ISSN:0975-9646



# Secure Image Transmission using Color Transformations and Difference Expansion Data Embedding Technique

**Pooja Shelar**
*ME Computer,*
*Dr D.Y Patil Institute of Engineering & Technology*
*Pune, India*

**Archana Chaugule**
*ME Computer,*
*Dr D.Y Patil Institute of Engineering & Technology*
*Pune, India*

***Abstract* :- Secret fragment visible mosaic image is an image generated by combining small tiles of secret image to form a target image in the sense of mosaic. When this mosaic image is viewed at close, the observer can view smaller elements, but when viewed at a distance mosaic image is collection of tiles combined together to yield the overall picture. To generate a mosaic image, divide original image into many tiles. Beforesplitting the image, compare the image for Mosaic creation. Mosaic image is created by composing small tiles of a given secret image into target image, achieving an effect of embedding the given secret image secretly in the resulting mosaic image .To create the mosaic image, first search a similar target image corresponding to the selected secret image .Then find a best fit secret image tile for embedding in the target image blocks .A new secure picture transmission system is proposed, which changes consequently a given expansive volume mystery picture into a purported mystery part noticeable mosaic picture of the same size. In proposed method there is automatic selection of target image which is done on the criteria of overflow and underflow to improve the quality of regenerated secret image and also a difference expansion technique is used for increasing embedding capacity of proposed system .Finally the results are compared using Time graph and PSNR graph for the existing system and proposed system. Experimental analysis shows that time required for embedding data into mosaic image by proposed system is less than compared to existing system and a greater PSNR value of secret images regenerated using proposed system is being achieved.**

**Keywords—Data hiding, image encryption, mosaic image, secure picture communication, color change.**

## I. INTRODUCTION

The photos are used for transmitting or hiding confidential information which is traded through web. Therefore the security of these images is the principal prerequisite for everyone. For the security of the photo transmission process data hiding and encryption these two concepts are generally used by the developers. Both these systems confronts a couple of issues hence building up a strategy for secure picture transmission by making a mosaic picture of relating secret picture with the assistance of arbitrarily selected target picture and using shading transformation.

A method which makes use of the common properties of an image like additional and three-dimensional relationship, using the Shannon's confusion and diffusion properties to get a picture already encrypted is known as Encryption. Encrypted image has noise that why one without using proper key can access the secret images while transmission. Any how the encoded image is a non-usable data which cannot disclose the information prior to encoding. In this way, this might bring out an attackers consideration amid the transmission of the picture in light of its discretionary in nature. One more way to handle this issue is covering up of data which hides a secret info in second image so that nobody can anticipate the survival of the secret data, in which the type of information of the secret message that is inspected in this paper is a picture. The method for data hiding definitely referred to for the most part use the systems, for example, recursive histogram modification, histogram shifting, discrete cosine/wavelet modifications, LSB substitution and so on. In order to reduce misrepresentation of the last picture, use set the upper bound for the distortion on payload of the cover picture. In this way, the main disadvantages of technique for hiding the data in images are the difficulty in merging a huge quantity of data into single picture. Particularly, if hiding a secret image into second image with same measurement, the secret image must be exceptionally compacted ahead of time.

In this exploration work, given the framework for secure image transmission is evaluated, which changes a secret picture into a mosaic picture with the same measurement and taking after a pre-selected last picture. Utilizing secret key, change strategy can be controlled and can a man recovers the secret picture about lossless from the mosaic picture. This strategy is in which new class of computerized painting picture, called mystery part obvious mosaic picture, is inspected. The outcome of reworking of the block of a secret picture in covering of second picture called mosaic picture. However, a conspicuous weakness is the essential of a broad picture database so that the produced mosaic picture can be sufficiently similar to the picked target picture. Using their framework, the client is not allowed to pick energetically his/her most loved picture for use as the target picture. It is along these lines craved in this study to evacuate this result of the method while keeping its merit, that is, it is planned to outline different system which is able change a secret picture into a secret patch- observable mosaic image of the similar dimension that has the graphic presence of any particular chosen target picture without the need of a database.

