



A Novel Approach for Secure Image Transmission Based on Secret-Fragment- Visible Mosaic Images

Sriram B Sriraksha B.G Ashwini S. Savanth

B.E Student, Department of TCE, BNMIT, Bangalore, India

B.E Student, Department of TCE, BNMIT, Bangalore, India

Assistant Professor, Department of TCE, BNMIT, Bangalore, India

ABSTRACT: The transfer of images from one entity to another using the internet as the medium of transfer is increasing at a rapid pace and hence the applications of digital image processing have become more widespread. Digital image transmission technology has found advanced applications in various fields where security is of paramount importance. Examples of such applications include business databases, medical databases and confidentiality of patient records, online document storage systems, military databases, etc. Although a lot of research has been done on secure image transmission, several issues still remain unresolved. In this paper, a new secure image transmission technique is proposed, which transforms automatically a given large-volume secret image into a so-called secret-fragment-visible mosaic image of the same size. The mosaic image, which looks similar to an arbitrarily selected target image and may be used as a camouflage of the secret image, is yielded by dividing the secret image into fragments and transforming their color characteristics to be those of the corresponding blocks of the target image. The information required for recovering the secret image is embedded into the created mosaic image by a lossless data hiding scheme using a key. The feasibility of the proposed method is supported with good experimental results.

KEYWORDS: Mosaic image, image security, color transformations, image encryption, data hiding, lossless

I. INTRODUCTION

Image transmission through the internet is very common in various applications, such as medical imaging systems, online personal photograph albums, document storage systems, confidential enterprise archives and military image databases. These images most of the time contain private or confidential information so it is important to protect them from leakages during transmissions. Image encryption and data hiding are the two most common approaches among the many methods proposed for secure image transmission. Image encryption is a technique that makes use of some of property of an image, such as strong spatial correlation and high redundancy to get an encrypted image based on Shannon's confusion and diffusion properties [2]. It transforms an image into a cryptic image using a key. The encrypted image looks like a noise image in order that it is not possible to obtain the secret image from it unless there is the correct key. This file does not provide any additional information before decryption. Its randomness may arouse an attacker's attention during transmission. Data hiding can be an alternative to avoid this problem. In this process a secret message is hidden into a cover image and the existence of secret data will not be obvious. Data hiding methods which have been proposed so far have utilized techniques such as the most common LSB substitution, histogram shifting, recursive histogram modification etc. [3]. In order to reduce the distortion of the resulting image, an upper bound for the distortion value is set on the payload of the cover image. Thus, an issue of concern in the data hiding methods is the difficulty to embed a large amount of message data into a single image. Specifically, if the secret image is of the same size as the cover image, then the secret image must be highly compressed beforehand in order to hide it in the cover image. However, for several applications, like medical images, military images, legal documents, etc., that are valuable with preferably no distortions, such data compression operations are practically not possible.

In this paper, a technique is proposed for a secured image transmission, where a secret image is first converted to a meaningful mosaic image which is of the same size and looks similar to a target image that has been selected. A secret



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

key controls the transformation process, and it is possible to recover the secret image from the mosaic image in an almost lossless manner, only with the help of the key. The proposed method is inspired by the work of Lai and Tsai [4], where a new type of computer art image was proposed called secret-fragment-visible mosaic image. The mosaic image is obtained by the rearrangement of the fragments of a secret image in disguise of another image called the target image which has been selected from a database. But a disadvantage of the method proposed by Lai and Tsai is the need for a large image database in order that the generated mosaic image can be very similar to the selected target image. With this method, there is no freedom to select a favourite image for use as the target image. In the proposed method an attempt is made to remove this drawback while keeping its merit. The aim here is to design a new method that converts a secret image into a mosaic image which is of the same size and has the visual appearance of target image which is selected freely without the need of a database.

The remaining part of the paper is organized as follows: a brief survey of literature is presented in section 2, followed by the methodology in section 3, section 4 gives the algorithm of the proposed method in brief. Experimental results and analysis performed are given in section 5, followed by conclusion and future scope in section 6.

