International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:6, 2018

Optimized and Secured Digital Watermarking Using Entropy, Chaotic Grid Map and Its Performance Analysis

R. Rama Kishore, Sunesh

Abstract**—**This paper presents an optimized, robust, and secured watermarking technique. The methodology used in this work is the combination of entropy and chaotic grid map. The proposed methodology incorporates Discrete Cosine Transform (DCT) on the host image. To improve the imperceptibility of the method, the host image DCT blocks, where the watermark is to be embedded, are further optimized by considering the entropy of the blocks. Chaotic grid is used as a key to reorder the DCT blocks so that it will further increase security while selecting the watermark embedding locations and its sequence. Without a key, one cannot reveal the exact watermark from the watermarked image. The proposed method is implemented on four different images. It is concluded that the proposed method is giving better results in terms of imperceptibility measured through PSNR and found to be above 50. In order to prove the effectiveness of the method, the performance analysis is done after implementing different attacks on the watermarked images. It is found that the methodology is very strong against JPEG compression attack even with the quality parameter up to 15. The experimental results are confirming that the combination of entropy and chaotic grid map method is strong and secured to different image processing attacks.

Keywords**—**Digital watermarking, discrete cosine transform, chaotic grid map, entropy.

I. Introduction

WITH the current development sand increase in the usage of internet, there is a great requirement to think about the security and copy right protection of the images being used over the networks. To improve the same, many algorithms are developed, but still there is a scope to improve the methods which are more imperceptible, robust, and secured. Several attempts were made already in that direction by using Visual cryptography and different encryption algorithms in the field of watermarking [14]. Here, just knowing the procedure of watermark embedding is not sufficient enough to extract the watermark. To extract the true watermark, it is required to know the key also [13]. The key patterns can be changed to increase the security further. Watermarking embedding method can be optimized by different methods like entropy, fuzzy entropy, artificial intelligence, Genetic algorithms, etc. On the basis of how watermark is extracted, the techniques are classified as non-blind, semi blind, and blind methods. If host image and procedure of embedding is required to extract the watermark, then it is considered to be non-blind method. If partial information is required to extract the watermark, then it is considered to be semi blind method. If no information regarding host image or any additional information to extract, then it is considered as blind method. Watermarking can be done in either spatial domain or transform domain [12]. It is considered that working in transform domain will give better results in terms of imperceptibility and robustness against different attacks. While working in transform domain, DCT, DWT, fractional Fourier transform, fractional discrete wavelet transform, etc. are used.

R. Rama Kishore (Associate Professor) is with the University School of Information Communication and Technology, Guru Gobind Singh Indraprastha University, Delhi-110078, India (e-mail: rama.kishore@ipu.ac.in).

Sunesh (Assistant professor) is with the Maharaja Surajmal Institute of Technology, Delhi, India.

II. Related Work

Robustness, security, and imperceptibility are important challenges considered in designing of digital watermarking scheme. Through the history, different watermarking methods are reported in literature with distinct aims. This section throws light on some of robust or imperceptible or secure watermarking methods based on different domain. Security of watermarking methods is enhanced by employing different techniques like Arnold transform, visual cryptography, etc. [1]-[6]. Imperceptibility of watermarking scheme may be magnified by entropy [7]-[9]. Primarily, watermarking scheme based on DCT, discrete wavelet domain and entropy are discussed [1]-[6], [10].

Kumar et al. [9] reported digital watermarking method in spatial domain based on block entropy and LSB substitution method. First, host image is divided into blocks, and entropy for each bock is calculated. Then, blocks with maximum entropy value are selected for watermark insertion. In selected blocks, watermark is embedded by LSB substitution method.

In 2016, Gurwindersingh et al. [7] also developed transform domain based digital image watermarking method with aim to enhance robustness and imperceptibility. Watermark is embedded into high entropy valued region by employing DWT and SVD method.

Chen et al. [8] reported an audio watermarking scheme based on wavelet based entropy in order to achieve robustness against different attacks. Watermark is embedded into low frequency co-efficient of wavelet based entropy, and watermark extraction is only possible by values of wavelet based entropy.

