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

Archana S. Jagtap[1], Prashant S. Malge[2]

[1, 2]Department of M.E Electronics, Walchand Institute of Technology, Solapur University, Solapur, Maharashtra, India

Abstract:***Hiding the data in digital images has been area of interest in the digital image processing domain. Although so much work has been carried out in the literature to resolve the issues like increasing the data capacity, creating the secret image alike of target image but most of the works fails to meet the practical requirements. This paper presents an approach 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 need of a database. Where, this mosaic image generation has done by dividing the secret image into fragments and transforming their respective color characteristics into corresponding blocks of the target image. Usage of the Pixel color transformations helps to yield the lossless recovered image based on the untransformed color space values. Generation of the key plays an important role to recover the data from the secret image in lossless manner. So, only with the key, a person canrecover the secret image nearly lossless, from the mosaic image.Good experimental results show the feasibility of the proposed method.***

Keywords: Data Hiding, Color Transformation, Mosaic Image, Image Encryption, Secret Key, MSSIM.

1. Introduction

The rapid growth of internet usage over high bandwidth and low cost computer hardware has propelled the explosive growth of Covert communication using images.In the present year, secure and hidden communication is the foremost requirement of the people. Therefore covert communication is gaining attraction by people due to the security issues over internet.

Many times, images from various sources are frequently used and transmitted through the internet for different applications, such as online personal photograph albums, defense organization secret data circulation, confidential enterprise archives, document storage systems, medical images, patient details are embedded within image proving protection to information, and militaryimaging databases. As these image contain private and confidential information, they should be protected from leakages during transmissions. So, there is need of secure image transmission technique.

There are many methods have been proposed for securing image transmission, in that, two common approaches are image encryption and data hiding. Image encryption 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[2]-[3**]**. 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 noise image so attracts an attacker's attention during transmission. An alternative is data hiding[4]-[5]**,** 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 in this paper is an image. Existing data hiding methods mainly utilize the techniques of LSB substitution, histogram shifting, difference expansion, prediction-error expansion, recursive histogram modification, and discrete cosine/wavelet transformations[1].

A main issue of the methods for hiding data/image in image is to embed a large size or same sizeimage into an image. Specifically, if one wants to hide means, it needs that image must be highly compressed in advance. But, for many applications, where embedded images short information is also so valuable, there must notbe the allowance of serious distortions, in such image applications, compression operations are usually impractical. This paper present a new technique for secure image transmission, which transforms a secret image into a meaningful mosaic image with the same size and looking like a preselected target image. The proposed method is new in that a meaningful mosaic image is created, in contrast with the image encryption and data hiding. Generation of the key plays an important role to recover the data from the secret image in lossless manner. An appropriate information is embedded into the mosaic image for the recovery of the transmitted secret image [1] [2].

The rest of this paper organized as follows: Section 2 gives proposed method. Section 3 discusses mosaic image generation and secret image recovery ideas. Section 4covers the detailed algorithms for mosaic image creation and secret image recovery and Section. 5 gives experimental results and discussion Section. 6 discusses security consideration. Section.7concludes the paper.

2. Proposed Method

To get secure images irrespective of leakages, we need to be develop a system for covert communication and this is to be developed by following designed technique which is based on mosaic image and pixel color transformation.
The proposed method includes two main phases:
1) A secret-fragment-visible mosaic image creation.
2) Secret image recovery

In the first phase, a mosaic image is obtained by,1) fitting the tile images of the secret image into the target blocks of a freely selected target image; 2) transforming the colorcharacteristics of each tile images in the secret image to match corresponding target blocks in the target image; 3) rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block; 4) generating a key and encrypt the relevant information with that randomly generated key; 5) embedding encrypted information into the created mosaic image for future recovery of the secret image. Then second phase is recovering secret image. This phase includes three stages: 1) decrypt the received mosaic image using secret key 2) extracting the embedded information for secret image recovery from the mosaic image, 3) recovering the secret image using the extracted information.

