

# Unique Image Transmission Technique Through Secret-Fragment-Visible Mosaic Images By Approximately Reversible Colour Transformations With High Security

A.THIRUMALA RAO<sup>1</sup>, N.PRAKASH<sup>2</sup>, M.APPARAO<sup>3</sup>

<sup>1</sup>PG Scholar, Dept of ECE, PACE Institute of Science and Technology, AP, India.

<sup>2</sup>Associate Professor, Dept of ECE, PACE Institute of Science and Technology, AP, India.

<sup>3</sup>Associate Professor, Dept of ECE, PACE Institute of Science and Technology, AP, India.

**Abstract:** Unique image transmission technique is proposed, which transforms automatically a given large-volume of secret image into a alleged secret-fragment-visible mosaic image of the same size. The mosaic image, which looks similar to an swiftly selected target image and may be used as a masquerade of the secret image, is generate by dividing the secret image into fragments and transforming their colour characteristics to be those of the corresponding blocks of the target image. Skillful techniques are designed to conduct the colour transformation process so that the secret image may be recovered nearly losslessly. A scheme of handling the overflows/underflows in the converted pixels' colour values by recording the colour differences in the untransformed colour space is also proposed. The information required for recovering the secret image is embedded into the created mosaic image by a lossless data hiding scheme using a key. Good experimental results show the feasibility of the proposed method.

**Key Words:** Colour transformation, data hiding, image encryption, mosaic image creation, secure image transmission.

## Introduction

The project develops a secure image transmission system which does not incite attacker's attention. Here the secret image is disguised in the form of an arbitrary selected target image and transmitted. At The receiver side the secret image can be recovered by using a secret key.

Here Coltuc and Chessery's[8] technique of reversible contrast mapping is used for embedding the recovery information. Which substitutes LSB's with message bits directly, the reversible contrast mapping method applies simple integral

transformation to pairs of pixel values. The method yields high data embedding capacities close to the highest bit rate and has the lowest complexity reported so far.

Currently, images from various sources are frequently utilized and transmitted through the internet for various applications, such as online personal photograph albums, confidential enterprise archives, document storage systems, medical imaging systems, and military image databases. These images usually contain private or confidential information so that they should be protected from leakages during transmissions. Recently, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding.

Image encryption is a technique that makes use of the natural property of an image, such as high redundancy and strong spatial correlation, to get an encrypted image based on Shannon's confusion and diffusion properties[4]. The encrypted image is a noise image so that no one can obtain the secret image from it unless he/she has the correct key.

However, the encrypted image is a meaningless file, which cannot provide additional information before decryption and may arouse an attacker's attention during transmission due to its randomness in form. An alternative to avoid this problem is data hiding that hides a secret message into a cover image so that no one can realize the existence of the secret data, in which the data type of the secret message investigated in this paper is an image. Existing data hiding methods mainly utilize the techniques of LSB substitution, histogram shifting, difference expansion[5], prediction-error expansion, recursive histogram modification, and discrete cosine/wavelet transformations.

Thus, a main issue of the methods for hiding data in images is the difficulty to embed a large amount of message data into a single image. Specifically, if one wants to hide a secret image into a cover image with the same size, the secret image must be highly compressed in advance. For example, for a data hiding method with an embedding rate of 0.5 bits per pixel, a secret image with 8 bits per pixel must be compressed at a rate of at least 93.75% beforehand in order to be hidden into a cover image. But, for many applications, such as keeping or transmitting medical pictures, military images, legal documents, etc., that are valuable with no allowance of serious distortions, such data compression operations are usually impractical. Moreover, most image compression methods, such as JPEG compression, are not suitable for line drawings and textual graphics, in which sharp contrasts between adjacent pixels are often destructed to become noticeable artifacts.

In this paper, a technique for secure image transmission is 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[6], 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[6] 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.

Specifically, after a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called secret blocks, which then are fit into similar blocks in the target image, called target blocks, according to a similarity criterion based on color variations. Next, the color characteristic of each secret block is transformed to be that of the corresponding target block in the target image, resulting in a mosaic image which looks like the target image. Relevant

schemes are also proposed to conduct nearly lossless recovery of the original secret image from the resulting mosaic image.