Yanyanhan et al. [2] presented digital image watermarking scheme in wavelet domain for color images that help in

enhancing security and robustness. This method extracts blue channel of host image and processed image in wavelet domain for watermark Embedding. Watermarks are embedded in high frequency as well as low frequency region of wavelet domain. For enhancing security of watermarking scheme, visual cryptography and Arnold transform are exploited with watermarking scheme. Rawat et al. [1] also proposed watermarking method that employs FrFT and Visual cryptography techniques with an aim to accomplish robustness and security. Security of method is ensured by means of visual cryptography.

Huai-bin et al. [6] reported blind digital image watermarking method based on fusion of DCT and DWT with the aim of improving imperceptibility, robustness and security. Arnold transform is exploited to ensure security of watermark. Watermark is embedded in middle frequency DCT coefficients of LL band of DWT.

Lin et al. [4] presented DCT based watermarking method in order to improve robustness against JPEG compression for color images. Watermark is embedded in low frequency DCT components of YUV domain by employing concept of mathematical remainder. In this, security and robustness of watermarking method is enhanced by exploiting properties of torus automorphism on watermark.

Fang et al. [5] reported a blind watermarking method that exploits concepts of Arnold and quantification. Watermark image is preprocessed by means of Arnold transform before embedding in order to increase security and robustness. Watermark bits are embedded in intermediate frequency coefficients of DCT domain.

In 2014, Musrrat et al. [3] proposed robust watermarking method by utilizing DE of DCT and SVD domain in order to maintain tradeoff between imperceptibility and robustness. Singular values of block DC coefficients are utilized for watermark embedding. In this, security of method is ensured by applying Arnold transform and differential evolution is applied to maintain the tradeoff.

In 2017, Sari et al. [10] developed a DCT and singular value decomposition based watermarking method to for color images in order to attain imperceptibility and robustness. This method converts image into YCbCr color space, and then, image is further processed for watermark embedding. Watermarking is embedded into singular values of DC coefficients of host image that helps in achieving robustness and imperceptibility.

III. Proposed Work

It is proposed to design and develop a watermarking technique which is optimized through entropy to give better imperceptibility and robustness and security method by using chaotic grid as a key to shuffle the embedding locations of the host image so that it will add one more step to the security of true watermark extraction process.

A. Watermark Embedding Method

In this section, watermarking embedding process is given. During embedding process, a cover image is preprocessed with DCT [11], [15], and then, entropy is considered to select location to insert the watermark bits. These selected locations are shuffled in a specified manner to increase the security of watermarking method. This algorithm is implemented in MATLAB software [16].

Proposed scheme is given in below steps:

Step 1: Read the input image and convert it into gray scale format.
Step 2: Split the image in to non-overlap blocks and compute entropy for each block and sort the blocks according to it's the increasing order of entropy.
Step 3: Select the first 1024 blocks only as watermark image of size 32X32 i.e.1024 bits.
Step 4: Reorder the blocks in a specific order described by a chaotic grid to add the security.
Step 5: Split the host image in to non-overlap blocks and then apply 2 dimensional – DCT on each block to compute DCT coefficients.
Step 6: Selecting the locations of the blocks of DCT coefficients based on the re ordered as per the shuffled blocks.
Step 7: Insert the watermark into the second row and second column of the each DCT blocks in the order of the re ordered sorted blocks based on its entropy.
Step 8: Apply Inverse DCT to obtain watermarked image.
Step 9: Display the Watermarked image.

B. Watermark Extraction Method

This process is almost following the reverse of the steps followed in embedding method,

Extraction method is given in below steps:

Step 1: Read the watermarked image.
Step 2: Split the image into non-overlap blocks and compute the entropy and sort them in the increasing order.
Step 3: Reorder the blocks in the same order specified by the key considering first 1024 blocks.
Step 4: Split the image in to non-overlap blocks and then apply two-dimensional – DCT on each block to compute DCT coefficients.
Step 5: Sort the DCT blocks corresponding to the reordered blocks based on the entropy.
Step 6: Extract the watermark value from the location of the blocks in the same sorted sequence and regenerates the watermark image.

