A Secure and Robust Reversible Watermarking Algorithm using Fuzzy Matching – Quad Tree Segmentation (F-QTS) Technique for Digital Images

Ruban R
Lecturer, Head of The Department of BCA & MSC Computer Science ST.Josephs college Arts& Science,Kovoor.

S.SanthoshBaboo
Associate Professor, DwarakaDossGoverdhanDossVaishnavCollege, Chennai.

ABSTRACT
The attainment incompetence of extracting the original image is one of the most challenging tasks in digital image watermarking methods. When an image is embedded into another image, this increases more complications. To overcome this problematic scenario, this paper proposes a Fuzzy based Quad Tree Segmentation (F-QTS) method. In this paper, a binary logo image is embedded into a RGB cover image. Due to the embedding data is an image, Quad Tree Segmentation method is applied in both the images in order to allocate the blocks for logo image. This space allocation is empowered by Fuzzy Rules and the binary logo image is embedded into the R-plane of the cover image. Moreover, performances of the proposed watermarking method is evaluated with the various watermarking attacks and presented in terms of PSNR (Peak signal-to-noise ratio).

Indexed Terms:
Watermarking, digital image, Fuzzy Rule, Quad Tree Segmentation, embedding, attacks, PSNR, extraction

1. INTRODUCTION
In recent years, digital media is excelled due to the thriving development of computer science and the Internet technology. Nevertheless, free reproduction and convenient manipulation of digital media origin to the considerable commercial damages to the data owners and the providers. Therefore, digital watermarking is introduced to thwart the above-mentioned contravention [1]. Digital watermarking is a process of embedding information into digital multimedia so that the information can be detected for a variety of purposes including copyright protection and digital right management. Digital watermarking has reached the most of data owners and becomes an active area of research [2]. Many researchers have presented various watermarking methods to embed secrete data, copyright information, into digital images in order to protect the secret information. Furthermore, this process only allows an insignificant modification to the original data [3-6].

Generally, digital watermarking can be classified as visible and invisible watermarking. Invisible digital watermarking is a process of permanently embedding a secret data into digital image carrying information. Therefore, the presence of the watermark is virtually imperceptible by human sensory system [7]. Among visible watermarking, it is difficult to remove unless exhaustive and expensive human interventions are involved. One of the most important encounter problems in watermarking is that as the quality of image increases the robustness of the watermarking decreases and vice versa. An efficient and robustness watermarking method is that which conquer this most encountered problem professionally [8]. On the other hand, restoration of the original contents after extraction of the hidden data is crucial task in watermarking and known as reversible watermarking. A numerous reversible watermarking methods have been presented in the past literatures; accordingly they can be approximately classified into three types: lossless compression based methods, difference expansion (DE) methods, and histogram modification (HM) methods [9].

Fuzzy based image watermarking methods are the most important research in the area of digital security. Many researchers have presented fuzzy based watermarking approaches in [7-8, 10-12].Hiding the image within another image earnestly causes many challenges: when the size of the logo image is lesser than the cover image and recovery of the logo image. In this scenario, fuzzy algorithms have attended numerous times for the decision making processes of embedding one image into another. Recently, fuzzy based watermarking technique AIWJFG [12]has proven that the protection capacity of image copyrights from being counterfeited efficiently. Brightening, darkening, cropping, painting, noising and blurring are the major watermarking attacks, in which watermarked image have been protected using AIWJFG method. On the other hand, quad tree segmentation method [13]can benefit the embedding process of a data into an image by estimating the payload of the image. Payload size is the allocated space for embedding the data into an image.

In this paper, we propose a Fuzzy based Quad Tree Segmentation (F-QTS) method for color image watermarking. Initially a RGB cover image is partitioned into numerous blocks based on quad tree segmentation. This method generates a private key in the form of bit-stream to embed a logo image into cover image. Based on this key, we generate Fuzzy Rules and allocate the data and space in cover image since the logo image is also on same size. The extraction of the original image from the watermarked image is also presented. Moreover, various watermarking attacks are applied to the watermarked image in order to validate the robustness of the proposed F-QTS method. After the extraction of the original image under these attacks, PSNR values are computed and plotted to prove the efficiency of the proposed method.