The proposed method is new in that a meaningful mosaic image is created, in contrast with the image encryption method that only creates meaningless noise images. Also, the proposed method can transform a secret image into a disguising mosaic image without compression, while a data hiding method must hide a highly compressed version of the secret image into a cover image when the secret image and the cover image have the same data volume.

The proposed method includes two main phases 1) mosaic image creation and 2) secret image recovery.

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

## 2. Basics

### 2.1 Standard Deviation

In statistics, the standard deviation (SD, also represented by the Greek letter sigma  $\sigma$  or  $s$ ) is a measure that is used to quantify the amount of variation or dispersion of a set of data values. A standard deviation close to 0 indicates that the data points tend to be very close to the mean (also called the expected value) of the set, while a high standard deviation indicates that the data points are spread out over a wider range of values. The standard deviation of a random variable, statistical population, data set, or probability distribution is the square root of its variance. It is algebraically simpler, though in practice less robust, than the average absolute deviation. A useful property of the standard deviation is that, unlike the variance, it is expressed in the same units as the data. There are also other measures of deviation from the norm, including mean absolute deviation, which provide different mathematical properties from standard deviation.

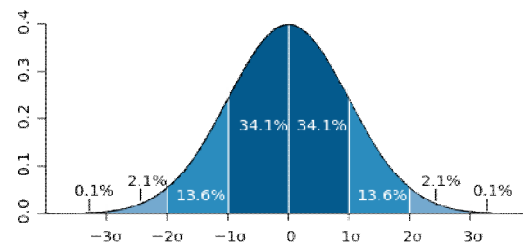


Figure 2.1

### 2.2 RMSE

The Root Mean Square Error (**RMSE**) (also called the root mean square deviation,

RMSE) is a frequently used measure of the difference between values predicted by a model and the values actually observed from the environment that is being modelled. These individual differences are also called residuals, and the RMSE serves to aggregate them into a single measure of predictive power.

The RMSE of a model prediction with respect to the estimated variable  $X_{model}$  is defined as the square root of the mean squared error:

$$RMSE = \sqrt{\frac{\sum_{i=1}^n (X_{obs,i} - X_{model,i})^2}{n}}$$

where  $X_{obs}$  is observed values and  $X_{model}$  is modelled values at time/place  $i$ .

The calculated RMSE values will have units, and RMSE for phosphorus concentrations can for this reason not be directly compared to RMSE values for chlorophyll  $a$  concentrations etc. However, the RMSE values can be used to distinguish model performance in a calibration period with that of a validation period as well as to compare the individual model performance to that of other predictive models.

### 2.3 Mean Structural Similarity Index (MSSIM):

For image quality assessment, it is useful to apply the SSIM index locally rather than globally. First, image statistical features are usually highly spatially non stationary. Second, image distortions, which may or may not depend on the local image statistics, may also be space variant. Third, at typical viewing distances, only a local area in the image can be perceived with high resolution by the human observer at one time instance (because of the foveation feature of the HVS). And finally, localized quality measurement can provide a spatially varying quality map of the image, which delivers more information about the quality degradation of the image and may be useful in some applications. The local statistics, and are computed within a local 8x8 square window, which moves pixel-by-pixel over the entire image. At each step, the local statistics and SSIM index are calculated within the local window. One problem with this is method that the resulting SSIM index map often exhibits undesirable “blocking” artifacts. An 11x11 circular-symmetric Gaussian weighting function  $w = \{w_i \mid i=1,2,3,\dots,N\}$ , with standard deviation of 1.5 samples, normalized to unit sum

