SECRET IMAGE TRANSMISSION THROUGH MOSAIC IMAGE

Shahanaz N and Greeshma R

Department of Computer Science and Engineering,
M Dasan Institute of Technology, Kozhikode, India

ABSTRACT

A secret image hiding scheme is proposed with new security features. This scheme utilizes the mosaic images, which is created from the secret and target images. A mosaic image is similar to that of the target image. The secret image fragments are hidden in the target image by performing appropriate color transformations. The inverse color transformation is performed for the lossless recovery of secret image. The color transformation is controlled by the proper overflow /underflow methods. The relevant information for recovering the secret image is embedded in the mosaic image by a lossless data hiding with the help of a key. Only with the proper key, the secret image is retrieved from the mosaic image

KEYWORDS

Image hiding, Mosaic images, Color transformation, Data hiding, Image encryption

1. INTRODUCTION

In the present world, enormous data are transmitted over networks around the clock and the security of the data is the major concern. By the boom of web, a large sort of data are being exchanged between devices, which may fall into different categories like images, audio, video, hypertext, graphics etc. Among these images play an important role. Various applications which are dealing with image data are business archives, medical images, space and research related graphics, confidential enterprise archives, document storage systems, and military image databases and so on. These images usually contain private or confidential information so that they should be protected from fraudulent access 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 makes use the Shannon diffusion confusion process. Here the natural properties like spatial correlation and data redundancy are utilized.[1][7]. These are mainly Chaos based algorithms which controls the encryption with variety of parameters like ergodicity , initial condition. When using the 3D cat maps [2] for encryption the statistical and gray code attacks are avoided due to the large key space. But it cannot resist the brute force attack. The pseudo random substitution and permutation [6] using standard map overcomes the brute force attack and chaos specific attacks. The computational complexity is the main issue. The encryption using Henon

Brajesh Kumar Kaushik et al. (Eds) : CCNET, CSIP, SCOM, DBDM - 2017
pp. 23– 32, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.70503

Chaotic map [7] provides a lossless recovery and easy implementation. Randomness is the result of all these Chaos based methods. But this makes the attraction of the eavesdroppers while in the transmission. An alternative is used for avoiding this problem that is data hiding [8][14]. In these types of approach a cover image is used for hiding the secret data. Any one cannot realize the existence of secret data in this cover image. Existing data hiding methods mainly utilize the techniques of LSB substitution [], histogram shifting [9], difference expansion [10], prediction-error expansion [13]. When using LSB substitution [8] the quality of stego image may loss depending bits substituted. The histogram shifting [9] method cannot provide security for the data embedding. Thus, a main problem 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.

Some of the methods that are similar to the proposed method are [15][19]. The mosaic images play an important role in these methods. Mosaic [21] is a kind of art in which small pieces of material such as glass, stone are composed together to form a single image. In digital form small fragments of images called as tiles are arranged to form a single image called as mosaic. Creation of mosaic by computer is a new research area now a day. Different mosaics can be created from a single image depending on their choice of tiles and their placement in resulting image. There are different types of mosaic that includes crystallization mosaic, ancient mosaic that are created by dividing the secret image into tiles and then reconstructing the image by properly painting the tiles so these types of mosaic can also be called as tile mosaic.

Other types of mosaic includes photo-mosaic, and puzzle image mosaic that are formed by painting or covering the given sources image by fitting different images from the database hence they can also be called as multi-picture mosaic image. A special kind of mosaic include secret fragment visible mosaic image that are created by dividing secret image into small fragments called as tiles and then arranging these tiles in a random or puzzled sequence with the help of another image called as carrier image. The resultant mosaic is such that all fragments of secret image are visible to user but as they are arranged in puzzled form no one will be able to guess or read the contents of secret image.

In [15] create a mosaic image using the preselected target from the database and secret image. But here keeping the large database makes the process very complex and the user is not free to select the target image as his/ her own wish. A genetic, algorithm [16] based method is proposed and use the pseudorandom permutation [20] to create the mosaic image. The fitting information is embedded in the mosaic image then extracted the for the recovery of the secret image. Here the user is free to select the target image, but the genetic algorithm feature makes the process complex. An Enhanced Image Steganography Technique in Art Images [17] is used for creating mosaic images. In this approach first create cubism like image from the target image and then divide each secret and target to form the mosaic image by computing the matching score of secret tiles with that of target.