II. RELATED WORK

J. Lai and W. H. Tsai proposed a new method for secure image transmission which involved creating a new type of image known as secret-fragment mosaic image. This image is created by composing small blocks of a confidential image to form a mosaic image that looks like a preselected target image selected from a target image database. This method is proposed for securing color images and also extended to create grayscale mosaic images. Lin-Yu Tseng, Yung-Kuan Chan, Yu-An Ho and Yen-Ping Chu proposed an image hiding technique using an optimal pixel adjustment process in the year 2008 [5]. In this technique, each pixel in the confidential image is disarranged and adjusted to make a suitable sequence of bits that can be embedded. Then these bit sequences are embedded into the target image in corresponding locations, and resulting image would become a stego-image that hides the confidential image. Sara Sajasi, Amir Masoud and Eftekhari Moghadam proposed a high quality image hiding scheme using an optimal chaotic based encryption method in the year 2013 [6]. In this technique, the payload of each region of the target image is determined to improve the visual quality of the image. The payload is determined based on the Noise visibility function (NVF). Then, an optimal chaotic based encryption method is used to convert the secret image into an encrypted image. The encryption is done using the optimal secret key generated by using GA/PSO algorithm. Cheng-Hsiang Yeh, Ching-Tang Hsieh, Kuo-Ming Hung and Li-Ming Chen proposed an image hiding method based on multilevel histogram modification and halftoning technique in 2011 [7]. In this technique, the data embedding and extracting process is done by applying multilevel histogram modification. The halftone data is extracted from the stego image and the confidential image is obtained using LUT inverse halftone method. This method provides high embedding capacity at low distortion level.

III. METHODOLOGY

In the proposed method, a target image is first selected arbitrarily. The given secret image is divided into rectangular portions called tile images. By using a similarity criterion based on color variations, these tile images are fitted into similar blocks in the target image, called target blocks. Next, the color characteristics of each tile in the secret image 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 [12]. In order to recover the original secret image in a nearly lossless manner from the resulting mosaic image relevant schemes are proposed. In comparison to the image encryption methods which create meaningless noise images, this proposed method is new in the sense that a meaningful mosaic image is created. Also, the proposed method creates a disguising mosaic image without using compression as compared to the other data hiding methods which require a highly compressed secret image to hide in the cover image.

The proposed method is shown in the form of a flow diagram in fig 1. It has two main phases: 1) mosaic image creation, and 2) secret image recovery. In the first phase, taking the fragments of the input secret image with color corrections according to a similarity criterion based on color variations, a mosaic image is formed. The phase includes four stages: (i) Fitting the tile images of the secret image into the target blocks of a preselected target image, (ii) Transforming the color characteristic of each tile image in the secret image to be that of the corresponding target block in the target image, (iii) Rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block, and (iv) Embedding relevant information into the created mosaic image for future

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

recovery of the secret image. In the second phase, the embedded information is extracted to recover nearly losslessly the secret image from the generated mosaic image. The phase includes two stages: (i) Extracting the embedded information for secret image recovery from the mosaic image, and (ii) Recovering the secret image using the extracted information.

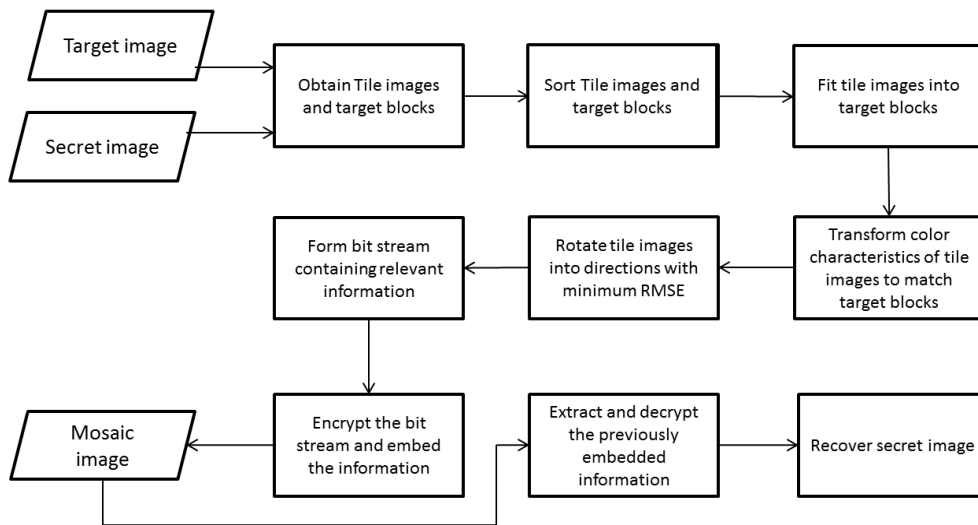


Fig1: Flow Diagram of the proposed method

IV. ALGORITHM OF THE PROPOSED METHOD

The proposed method is implemented in three stages: 1) mosaic image creation, 2) embedding necessary information, and 3) secret image recovery. The algorithms related to the three stages are discussed in this section.

