A MOSAIC IMAGE CREATION FOR SECURE SECRET IMAGE TRANSMISSION

PROF. M. R. JOSHI[1], MISS. RENUKA A. KARKADE[2]

[1]*AssistantProfessor, Department of CSIT, HVPMCOET, AMRAVATI, INDIA*

[2]*PG Student, Department of CSIT, HVPMCOET, AMRAVATI, INDIA*

---***---

Abstract-*In the present world as the data world advances and information turn out to be increasingly significant, security concern is the real issue and insurance of that information, which originates from content information to media information. The pictures may contain private or secret data with the goal that they ought to be shielded from spillages amid transmissions. Secure Image Transmission has the capability of being received for mass correspondence of delicate information under the investigation of an unfriendly controlling power. A procedure for secure picture transmission is required, to change a mystery picture into one significant Mosaic tile picture with size just about the same and seeming as though one target picture. Be that as it may, mystery part noticeable mosaic pictures permit the client to safely transmit a picture under the front of another picture of same size. Another safe picture transmission strategy is proposed, which changes naturally a given substantial volume mystery picture into a supposed mystery section obvious mosaic picture of the same size. To safely transmit the mosaic picture, mystery sharing calculation must be utilized.*

Keywords: Secret image, Target image, Mosaic image, Image Steganography

1. INTRODUCTION

Pictures from different sources are often used and to be transmitted through the web for different applications, for example, online individual photo collections, secret undertaking files, record stockpiling frameworks, therapeutic imaging frameworks, and military picture databases are utilized. These pictures for the most part contain private or secret data so they ought to be shielded from spillages amid the safe transmissions. At the point when a picture is transmitted, two normal methodologies that are connected for secure transmission are picture encryption and information stowing away. Picture encryption is a strategy that changes over the first picture into another structure that is hard to get it. The encoded picture is a clamor picture so that nobody can acquire the mystery picture without knowing an unscrambling unique picture into another structure that is hard to get it. Information concealing that shrouds a mystery message into a spread picture so that nobody can understand the presence of the mystery information, in which the information kind of the mystery message is a picture. Yet, a primary issue of concealing information in pictures is the trouble to insert a lot of message information into a solitary picture. There are distinctive methodologies that are being used to empower picture security, the ordinarily utilized methodologies are steganography and cryptography. To be sure, the greater part of the strategies that join cryptography and steganography comprise in encoding the mystery message before concealing its presence in a spread article.

To make mystery picture more secure another idea of mosaic picture is being used alongside steganography called as mosaic picture steganography. Another sort of craftsmanship picture, called mystery piece noticeable mosaic picture, which contains little sections of a given source picture is proposed in this study. Watching such a kind of mosaic picture, one can see all the pieces of the source picture, yet the sections are so modest in size thus irregular in position that the spectator can't make sense of what the source picture resembles. In this way, the source picture might be said to be covertly inserted in the subsequent mosaic picture, however the part pieces are all obvious to the eyewitness. Furthermore, this is the motivation behind why the subsequent mosaic picture is named mystery piece unmistakable which is the consequence of irregular revision of the parts of a mystery picture in mask of another picture called target picture, making precisely an impact of picture steganography. The trouble of concealing an immense volume of picture information behind a spread picture is explained consequently by this sort of mosaic picture. This is another method of data stowing away, not found in the writing as such.

2. LITERATURE REVIEW

Pictures which really contain private information must be shielded from spillages amid transmissions for that numerous strategies have been proposed for securing picture transmission. Up to now whatever the current framework are and business related to this procedure is clarified underneath.

Another safe picture transmission procedure is proposed, which changes naturally a given huge volume mystery picture into a supposed mystery piece obvious mosaic picture of the same size. The mosaic picture, which appears to be like a self-assertively chose target picture and might be utilized as a cover of the mystery picture, is yielded by isolating the mystery picture into sections and changing their shading attributes to be those of the comparing pieces of the objective picture [1].State-of-the-craftsmanship plans proposed for reversible information concealing which for the most part comprise of two stages: first build a host grouping with a sharp histogram by means of forecast blunders, and afterward install messages by adjusting the histogram with techniques, for example, distinction extension and histogram shift [2].