In this paper further we will discuss about related work studied on Section II. After that in Section II we will talk about proposed method and implementation details and introductory definitions and documentations. And Last Section IV display conclusions and presents future work.

## II. RELATED WORK

In this section discuss previous work done by the researchers for image processing.

In J.Fridich [1], given that some chaos-based image figures using bit-level stage have proposed as well as indicated likely result. The load of the time-consuming diffusion stage is decreased and afterward the execution of the cryptosystem is progressed due to the diffusion effect given in the new organize. Depending on spatial bit level change process, a symmetric chaos based image figure with a 3D cat guide is given in this paper. Compared to the last bit-level change methods, the diffusion effect of the novel strategy is prevalent as the bits are shuffled between various bit planes in place of inside of the same piece plane. As well as, the diffusion key stream separated from hyper chaotic system is identified with both the secret key as well as the normal image that prevents and improves the security against known plaintext attack.

In G. Chen,Y. Mao, and C. K. Chui [2], given encryption plans of assortment of effective chaos-based image. The typical structure of these plans has the modification as well as the diffusion stages performed on the other hand. The confusion and diffusion effect is exclusively inserted by the modification and the diffusion stage, separately. Subsequently, more general rounds than would normally be proper are needed to accomplish a particular step of security. They state to existing certain diffusion effect in the disarray phase by basic successive add and shift technique in this paper. The main purpose of this procedure to minimize the workload of the tedious diffusion chunk so that fewer general rounds and afterward a littler encoding time is must.

In L. H. Zhang, X. F. Liao, and X. B. Wang [3], To start with, for the imperviousness to differential attack and straight attack, they set forward the fairly great measurement properties of discrete exponential turbulent charts, In benefit of them, they implemented a 3-D S-box, as well as next, then outline a foremost plan for the imperviousness to measurement attacks and grey code attack. Indeed, the plan can oppose to the error function attack (EFA) that will be seen as an exceptionally effective assault as of late. At last, Experimental and systematic outcome shows that the plan is efficient and highly secure.

In H. S. Kwok and W. K. S. Tang [4] clarifies image encryption arrangement using a secret key of 144-bits is given. In the substitution strategy of the arrangement, image is apportioned into squares and along these lines in shading fragments. Every performing to shade part is balanced bitwise operation which based on secret key such as two or three most basic bits of its last and upcoming shading section. Three rounds are taken to complete substitution process. To make image all the more capable, a feedback part is in like manner joined by conforming used secret key in the wake of scrambling every square. Next, resultant image is divided a couple key depending component sub-images. Each sub-image experiences the scrambling system where pixels of sub-image are reshuffled within itself by making use of a delivered charm square cross section. Five rounds are taken for scrambling technique. The propose arrangement is essential, speedy and fragile to the puzzle key. As an outcome of high demand of substitution as well as stage, general attacks such as straight and also differential cryptanalysis are infeasible. The exploratory results expression that the current encryption technique is effective and has high security highlight.

In S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan[5], exhibited depending on blocked image scrambling encryption; this study shows another image encryption computation by presenting mayhem hypothesis. This computation firstly makes spatial scrambling in view of image blocking keeping in mind the end goal to interfere with pixel position, then assisting this interference through Arnold Mapping in the chaos and changes pixel RGB color space through enhanced Arnold Mapping. After this process, we get the final encoded image through a progression of iteration.

In J. Tian [6], clarified a reversible watermarking algorithm with high data disguising limit has been made for shading images. The computation allows the watermarking method to be interchanged, that restores the exact new image. The count covers a couple of bits in the refinement augmentation of vectors of nearby pixels. The required general reversible number updating and the major conditions to keep up a key separation from undercurrent and flood are solved for any vector of subjective length. In like manner, the potential payload calculate that can be embedded in a host image is given, as well as an input system for controlling this size is created. Besides, increase the measure of information which can be concealed into, the introducing count can be associated recursively an over the shading portions. Reproduction outcome utilizing spatial triplets, spatial quads, cross-shading triplets, and cross-shading quads are given and thought about the current reversible watermarking computation. These outcomes exhibit which the spatial quad-based estimation takes into mind hiding the greatest payload at the most lifted signal-to-noise ratio (SNR).