IV. Results and Discussion with Performance Evaluation the Proposed Method

The proposed method is implemented on four different images like Lena, Cameraman, Coins and pepper. To prove the effectiveness of the method, the performance evaluation is done after applying different attacks.

A. Imperceptibility

The proposed method is evaluated in terms of perception of the watermarked image by measuring imperceptibility. Peak signal to noise ratio (PSNR) and Mean square error (MSE) value is calculated using watermarked image and the original

image. MSE is computed which represents the cumulative squared error between original image and watermarked image.

$$\text{MSE} = \frac{\sum_{MN}[I_{1(m,n)} - I_2(m,n)]^2}{M*N} \quad (1)$$

Here, M and N are representing the size of the given input image [17], I(m,n) represents the pixel intensity at coordinate(i,j). Then PSNR is computed by using [17]:

$$\text{PSNR} = 10 \log_{10}\left(\frac{R^2}{MSE}\right) \quad (2)$$

R denotes maximum pixel intensity value of the image.

The proposed method is implemented on different images and the resultant PSNR and MSE values for the watermarked images are shown in Table I.

TABLE I
PSNR AND MSE VALUES FOR THE DIFFERENT WATERMARKED IMAGES

	Camera man image	Coins Image	Lena Image	Pepper Image
PSNR	50.5808	51.1199	50.5808	50.5808
MSE	0.5688	0.5025	0.5688	0.5688

The above table shows very convincing PSNR above 50 and it shows that the proposed embedding method is very good imperceptible.

The original and watermarked images are shown in Fig. 1.

B. Robustness

The robustness of the proposed method is evaluated by measuring the Normalized correlation (NC) using original watermark image and extracted watermark from the watermarked image after applying different attacks on the watermarked image. NC is measures similarity between original watermark and extracted watermark. This value indicates how strongly the proposed method withstands the attacks to protect the imbedded watermark.

$$NC(W, W^*) = \frac{\sum_{i=1}^{N1}\sum_{j=1}^{N2} W(i,j) * W^*(i,j)}{\sqrt{\sum_{i=1}^{N1}\sum_{j=1}^{N2} W^2(i,j)}\sqrt{\sum_{i=1}^{N1}\sum_{j=1}^{N2} W^{*2}(i,j)}} \quad (3)$$

where W(i,j) and W*(i,j) denotes the (i,j)th pixel value of the original and extracted watermark.N1 and N2 are the sizes of the watermark [17].

To measure robustness of the method, different attacks are applied on the watermarked image like

1. Median filtering attack
2. AVG filtering attack
3. Resizing Attack
4. JPEG compression attack
5. Cropping from Centre attack
6. Rotation attack
7. Histogram equalization attack
8. Addition of Gaussian noise
9. Addition of wiener Filtering
10. Gaussian average Filtering