( $\sum_{i=1}^N w_i = 1$ ). The estimates of local statistics  $\mu_x$ ,  $\sigma_x$  and  $\sigma_{xy}$  are then modified accordingly as

$$\mu_x = \sum_{i=1}^N w_i x_i$$

$$\sigma_x = \left( \sum_{i=1}^N w_i (x_i - \mu_x)^2 \right)^{1/2}$$

$$\sigma_{xy} = \sum_{i=1}^N w_i (x_i - \mu_x)(y_i - \mu_y)$$

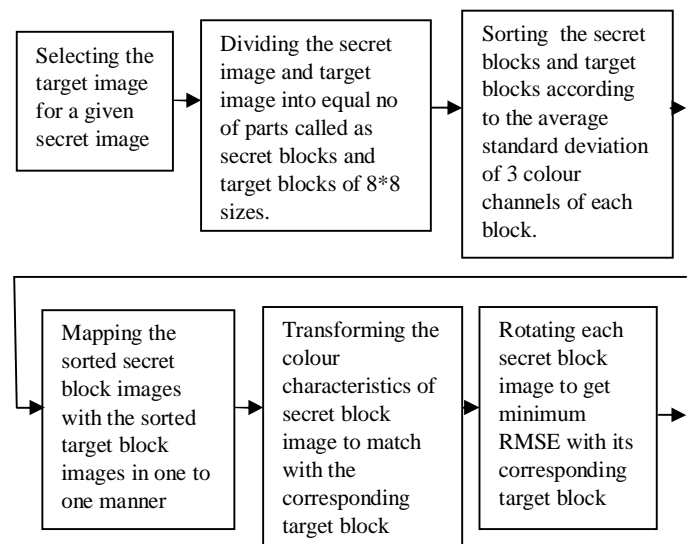
With such a windowing approach, the quality maps exhibit a locally isotropic property. Throughout this paper, the SSIM measure uses the following parameter settings:  $K1 = 0.01$ ;  $K2 = 0.03$ . These values are somewhat arbitrary, but current experiment shows the performance of the SSIM index algorithm is fairly insensitive to variations of these values. In practice, one usually requires a single overall quality measure of the entire image. Mean SSIM (MSSIM) index is used to evaluate the overall image quality.

$$MSSIM(X, Y) = \frac{1}{M} \sum_{j=1}^M SSIM(x_j, y_j)$$

Where  $X$  and  $Y$  are the reference and the distorted images, respectively  $x_j$  and  $y_j$  are the images contents at the  $j$ th local window and  $M$  is the number of local windows of the image and SSIM is calculated from below equation,

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

### 3 Creating Secret Mosaic Image: Block Diagram Secret MOSAIC Image Creation:



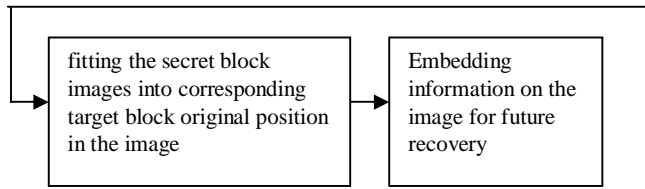


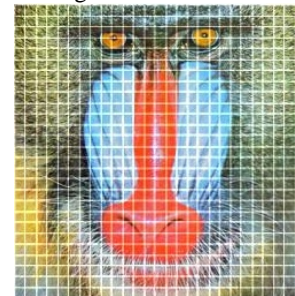
Figure 3.1



Secret Image  
 Figure 3.3



Target Image Divided Into Blocks  
 Figure 3.4



Secret Image Divided Into Blocks  
 Figure 3.5

### 3.1 Selecting the Target Image for the Secret Image and Dividing into Blocks

Both secret image and target image are divided into equal no of parts called as secret blocks and target blocks. The secret blocks of secret image are mapped to the target blocks of target image with maximum similarity. The colour characteristics of secret block are transformed to match with the corresponding target block by a technique called reversible colour transformation. The secret blocks are rotated to appropriate angles to minimise the RMSE value. The rotating information is kept for future use. Fit the secret block into corresponding target blocks. The relevant information for the image recovery is embedded on the image by using a technique called reversible contrast mapping.

On the receiver side the embedded information is retrieved first by using a secret key. By using the embedded information the secret image can be recovered.

- First take a secret image of 256\*256 sizes and a target image. Resize the target image so that its size is equal to secret image size.
- Divide the secret image into 8\*8 size small images, each 8\*8 small part of secret image is called secret blocks.
- Divide the target image into 8\*8 size small images, each 8\*8 small part of target image is called as target block.