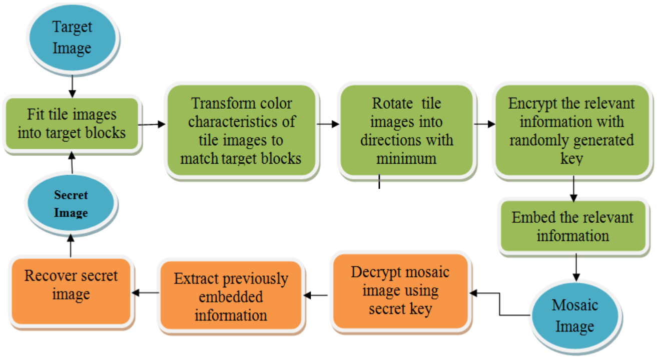

Target Image
Fit tile images into target blocks
Transform color characteristics of tile images to match target blocks
Rotate tile images into directions with minimum
Encrypt the relevant information with randomly generated key
Secret Image
Embed the relevant information
Recover secret image
Extract previously embedded information
Decrypt mosaic image using secret key
Mosaic Image

Figure 1: Flow diagram of proposed method

3. Discussion of Proposed Work

3.1 Mosaic Image Generation Ideas

3.1.1 Choosing appropriate target blocks for each tile images

A secret image is divideintotile images T as well as the target image intotarget blocks B. To obtain a better color similarity we need to transform color characteristics of tile images T in the given secret image,to that of a corresponding target block Bin a preselected target image. But, how to choose an appropriate Bfor each T,is an issue. For this, we use the standard deviation of the colors in the block as a measure to select the most similar Bfor each T. Specially, we sort all the tile images to form a sequence, S_{tile}, and all the target blocks to form another, $S_{target,}$ according to the average values of the standard deviations of the three color channels. Then, we fit the first in S_{tile}into the first in S_{target}, fit the second in S_{tile}into the second in S_{target}, and so on.

3.1.2 Transformation of color characteristics between Blocks

As obvious, the color characteristics of T and Bare different from each other, we need to change their color distributions to make them look alike. Let the Tand B are the blocks having pixel sets $p_i$and $p_i^{'}$. Let the color of each $p_i$be (r_i, g_i, b_i) and that of each $p_i^{'}$ be ($r_i^{'}$, $g_i^{'}$, $b_i^{'}$). Firstly, we compute the means and standard deviations of Tand B, respectively, in each of the three color channels R, G, and B by the following formulas:

$$\mu_c = \frac{1}{n}\sum_{i=1}^{n} c_i, \mu_c^{'} = \frac{1}{n}\sum_{i=1}^{n} c_i \quad '(1)$$

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n} \left(c_i - \square c\right)^2}, \sigma_c^{'} = \sqrt{\frac{1}{n}\sum_{i=1}^{n} \left(c_i{}' - \square c'\right)^2} (2)$$

Where, $c_i$and $c_i^{'}$denote the C-channel values of pixels p_i and $p_i^{'}$, respectively, with c= r, g, or band C = R, G, or B. The color transformation is done by, i.e. new color values ($r_i^{''}$, $g_i^{''}$, $b_i^{''}$) for each $p_i$in T givenby

$$c_i^{''} = q_c \left(c_i - \mu_c\right) + \mu_c \quad ' (3)$$

Where$q_c = \sigma_c^{'}/\sigma_c$is the standard deviation quotient and c= r,g, or b.

3.1.3 Rotate blocks with smaller RMSE value

After a target block Bis chosen to fit a tile image Tand after the color characteristic of Tis transformed, we conduct rotated version of T' with the minimum root mean square error (RMSE) value with respect to B,to get further improvement on the color similarity between the resulting tile image T' and the target block Bby rotating T' into one of the four directions, 0°, 90°, 180°, and 270°, for final use to fit Tinto B. By analysis, we must say that the obtained mosaic image is look similar to that of target image because, it can be verified easily that the new color mean andvariance of the resulting tile image T' are equal to those of B.

3.1.4 Embed the relevant secret image recovery information into obtained mosaic image

The information required to recover secret image fromreceived mosaic imageincludes: 1) the optimal rotation angle of T; 2) the means of T and B;and 3) the standard deviation quotients, of all color channels; these data itemsare integrated as a three-component bit stream of the form,

$$M = r_1 r_2 m_1 m_2 ... m_{48} q_1 q_2 ... q_{21} \qquad (4)$$

3.1.5 Total length of recovery information

The involved mean and standard deviation values are all real numbers, and it is impractical to embed real numbers, each with many digits, in the generated mosaic image. Therefore, we limit the numbers of bits used to represent relevant parameter values. Specifically, for each color channel we allow each of the means of Tand B to have 8 bits with its value in the range of 0 to 255, and the standard deviation quotient q_c to have 7 bits with its value in the range of 0.1 to 12.8. That is, each mean is changed to be the closest value in the range of 0 to 255, and each $q_c$is changed to be the closest value in the range of 0.1 to 12.8.

