'$$

Where qc – standard deviation quotient
Step 5: Sort the tile blocks and target blocks as per sorted average standard deviations respectively.
Step 6: Map sorted tile blocks with the sorted target blocks.
Step 7: Create mosaic image fitting tile box as per the mapped target blocks.
Step 8: Transform the color of all the pixel of each tile image using means and standard deviations.
Step 9: Rotate each transformed tile to 90,180 and 270 degrees and calculate root mean square error.
Step 10: Retain the rotation with minimum RMSE.
Step 11: Convert the mean and standard deviations for each tile block and mapped target block to binary.
Step 12: Convert tile rotation performed into 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 2: Secret image recovery

Input: a mosaic image F with n tile images and secret key k.
Output: the secret image S.
Steps:
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 recover the original pixel values.

Step 5: Take the results as the final pixel values, resulting in a final tile image.
Step 6: Compose all the final tile images to form the desired secret image S as output.

III. RESULT AND DISCUSSIONS

The quantity of required bits embedded for convalescing the key photograph will be enlarged when the tile image turns into minor, nevertheless, on the grounds that the mosaic image is yielded with the aid of dividing the secret snapshot into tile photographs and remodeling their color traits to be those of the corresponding goal blocks, the worldwide colour traits of a changed tile picture and its corresponding target block are the same but the colour distributions of them is also particularly one of a kind. Hence, even though the mosaic snapshot has the visual appearance of the goal image, the small print of each and every fragment within the mosaic picture may have low similarity to those of its corresponding goal block.

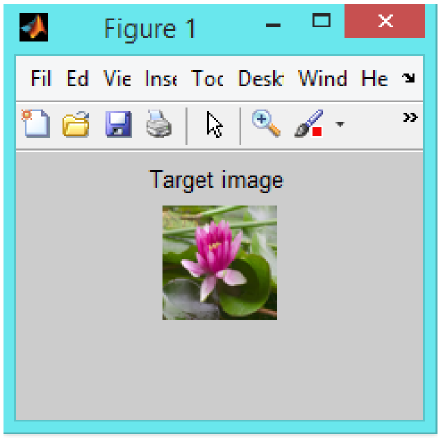

Fig 1: Target Image

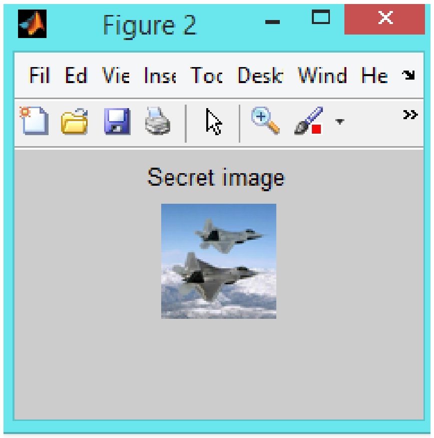

Fig 2: Secret Image

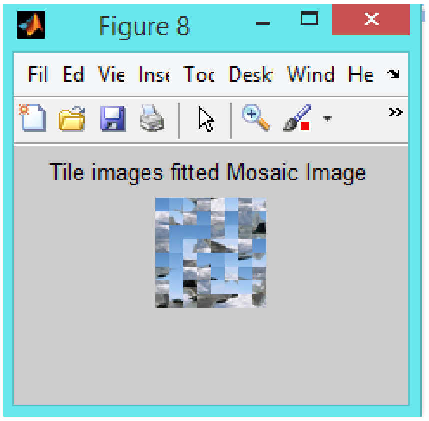
Figure 8
Fil Ed Vie Inse Toc Desk Wind He
Tile images fitted Mosaic Image

Fig 3: Tile Images Fitted Mosaic Image

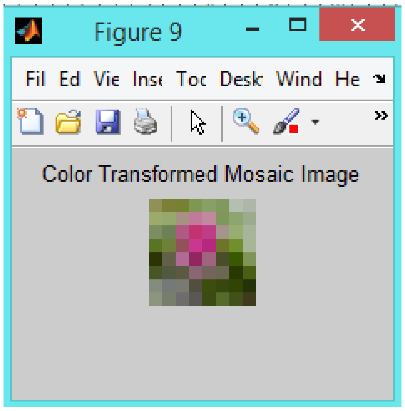
Figure 9
Fil Ed Vie Inse Toc Desk Wind He
Color Transformed Mosaic Image

Fig 4: Color Transformed Mosaic Image

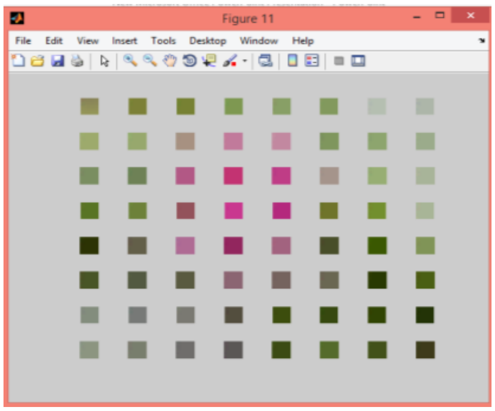

Fig 5: Embed Relevant Information

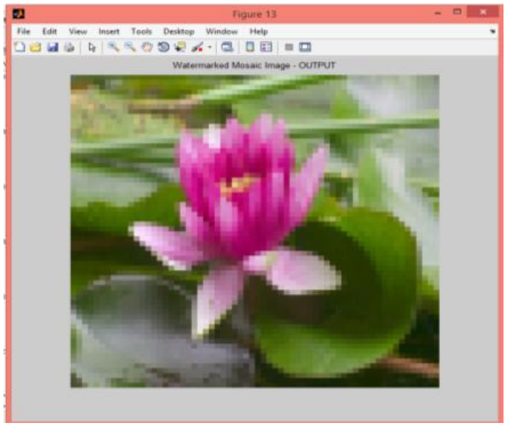
Figure 13
File Edit View Insert Tools Desktop Window Help
Watermarked Mosaic Image - OUTPUT