TargetImage  
 Figure 3.2

### 3.2 Finding Standard Deviation of the Blocks

- Take each secret block in secret image and find standard deviation value for each colour channel at the same time take each target block in target image and find standard deviation value for each colour channel.

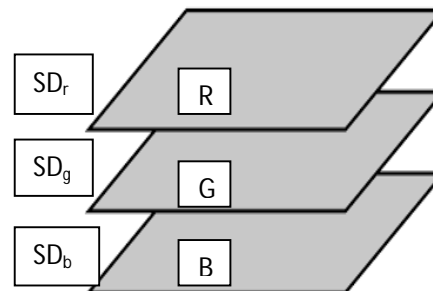


Figure 3.6



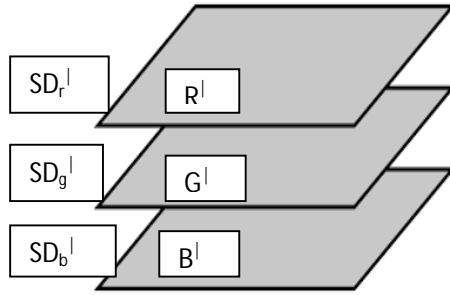


Figure 3.7

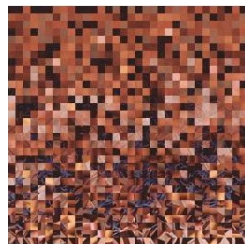
$(SD_r), (SD_g), (SD_b)$  = standard deviations of R,G,B planes in SECRET image block  
 $SD_{secret} = [(SD_r) + (SD_g) + (SD_b)] / 3 =$  standard deviation of secret image block

$(SD_r)^l, (SD_g)^l, (SD_b)^l$  = standard deviations of R,G,B planes in TARGET image block  
 $SD_{target} = [(SD_r)^l + (SD_g)^l + (SD_b)^l] / 3 =$  standard deviation of target image block

- Standard deviation of the secret block by taking average of the  $SD_R, SD_G, SD_B$ .  
 $SD_{secret\ block} = (SD_R + SD_G + SD_B) / 3$ .
- Standard deviation of the block by taking average of the  $SD_R^l, SD_G^l, SD_B^l$ .  
 $SD_{target\ block} = (SD_R^l + SD_G^l + SD_B^l) / 3$ .

### 3.3 Sorting the blocks

- Sort all secret blocks in secret image according to their standard deviations in ascending order and put all the secret blocks in an array.
- Sort all blocks in target image according to their standard deviations in ascending order and put all the block in an array.
- Save the identifier values of secret blocks array and target blocks array.
- Target and secret blocks after sorting will be like this.



SortedTargetBlocks  
 Figure 3.8



Sorted Secret Blocks  
 Figure 3.9

### 3.4 Applying Transformations

#### Applying colour transformation to the pixel values of secret blocks in secret image:

- Take the first secret block in the secret image array and first target block in the target image array. Now find the standard deviations and mean values for each colour channel in secret block image and target block image.

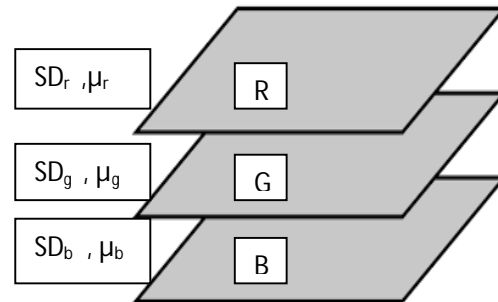


Figure 3.10

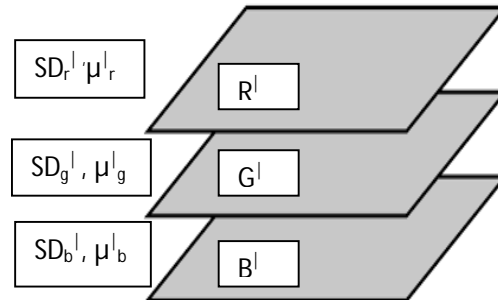


Figure 3.11

- Take the first colour channel of the secret block and target block, apply colour transformations for every pixel of secret block colour channel and find new pixel values.