A new scheme is introduced in which the user is free to select the target image of his/her own wish. The created mosaic image looks similar to that of target image selected. The secret image retrieval is done perfectly.

In the proposed method two phases are there. In the first phase the secret and target image are divided in to tiles and blocks respectively. The fitting is done based on the standard deviation of

each tile and block, while performing the appropriate colour transformation and rotating each tile with respect to lowest RMSE value. Thus mosaic image is created. Then embed the relevant information. In the second phase the recovery information is extracted and inverse colour transformation is done. Then the secret image is recovered.

The following sections, In Section 2 introduce proposed method and presents necessary algorithms used by the proposed method. Section 3 explains the implementation details. In section 4 relates the results and discussions. Conclusion are summarised in section 5. Last section contains the papers, books, referred during the preparation of this paper.

2. PROPOSED METHOD

The overview of the proposed system is shown in Fig.1. The proposed method includes two main phases.1) mosaic image generation and 2) secret image recovery.

In the first phase a mosaic image is generated, which consists of the fragments of an input secret image with modified color properties that of target selected. In this phase 1) fitting of the secret tiles into target blocks, 2) transforming color characteristics of each tile image in the secret image to become that of the corresponding target block in the target image;3) rotating extracted to recover the secret image losselessly. The phase includes two stages: 1) extracting the embedded each tile image to find the maximum match with target with respect to smallest RMSE value.; and 4) embedding relevant information in to the mosaic image for the future recovery of the secret image.

In the second phase the embedded information is information for secret image recovery, and 2) recovering the secret image using the extracted information.

For the first phase we give two input images secret and target. A key can also be used to assure the security purpose. If the key is correctly decrypted then only the secret image is recovered. The output of this phase is a mosaic image with embedded information

For the next phase the input is a mosaic image and a key. Performing the decryption and decoding step by step the information needed to recover secret image is gathered. Thus the output of this phase is the secret image.

Algorithm 1 Mosaic image generation

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

Stage 1.Fitting the tile images into the target blocks.

1. Divide the secret image in to tile image fragments and target in to blocks up to n.

2. Compute the mean and standard deviation of each tile and blocks.

3. Sort the tiles images and the target blocks according to the computed standard deviation and create a hash map.

4. Create a blank image and fit the first block from the target in that and again fit the secret tile up to n with respect to the mean and standard deviation calculated.

Stage 2. Performing color conversions between tile images and the target blocks.

5. Based on the mean, standard deviation, standard deviation quotient transform the color of each pixel in the tile image.

Stage 3. Rotate tile images.

6. Compute the RMSE values of each color transformed tile image with respect to its corresponding target block after rotating in to each of directions Θ =0˚,90˚,180˚ and 270˚ with smallest RMSE value.

Stage 4. Embedding the secret image recovery information.

7. Construct Huffman table using the mapping sequence constructed previously.

8. Construct a bit stream with; 1) index of target blocks, 2) optimal rotation angle, 3) the mean, 3) standard deviation quotients of three color channels, 4) the bit sequence for over flows/underflows.

9. Embed the bit streams with reversible contrast mapping [14]

10. Construct the bit stream I including 1) number of iterations for embedding;2) the number of pixel pairs in the last iteration; 3)The Huffman Table constructed above.

