An High Equipped Data Hiding Algorithm On Secret Fragment Visible Mosaic Images And Pixel Transformation For Secure Image Transmission

C.Sravani[1], Dr.P.Jagadamba[2]

[1]*student of M.Tech ,Dept. of Electronics and Communication, Srikalahasteeswara Institute of Technology, Srikalahasti, India*
[2] *Assistant Professor(sr), Dept. of ECE, Srikalahasteeswara Institute of Technology, Srikalahasti, India*

---***---

Abstract - *Information security is becoming increasingly important in the modern world. Secure Image Transmission has a potential of being adopted for mass communication. Several stenographic techniques for transmitting information without raising suspicion are found in [8]-[12] . However A new secure image Transmission technique is proposed, known as secret fragment visible mosaic image which allows the user to securely transmit an image under the cover of another image of same size, This paper presents an approach where 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 secret image from the mosaic image in lossless manner. Finally the same approach can be performed on videos also which helps to eliminate the flickering artifact to achieve the lossless data recovery in motion related videos. The experimental results show good robust behavior against all incidental and accidental attacks and compare to the conventional algorithms.*

***Key Words*: Data hiding, Image encryption, Reversible Contrast mapping, Secrete Fragment Visible Mosaic Image, Steganography.**

1.INTRODUCTION

Currently, images obtained 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 used for securing image transmission. The two common approaches are image encryption and data hiding. Image encryption is a technique that uses the natural property of an image, like high redundancy and strong spatial correlation.

The encrypted image is a noise image so none can obtain the secret image from it unless he/she has the correct key. However, the encrypted image is a useless file, which can't provide any additional information before decryption and may arouse an attacker's mind during transmission due to the randomness in form. An alternative for the above problem is data hiding, which hides a secret message into a target image due to that no one can find the existence of the secret data, in which the data type of the secret message learnt in this paper is an image. But these data hiding yield good result only when target image must be large compare to secret image

In order to over both problems in this paper, a new technique for secure image transmission 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 [2] 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 a main problem of Lai and Tsai [2] 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 favourite image for use as a 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.

(a) (b) (C)

FIGURE 1. Result yielded by the proposed method. (a) Secret image of size (256*256). (b) Target image of size (256*256). (c) Secret-fragment-visible mosaic image of size (256*256) created from (a) and (b) by the proposed method.

As an illustration, Fig. 1 shows a result yielded by the proposed method. Specifically, after a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, 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 tile 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.

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 in data hiding method must hide a highly compressed version of the secret image into a cover image when the secret image is large compare to the target image. The whole process is controlled by a secret key only the person who has a matched key can retrieve the secret image.

2. RELATED W0RK

Chin Chen chang, Min- Shian Hwang, and Tung Shou Chen [3] have given a fast encryption algorithm for secure image cryptosystems in 2001. Vector Quantization, cryptography and other theorem is the major platform for the cryptosystems to transmit images. It was a meaningful technique to lower bit rate image compression. In VQ firstly transformation of images into vectors takes place and further vector by vector then are sequentially encoded

W. B. Pennebaker tried to explain that the main obstacle in quantity of data required representing a digital image. For this we would have to make image compression standard to maintain quality of the images after compression. To meet all the needs the JPEG standard for image compression includes two basic methods having different operation modes: A DCT method for “loss” compression and a predictive method for “lossless” compression [4].

I-Jen Lai and Wen-Hsiang Tsai [2] have presented technique for information hiding, which proposes that secret image is divided into tile images and then for mosaic image they were fix to its next target image selected from a database. Secret key randomly selects few blocks of mosaic image to embedding the information of the tile image This color transformation was controlled and then the secret image is recovered lossless from the tile image with the help of the embedded extracted relevant information used for the recovery of the image [1].