$$\text{New pixel value } C^l = (SD_r^l / SD_r) (\text{secret block pixel value} - \mu_r) + \mu_r^l$$

$C^l =$  new pixel value

Repeat this operation for all colour channels

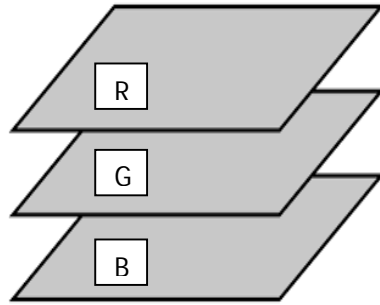


Figure 3.12

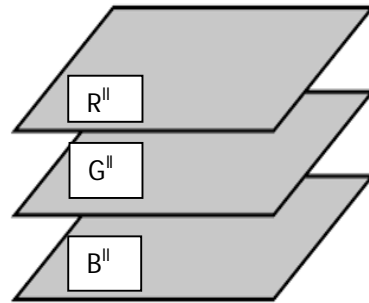


Figure 3.13

After applying colour transformation for each block, for each colour channel pair save standard deviation ratio, mean values of the secret block colour channel and target block colour channel.

### 3.5 Rotating the blocks

Now the new secret image block appears like target image block, rotate the new secret block to  $0^{\circ}, 90^{\circ}, 180^{\circ}, 270^{\circ}$  till the RMSE with its corresponding target block is minimum and save the rotations of each secret block

- For every rotated secret block save the rotated information. Rotation information is represented by 00,01,10,11 respectively with  $0^{\circ}, 90^{\circ}, 180^{\circ}, 270^{\circ}$ .
- Repeat this process to all secret blocks in the secret blocks array.

Secret blocks after applying colour transformation and rearranging the blocks.

### 3.6 Rearranging the blocks

**Rearranging the secret image blocks to get mosaic image:**

- Now replace the identifier values of target blocks to its corresponding secret blocks in the array.
- Arrange the secret blocks according to their identifiers in the matrix, the secret mosaic image is formed.

- The RMSE value between secret MOSAIC image and TARGET image increases with increase in block size.



Secret Mosaic Images

Figure 3.14

Block Size 8\*8

RMSE 23.26

### 3.7 Creating the transform Information Saved Information is transformed from decimal to binary

Identifier value

1.  $\mu_R, \mu_R'$
2.  $(SD_R / SD_R')$
3. 2 bits rotating information

#### Arranging the binary information in an array

[ identifier  $\mu_R, \mu_R'$   $(SD_R / SD_R')$  rotated information]

Calculating the length of the binary information array

Length of each mean value in binary form = 8

Length of standard deviation ratio in binary form = 8

Length of mean values of 3 planes of secret block =  $8 + 8 + 8 = 24$

Length of mean values of corresponding target block =  $8 + 8 + 8 = 24$

Length of standard deviation ratios of 3 planes =  $8 + 8 + 8 = 24$

Length of rotating information = 2

Total length of information for one block is =  $24 + 24 + 2 = 74$

Total no of blocks in 256\*256 image with 8\*8 block size is = 1024

Total length of information for all the blocks =  $1024 * 74 = 75776$

(Since there are 1024 blocks) Length of the identifier = 10 bits

Total length of identifier =  $10 * 1024 = 10240$   
 Total length of information including identifier =  $75776 + 10240 = 86016$

**Creating the secret key**

To create secret key the saved binary array is XOR operated with randomly generated binary sequence of same size (86016).

[Identifier  $\mu_R, \mu_R^l$  ( $SD_R^l / SD_R$ ) rotated information]  
 XOR  
 [ Randomly Generated Binary Sequence ]



[ Modified Transform Information ]

- Randomly generated binary sequence is saved as secret key.

**3.8 Embedding the Information**

In order to recover the secret image from the mosaic image, embed modified transform information into the mosaic image. For this, adopt a technique proposed by Coltuc and Chassery[8] and apply it to the least significant bits of the pixels in the created mosaic image to conduct data embedding. Unlike the classical LSB replacement methods, which substitute LSBs with message bits directly, the reversible contrast mapping method applies simple integer transformations to pairs of pixel values. Specifically, the method conducts forward and backward integer transformations as follows, respectively, in which (x, y) are a pair of pixel values and (x', y') are the transformed ones.