In V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud [7], given a strategy based on pseudo random permutation substitution is given .The pseudo random image groupings generated through 2D riotous slope tent guide have been used as a part of an effective method to accomplish the fancied level of disarray and diffusion in the encryption process. All the stage forms have been made reliant on the plain content and also figure keys, which create a fabulous mix of plain content affectability as well as key affectability in the encryption method. All the change forms have been made reliant on the plain content and additionally figure keys that deliver a magnificent blend of plain content affectability as well as key affectability in the encryption method. As well as the substitution procedure utilized as a part of the proposed image encryption

moreover adds to both the key and plain substance affectability, as it is begun by the starting routes made from the figure key and tent aide and after that took after by a mixing of the properties of picture pixels and pseudo irregular successions.

In C. K. Chan and L. M. Cheng [8], given Simple least-significant-bit (LSB) replacement is a technique that is utilized to embedding secret data in least significant bits of pixel value in target image. The LSB method commonly accomplishes high capacity. A straightforward LSB substitution that shrouds secret information directly into LSBs, is effortlessly executed however will bring about bad quality of the stego-image. Remembering the goal which minimizes the corruption of the target image subsequent to insert, a LSB replacement method was given by Wang et al. They provide a hereditary computing to hunt down inexact arrangements. Also, Chang et al. given a dynamic programming system to efficiently get an answer in which they given a broader model of Wang etal.s LSB substitution plan, called as transforming LSB substitution. Remembering the goal to defeat the problem connected with the two past techniques of a long running time, a more efficient techniques, alluded to as the coordinating methods, is proposed to find a superior arrangement. A few tests, exhibits and investigations are appeared in this paper to show this novel plan and approach.

## III. Implementation Details

### A. System Overview

The below figure 1 shows the architectural view of implement system. The explanation of the system is as follows:

The current method contains 2 important part

1. Mosaic picture creation and
2. Recover secret image.

In the initial segment, produced a mosaic image that has of the patch of an input secret image with color change providing for a match measure made on color contrasts. The Mosaic picture creation stage incorporates four phases:

1. To form target image by using the block image of secret image.
2. Changing the color properties of every block picture in the secret image to make that of the equivalent target block in the target picture;
3. Each block image rotate into a direction with less RMSE value according to its corresponding target block;
4. In future recovery the secret image so embedding relevant information into the created mosaic picture.

In the second part, extracted the embedding information and recover the secret image from the generated mosaic image.

The phase includes two steps:

1. Recovery and extracting the embedding data for secret picture from the mosaic picture.
2. Using the extracted information, recovering the secret image.

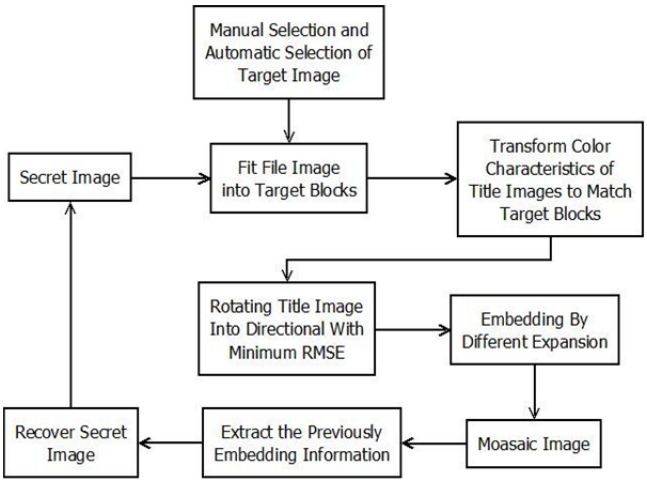


Figure 1: System Architecture

### B. Algorithm

For Mosaic image formation and for Secret Image recovery following algorithm are been used:

**Algorithm 1: Mosaic image formation [1]**

**Input:** a secret picture S, a target picture T, and a secret key K.

**Output**: a secret-patch-visible mosaic picture F.

**Process**:

Step 1: Take the input s are secret image, target image selected automatically or manually by user 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 secret tile and target block.