3. PROPOSED METHOD

The proposed method contains two phases

1. Mosaic image Generation and

2. Secret image recovery

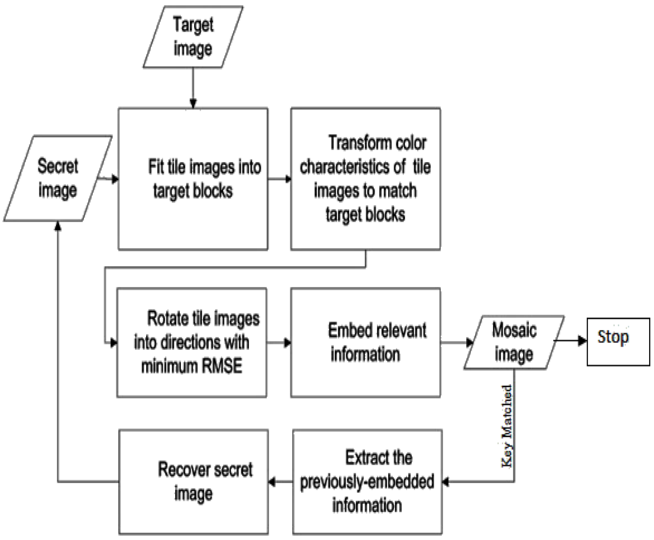


FIGURE 2. Flow diagram of the proposed method

In the first phase, a mosaic image is generated, after the target image is selected randomly, the given secret image is first divided into rectangular fragments called tile images, which then are fit into similar blocks in the target image called target blocks, next the color characteristics of each tile image is transformed to the corresponding blocks of target image resulting a mosaic image which look similar to target image. Image transmission technique contains four stages. 1) Fitting tile images of the secret image into target image; 2) Transforming the each tile of secret image to the corresponding target blocks of target image; 3) Rotating each newly tile with minimum RMSE value with respect to target block; 4) Embedding the secret image recovery information.

In the second phase, it contains two stages. 1) Extracting embedded information from recovery; and 2) Recovering the Secret image.

4. ALGORITHMS OF THE PROPOSED METHOD

The Detailed algorithms for mosaic image creation and secret image recovery may be stated in algorithm 1 and 2.

Algorithm 1: Mosaic Image Creation.

T-Target Image; S-Secret Image; F-Secret Fragment visible mosaic image

Stage 1: Fitting tile images of the secret image into target image.

1. If the size of T is different from Size of S, Change the Sizes and Make them Identical.

2. Divide S into ‘n’ tiles and T into ‘n’ blocks.

3. Compute mean and standard deviation for each tile and block for three color channels.

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

$$\sigma_c = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i-\mu_c)^2} \qquad \sigma_c' = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(c_i'-\mu_c')^2} \quad \text{...(2)}$$

Where μ_c , σ_c are the mean and standard deviation of tile images ; μ_c', σ_c' are the mean and standard deviation of target block image.

4. Compute average Standard deviation.

5. Sort both tiles images and block images.

6. Based on Average Standard Deviation values of blocks, map tile between S and T

7. Create F

Stage 2: Transforming the each tile of secret image to the corresponding target blocks of target image

8. Create Counting Table TB with 256 entries, each with corresponding to a residual value and assign an initial value to zero
9. Calculate mean and standard deviation for each mapping from secret to target.
10. For Each pixel p_i in each block of T with the color value of c_i transform c_i into a new value (r_i', g_i', b_i') using

$$c_i'' = q_c(c_i - \mu_c) + \mu_c' \quad \text{.....................(3)}$$

Where $q_c = \sigma_c / \sigma_c'$

Stage 3: Rotating each tile images.
11. Color similarity between the resultant tile T' and target block b by rotating T' into one of direction $(0^\circ, 90^\circ, 180^\circ, 270^\circ)$ Which yield rotated version of T' with minimum RMSE with respect to B.
Stage 4: Embedding the secret image recovery information.
12. For each tile image T_i in Mosaic image F, construct a bit stream M_i for recovering T

$$M = t_1 t_2 \cdots t_m r_1 r_2 m_1 m_2 \cdots m_{48} q_1 q_2 \cdots q_{21} d_1 d_2 \cdots d_k$$

in which the bit segments $t_1t_2 \dots t_m, r_1r_2, m_1m_2 \dots m_{48}, q_1q_2 \dots q_{21}$, and $d_1d_2 \dots d_k$ represent the values of the index of B, the rotation angle of T, the means of T and B, the standard deviation quotients, and the residuals, respectively.