2. LITERATURE SURVEY
Chip-Hong Chang et.al proposed a transform domain watermarking scheme using Fuzzy-ART [7]in binary image watermarking for image authentication. Their proposed Fuzzy- ART was utilized to locate the spectral positions and the modulating factors according to the perceptibility of the image. As they have embedded the cryptographically randomized watermark

Information into the image, the embedding strength was efficient. In [14], Liu Jinhu a and She Kun have proposed a quantization-based image watermarking in the dual tree complex wavelet domain. They embedded each watermark

bits by modulating a set of dual tree complex wavelet coefficients using quantization approach. When this method was applied, the effect of geometric distortion on the watermarked image has been reduced.

Hong Peng et.al have proposed a blind image watermarking approach [15], which has combined the multi wavelet and support vector machine to effectively capture line-like, curve-like and wedge-like, contour-like features of image. They have used the mean value modulation technique to modulate a set of multi wavelet coefficients in approximation sub-bands, hence effects of the image distortion has been reduced when it was suffering from different attacks. SVMs classifier was proposed to learn mean value relationship between watermark and coefficients in multi wavelet sub-bands. In [13], a quad-tree segmentation based reversible watermarking has been proposed by Yih-Chuan Lin and Tzung-Shian Li. They have utilized the histogram shifting method to embed the data into the gray image. As this technique presented with block-by-block embedding, quad tree segmentation methods has estimated the embedding capacity of each blocks.

In [9], Xinpeng Zhang has achieved the good payload-distortion performance of reversible data hiding by the proposed practical reversible data hiding scheme. They have performed the iterative based optimization to find the optimal value transfer matrix by maximizing the target function of pure payload. By using this matrix, the auxiliary information was generated and embedded into a number of subsets of the image, which has been increased the accuracy of the extraction of the original image. A content reconstruction problem in self-embedding systems has been stated in [16]. They have analyzed about the of the inherent restoration trade-offs. Based on this analysis, they have proposed the image authentication and reconstruction scheme. In [2], Huawei Ti et.al proposed an efficient resynchronization method to protect the data from the Desynchronization Attacks (DAs). This proposed watermarking scheme has presented with the local and global RST-invariant transform (LDFT) feature by the BSP tree partition.

The authors of [8], [10-12] have presented the watermarking techniques with Fuzzy Rules. In [8], a transform domain watermarking scheme (FGRW) has been proposed with fuzzy-ART and image normalization techniques. The watermark data was embedded by adjusting the particular DCT coefficients of the host image using an adaptive embedding strength. The Fuzzy-ART clustering has applied to select the appropriate clusters for watermark insertion. In [10], the DCT algorithm was applied to the copyright protection of the image by inserting the fuzzy vault into the host image. Initially, they have extracted the minutiae features from a fingerprint image to project the polynomial then a set of genuine and chaff points were calculated accordingly utilized as the fuzzy vault.

In [11], a watermarking scheme called Fuzzy based Chaotic and Logistic (FCL) was proposed to overcome the problems presented in embedding the image in the spatial domain. The FCL method has many properties such as the initial conditions, no periodicity, pseudo-random property and topological transitivity, which made this method to meet the requirements of diffusion and mixing. Recently, Hung-Hsu Tsai and Shih-Che Lo have proposed an adaptive image-watermarking scheme using just-noticeable distortion (JND) profile and Fuzzy Inference System (FIS) optimized with Genetic Algorithm (GA) called AIWJFG [12]. To make the watermarked image invisible, JND profile of an image was referred to embed the data into original image. FIS was generated with the image features and local statistics of the watermarked image. Finally, they optimized the FIS to improve the performance in the extraction phase.