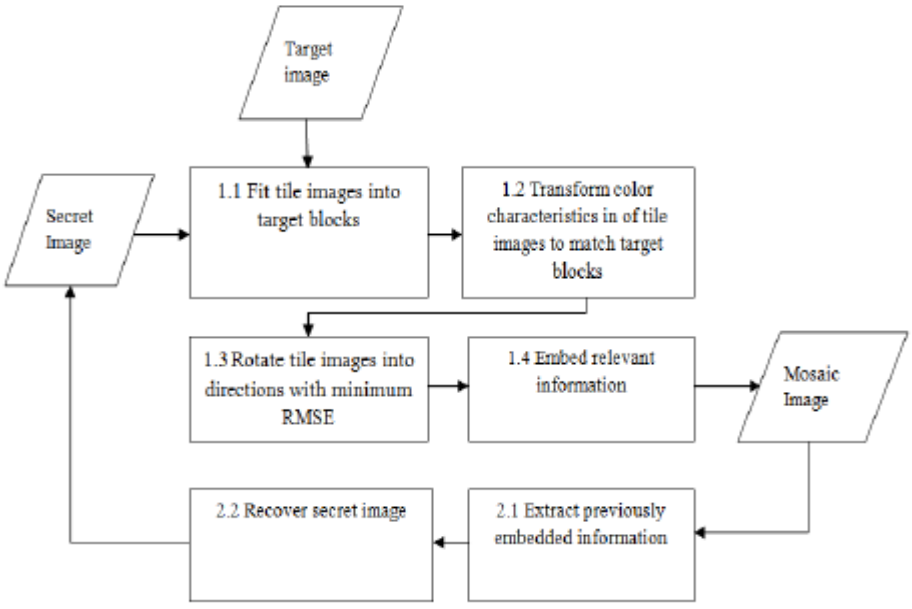

Fig. 1 Overview of Proposed System

Algorithm 2 Secret image Recovery

Input: a mosaic image F with *n* tile images and the key.

Output: the secret image S.

Stage 1. Extracting the secret image recovery information.

1. Extract from F using reversible contrast mapping [14] and decode them to obtain the recovery information and extract the bit sequences.

2. Decrypt the bit stream.

3. Decompose the bit stream to get n tile image information.

4. Decode the tile image information to get the following data items: 1) the index of target blocks, 2) the optimal rotation angle, 3) the means, standard deviation quotients of all color channels, and 4) the overflow /underflow residual values.

Stage 2. Recovering the secret image.

1. Recover in a raster scan order as one by one of the tile images from i=1 to n to get the secret image S by following steps: 1) rotate the tiles in a reverse angle, 2) use the mean, standard deviation quotients to recover the original pixel values, 3)use mean, standard deviation quotients to compute the parameters to balance the overflow/under flow problems, 4) take the results as the final tile image.

2. Compose all the final tile images to form the secret image S as output.

3. IMPLEMENTATION DETAILS

The proposed method can be implemented in two modules like mosaic image generation and secret image recovery. For the first we select two images as secret and target from the web. Each selected images can be saved in a folder that it can be viewed when the particular user wishes. For the purpose of finding the similarity a score can be calculated. It helps the user to select the appropriate target for the secret image. Then each image is divided in to tiles and blocks respectively. Mean, standard deviation and standard deviation quotient of three color channel(R, G, B) are calculated. This can be mapped into a hash map and sorted.

Thus we get two maps sorted. Then a blank image is created and each target block is placed in that and corresponding secret tile. This can be continued up to the divided units (that is if 8 x 8; 64 tiles, 16 x 16; 256 tiles and so on. For each tile image perform the color conversion of each pixel using the mean and standard deviation quotient. Then rotate each tile image in different angles and fix when lowest RMSE value is reached. This can be done for all n tiles. Next we have to embed the all information that we used to generate the mosaic image in the mosaic image itself and it can be controlled using a key. The hash map, rotation angles, bits that control under flow /over flow are embedded. The bit stream is encoded to particular stream.

Secret image is recovered only when the key is decrypted correctly. This is the main security feature that the proposed system offers. When the key is decrypted all the embedded information is decoded. The reverse rotation and inverse color transformation are performed. From the map we get the original positions of the secret tiles. A blank image is created and each tile is fitted as in the previous step. Thus the secret image is created.

4. RESULT AND DISCUSSIONS

4.1 Results

A series of experiments have been conducted to test the proposed method using many secret and target images with different sizes. To show that the created mosaic images looks the preselected target image, the quality metric of root mean square error (RMSE) is used.