A keyless methodology is proposed for keeping up the mystery and privacy of pictures with two diverse methodologies being taken after, the first being scrambling the pictures through encryption calculations utilizing keys; the other methodology includes isolating the picture into arbitrary shares to keep up the pictures mystery [3]. A novel plan for distinguishable reversible information stowing away in encoded pictures is proposed. In the main stage, a substance proprietor scrambles the first uncompressed picture utilizing an encryption key. At that point, an information hider may pack the slightest critical bits of the scrambled picture utilizing an information concealing key to make a scanty space to oblige some extra information [4].

Another sort of PC workmanship picture called mystery part unmistakable mosaic picture is proposed which is made consequently by making little sections out of an offered picture to end up an objective picture in a mosaic structure, accomplishing an impact of implanting the given picture obviously yet subtly in the subsequent mosaic picture [5]. A picture mosaicing strategy for camera-caught archive pictures is proposed, and it can be utilized to join different covering report pictures into a huge high determination picture [6].

3. PROPOSED WORK

The proposed method is based on secret-fragment-visible mosaic image which includes two phases

1] Mosaic image creation

2] Secret image recovery

As shown in the following diagram:

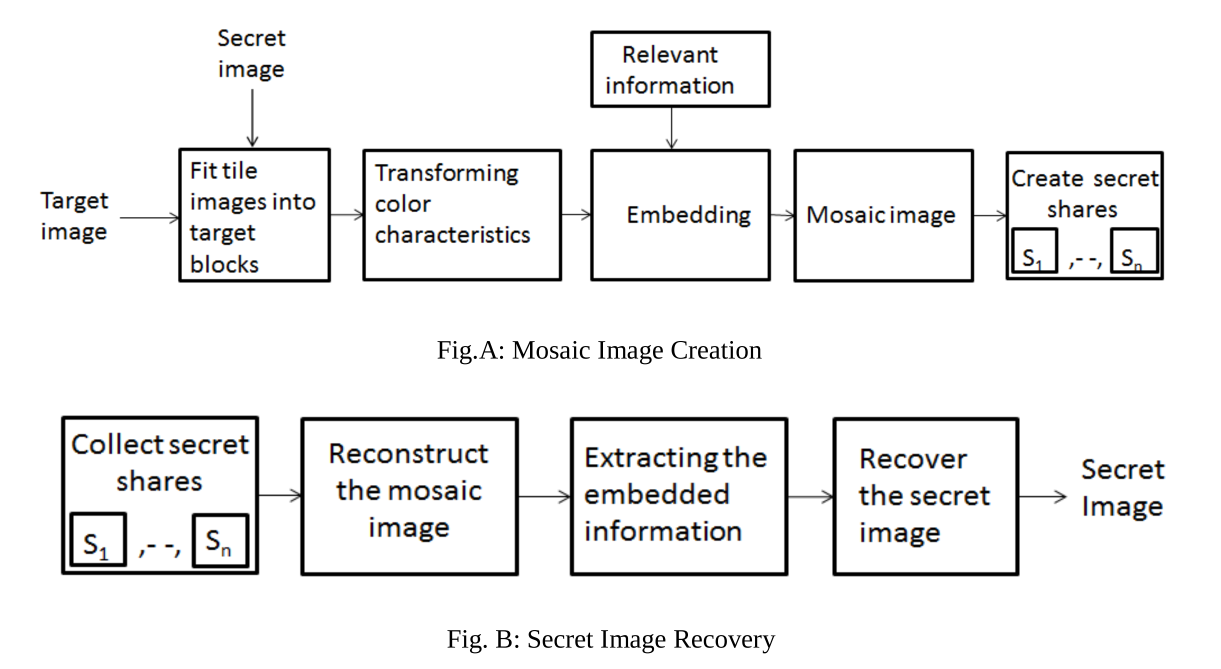


Fig.A: Mosaic Image Creation

Fig. B: Secret Image Recovery

Fig.1 Block Diagram of Proposed System

The two phases of this method are:

3.1 Mosaic image creation:

I. Select secret image and target image:

Firstly select the secret image and target image. We can choose any image without any need of database.