3. PROPOSEDF-QTS METHOD

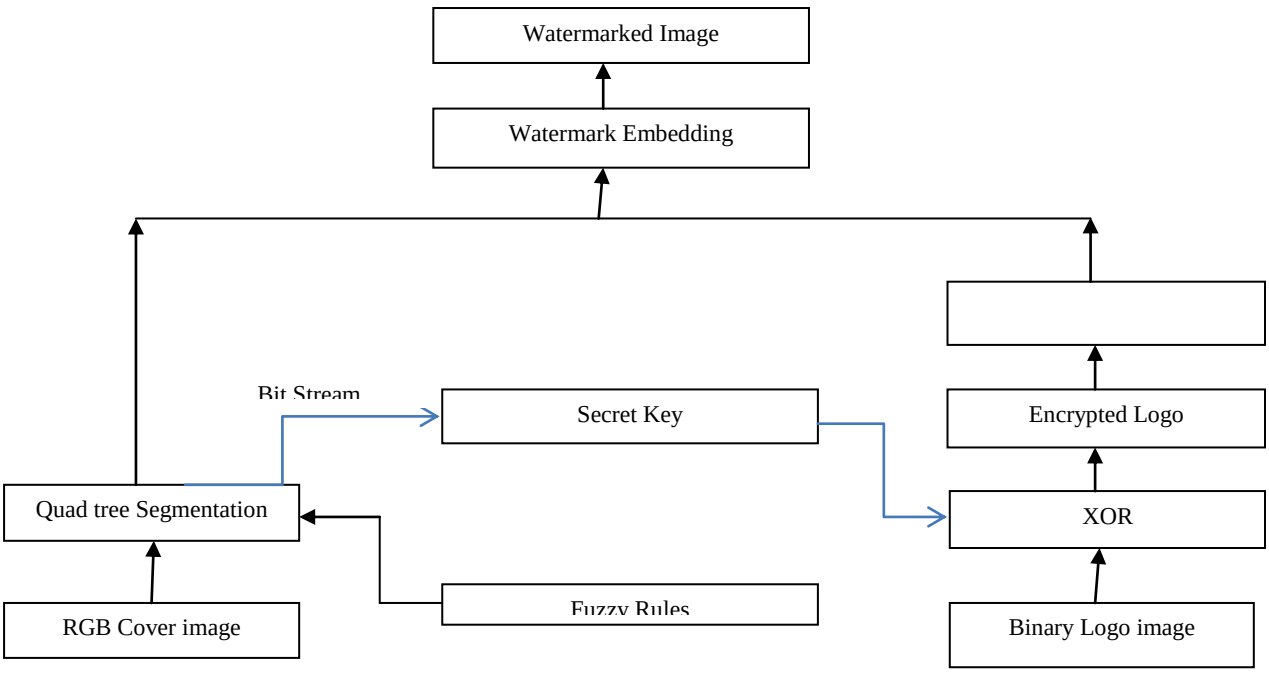

Fig.1. Flow chart of the Proposed F-QTS Watermarking method

In the proposed method as represented in fig.1, an RGB cover image is given as input to the quad-tree segmentation. The fuzzy rule based quad-tree segmentation segments the cover image into various blocks and the payload is calculated for each blocks. Then this payload is tested against the total payload size of the incoming block. If the testing condition is satisfied then the incoming block is again partitioned into four sub blocks and the binary variable is set to one otherwise the binary variable is set to zero. This forms a bit stream for example 11000110000. This bit stream is used as the secret key and it is added to the binary logo image by using XOR operation in order to get the encrypted image. The encrypted logo image is also partitioned into the sub blocks using the secret key. Therefore, the space allocation in the logo image is balanced with respect to blocks of the cover image. Finally, the partitioned blocks of the logo image are embedded in the R-plane of the RGB cover image.

Fuzzy based Quad-tree segmentation (F-QTS)

A quad-tree is a tree data structure in which each internal node has exactly four blocks. These blocks are formed by splitting the cover image and organized as a form of quad-tree structure. RGB image is used as cover image in the proposed method. In the quad-tree segmentation process the first step is to make a decision on whether a further division is required or not. For that, the payload is found out for each sub blocks individually. If the total payload size of the four blocks is larger than that of incoming block, then the incoming block is divided into another four sub blocks. The process is continued until all the block partitions are traversed.