Algorithm 1: Mosaic image creation

Input: Target image T and secret image S

Output: Secret-fragment-visible mosaic image formed before embedding M

Stage 1: *Fitting the tile blocks of secret image into the target blocks*

Step 1: Given a secret image S and a target image T, resize both the images to an equal size and divide the secret image S into n tile blocks $\{T_1, T_2, T_3, \dots, T_n\}$ and the target image T into n target blocks $\{B_1, B_2, B_3, \dots, B_n\}$ where the size of each B_i or T_i is N_T .

Step 2: Compute the means and standard deviations of each tile block T_i and target block B_j for the R, G and B color channels respectively according to (1) and (2). Accordingly, compute the average standard deviation of the three color channels for T_i and B_j respectively.

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

$$\sigma_c = \sqrt{\frac{1}{n} \sum_{i=1}^n (c_i - \mu_c)^2}, \quad \sigma_{c'} = \sqrt{\frac{1}{n} \sum_{i=1}^n (c_i' - \mu_{c'})^2} \quad \dots(2)$$

Step 3: Sort all the tile blocks in the set S_{tile} and the target blocks in the set S_{target} according to the average standard deviation values of the blocks. Map in order the sorted tile blocks to those in the sorted target blocks in a one-to-one manner.

Step 4: Form a secret-fragment-visible mosaic image M by fitting the tile blocks into the corresponding target blocks according to the mappings in step 3.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Stage 2: Color transformations between Tile blocks and target blocks

Step 5: For each mapping $T_i \rightarrow B_{ji}$, represent the means μ_c and μ_c' of T_i and B_{ji} , respectively, by 8 bits and the standard deviation quotient q_c by 7 bits.

Step 6: For each pixel p_i in each tile block T_i of mosaic image M with color value $c_i = R, G$ or B , transform c_i into a new value c_i' according to (3).

$$c_i'' = q_c(c_i - \mu_c) + \mu_c', \dots(3)$$

Stage 3: Optimum rotation of tile blocks

Step 7: Compute the RMSE values of each color transformed tile image T_i in M with its corresponding target block B_{ji} after rotating T_i into each of the directions $\theta = 0, 90, 180$ and 360 degrees and find the optimum rotation θ_0 with minimum RMSE.

Step 8: Rotate each tile block into its optimum rotation angle θ_0 as found in step 7.

Algorithm 2: Embedding necessary information

Input: Secret key K , mosaic image formed before embedding M

Output: Secret-fragment-visible mosaic image formed after embedding F

Step 1: For each tile block T_i in M , construct a bit stream M_i for recovery of T_i as described previously, including bit segments containing 1) the index of target block B_{ji} , 2) optimal rotation angle θ_0 , and 3) the means and related standard deviation quotients of T_i and B_{ji} .

Step 2: Concatenate the bit streams M_i of all T_i to form a total bit stream M_t .

Step 3: Encrypt M_t into another bit stream M_t' using secret key K and embed M_t' into M by the proposed method of Reversible contrast mapping [13].

Step 4: Construct a bit stream I that includes the number of conducted iterations N_i and the number of pixel pairs used in the last iteration.

Step 5: Embed the bit stream I into mosaic image F using the same method used in step 3.

Algorithm 3: Secret image recovery

Input: Secret-fragment-visible mosaic image formed after embedding F

Output: Secret image S

Stage 1: Extracting information for secret image recovery

Step 1: Extract the bit stream I from F by a reverse version of the method proposed in [13] and decode them to obtain the number of conducted iterations and the number of pixel pairs used in the last iteration.

Step 2: Extract the bit stream M_t' using the decoded values obtained in step 1.

Step 3: Obtain M_t by decrypting M_t' using secret key K .

Step 4: Decompose M_t into n bit streams for the n to-be-constructed tile blocks of S .

Step 5: Decode M_i for each tile block T_i to obtain 1) the index of target block B_{ji} , 2) optimal rotation angle θ_0 , and 3) the means and related standard deviation quotients of T_i and B_{ji} .

Stage 2: Recovering the secret image

Step 6: Recover the tile blocks T_i one by one by the following steps: 1) Rotate the block B_{ji} indexed by j through the optimal angle θ_0 and fit the resulting block into T_i to form an *initial* tile image T_i ; 2) use the extracted means and standard deviation quotients to recover the original pixel values in T_i ; and 3) take the results as the final pixel values to get *final* tile image T_i .