In more detail, the numbers of required bits for the four data items in *M* are discussed below: 1) it needs two bits to represent the rotation angle of T because there are four possible rotation directions; 2) 48 bits are required to represent the means of Tand Bbecause we useeight bits to represent a mean value in each color channel; 3) it needs 21 bits to represent the quotients of Tover Bin the three color channels with each channel requiring 7 bits. Then, the above-defined bit streams of all the tile images are concatenated in order further into a total bit stream M_t for the entire secret image, which is finally embedded into the pixel pairs in the mosaic image using the RCM (Reverse Contrast Mapping) technique.[6]

So, for one tile image we required to embed 71 bit length information and for entire secret image we requires:

Total Recovery bits have to embed= 71 bits * total no. of blocks in an image for entire secret image

Table 1: Total length of information embedded

Parameters	Values
Image resize to	768 * 1024
Divide image into blocks having block size	8 * 8
Each row having blocks	1024 \ 8 = 128
Each column having blocks	768\8 = 96
Total number of blocks	128 * 96 = 12,288
Embedding length of information for one block	71
Total length of information embedded	12,288 * 71 = 8,72,448

3.2 Ideas of Secret Image Recovery

The second phase specifically involves,
The embedded information we have to extract to recover nearly lossless the secret image from the generated mosaic image.

Here, we will have to do totally inverse procedure that we done in mosaic image creation.For extraction will use Inverse Reverse Contrast Mapping (Inverse RCM).

To compute the original color values (r_i, g_i, b_i) of p_i from the new ones (r_i'', g_i'', b_i''),we use the formula which is inverse form of previous used equation (3),

$$c_i = 1\backslash q_c (c_i'' - \mu_c') + \mu_c (5)$$

4. Algorithmic Flow

The algorithm for mosaic image generation and secret image recovery process are given below in detail as algorithm 1 and algorithm 2 respectively.

Algorithm 1: Mosaic image creation

Input: a secret image *S*, a target image T, and a secret key K
Output: a mosaic image F.

Stage 1. Fitting the tiles of secret images into the blocks of target images.

Step-1. Change the sizes of target image Tand secret image S and make them identical. (Here we resize both to 768*1024); and divide the secret imageinto *n* tile images as well as the target image into *n* target blocks with eachbeing of equal size. (Here each block and tile is of 8*8 size)

Step-2. Compute the means and the standard deviations of each tile image and each target block for the three color channels, and compute accordingly the average standard deviations for each individual of them.

Step-3. According to values of average standard deviation obtained, keeping it in ascending order, sort the tile images and the target blocks in separate sets.; map in order the blocks in the sorted tile setto those in the sorted target setin 1-to-1 manner; and re-order the mappings according to the indices of the target images, new sequence named as L.

Step-4. According to L, create a mosaic image Fby fitting the tile images into the corresponding target blocks.

Stage 2. Performing color conversions of tile images to that of target blocks.

Step-5. Create a counting tableTBwith 256 entries, each with an index corresponding to a residual value (where, each residual value will be in the range of 0 to 255), and assign an initial value of zero to each entry.

Step-6. For each mapping, represent the means of tile image and target block, present at that particular mapping point, respectively, by eight bits; and represent thestandard deviation quotient qc by seven bits, where c = r, g, or b.

Step-7. For each pixel $p_i$in each tile image $T_i$of mosaic image Fwith color value $c_i$where c= r, g, or b, transform $c_i$into a new value c_i'' by (3); if c_i'' is not smaller than 255 or if it is not larger than 0, then change c_i'' to be 255 or 0, respectively.

Stage 3. Rotating the tile images with minimum RMSE.

Step-8.Compute the RMSE values of each color transformed tile image $T_i$in Fwith respect to its corresponding target block B_{ji}after rotating $T_i$into each of the directions θ=0°, 90°, 180° and 270°; and fix the rotation of $T_i$into the optimal direction θ° with the smallest RMSE value.

Stage 4. Embedding recovery information.