At first, generate a histogram h(x) for the cover image I. Then find the maximum and minimum point m_1 and z_1 respectively in the histogram.

$$m_1 = arg_x \max h(x) \quad (1)$$

$$z_1 = arg_x \min h(x) \quad (2)$$

The cover image I is divided into sequence of non-overlapped blocks $b_1, b_2 \ldots b_p$. Here the payload for the actual secret data is calculated using,

$$PS_1(I) = h(m_1) - (\log N)^2 \times h(z_1) - 16 \quad (3)$$

The total payload size is defined by,

$$PS_3(I,P) = \sum_{i=1}^{P} h_i(m_{i,1}) - (\log N)^2 \times \sum_{i=1}^{P} h_i\left(z_{i,1}\right) - P \times 16 \quad (4)$$

Where $(m_{i,1}, z_{i,1})$ is the pair of maximum and minimum points of the i-th image block and $h_i(x)$ represent the histogram of the i-th image block. For any incoming block b(x, z_x), the following Fuzzy Rule condition is applied as in Table.1.

Table.1: FUZZY RULE SELECTION FOR QUAD TREE SEGMENTATION

Rule1:If $\boldsymbol{PS_3(b(x,z_x)) > PS_1(b(x,z_x))}$then b(x,$z_x$) = b(x+1,$z_{x+1}$+1)+b(x+1,$z_{x+1}$+2)+b(x+1,$z_{x+1}$+3) +b(x+1,$z_{x+1}$+4)
Rule2:If $\boldsymbol{PS_3(b(x,z_x)) < PS_1(b(x,z_x))}$then b(x, z_x) = b(x, z_x)
Rule3:If $\boldsymbol{PS_3(b(x,z_x)) = PS_1(b(x,z_x))}$then b(x,$z_x$)=b(x+1,$z_{x+1}$+1)+b(x+1,$z_{x+1}$+2)+b(x+1,$z_{x+1}$+3) +b(x+1,$z_{x+1}$+4
Rule4: Ifb(x,z_x)=b(x+1,z_{x+1}+1)+b(x+1,z_{x+1}+2)+b(x+1,z_{x+1}+3) +b(x+1,z_{x+1}+4, then n(x,z_x) = 1
Rule5: Ifb(x, z_x) =b(x, z_x), then n(x,z_x) = 0

When total payload size (PS_3) of the incoming block(x, z_x) is higher than the actual payload of that block (PS_1), then the incoming block is partitioned into four sub blocks b(x+1,z_{x+1}+1),b(x+1,z_{x+1}+2),b(x+1,z_{x+1}+3)and b(x+1,z_{x+1}+4) and the binary variable n(x,z_x) is set to one, otherwise the incoming block is considered as a terminal node and the binary variable n(x,z_x) is set to zero, indicating that there is no need of further partition for incoming block b(x,z_x).

Algorithm for Quad-tree Segmentation

***Input*:** Nodes *b*(*x*, z_x)

***Output*:** Bit-stream: *t*

***Initialization*:** *b*(*x*, z_x)=*b*(0,1)

BeginPre order_bitstream (*b*(*x*,z_x))

1. *t*= *t* // *n*(*x*, *zx*)
2. If*n*(*x*, z_x)!= 0
3. Preorder_bitstream (*b*(*x*+1,z_x))
4. Else
5. Preorder_bitstream (*b*(*x*-1, z_{x-1}+1))
6. ***End if***

End

Watermark Embedding

The space is allocated based on the payload evaluation process. The watermark embedding is done by the below formula,

$$I'(x,y) = I_i(x,y) + J_i(x,y) \text{ where, } i=1,2,3,\ldots p. \quad (5)$$

Where i is the number of sub blocks, I'(x,y) is the watermark image, $I_i(x,y)$ is the RGB cover image, $J_i(x,y)$ is the binary logo image. After we get embeddable blocks from qud-tree segmentation we embed secret data in these blocks. Finally, we get the output of watermarked cover image

.