Step 7: Compose all the final tile images T_i , $i=1$ to n , to form the secret image S .

V. EXPERIMENTAL RESULTS AND ANALYSIS

A series of experiments have been conducted to test the proposed method using many secret and target images with different image sizes of 1024×768 , 512×512 and 256×256 . To show that the created mosaic image looks like the

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

preselected target image, the quality metric of root mean square error (RMSE) and peak signal to noise ratio (PSNR) is utilized.

An example of the experimental results is shown in Fig. 2; Fig. 2(c) shows the created mosaic image using 2(a) as the secret image and 2(b) as the target image. The tile image size is 8×8 and the image sizes are 1024×768 . The recovered secret image using a correct key is shown in Fig. 2(d) with $RMSE = 0.948$ with respect to the secret image. 2(e) shows the recovered secret image using a wrong key, which is a noise image.



(a) Secret image (b) Target image (c) Mosaic image (d) Recovered secret image (e) Recovered secret image using wrong key
Fig2: Experimental results for image size 1024×768 and tile size 8×8

Figure 3 shows mosaic images yielded for different sizes of the same secret and target images used in example 2. The mosaic images obtained for secret and target images of sizes 1024×768 , 512×512 , 256×256 and 128×128 are shown in figures 3(a), 3(b), 3(c) and 3(d) respectively.

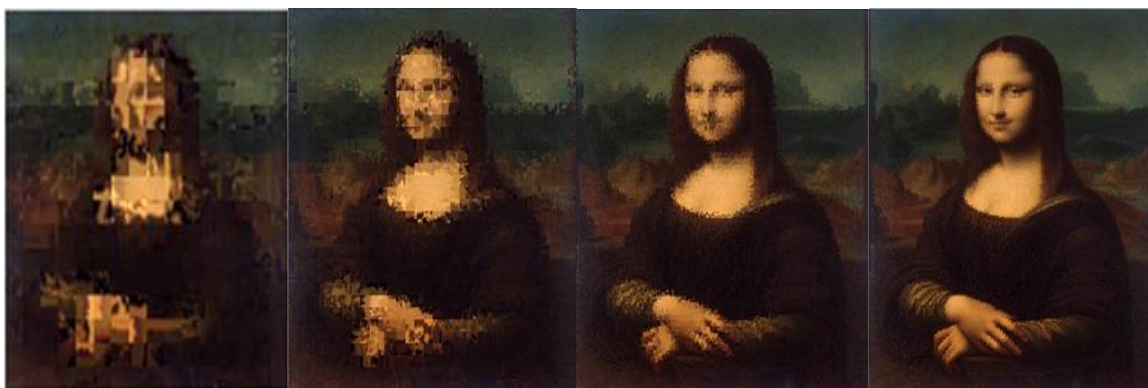


Fig 3: Mosaic images obtained for different image sizes (a) 128×128 (b) 256×256 (c) 512×512 (d) 1024×1024

In the previous examples, the block size was kept constant at 8×8 while the image size was varied. In the next example, the image size of secret and target images were kept constant at 1024×768 and the block size was varied. Figure 4 shows the results obtained for different block sizes of 8×8 , 16×16 , 24×24 and 32×32 for a given secret image and target image of size 1024×768 . It can be seen from the figures that the created mosaic image retains more details of the target image when the block size is smaller. On the other hand, the number of required bits embedded for recovering the secret image will be increased when the tile size becomes smaller.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