The method yields high data embedding capacities close to the highest bit rates and has the lowest complexity reported so far.

For each pair (x,y), The pixel values are transformed using the equation.  $x' = 2x - y$   $y' = 2y - x$ .

Now new pixel value is (x', y').



Secret Mosaic Image after Embedding Transform Information

With 8\*8 block size

Figure 3.15

**4 Extracting Secret Image**

**4.1 Extracting the Transform Information**

After Saving the LSB of  $y^l$  as recovery data.

The pixel values are transformed as

$$X = (2/3) * x^l + (1/3) * y^l$$

$$Y = (1/3) * x^l + (2/3) * y^l$$

So the original pixel value is recovered.

**Recovering the transform information from the secret key**

To get the original Transform Information extracted bit sequence is XOR operated with saved secret key

[Extracted Bit Sequence Using Reverse Contrast Mapping Algorithm]

XOR

[ Saved Secret Key ]

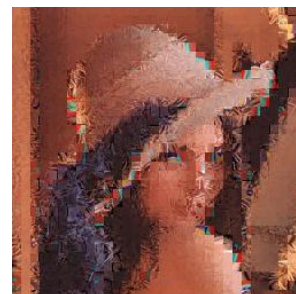
[ Transform information in binary form ]

**Transforming the binary information into decimal form**

[ Identifier  $\mu_R, \mu_R^l$  ( $SD_R^l / SD_R$ ) rotated information]

**4.2 Rearranging the blocks**

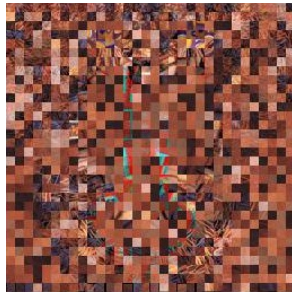
The secret image blocks are arranged according to the secret block identifier values



Secret Mosaic Image Before

Rearrangement of Blocks

Figure4.1



Secret Mosaic Image After  
 Rearrangement of Blocks

Figure 4.2

#### 4.3 Rotating the blocks

- The secret image blocks are rotated using rotating information

#### 4.4 Applying Reverse Transformation to the Blocks

- The color characteristics are transformed using the equation

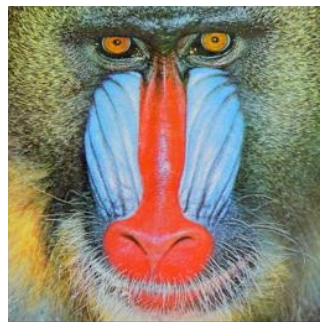
$$r_i = (q_c) (r_i^{\parallel} - \mu_R^{\parallel}) + \mu_R$$

$r_i^{\parallel}$  = its corresponding pixel value in the new secret image block

$r_i$  = a pixel value in retrieved secret image block

$\mu_r, \mu_r^{\parallel}, q_c$  from the saved information

- The secret image is extracted from mosaic image.



Secret Mosaic Image after Applying Color Transformation

Figure4.3

Secret Mosaic Image after Applying Color Transformation is same as the secret image

### 5. Result

Figures 5.1.1, Figure 5.1.2 are selected as secret image and target image with 256\*256 size



SecretImage(256\*256)

Figure 5.1.1



TargetImage (256\*256)

Figure51.2

Figure 5.1.3, Figure 5.1.4, Figure 5.1.5, and Figure 5.1.6 shows the secret image with each block sorted according to standard deviation in ascending order.

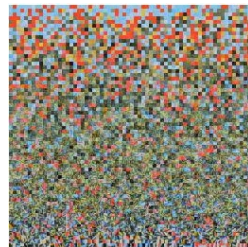
Here Figure 5.1.3, Figure 5.1.4, Figure 5.1.5, and Figure 5.1.6 are with 2\*2, 4\*4, 8\*8, 16\*16 block sizes respectively.