An example is shown in the Fig. (2); Fig.2(c) shows the mosaic image created from Fig.2(a) as secret image and Fig.2(b) as target image. The tile image size is 16 x 16. The recovered secret image using the correct key is shown in Fig.2 (d) which is similar to that of the secret image in Fig.2 (a) with an RMSE value of 0.91 to that of the original one. Another example is shown in Fig. (3); Fig.3(c) shows the mosaic image created from Fig.3(a) as secret image and Fig.3(b) as target image. The tile image size is 8 x 8. The recovered secret image using the correct key is shown in Fig.3 (d) which is similar to that of the secret image in Fig.3 (a) with an RMSE value of 0.948 to that of the original one. Fig.3 (e) and Fig.3 (f) shows the mosaic image created from with tile image size 16 x 16 and 32 x 32 respectively. This means that when the tile size increases the clarity of the mosaic image get reduced.

4.2 Performance Evaluation

In this section, present several performance evaluation metrics that have been used for the quality of mosaic images and secret images. The various parameters are: 1) RMSE values of created mosaic images with respect to target image; 2) RMSE values of recovered secret image with respect to original secret image; 3) MSSIM values of created mosaic images with respect to target images. RMSE values find the mean square errors between the images, while the MSSIM values shows the similarity of images. Both can be used in alternatively.

It is recommended that we can use the PSNR values also for finding the difference in mosaic and target images. It will give how much data is hidden in the mosaic image when the ratio is calculated. The signal can be the mosaic and the secret hidden is considered to be the noise.

It is recommended that we can use the PSNR values also for finding the difference in mosaic and target images. It will give how much data is hidden in the mosaic image when the ratio is calculated. The signal can be the mosaic and the secret hidden is considered to be the noise.

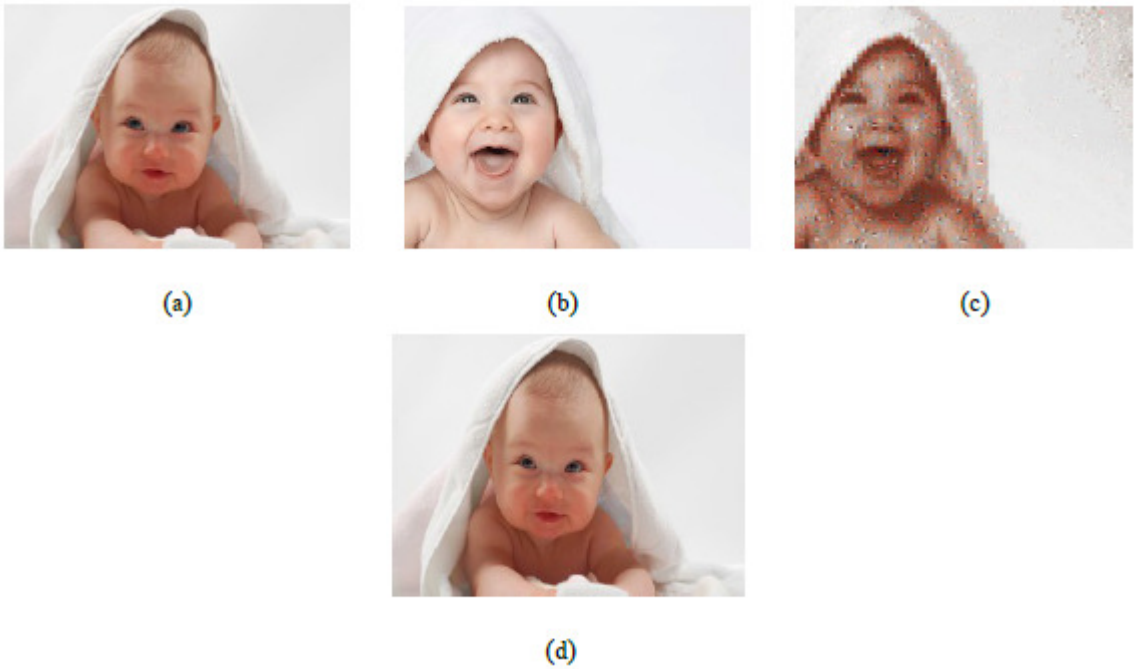

Fig. 2. Result yielded by the proposed method. (a) Secret image. (b) Target image. (c) Mosaic image created with tile image size 16 x 16 from (a) and (b) by the proposed method. (d) Secret image recovered from the mosaic image.