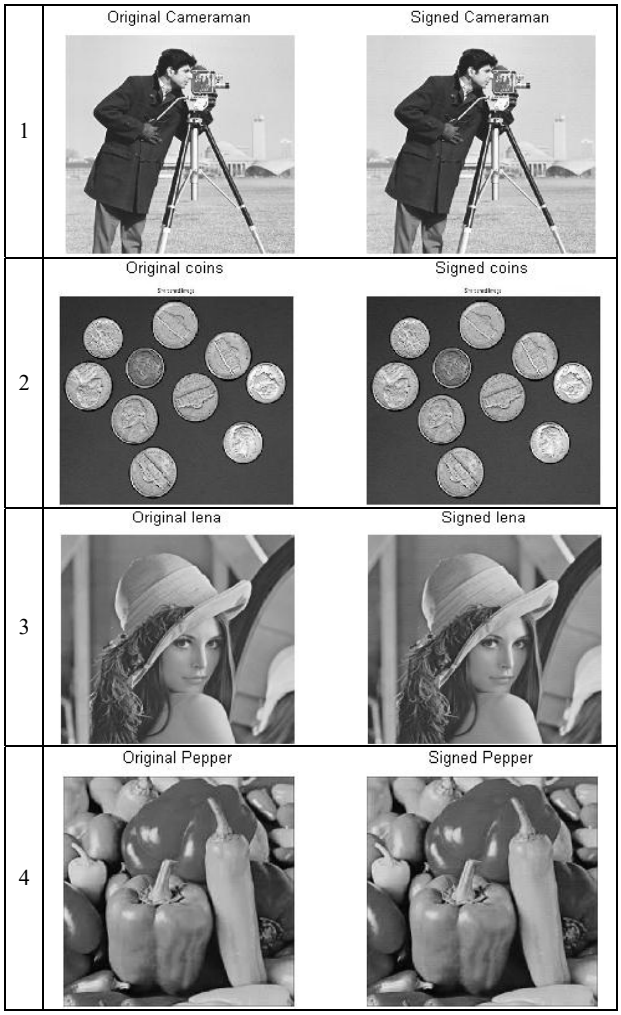

Fig. 1 Original and watermarked images

Normalized Correlation between original watermark and extracted watermark images using the proposed technique are as follows

1. Cameraman Image

The NC values observed after applying different attacks are shown in Figs. 2 (a)-(j).

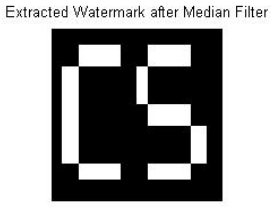

Fig. 2 (a) NC value is 1with Median filter attack

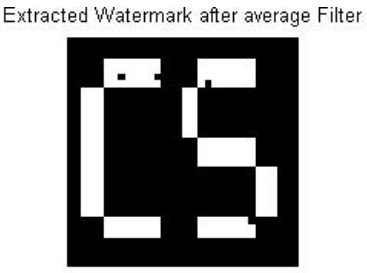

Fig. 2 (b) NC value is 0.9914 with Average filter attack

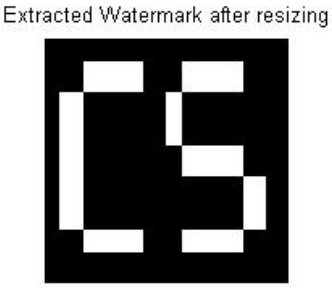

Fig. 2 (c) NC value is 1 with Resizing attack

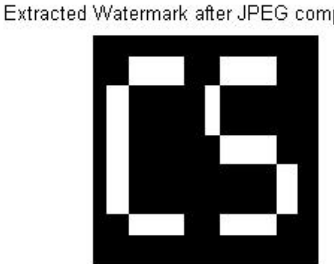

Fig. 2 (d) NC value is 1 with JPEG attack

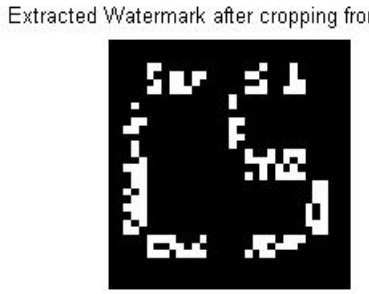

Fig. 2 (e) NC value is 0.7498 with Cropping attack

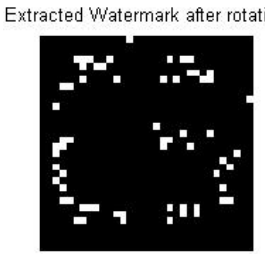

Fig. 2 (f) NC value is 0.4952 with Rotation attack

Fig. 2 (g) NC value is 0.7830 with Histogram equalization attack

Fig. 2 (h) NC value is 0.5314 with Gaussian noise attack

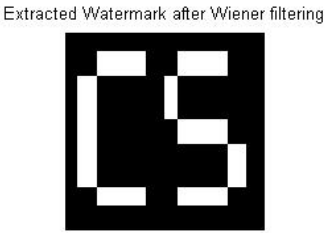

Fig. 2 (i) NC value is 1 with Wiener filtering attack

Fig. 2 (j) NC value is 0.9914 with Gaussian average filter attack

2. Coins Image

The NC values observed after applying different attacks are shown in Figs. 3 (a)-(j).