II. Fit tile images into the target blocks:

Divide the secret image S into n tile images {T1, T2, . . . , Tn} as well as the target image T into n target blocks {B1, B2, . . . , Bn} with each Ti or B_j being of size NT .

Compute the means and the standard deviations of each tile image Ti and each target block Bj for the three color channels and compute accordingly the average standard deviations for Ti and Bj , respectively, for i = 1 through n and j = 1 through n.

Sort the tile images in the set Stile = {T1, T2, . . ., Tn} and the target blocks in the set Starget = {B1, B2, . .. , Bn} according to the computed average standard deviation values of the blocks; resulting in a mapping sequence L of the form: T1 →B1 , T2 →B2 , . . . , Tn →Bn .

Create a mosaic image F by fitting the tile images into the corresponding target blocks according to L.

III. Transforming color characteristics:

Transforming the color characteristics of each tile image in the secret image to become that of the corresponding target block in the target image. Color characteristics must be transformed on the basis of mean and standard deviation.

IV. Embedding relevant information:

Embedding the relevant information in the mosaic image.Here we are embedding one codeword in the mosaic image.The codeword must be check and match for the recovery of secret image from the mosaic image. If the codeword is not matched at the time of recovery then the process will not go further and stop.

V. Create secret shares:

Before transmitting the mosaic image, we will create multiple shares of it. The shares of mosaic image will transfer to the receiving side. Among all the shares, only with few shares we can reconstruct the mosaic image. Dividing the mosaic image in multiple shares is necessary for achieving the high security. To make shares of mosaic image we are going to use the Shamir Algorithm.

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret isdivided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. The goal is to divide secret S (e.g., a safe combination) into n pieces of data $S_{1,............,}S_n$such a way that:

1. Knowledge of any k or more S_i pieces makes S easily computable.
2. Knowledge of any k-1 or fewer S_i pieces leaves S completely undetermined (in the sense that all its possible values are equally likely).

This scheme is called (k, n) threshold scheme. If k = n then all participants are required to reconstruct the secret.

3.2 Secret image recovery:

I. Collect secret shares:

At the receiving side we have to collect the shares of mosaic image from which we have to reconstruct the mosaic image. We can reconstruct the mosaic image by collecting all or few shares. In this we have created four shares and at the time of recovery only two shares are required for the reconstruction of mosaic image.

II. Extracting the embedded information:

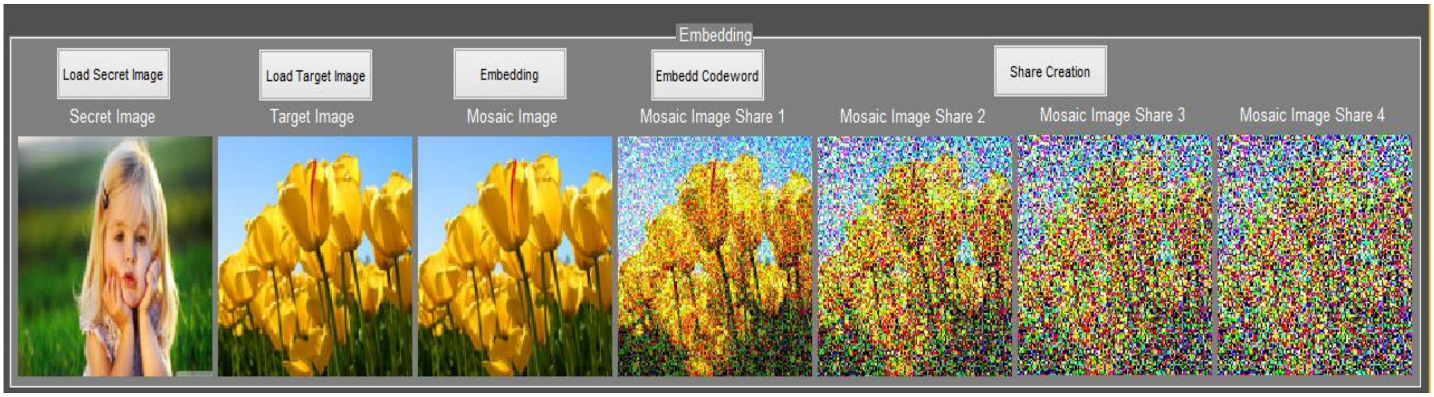
Extracting the embedded information for secret image recovery from the mosaic image. Here we are extracting the embedded codeword in the mosaic image. Codeword must be matched for the recovery of secret image and also for further process. Once the codeword is matched we will move to the next step; but if not matches the process will stop here.