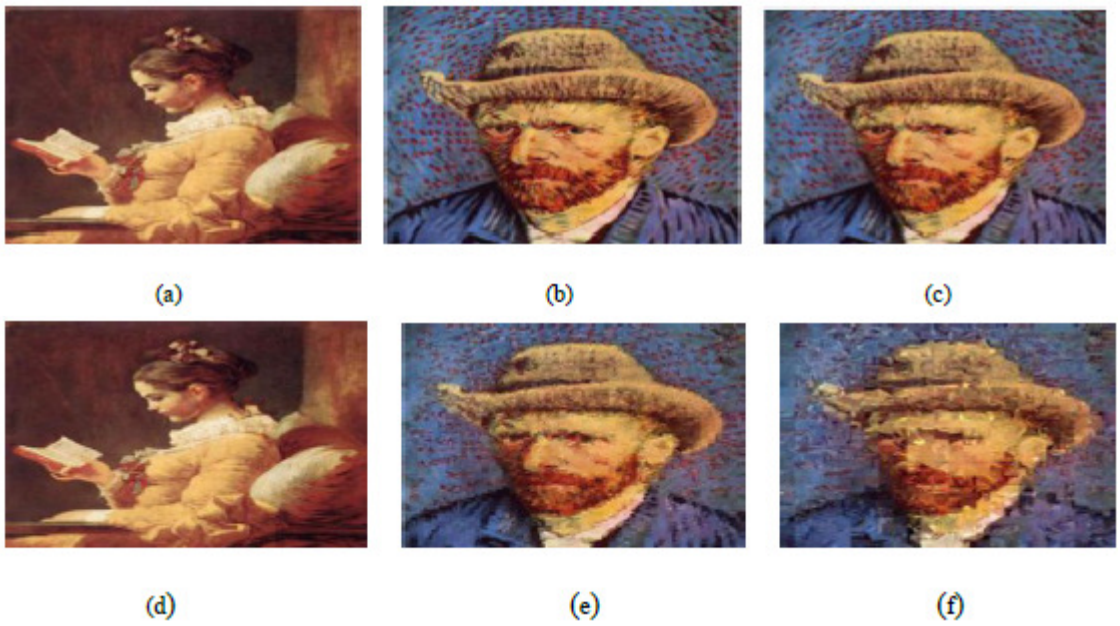

Fig. 3. Experimental result of mosaic image creation. (a) Secret image. (b) Target image. (c) Mosaic image created with tile image size 8×8. (d) Recovered secret image using a correct key with RMSE= 0.948 with respect to secret image (a). (e) And (f) Mosaic images created with different tile image sizes: 16×16, 32×32

The following graphs shows variations of RMSE values when different tile image sizes are used. The Fig. (4) Shows the RMSE value lies between 25 and 45, that is the mosaic image contains the target and secret images. So when calculating RMSE value of mosaic image with respect to target image it shows high variation when comparing with the next graph values, it lies between 0.5 and 2. From the graph Fig.(5), we can infer that the RMSE value quite increases when the tile size increases for the Fig. (2) and also for Fig.(3). We can achieve high similarity and low RMSE value when using the reduced tile image size. So it is preferred to use small sized tile images and high quantity of tiles.

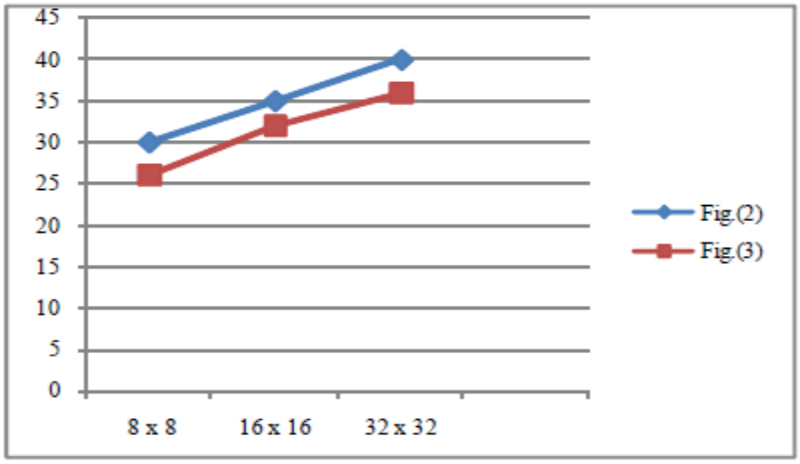

Fig 4. Graph showing the RMSE values of created mosaic images w.r.t. target images