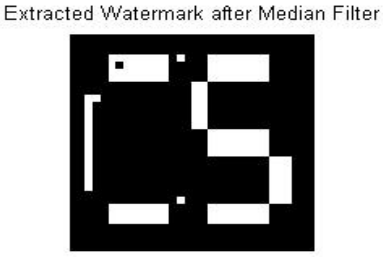

Fig. 3 (a) NC value is 0.9054 with Median filter attack

Extracted Watermark after Median Filter

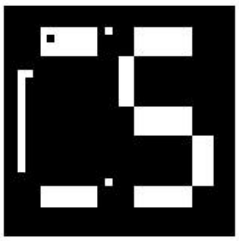

Fig. 3 (b) NC value is 0.8235 with Average filter attack

Extracted Watermark after resizing

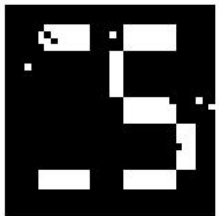

Fig. 3 (c) NC value is 0.8568 with Resizing attack

Extracted Watermark after JPEG compression

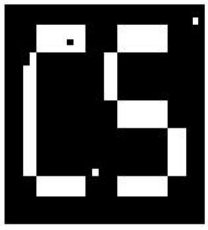

Fig. 3 (d) NC value is 0.9494 with JPEG attack

Extracted Watermark after cropping from center

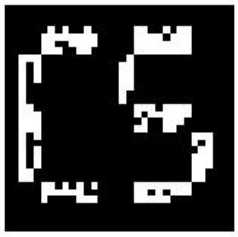

Fig. 3 (e) NC value is 0.8542 with Cropping attack

Extracted Watermark after rotation

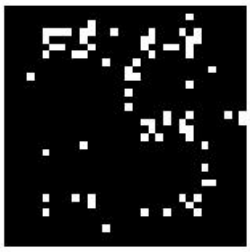

Fig. 3 (f) NC value is 0.4677 with Rotation attack

Extracted Watermark after histogram equalization

Fig. 3 (g) NC value is 0.7212 with Histogram equalization attack

Extracted Watermark after addition of Gaussian noise

Fig. 3 (h) NC value is 0.444 with Gaussian noise attack

Extracted Watermark after Wiener filtering

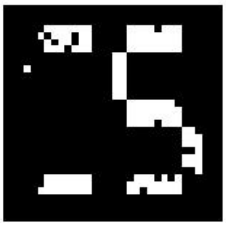

Fig. 3 (i) NC value is 0.8235 with Wiener filtering attack

Extracted Watermark after Gaussian Average Filterin

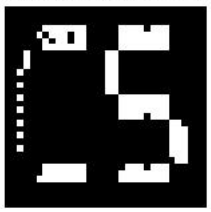

Fig. 3 (j) NC value is 0.8642 with Gaussian average filter attack

3. Lena Image

The NC values observed after applying different attacks are shown in Figs. 4 (a)-(j).