$\mu_C = \frac{1}{n}\sum_{i=1}^{n} C_i$--------- (1)

where $C_i$ pixel values of C-channels and value may have red, green and blue and n is number of pixels.

$\sigma_{C=\sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i-\mu_i)^2}}$ ---------- (2)

Step 4: Calculate the average standard deviation for each block and sort them. Where $q_c$ standard deviation quotient.

Step 5: Sort the secret tile and target as per sorted average standard deviations respectively.

Step 6: Map sorted tile 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 (RMSE).

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.

In the above algorithm describe the steps of the current method. Initially provide the input a secret picture, a target picture, and a secret key to the system.

**Algorithm 2: Secret picture recover.**
**Input:** a mosaic picture F with n tile images and secret key k.
**Output**: the secret picture S.
**Process**:
Step 1: Extract the bit stream from mosaic image F by performing reverse operation.
Step 2: Decoding the bit stream by using secret key K.
Step 3: Recover the desired secret picture S by rotating the tile images in a reverse direction.
Step 4: Recover the original pixel values by use the extracted mean and standard deviation quotients.
Step 5: Take the outcomes as the final pixel values, resulting in a final tile image.
Step 6: Create the desired secret image S as output to combine all the final tile image.

In the above algorithm shows the steps for recovery secret image. Initially extract bit stream from mosaic picture and decoding the bit stream. Get final image.

*C. Mathematical Model*

System S is represented as S= {I, T, B, C, R, E, M, P, O} (3)
**Input**
Input Secret Image I= $\{i_1, i_2, i_3... i_n\}$ . (4)
Where I is the set of secrete images and i1, i2, i3... in representing a secrete image

Target Image T= $\{ t_1, t_2, t_3,.....,t_n.\}$ (5)
Where T represent a set of Target image $t_1, t_2, t_3,.....,t_n$.

Target Blocks B = $\{b_1, b_2, b_3,...., b_n \}$ (6)
Where B is the set of target block and $b_1, b_2, b_3,...., b_n$ represent as a number of blocks to Fit Title Images into Target Blocks.

Transform color properties of title picture to match target blocks=C (7)
Rotate Title picture into Directions with Minimum RMSE = R (8)
Embedding Using Difference Expansion = E (9)

Mosaic picture M= $\{m_1, m_2, m_3,.....,m_n\}$ (10)
Where, M is the set of Mosaic picture and $m_1, m_2, m_3,.....,m_n$ are the number of mosaic pictures.
Extract the Previously-Embedded Information = P (11)
Recover Secret Images = O (12)

*D. Experimental Setup*

The system is built using JDK 1.8 on Window 7 platform and IDE tool (Net beans) is used as a development tool. The system doesn't need any particular hardware to run, any standard machine is capable of running the application.

## RESULT AND DISCUSSION

*A. Dataset*

This system used a secret image, a target image, and a secret key for the secret-fragment-visible mosaic image

*B. Results*

In this system generate secret-fragment-visible mosaic picture utilized a secret image, a target image, and a secret key. In this section we have discussed the outcome` produced by the proposed system and compare those outcomes with existing system.

In the table 1 shows the PSNR by the existing and proposed system. From the below table it display that the PSNR for the existing system is less than the PSNR for the proposed paper.