III. Recover the secret image:

Once the codeword is matched we can recover the original secret image.

4. RESULT& DISCUSSION

To provide greater protection to mosaic photograph, we've implemented the secret sharing set of rules. Picture fine is a function of a picture that measures the perceived photograph degradation (generally, compared to an ideal or ideal photograph). Imaging systems may introduce some quantities of distortion or artifacts in the signal, so the nice evaluation is a crucial trouble. Photo pleasant is measured with extraordinary overall performance parameters like Peak Signal to Noise Ratio (PSNR), Root Mean square error (RMSE), and Correlation and many others. The outcomes of proposed gadget are proven in following diagrams.

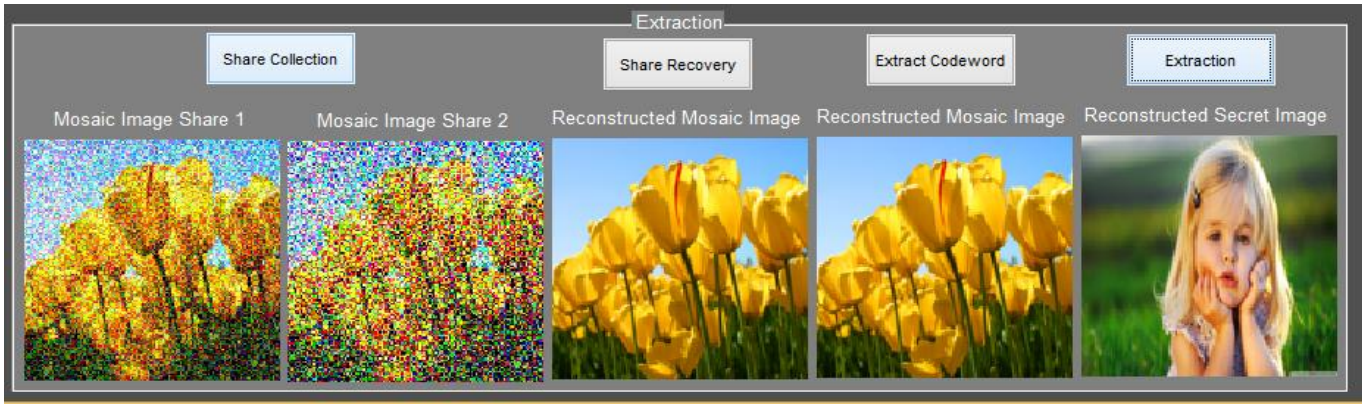


(a) (b) (c) (d1) (d2) (d3) (d4)

Fig 2. RGB Image Result of Proposed System with Mosaic Image Creation and Share Creation

In fig 2 we have load the secret image (a) and target image (b). Mosaic image(c) is formed after fitting the tile images into target blocks and transforming color characteristics.

After embedding the relevant information in mosaic image we have generated the secret shares of mosaic image as from (d1) to (d4).



(e1) **(e2)** **(f)** **(g)** **(h)**

Fig 3. RGB Image Result of Proposed System with Share Collection and Secret Image Recovery

In fig 3 we have collect the secret shares of mosaic image (e1), (e2) and recovered the mosaic image. Then if relevant information is matched with previously embedded information then the mosaic image is reconstructed and then after secret image is recovered.