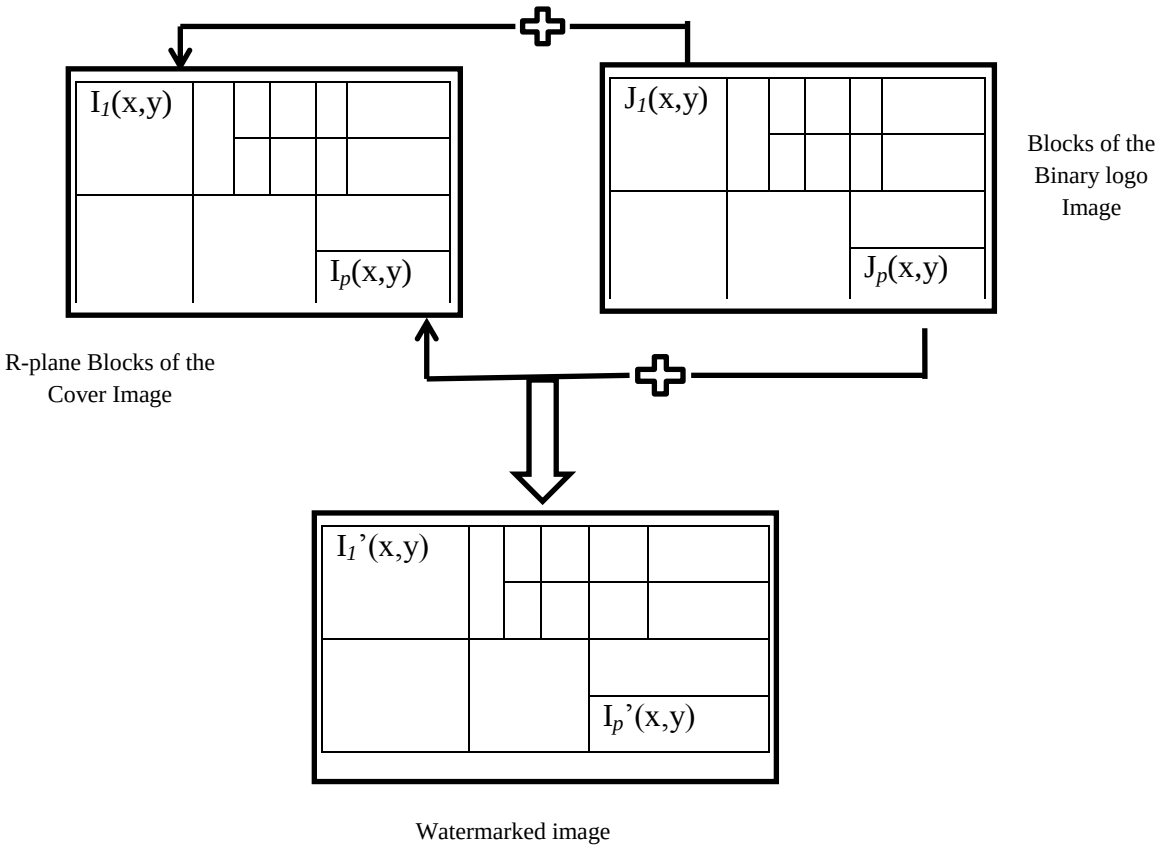

Fig.2. Watermark embedding process in R-Plane of the cover image

4. PERFORMANCE ANALYSIS

In the process of evaluating the robustness of the F-QTS method, several common image watermarking attacks, including brighten, darken and salt & pepper Noising is simulated as attacks to degrade watermarked images. To evaluate the performance, we consider the following images.

Brightening attack:

The brighten attack is done by adding a positive constant to the luminance of every pixel in the entire watermarked image I'(x,y). After the brightening of the image, the image becomes authentic.