In more detail, the numbers of required bits for the five data items in M are discussed below: 1) the index of B needs m bits to represent, with m computed by

$$m = log[(W_S \times H_S)/N_T]$$

in which W_S and H_S are respectively the width and height of the secret image S, and N_T is the size of the target image T; 2) it needs two bits to represent the rotation angle of T because there are four possible rotation directions; 3) 48 bits are required to represent the means of T and B because we use eight bits to represent a mean value in each color channel; 4) it needs 21 bits to represent the quotients of T over B in the three color channels with each channel requiring 7 bits; and 5) the total number k of required bits for representing all the residuals depends on the number of overflows or underflows in T'.

13. Concatenate the bit stream M_is of all T_i in F; use the secret key K to encrypt.

14. Embed the bit stream I into mosaic image F by using reversible contrast mapping method [13] applies simple integer transformation to pair of pixel values. Specifically, the method conducts forward and backward integer transformation as follows respectively in which (x ,y) are a pair of pixel values and (x', y') are transformed ones

$$x' = 2x - y, \qquad y' = 2y - x$$

$$x = \left[\frac{2}{3}x' + \frac{1}{3}y'\right] \qquad y = \left[\frac{1}{3}x' + \frac{2}{3}y'\right]$$

Algorithm 2: Secret image recovery

T-Target Image; S-Secret image: F-Mosaic image

Stage 1: Extracting embedded information from recovery.

1. Extract the bit stream M_t by Secret key
2. Decompose M_t into n bit streams M_1 through M_n.
3. Decode M_i for each tile T_i to obtain data items.

Stage 2: Recovering the Secret image.

4. Recovering tile images by the following steps

- Rotate tile in reverse direction and fit the resulting block content into T to form initial tile image.
- Make use of Extracted Mean and related Standard Deviation quotients
- Compute the original pixel value

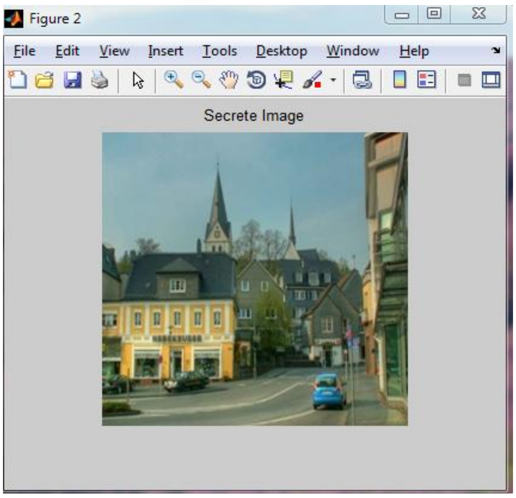
$$c_i = \frac{1}{q_c}(c_i'' - \mu_c') + \mu_c \dots\dots\dots\dots (4)$$

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

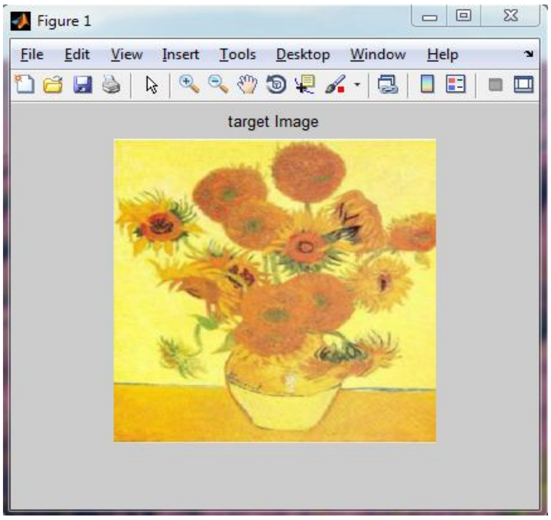
5. EXPERIMENTEL RESULTS

A series of experiments have been conducted to test the proposed method using many secret and target images with sizes 256 *256. To show that the created mosaic image looks like the preselected target image, the quality metric of root mean square error (RMSE) is utilized.