Table 1: PSNR Comparison

| Image | Existing System | Proposed System |
|---|---|---|
| 1 | 48.2569db | 51.2356db |
| 2 | 42.159db | 47.58216db |
| 3 | 51.452db | 55.4917db |

In the underlying step, created a mosaic image, that has of the patch of an input secret picture with shading change given for a match measure made on shading contrasts. The stage consolidates four stages:

$$MSE = \frac{\sum_{M,N}(I_1(m,n)-I_2(m,n))^2}{M*N} \quad \text{---------- (13)}$$

*M* and *N* are the number of rows and columns in the input images, respectively
Then the block calculates the PSNR using the following equation

$$PSNR = 10log_{10}(\frac{R^2}{MSE}) \quad \text{---------- (14)}$$

*R* is the maximum fluctuation in the input image data type .If the input picture has a double-precision floating-point data type, then *R* is 1. If it has an 8-bit unsigned integer data type, *R* is 255, etc.

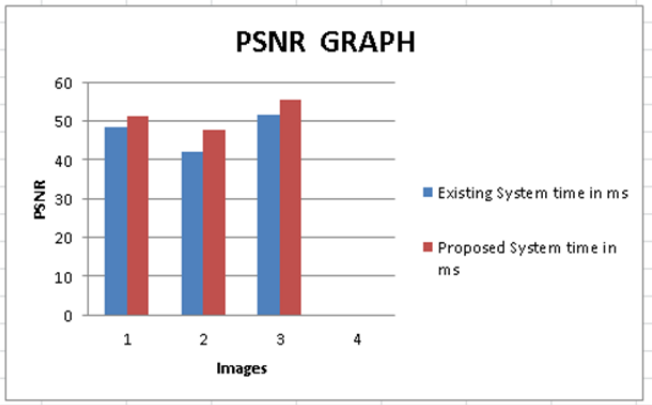


Figure 3: PSNR Graph

## IV. Conclusion And Future Scope

Therefore we give secure image transmission technique that makes a critical mosaic picture and can in like manner change the secret image in a secret-fragment-visible mosaic image with similar dimension as well as has the similar visual appearance as the target image which is pre-selected from the database. With this framework user can select his/her most loved image to be used as an target picture without the need of costly database. In like manner recuperating the first picture from the generated mosaic picture without misfortune data. We utilize distinction extension for expanding embedding limit of our framework. At last compare the outcomes with PSNR for the current framework and proposed framework. Tests results demonstrate that time and PSNR of proposed framework is more than to existing framework.

## Acknowledgment

The authors would like to thank the teachers for their guidance and also thank to researchers as well as publishers for making their resources available. We are grateful to the authorities of Savitribai Phule University of Pune and concern members of cPGCON2016 conference, organized by, for their constant guidelines and support. We are also thankful to the reviewer for their valuable suggestions. We also thank the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

## References

[1] J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,” Int. J. Bifurcat. Chaos, vol. 8, no. 6, pp. 12591284, 1998

[2] G. Chen,Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos Solit. Fract., vol. 21 , no. 3, pp. 749761, 2004.

[3] L. H. Zhang, X. F. Liao, and X. B. Wang, An image encryption approach based on chaotic maps, Chaos Solit. Fract., vol. 24, no. 3, pp. 759765, 2005.

[4] H. S. Kwok and W. K. S. Tang, “A fast image encryption system based on chaotic maps with finite precision representation, Chaos Solit. *Fract.,* vol. 32, no. 4, pp. 15181529, 2007

[5] S. Behnia , A. Akhshani, H. Mahmodi , and A. Akhavan, “A novel algorithm for image encryption based on mixture of chaotic maps,” Chaos Solit . Fract., vol. 35 , no. 2, pp. 408419, 2008.

[6] J. Tian, “Reversible data embedding using a difference expansion, IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890 896, Aug. 2003.

[7] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, “A robust and secure chaotic standard map based pseudo random permutation substitution scheme for image encryption, Opt. Commun., vol. 284, no. 19, pp. 43314339, 2011

[8] C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognit.., vol. 37, pp. 469474, Mar. 2004.