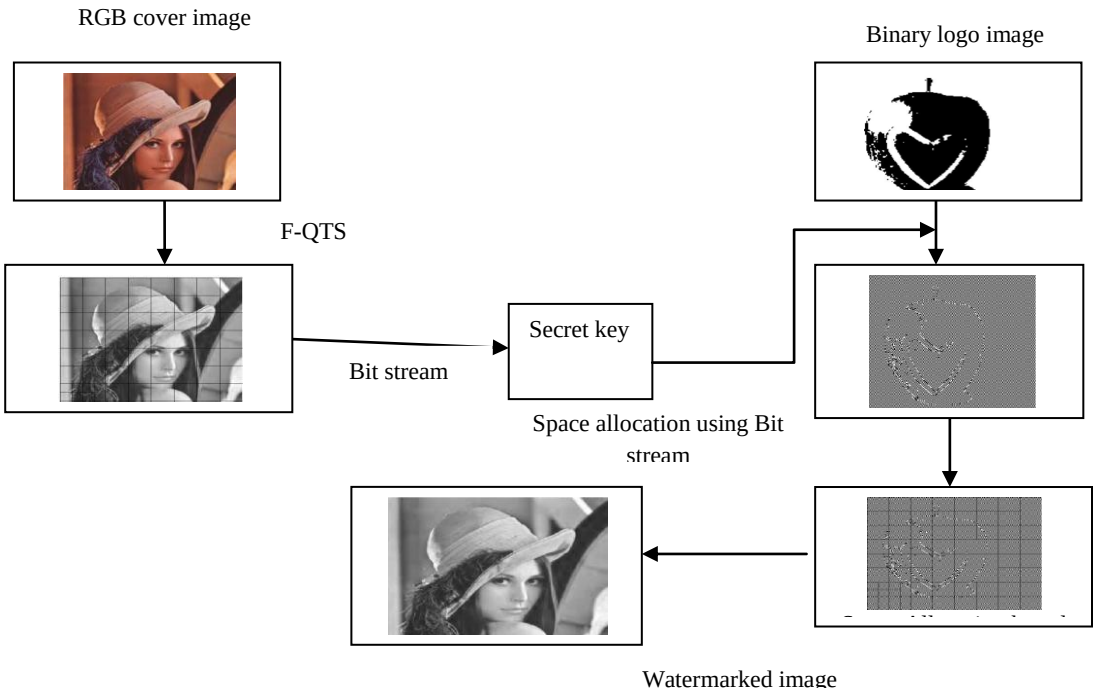

Fig.3. Watermarking Scheme of F-QTS

Darkening attack:
The darkening attack is created by subtracting a positive constant from the pixels of watermarked image, I'(x,y). Darkening the image make easier to remove the watermark and would become visible to the naked eyes.

Painting attack:
We paint the watermarked image I'(x,y) and then we get I_p'(x,y)painting. Paint attack is capable for scaling the images. The watermarked image will be downscaled and it will be extracted.

Salt and pepper attack:
The common attack used on watermark image is salt and pepper attack. Salt and pepper noise often occurs in images due to faulty memory locations. The effect of salt and pepper noise is similar to a Gaussian noise attack since it increases the variation in pixel values in spatial domain.

Table.2. PSNR Comparison of various attacks for F-QTS method

Attack Types	PSNR [Baby Image]	PSNR [Nature Image]	PSNR [Lena Image]
No Attack	55.8922	55.906	55.8717
Salt & pepper	34.8202	35.751	35.0777
Painting	29.5995	37.9299	34.9571
Brighten	55.326	55.0943	55.094
Darken	55.0907	55.1717	55.1017