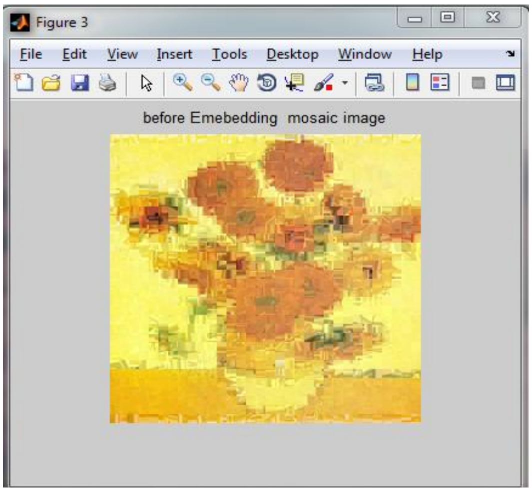
An example of the experimental results of mosaic image shown in Fig.3; Fig.3(d) shows the after embedding created mosaic image using Fig.3(a) as the Secret image and Fig.3(b)target image. The tile image size is 8*8



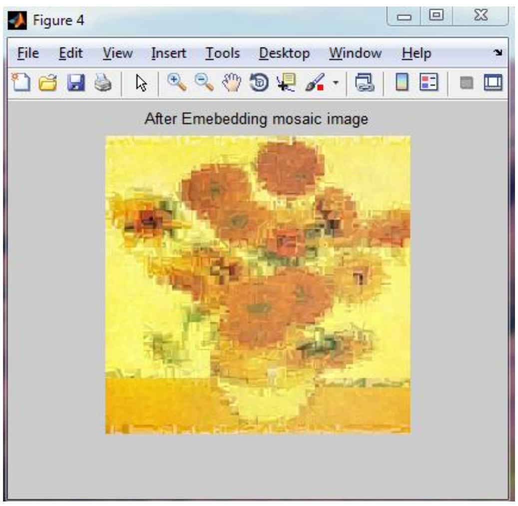
3(a) Secret image



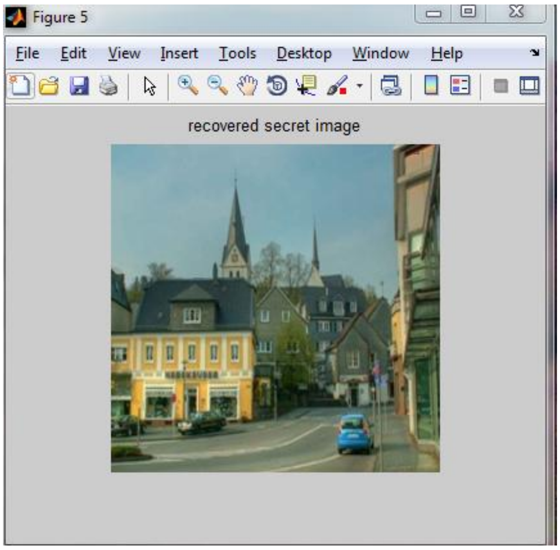
3(b) Target image



3(c) Before embedding mosaic image



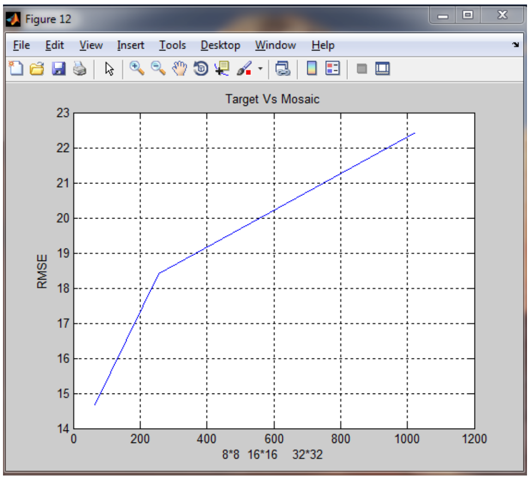
3(d) After embedding mosaic image



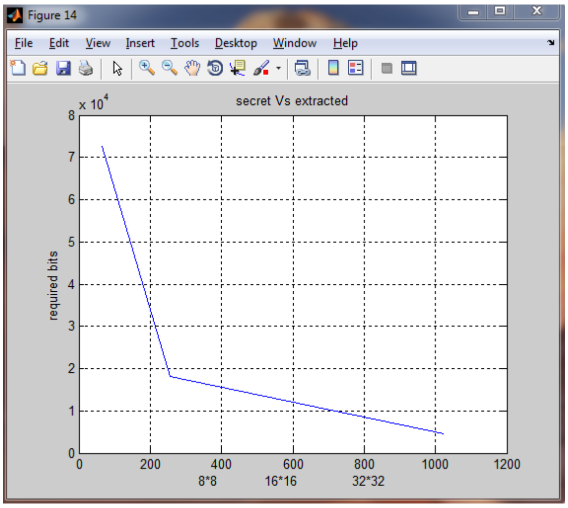
3(e) Recovered secret image

FIGURE 3. An example of the experimental results of mosaic image created with tile image size 8*8.3(a) Secret image,3(b)target image,3(c)before embedded mosaic image,3(d)after embedded mosaic image .3(e) recovery of secret image

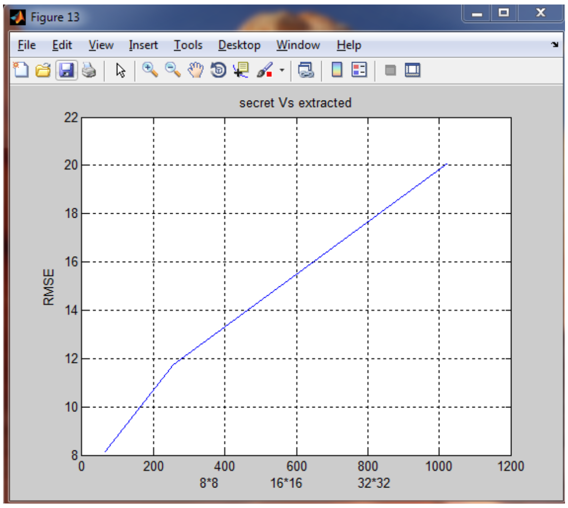