Extracted Watermark after Median Filter

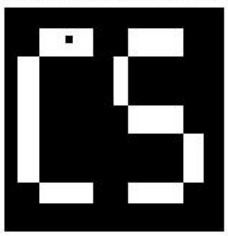

Fig. 4 (a) NC value is 0.9979 with Median filter attack

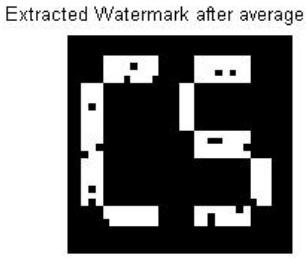

Fig. 4 (b) NC value is 0.9606 with Average filter attack

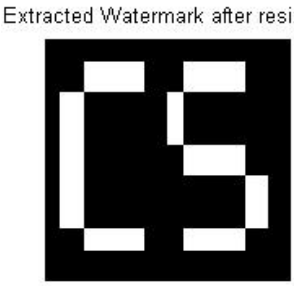

Fig. 4 (c) NC value is 1 with Resizing attack

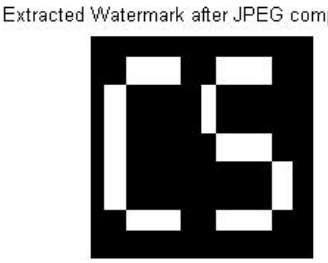

Fig. 4 (d) NC value is 1 with JPEG attack

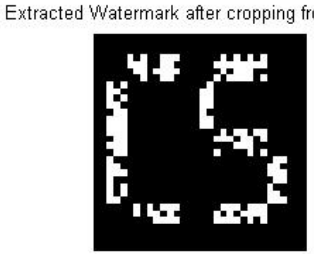

Fig. 4 (e) NC value is 0.8156 with Cropping attack

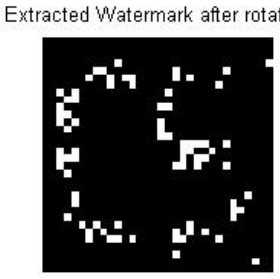

Fig. 4 (f) NC value is 0.5640 with Rotation attack

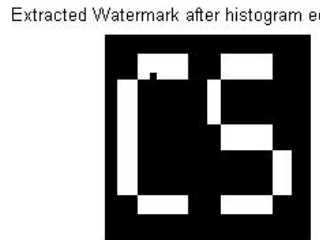

Fig. 4 (g) NC value is 0.9979 with Histogram equalization attack

Fig. 4 (h) NC value is 0.5383 with Gaussian noise attack

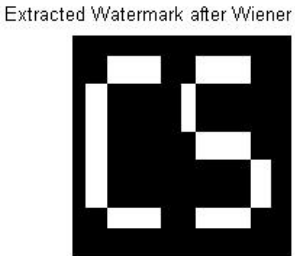

Fig. 4 (i) NC value is 1 with Wiener filtering attack

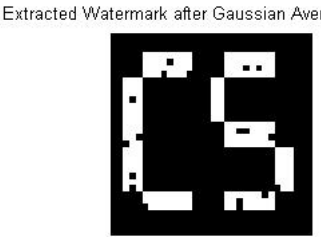

Fig. 4 (j) NC value is 0.9606 with Gaussian average filter attack

4. Pepper Image

The NC values observed after applying different attacks are shown in Fig. 5 (a)-(j).