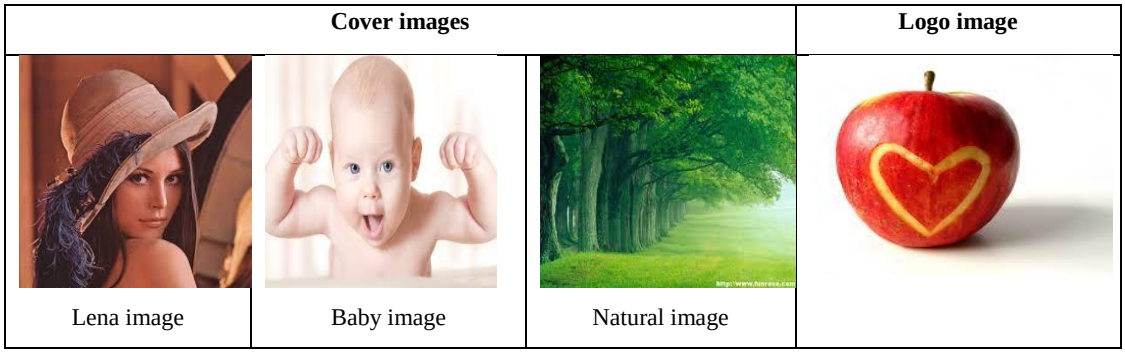

Fig.4. Input images for the performance evaluation

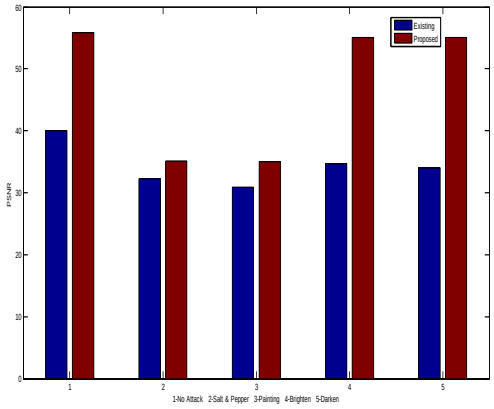

Fig.5. Comparison graph between existing and proposed method

Table3. Comparison of Existing Watermarking Method with our proposed method

Type of Attack	PSNR value for Existing Watermarking Method [Lena Image]	PSNR value for Proposed Watermarking Method [Lena Image]
No Attack	39.973	55.8717
Salt & Pepper	32.21	35.0777
Painting	30.901	34.9571
Brighten	34.67	55.094
Darken	33.9739	55.1017

Table 4: Comparison of various Existing methods with our proposed method

Type of Attack	Existing Method		Proposed Method
	Method Names	PSNR value	PSNR value
Salt & pepper Noise	Watermarking Algorithm [17]	25.2658	35.751
Brighten	Robust Watermarking method [18]	54.45	55.0943
Darken	Wavelet transformation watermarking scheme [19]	22.74	55.1717
Painting	Watermarking Scheme based DWT [20]	30.9013	37.9299

5. CONCLUSION

In this paper, an efficient and robust image watermarking method was presented to secure the digital images, copyright information and important logo images. The proposed method has been developed in the environment of MATLAB R2012a simulation tool. A binary logo image was embedded into another RGB cover image using the proposed Fuzzy based Quad Tree Segmentation (F-QTS) method. This method has partitioned the RGB image into sub-blocks using QTS

technique, in which Fuzzy Rule was applied to check the conditions for dividing the blocks into further sub blocks. Using this F-QTS method, a binary bit stream was generated and utilized as the secret key for encryption of the logo image by XOR operation. Therefore, space allocation in the logo image has been balanced to the block size of the cover image based on the payload sizes calculated with the QTS technique. Finally, watermark embedding the logo image was performed into the R-plane of the cover image.

As the secret key or bit stream was added to the image, original image extraction has been applied in the reverse order. Moreover, the proposed method has been evaluated against the watermarking attacks such as brightening, darkening, painting and salt& pepper attack. The PSNR performance of the proposed method has been presented for these watermarking attacks to prove the robustness of the F-QTS method.

6. REFERENCES

[1] Y.-T.Wu and F. Y.Shih, "Genetic algorithm based methodology for breaking the steganalytic systems," IEEE Trans. Syst., Man, Cybern. B, Cybern, Vol. 36, no. 1, pp. 24–31, Feb. 2006

[2] Huawei Tian, Yao Zhao and Rongrong Ni, "LDFT-Based Watermarking Resilient to Local Desynchronization Attacks", IEEE Transactions on Cybernetics, Vol. 43, pp. 2190- 2201, 2013

[3] W. Zeng, "Digital watermarking and data hiding: technologies and applications," in Proc. Int. Conf. Inf. Syst. Anal. Synth., vol. 3, pp.223-229,1998

[4] C. W. Honsinger, P. Jones, M. Rabbani and J. C. Stoffel, "Reversible recovery of an original image containing embedded data," U.S. patent: 6,278,791, 2001

[5] J. Fridrich, M. Goljan and R. Du, "Invertible authentication," in Proc. Security Watermarking Multimedia Contents, pp. 197-208, 2001

[6] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible watermarking techniques: an overview and aclassification," EURASIP Journal on Information Security, vol. 2010, Article ID 134546, 19 pages, 2010

[7] Chip-Hong Chang, Zhi Ye, and Mingyan Zhang, "Fuzzy-ART Based Adaptive Digital Watermarking Scheme", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 15, pp. 65-81, 2005

[8] Neethu V. Gopal and Madhu S. Nair, "Fuzzy-ART Based Geometrically Invariant Robust Watermarking Scheme", Engineering Letters, Vol. 22, 2014

[9] Xinpeng Zhang, "Reversible Data Hiding with Optimal Value Transfer", IEEE Transactions on Multimedia, Vol. 15, pp.316-325, 2013