Furthermore, as shown in figure 4, we have drawn plots of various parameter versus different tile image sizes including those of parameters of 4(a) RMSE value of created mosaic images with respect to target images .4(b) numbers of required bits embedded for recovering secret images .4(c) RMSE values of recovered secret images with respect to original image. 4(d) PSNR value of created mosaic images with respect to target images.



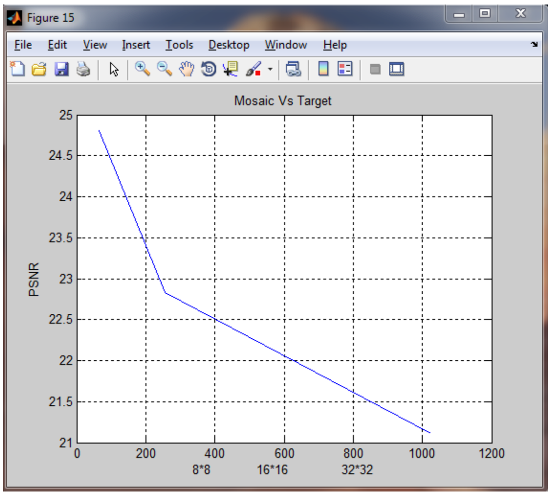
4(a)



4(b)



4(c)



4(d)

FIGURE 4 Plots of tends of various parameters versus different tile image sizes (8*8, 16*16, 32*32) with input secret image shown previously. a) RMSE value of created mosaic images with respect to target images .b) numbers of required bits embedded for recovering secret images .c) RMSE values of recovered secret images with respect to original image. d) PSNR value of created mosaic images with respect to target images.