Step-9.For each tile image $T_i$in mosaic image F, construct a bit stream $M_i$for recovering T_i, in the way as described in section 3.1.4, including the bit-segments which encode the data items of (4):

1) The optimal rotation angle θ° of T_i;
2) The means of T_i and B_{ji} and
3) The related standard deviation quotients of all three color channels.

Step-10. Concatenate the bit streams M_i of all $T_i$in Fina raster-scan order to form a total bit stream M_t; generate a random key and use this secret key Kto encrypt $M_t$into another bit stream M_t'; and embed M_t' into Fby the reversible contrast mapping scheme.

Step-11. Obtain the final form of a secret-fragment-visible mosaic image F.

Algorithm 2: Secret image recovery

Input: a mosaic image Fand the secret key K.
Output: the secret image S.

Stage 1. Extracting the recovery information.

Step-1. Extract the bit stream M_t' using the reverse version ofscheme (inverse Reverse contrast mapping) used in an encoding previously.

Step-2. Decrypt the bit stream M_t' into $M_t$by secret key K.

Step-3. Decompose $M_t$into nbit streams M_1 through $M_n$for the nto-be-constructedtile images T_1 through $T_n$in S, respectively.

Step-4. Decode $M_i$for each tile image $T_i$to obtain the following data items:
1) The optimal rotation angle θ° of T_i;
2) The means of $T_i$and $B_{ji}$and
3) The related standard deviation quotients of all color channels.

Stage 2. Recovering the secret image.

Step-5.Recover one by one in a raster-scan order the tile images, of the desired secret image Sby the following steps:
1) rotate in the reverse direction the block indexed by j_i, namely B_{ji}, in F through the optimal angle θ° and fit the resulting block content into T_i to form an initialtile image T_i;
2) Use the extracted means and related standard deviation quotients to recover the original pixel values in T_i according to (5).
3) Take the results as the final pixel values, resulting in a finaltile image T_i.

Step-6. Compose all the final tile images to form the desired secret image Sas output.

5. Experimental Results

5.1 Simulation Results

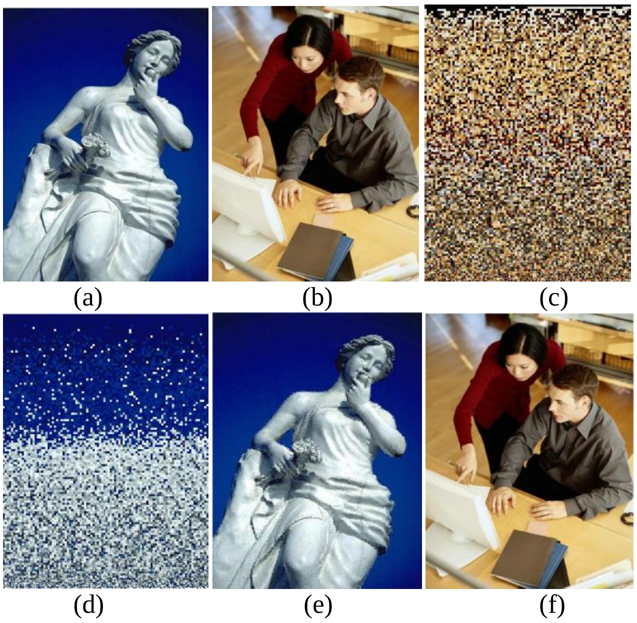
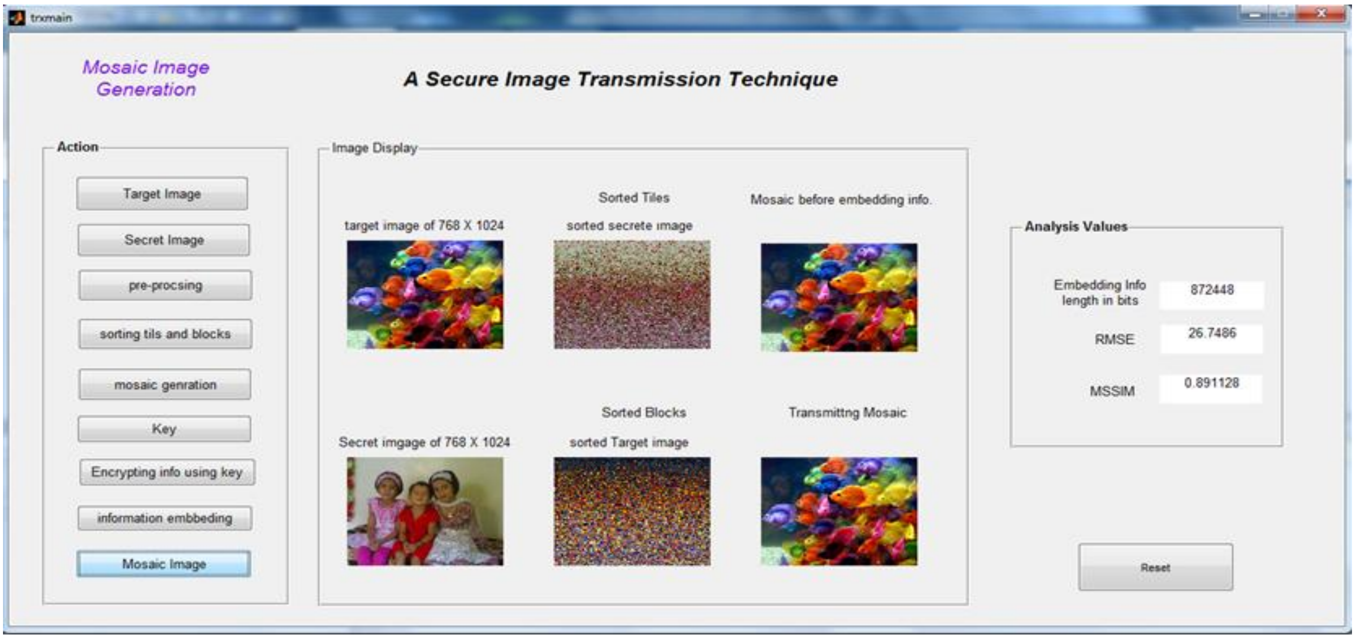