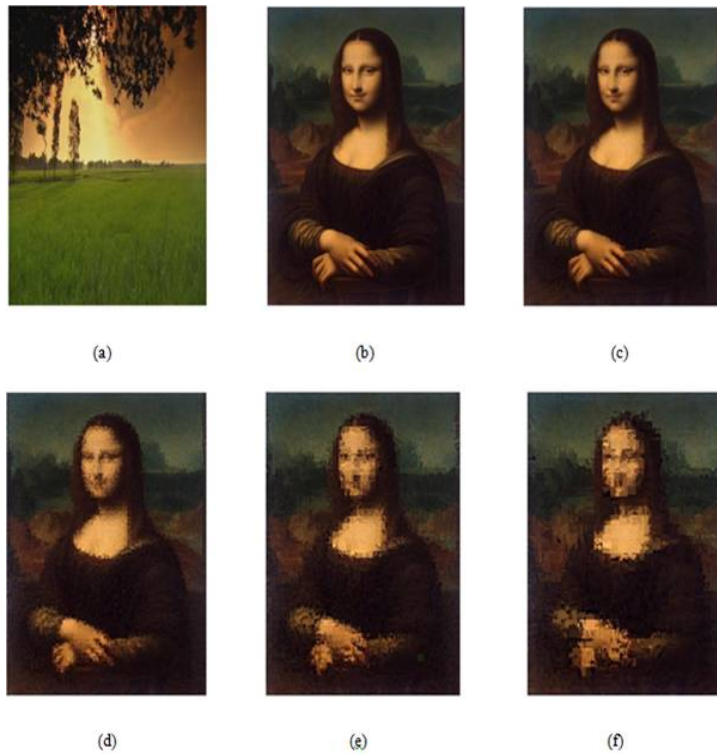


Fig 4: Experimental results for different block sizes (a) secret image (b) target image (c)-(f) Mosaic Images Created Using block sizes 8x8,16x16,24x24,32x32

A. Performance Measures

1) *Root Mean Square Error (RMSE)*: Root mean square error (RMSE) is defined as the square root of the mean square difference between the pixel values of the two images. To analyse the performance of the proposed method, plots of RMSE for target image v/s mosaic image and secret image v/s extracted image was computed for different block sizes. It is seen that the RMSE increases with block size and the minimum RMSE was obtained for block size 8x8. Figure 5 shows the RMSE plots obtained for a given secret and target image of size 512x512.

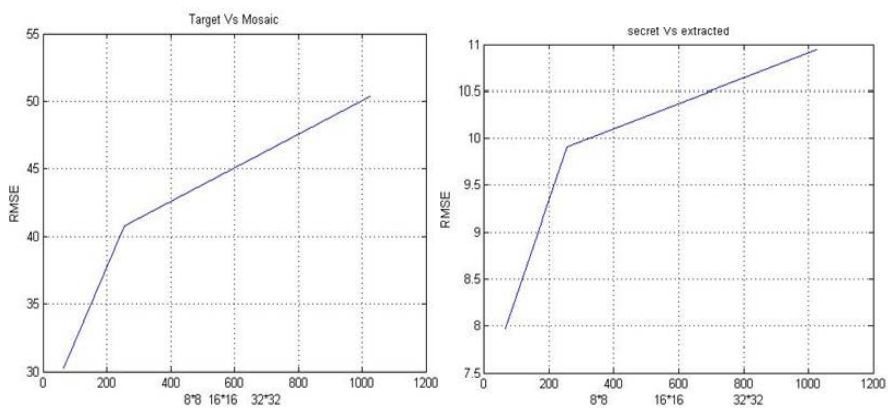


Fig 5: RMSE Plots for different block sizes (a) Target image v/s mosaic image (b) Secret image v/s extracted image

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

2) *Peak Signal To Noise Ratio (PSNR)*: Peak signal-to-noise ratio (PSNR) is defined as the ratio of the maximum possible value (power) of a signal to the power of distorting noise that affects the quality of its representation. PSNR can be used as an efficient quality metric to assess performance in image processing. To analyse the performance of the proposed method, PSNR was computed for the created mosaic image versus the target image for different block sizes and the results were plotted and is shown in Figure 6. It can be seen from the figure that the PSNR decreases when the block size increases and the PSNR is maximum for block size 8x8 and minimum for block size 32x32.

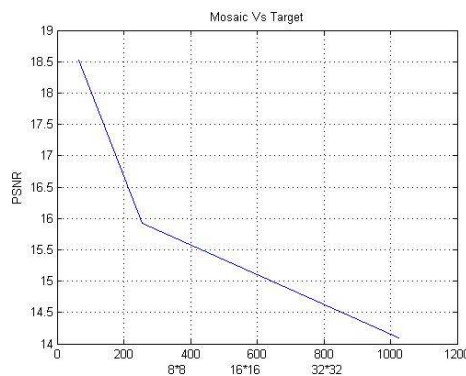


Fig 6: PSNR of Mosaic v/s Target image for Block sizes 8x8, 16x16 and 32x32

The RMSE and PSNR values obtained for different pairs of secret and target images of size 256 x 256 are tabulated in table 1. The PSNR and RMSE values are shown for two different block sizes of 8x8 and 16x16 and 32x32. To summarize the results, it is seen that the RMSE increases when the block size increases and PSNR decreases when the block size increases. The quality of the created mosaic image increases when the image size is increased and vice versa. Hence, the best results for the proposed method are obtained when the block size is kept minimum and the image size is kept maximum.