TABLE 1 Comparison of RMSE value with respect to different tile image sizes of created mosaic image with respect to target images.

S.NO	Tile size	RMSE
1	8*8	14.664
2	16*16	18.403
3	32*32	22.428

TABLE 2 Comparison of Number of required bits embedded for recovering secret image of different tile images.

S.NO	Tile size	Required bits
1	8*8	72704
2	16*16	18176
3	32*32	4544

TABLE 3 Comparison of RMSE value with respect to different tile image sizes of Recovered secret image with respect to original secret image.

S.NO	Tile size	RMSE
1	8*8	8.124
2	16*16	11.753
3	32*32	20.089

TABLE 4 Comparison of PSNR value with respect to different tile image sizes of created mosaic image with respect to target image.

S.NO	Tile size	PSNR
1	8*8	24.805
2	16*16	22.832
3	32*32	21.115

If the recovery key doesn't matches with the key used for hiding key then the process ends at that point, without any further process.

6. CONCLUSION

A Secure image Steganography technique is proposed, where secret images are embed into an target image and encrypted with a key to transmit. Mosaic image which look similar to the target image is formed with secret tile image and target image .Also, the original secret image s can be recovered nearly lossless from the created mosaic image Experimental results are shown the feasibility of secure transmission of image in the proposed method is good. Future studies may be directed to applying proposed method to video, where video frames are used as target image, by using video frames as a target image we can recover secret image with less RMSE value as compared to single target image.

REFERENCES

[1] Ya-Lin Lee 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, vol. 24, no. 4, April 2014.

[2] J. Lai and W. H. Tsai, "Secret-fragment-visible mosaic image—A new computer art and its application to information hiding," IEEE Trans. Inf. Forensic. Secure, vol. 6, no. 3, pp. 936–945, Sep. 2011.

[3] Chin chenChang , MinShin Hwang and Tung Shou Chen," A new image encryption algorithm for image cryptosystems", the journal of system and software 58(2001).

[4] W. B. Pennebaker and J. L. Mitchell, "JPEG: Still Image Data Compression Standard", New York, NY, USA: Van Nastran Reinhold, pp. 34–38, 1993.

[5] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su," Reversible Data Hiding", IEEE transactions on circuits and system for video technology, vol. 16, no. 3, march 2006.

[6] C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "Reversible hiding in DCT-based compressed images," Inf. Sci., vol. 177, no. 13, pp. 2768–2786, 2007.

[7] E. Rein hard, M. Ashikhmin, B. Gooch, and P. Shirley, "Color transfer between images," IEEE C computed. Graph. Appl., vol. 21, no. 5, pp. 34–41, Sep.–Oct. 2001.

[8] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurcat. Chaos, vol. 8, no. 6, pp. 1259–1284, 1998.

[9] 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.

[10] Y. Hu, H.-K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1500–1512, Dec. 2008.

[11] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technology., vol. 19, no. 7, pp. 989–999, Jul. 2009.

[12] 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[11] Y. Hu, H.-K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1500–1512, Dec. 2008.

[13] 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.

BIOGRAPHIES

C.SRAVANI,

Completed B.Tech in Siddhartha Institute Of Science and Technology, Puttur. Pursuing M.Tech in Srikalahasteeswara Institute Of Technology,Srikalahasti.

Dr. P. JAGADAMBA,

She did her Ph.D from S.V. University, Tirupati.Presently working as Assistant professor(sr) Department of ECE in Srikalahasteeswara Institute of Technology. She has 10 years of teaching experience. She Published many research papers in National and International Journals.