Sorted Secret Image with  
 BlockSize2\*2

Figure5.1.3





Sorted Secret Image with  
 Block Size 4\*4

Figure 5.1.4



Sorted Secret Image with  
 BlockSize8\*8

Figure5.1.5



Sorted Secret Image with  
 Block Size 16\*16

Figure 5.1.6

Figure 5.1.7, Figure 5.1.8, Figure 5.1.9, Figure 5.1.10 are secret mosaic images created after applying transformation to the secret image with block size 2\*2, 4\*4, 8\*8, 16\*16 respectively.

Here the results show that RMSE between target image and created secret mosaic image increases by increasing the block size.

Between Target Image And SecretMosaic Image	2*2 Block size	4*4 Block size	8*8 Block size	16*16 Block size
RMSE	7.89	15.92	24.99	36.96

MSSIM	0.912	0.824	0.658	0.435
-------	-------	-------	-------	-------



Secret Mosaic Image With 2\*2 Block

Rmse 7.89 Mssim 0.912

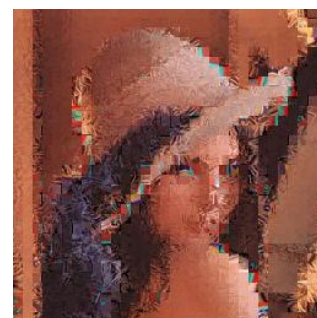
Figure 5.1.7



Secret Mosaic Image With 4\*4 Block

Rmse 15.92 Mssim 0.824

Figure 5.1.8



Secret Mosaic Image With 8\*8 Block

Rmse 24.99 Mssim 0.658

Figure5.1.9



Secret Mosaic Image With 16\*16 Block

Rmse 36.96 Mssim 0.435

Figure 5.1.10



Secret Mosaic Image After Rearrangement

With Block Size 2\*2

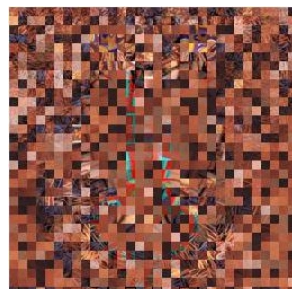
Figure 5.1.11



Secret Mosaic Image After Rearrangement

with Block Size 4\*4

Figure 5.1.12



Secret Mosaic Image After Rearrangement

with Block Size 8\*8

Figure 5.1.13



Secret Mosaic Image After Rearrangement

with Block Size 16\*16

Figure 5.1.14



Extracted Secret Image

Figure 5.1.15

The extracted secret image is same to the selected secret image.

## 6. Conclusion:

Unique image transmission method has been proposed, which not only can create meaningful mosaic images but also can transform a secret image into a mosaic one for use as a masquerade of the secret image.

By the use of proper pixel colour transformations secret mosaic images with very giant visual similarities to arbitrarily-selected target images can be created with no need of a target image database. Also, the primary secret images can be recovered nearly lossless from the created mosaic images. Good experimental results have shown the usefulness of the proposed method. Future studies may be directed to applying the proposed method to images of color models other than the RGB.

## References

[1] 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. 749–761, 2004. [2] 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. 759–765, 2005.

[3] 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. 1518–1529, 2007.

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

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

[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.

[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.

[8] 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.

[9] C. H. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution," *Pattern Recog.*, vol. 41, no. 8, pp. 2674–2683, 2008.

[10] Ya-Lin Lee and Wen-Hsiang Tsai "A New Secure Image Transmission Technique via Secret-Fragment-VisibleMosaic Images by Nearly Reversible Color Transformations" *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 4, pp. 695–703, Apr. 2014.

#### AUTHOR'S BIOGRAPHY



**Author1: A. Thirumala Rao** Pursued B.Tech with stream electronics and communication engineering from Pace Institute of technology and sciences, ongole JNTUKuniversity. Pursuing M.Tech with stream VLSI&ES from Pace Institute of technology and sciences, ongole JNTUKuniversity.



**Author2: Mr. N. Prakash Babu** working as associate professor in Pace Institute of technology and sciences, Ongole. He is having eight years of experience in teaching.



**Author3: Mr. M. Apparao** working as associate professor and also the Head of the Department in Pace Institute of technology and sciences, Ongole. He is having thirteen years of experience in teaching.