Figure 2: (a) Target Image (b) Secret Image (c), (d) Sorted secret and target imagesaccording to standard deviationwith tile image sizes 8 × 8.(e) Mosaic image formed after embedding the relevant information and encrypting which randomly generated secret key, with RMSE = 22.92203 with respect to target image (f) Recovered secret image using a correct key with RMSE = 2.56653 with respect to secret image (b)



Embedding Info length in bits 872448
RMSE 26.7486
MSSIM 0.891128

Figure 3: Simulation Results of Mosaic Image Generation

An experiments have been conducted to test the proposed method with image sizes 768 * 1024or 1024 * 768. To analyze, the created mosaic image or recovered secret image is look like a preselected target image or like original secret image, calculating the root mean square error (RMSE) which gives the square root of the mean square difference between the pixel values of the two images. By the way it is noted that other experimental results shows also the smaller RMSE as well. Also, metric of mean structural similarity (MSSIM) is used. It gives structural similarity between previous distortion-free image and resulted image. It is designed to improve on traditional methods like PSNR and actually RMSE too. It is proven to be inconsistent with human eye perception.

An example of the experimental results is shown in Figure. 2; Figure2(e) shows the created mosaic image with RMSE = 22.92203 and MSSIM = 0.8273 (with respect to target image), using Figure 2(b) as the secret image (original size = 528*385) and Figure 2(c) as the target image (original size = 600*400). Firstly, we are resized these secret and target images to 1024* 768. figure2 (c) and (d) are sorted secret and target images respectively, according to standard deviation of respective 8*8 tile and target blocks. The recovered secret image is shown in Figure 2(f) which look nearly similar to original secret image with RMSE = 2.56653.

Figure3 shows the simulation results of mosaic image generation. It gives another example wich are originaly size . of 768 * 1024. also figure 3. shown sorted secret and target image according to respective standartd deviation values of tiles and blocks, then created mosaic image before embedding the relevant information is dissplayed and final generated mosaic image (transmitting mosaic) after embedding relevent information wich encrypted with secret key is displayed. Analysis values like RMSE and MSSIM values of transmitting mosaic image with respect to target image are also displayed.

Figure4 shows the simulation results of secret image formation. It displyed first, the received mosaic image and then retrived secret image with RMSE = 2.76012 and MSSIM = 0.9968 with respect to original secret image.