Target Image	Secret Image	8x8		16x16		32x32	
		RMSE	PSNR	RMSE	PSNR	RMSE	PSNR
		27.47	19.35	33.59	17.61	37.89	15.8
		32.21	17.98	40.74	15.93	45.65	12.34
		19.36	22.39	26.91	19.53	39.32	17.65

Table 1: RMSE and PSNR values for different sets of secret and target images



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

VI. CONCLUSION

A new secure 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 with the same data size for use as a camouflage of the secret image. By the use of proper pixel color transformations as well as a skilful scheme for handling overflows and underflows in the converted values of the pixels' colours, secret-fragment visible mosaic images with very high visual similarities to arbitrarily-selected target images can be created with no need of a target image database. Also, the original secret images can be recovered nearly losslessly from the created mosaic images. Good experimental results have shown the feasibility of the proposed method.

Future studies may be directed in applying the proposed method to images of color models other than the RGB such as HSI or YCbCr. Another research direction can be the application of the proposed method to video, where a video frame is used as a target image which further increases the image security.

REFERENCES

- [1] Lee, Ya-Lin, and Wen-Hsiang Tsai, "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* 24, no. 4: 695-703,2014
- [2] Oad, Ambika, Himanshu Yadav, and Anurag Jain, "A Review: Image Encryption Techniques and its Terminologies." *International Journal of Engineering and Advanced Technology(IJEAT)* ISSN: 2249-8958,2014
- [3] Mishra, Minati, Priyadarsini Mishra, and M. C. Adhikary. "Digital Image Data Hiding Techniques: A Comparative Study." ARXIV PREPRINT ARXIV: 1408.3564,2014.
- [4] Lai, I-Jen, and Wen-Hsiang Tsai. "Secret-Fragment-Visible Mosaic Image–A New Computer Art And Its Application To Information Hiding." *Information Forensics and Security*, IEEETransactions ON 6, NO. 3: 936-945,2011.
- [5] Tseng, Lin-Yu, Yung-Kuan Chan, Yu-AnHo, and Yen-Ping Chu. "Image Hiding With An Improved Genetic Algorithm And An Optimal Pixel Adjustment Process." In *Intelligent Systems Design and Applications*, . ISDA'08. Eighth International Conference On, Vol. 3, PP. 320-325. IEEE, 2008.
- [6] Sajasi, Sara, and Amir-Masoud Eftekhari-Moghadam. "A High Quality Image Hiding Scheme Based Upon Noise Visibility Function and an Optimal Chaotic Based Encryption Method." In *Ai & Robotics and 5th Robocup Iran Open International Symposium (Rios), 3rd Joint Conference Of*, PP. 1-7. IEEE, 2013.
- [7] Yeh, Cheng-Hsiang, Ching-Tang Hsieh, Kuo-Ming Hung, and Li-Ming Chen. "Reversible Digital Image Hiding Based On Multilevel Histogram Modification And Halftoning Technique." *IEEEInternational Conference on Systems, Man, and Cybernetics*. 2011.
- [8] Hastings, G. D., and A. Rubin. "Color Spaces-A Review of Historic and Modern Color Models*." *African Vision and Eye Health* 71, no.3:133-143,2012.
- [9] Toony, Zahra, and Mansour Jamzad. "A Novel Image Hiding Scheme Using Content Aware Seam Carving Method." in *Availability, Reliability, and Security, 2010. Ares'10 International Conference on*, PP. 702-707. IEEE, 2010.
- [10] Zhang, Yonghong. "Digital Image Hiding Using Curvelet Transform." In *Computer Science and Automation Engineering (CSAE),IEEEInternational Conference ON*, VOL. 4, PP. 488-490. IEEE, 2011.
- [11] Ye, Ruisong, Wei Zhou, and Haiying Zhao. "An Image Hiding Scheme Based On 3d Skew Tent Map and Discrete Wavelet Transform." In *Computational and Information Sciences (ICCIS), 2012 Fourth International Conference on*, PP. 25-28. IEEE, 2012.
- [12] Reinhard, Erik, Michael Ashikhmin, Bruce Gooch, and Peter Shirley. "Color Transfer between Images." *IEEEComputer Graphics And Applications* 5 : 34-41,2001
- [13] Coltuc, Dinu, and Jean-Marc Chassery. "Very Fast Watermarking By Reversible Contrast Mapping." *Signal Processing Letters, IEEE* 14, NO. 4 : 255-258,2007.