A test has been performed to check the proposed approach with image sizes 768 * 1024 or 1024 * 768. To research recovered secret photo that is seem like an authentic secret image, calculating the peak signal to Noise Ratio (PSNR), Root mean square error (RMSE), and Correlation. Following table indicates the values of PSNR, RMSE, ENTROPY and CORRELATION for secret photo with color image.

Secret image	Target image	PSNR	RMSE	CORRELATION	ENTROPY
Fig 2. (a)	Fig 2. (b)	73.115	0.0592	1	7.4414

Table 1: Performance Measures of Proposed System

5. CONCLUSION

Another safe picture transmission technique has been expert postured, which can make important mosaic pictures as well as can change a mystery picture into a mosaic one with the same information size for use as a camouflage of the mystery picture. The mosaic picture creation includes obstruct by piece handling of the pictures. With this strategy client can choose his/her most loved picture to be utilized as an objective picture without the need of huge database. Likewise the first mystery picture can be recuperated almost losslessly from the made mosaic picture. To give more security to made mosaic picture the mystery sharing calculation is utilized. Proposed framework is additionally effectively worked with grayscale pictures alongside RGB pictures. Future work will stretch out to video preparing. Further studies will attempt a procedure for secure picture transmission through recordings, which changes a mystery picture into a significant mosaic picture with the same size and which resembles a preselected target picture of the accessible video outlines.

REFERENCES

[1] Ya-Lin Lee, Student Member, IEEE, and Wen- Hsiang Tsai, Senior Member, IEEE‖ 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] W. Zhang, X. Hu, X. Li, and N. Yu, "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.

[3] A Keyless Approach to Image Encryption, Siddharth Malik, Anjali. Sardana Indian Institute of Technology Roorkee, India. 2012 International Conference on communication Systems.

[4] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image", in in Proc. IEEE Trans. On Information Forensics and security, Vol. 7, No. 2, APRIL 2012.

[5] 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, pp. 936-945, Sep. 2011.

[6] Miao Ligang, Yue Yongjuan, "Automatic Document Image Mosaicing Algorithm with Hand-held Camera", *IEEE International Conference on Intelligent Control and Information Processing (ICICIP),* vol. 2 pp: 1094 – 1097, July 2011.

[7] 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.

[8] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, 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.

[9] 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.

[10]Y. Hu, H.-K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1500–1512, Dec. 2008.

[11] D. Coltuc and J.-M. Chassery, "Very fast watermarking by reversible contrast mapping," *IEEE Signal Process. Lett,* vol. 14, no. 4, pp. 255–258, Apr. 2007."

[12] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," *IEEE Trans. Inf. Forens. Secure*, vol. 2, no. 3, pp. 321–330, Sep. 2007.

[13] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEETrans. Circuits Syst. Video Technol*., vol. 16, no. 3, pp. 354–362, Mar.2006.

[14] M. S. Lew, N. Sebe, C. Djeraba, and R. Jain, "Content-based multimedia information retrieval: State of the art and challenges," *ACM Trans. Multimedia Comput., Commun, Appl.*, pp. 1–19, Feb. 2006.

[15] G.Di Blasi, G. Gallo, and M. Petralia, "Puzzle image mosaic," in *Proc. IASTED/VIIP*, Benidorm, Spain, Sep. 2005, pp. 33–37.

[16] G. Di Blasi and G. Gallo, "Artificial mosaics," *Vis. Comput.*, vol. 21, pp. 373–383, 2005.

[17] Gehua Yang, Charles V. Stewart, "Covariance-Driven Mosaic Formation from Sparsely-Overlapping Image Sets with Application to Retinal Image Mosaicing", IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'04), vol. 1, pp: I-804 - I-810, July 2004.

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

[19] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, ―Image quality assessment: From error visibility to structural similarity,‖ IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004

[20] G. Elber and G. Wolberg, "Rendering traditional mosaics, Vis.Comput" vol. 19, pp. 67–78, 2003.