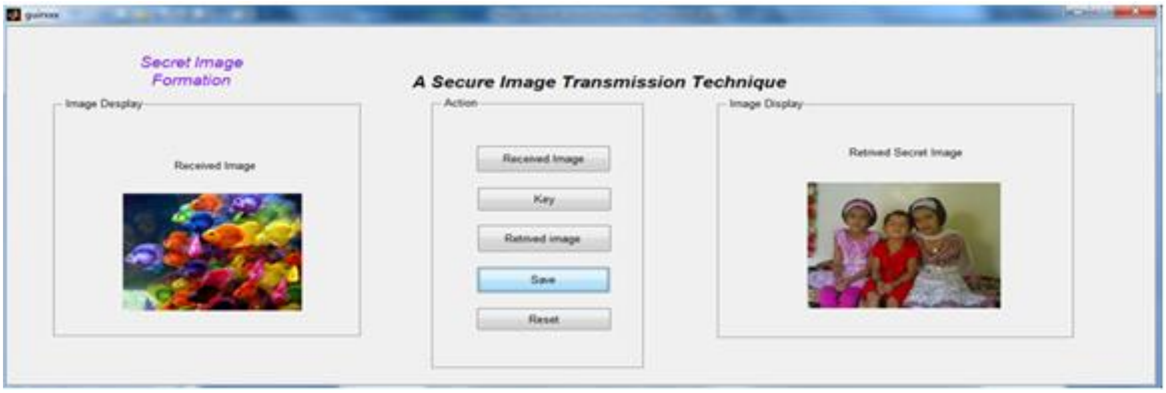


Figure 4: Simulation Results of Secret Image Formation

6. Security Consideration

To increase the security level, the embedded information for later recovery is encrypted with a secrete key.Only the receiver who has the correct key can decode the secret image.An eaves-droppermay try for all possible permutations of tile images in the mosaic image to get secret image back. Buthere the number of all permutations is n! So, the probability for his/herto guessthe correct permutation is p=1/n!, which is very small in value.So, as large value of *n* should be used to increase the security of the proposed method. Furthermore, even if one happens to guess the permutation correctly, still he/she still does not know the correct parameters for recovering the original color appearance of the secret image as those parameter information for color recovery is encrypted as a bit stream using a secret key. In the extreme case, if he/she will observe the content of the mosaic image with correct permutation, we again used the key to randomize important information of a secret image, before transforming the secret image into a mosaic image. So finally, only an authorized users with the key can know the correct secret image while an attacker can't.

7. Conclusion

As hiding the data in digital images has been area of interest in the digital image processing domain, there is requirement of highly secure transmission technique. The proposed method can be taken as a strong technique for secure image transmission as the method creates a new type of art image for hiding the secret image. By the use of proper pixel color transformations, mosaic images with very high visual similarities to arbitrarily-selected target images is created with no need of a target image database or without any type of compression. Also, the original secret images can be recovered nearly lossless from the received mosaic images. Again, lossless recovery of secret image is achieved byusage of the Pixel color transformations based on the untransformed color space values. In lossless recovery of thesecret data from the secret image, key plays an importantrole.Good experimental results shows the feasibility of the proposed method.

8. Acknowledgments

We would like to take this opportunity to thank one and all who have provided their valuable advice, without their guidance this work would not have been a success, we have to thank who have helped us directly or indirectly since they have given us more than just guidance.

Our profound thanks to **Dr. S. R. Gengaje**, Head of the Department, Department of Electronics Engineering, Walchand Institute of Technology, Solapur, for his valuable advice and constant encouragement to complete this work in a successful manner.

I would like to convey our sincere thanks to management and supportive staff of Walchand Institute of Technology, Solapur, for encouraging us to come up with this paper work.

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.

Author Profile

ArchanaS. Jagtap hasreceived the B.E. degrees in Electronics and Telecommunication Engineering from Brahmadev dada Mane Institute of Technology, Solapur, in 2013. Currently she is pursuing Master in Engineering from Walchand Institute of Technology Solapur, in Electronics branch. Her area of interest is computer vision, Image processing and Mobile communication.

Prashant S.Malge received his B.E. and M.E degree in Electronics Engineering from Shivaji University, Kolhapur, Maharashtra, India in 1990 and 2007 respectively. Currently, He is an Assistant Professor, with Department of Electronics Engineering, Walchand Institute of Technology, Solapur, Maharashtra, India. At present, pursuing Ph.D from Deparment of Electronics & Telecommunication Engineering SGGSIE&T, Nanded, Maharashtra, India. His research interests include VLSI architectures for image processing and Signal Processing.