[10] Priyanka D. Godase, Snehal B. Kale, Sonika S. Shelke, S.M.Sangve and S.P.Deshmukh, "Robust Digital Watermarking for Color Images Using Fuzzy Vault", Global Journal of Computer Science and Technology, Vol. 12, 2012

[11] G.RoslineNesakumari, L.Sumalatha and V.Vijayakumar, "Fuzzy Based Chaotic and Logistic Method for Digital Watermarking Systems", International Journal of Scientific & Engineering Research Vol. 3, 2012

[12] Hung-Hsu TSAI and Shih-Che LO, "JND-Based Watermark Embedding and GA-Based Watermark Extraction with Fuzzy Inference System for Image Verification", Informatica, Vol. 25, 2014

[13] Yih-Chuan Lin and Tzung-Shian Li, "Reversible Image Data Hiding Using Quad-tree Segmentation and Histogram Shifting", Journal of Multimedia, Vol. 6, pp.349-358, 2011

[14] LIU Jinhua and SHE Kun, "Quantization-Based Robust Image Watermarking Using the Dual Tree Complex Wavelet Transform", China Communications, pp.1-6, 2010

[15] Hong Peng, Jun Wang and Weixing Wang, "Image watermarking method in multiwavelet domain based on support vector machines", The Journal of Systems and Software, Vol. 83, pp. 1470–1477, 2010

[16] Paweł Korus and AndrzejDziech, "Efficient Method for Content Reconstruction with Self-Embedding", IEEE Transactions on Image Processing, Vol. 22, pp. 1134-1147, 2013.

[17] L. Agilandeswari and K.Muralibabu, "A novel block based video in video watermarking algorithm using discrete wavelet transform and singular value decomposition", International journal of advanced research in computer science and software engineering, vol. 3, Issue: 4, April 2014

[18] S. Ponni, S. Ramakrishnan, S. Arjun and V. Mahendran, "Selective Pixel based efficient video watermarking using dual singular value decomposition in the discrete wavelet transform domain", Research journal of computer science and engineering, vol. 4, pp. 720-725, June 2013

[19] Young-Chang Hou, Shih-Chieh Wei, Hsin-Ju Liu, and A-Yu Tseng, "Watermarking Scheme based on wavelet transformation and visual cryptography", Journal of Electronic science and technology, vol. 12, No. 1, March 2014

[20] Li Zhang, Xilan Yan1, Hongsong Li and Minrong Chen, "A Dynamic Multiple Watermarking Algorithm Based on DWT and HVS", International Journal of Communications, Network and System Sciences, vol. 5, pp. 490-495, 2012.

7. AUTHOR'S PROFILE

Ruban. R completed his MCA, Mphil in department in year 2006 from BHARATHIDASAN UNIVERSITY Currently, he is pursuing her PhD degree from MANONMANIAM SUNDRANAR UNIVERSITY. He is working as an Lecturer in the Department of BCA&MSc Computer Science ST.Joseph's College Arts & Science, Kovoor. His research areas include (image processing). He is having more than 10 years teaching experience in engineering colleges.

Capt..Dr.S.SanthoshBaboo, aged forty five, has around **TwentyTwo years** of postgraduate teaching experience in Computer Science, which includes Six years of administrative experience. He is a member, board of studies, in several autonomous colleges, and designs the curriculum of undergraduate and postgraduate programmes. He is a consultant for starting new courses, setting up computer labs, and recruiting lecturers for many colleges. Equipped with a Masters degree in Computer Science and a Doctorate in Computer Science, he is a visiting faculty to IT companies.

It is customary to see him at several national/international conferences and training programmes, both as a participant and as a resource person. He has been keenly involved in organizing training programmes for students and faculty members. His good rapport with the IT companies has been instrumental in on/off campus interviews, and has helped the post graduate students to get real time projects. He has also guided many such live projects. So far 12 Scholars have been awarded Ph.D. in Computer Science under his guidance.

Capt. Dr.SanthoshBaboo has authored a commendable number of research papers in international/national Conference/journals and also guides research scholars in Computer Science. Currently he is Associate Professor in the Postgraduate and Research department of Computer Science at DwarakaDossGoverdhanDossVaishnavCollege (accredited at 'A' grade by NAAC), one of the premier institutions in Chennai.