Fig 6: Water Marked Mosaic Image – Output

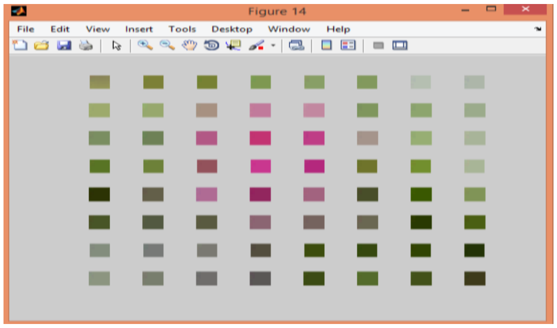

Fig 7: Extract Relevant Information

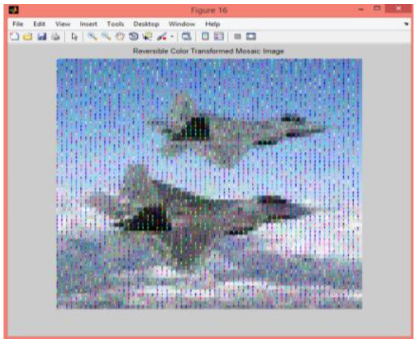
Figure 16
File Edit View Insert Tools Desktop Window Help
Reversible Color Transformed Mosaic Image

Fig 8: Reversible Color Transformed Mosaic Image

The primary figure is the objective image which is preselected from the database and is separated into target pieces and the second figure is the plane which is the mystery image and it is isolated into tile squares.

Third figure is the consequence of ascertaining mean, standard deviation and normal standard deviation for every objective square and tile piece and afterward sorting the pieces as indicated by the aftereffect of normal standard deviation. Next guide the sorted target obstructs with the tile squares, fit these pieces in a mosaic frame. In fig 4 change the shade of the considerable number of pixels of every tile piece utilizing mean and standard deviation pivot each changed tile square to 90, 180 and 270 degrees, and ascertain the root mean square mistake. In fig 5 install the pertinent data for future recuperation of the mystery image about losslessly. Fig 6 is the yield of the watermarked mosaic image. In fig 7 we do the turn around procedure to recoup the mystery image by separating the data that we implanted in the mosaic image. In fig 8 we recoup the mystery image utilizing the separated data.

IV. Security Consideration

To expand the security level, the implanted data for later recuperation is scrambled with an emit key. Only the recipient who has the right key can translate the mystery image. A roof dropper may strive for every conceivable stage of tile pictures in the mosaic picture to get mystery picture back. But here the quantity of all changes is n! Along these lines, the likelihood for his/her to guess the remedy change is p=1/n!, which is little in value. So, as substantial estimation of n ought to be utilized to build the security of the proposed technique. Moreover, regardless of the possibility that one happens to figure the change accurately, still he/regardless she doesn't know the revise parameters for recouping the first shading appearance of the mystery picture as those parameter data for shading recuperation is encoded as a bit stream utilizing a mystery key. In the outrageous case, on the off chance that he/she will watch the substance of the mosaic picture with right change, we again utilized the way to randomize vital data of a mystery picture, before changing the mystery picture into a mosaic picture. So at long last, just an approved clients with the key can know the right mystery picture while an assailant can't.

V. CONCLUSION

As concealing the information in computerized pictures has been territory of enthusiasm for the advanced picture handling space, there is prerequisite of profoundly secure transmission method. The proposed strategy can be taken as a solid procedure for secure picture transmission as the technique makes another sort of workmanship picture for concealing the mystery picture. By the utilization of legitimate pixel shading changes, mosaic pictures with high visual likenesses to subjectively chose target pictures is made with no need of an objective picture database or with no kind of pressure. Additionally, the first mystery pictures can be recouped almost lossless from the got mosaic pictures. Once more, lossless recuperation of mystery picture is accomplished by utilization of the Pixel shading changes in view of the untransformed shading space values. In lossless recuperation of the mystery information from the mystery picture, key assumes a critical part. A great exploratory outcome demonstrates the possibility of the proposed strategy.

REFERENCES

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

[2] J. Fridrich, “Symmetric ciphers based on two dimensional chaotic maps,” Int. J. Bifurcat. Chaos, vol.8, no. 6, pp. 1259–1284, 1998.

[3] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, “A robust and secure chaotic standard map based pseudorandom permutationsubstitution scheme for image encryption,” Opt. Commun., vol. 284, no. 19, pp. 4331–4339, 2011.

[4] C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognit.., vol. 37, pp. 469–474, Mar. 2004.

[5] W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, 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.

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