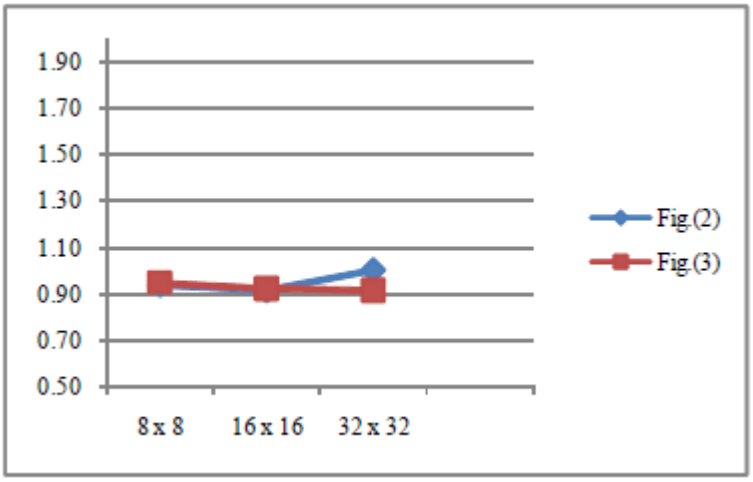

Fig 5. Graph showing the RMSE values of recoverd secret images w.r.t original secret images

5. CONCLUSION

A secret image hiding scheme has been proposed with new security features. A meaning full mosaic image is created from the secret image and the selected target image. The fitting is done properly for generating the mosaic image. By using the proper color transformation to each pixel of secret image, we can achieve high visual similarities to the selected target image. These similarities are checked using the quality metric RMSE value. The main advantage of this scheme is that the secret image is recovered nearly without any loss. The security can be achieved by using a key that controls the recovery information embedding process.

ACKNOWLEDGEMENT

The authors would like to thank everyone, in the Department of Computer Science and Engineering for their support and help

REFERENCES

[1] J. Fridrich, “Symmetric ciphers based on 2D chaotic maps,” Int. J. Bifurcat. Chaos vol. 8, no. 6, pp. 1259–1284, 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. 749–761, 2004.

[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] “Arnold’s Cat Map Gabriel Peterson” Math 45 – “ Linear Algebra” Fall 1997

[5] Yen JC, Guo JI. “A new chaotic key-based design for image encryption and decryption”. In: Proc IEEE Int Conference Circuits and Systems, vol. 4, 2000. p.49– 52.

[6] 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.

[7] Asia Mahdi Naser Alzubaidi, “Color Image Encryption and Decryption using Pixel Shuffling with Henon Chaotic System”, “International Journal of Engineering Research & Technology”,ISSN:2278-0181, vol. 3, issue 3, March – 2014

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

[9] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

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

[11] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Reversible data hiding,” in Proc. IEEE Int. Conf. Image Process., vol. 2, Sep. 2002, pp. 157–160.

[12] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin,"Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recognition 34 (3) (2001) 671– 683.

[13] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[14] 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.

[15] 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.

AUTHORS

Mrs. Shahanaz N is an Assistant Professor in the Information Technology Department of College of Engineering Vadakara, Kerala, India. She did her B.Tech in 2006 from College of Engineering, Vadakara, Kerala,India under the Cohin University of Science and Technology, followed by her M.Tech Post Graduation at M.Dasan Institute of Techology, Ulliyeri,Kerala,India, Calicut University, in 2016. Her interested areas are Digital Image Processing, Bioinformatics.

Mrs. Greeshma R is an Assistant Professor in Department of Computer Science and Engineering, M.Dasan Institute of Technology ,Kozhikode, Keral a, India.Her interested area is Image Processessing.