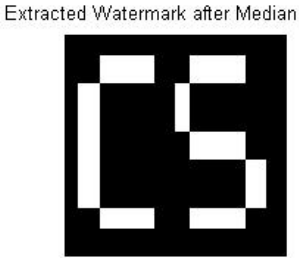

Fig. 5 (a) NC value is 1 with Median filter attack

Extracted Watermark after average Filter

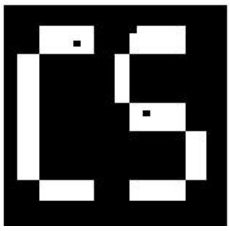

Fig. 5 (b) NC value is 0.9935 with Average filter attack

Extracted Watermark after resizing

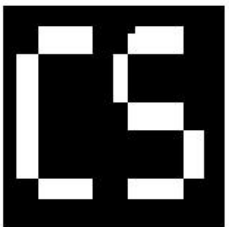

Fig. 5 (c) NC value is 0.9979 with Resizing attack

Extracted Watermark after JPEG compression

Fig. 5 (d) NC value is 0.9894 with JPEG attack

Extracted Watermark after cropping from center

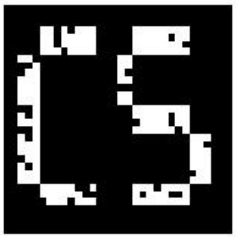

Fig. 5 (e) NC value is 0.9148 with Cropping attack

Extracted Watermark after rotation

Fig. 5 (f) NC value is 0.6493 with Rotation attack

Extracted Watermark after histogram equalization

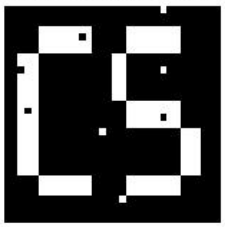

Fig. 5 (g) NC value is 0.9828 with Histogram equalization attack

Extracted Watermark after addition of Gaussian noise

Fig. 5 (h) NC value is 0.5321 with Gaussian noise attack

Extracted Watermark after Wiener filtering

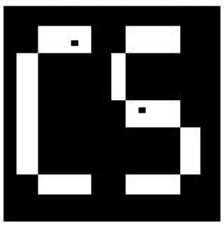

Fig. 5 (i) NC value is 0.9957 with Wiener filtering attack

Extracted Watermark after Gaussian Average Filtering

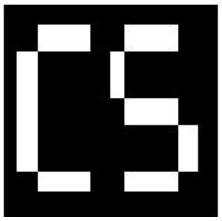

Fig. 5 (j) NC value is 1 with Gaussian average filter attack

V. Conclusions

The results show that the proposed technique is very good in terms of imperceptibility as the embedding locations are optimized using entropy. The same was calculated through MSE and PSNR and it is found to be in the range of 50. The proposed method is found to be robust against different attacks and is proved by considering 10 different attacks. It is observed that it has given very good results of normalized correlation (NC) is 1 for some attacks and it very closed to 1 for some. This method is not able to give very good results for rotation and Gaussian noise attack. This method is not only proving the convincing results in terms of imperceptibility and robustness, it is very secured also as no one can be able to

extract the true watermark just by knowing the procedure used in embedding. It requires key which is a grid pattern to reveal the true watermark.

VI. Future Scope

This method can be further optimized by using different machine learning algorithms. The proposed method being non-blind, this can be converted in to semi blind and blind methods.

References

[1] B. R. Sanjay Rawat, "A blind Watermarking Algorithm based on fractional fourier transform and visual cryptography," Signal Processing, Elsevier, pp. 1480-1491, 2011.
[2] W. H. a. Y. s. Yanyan Han, "DWT- domain Dual watermarking algorithm of color image based on visual cryptography," in IEEE, 2013.
[3] C. W. A. M. P. Musrrat Ali, "A robust image watermarking technique using SVD and differential evolution in DCT domain.," Optik-International Journal for Light and Electron Optics,Elsevier, vol. 125, no. 1, pp. 428-34., 2014.
[4] S.-C. S. J. G. Shinfeng D. Lin, "Improving the robustness of DCT-based image watermarking against JPEG compression," Computer Standards & Interfaces, vol. 32, no. 1-2, pp. 54-60, 2010.
[5] F. M. Z. Zhang, "A Blind Watermarking Thchnology Based on DCT Domain," in International Conference on Computer Science and Service System, 2012.
[6] Y. H.-l. C.-d. W. S.-m. WANG Huai-bin, "A New Watermarking Algorithm Based on DCT and DWT Fusion," in International Conference on Electrical and Control Engineering, 2010.
[7] N. G. Gurwinder Singh, "Entropy Based Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition," in 2016 IEEE International Conference on Computing for Sustainable Global Development, New Delhi, 2016.
[8] H.-N. H.-J. C.-K. T.-Y. T. Sho-Tsung Chenn, "Adaptive Audio Watermarking Via Optimization Point of View On The Wavelet-Based Entropy," Digital Signal Processing, vol. 23, pp. 971-980, 2013.
[9] A. D. Sanjay kumar, "A novel Spatial domain Technique for Digital Image Watermarking using Block Entropy," in IEEE Conference on Recent Trends in Information Technology (ICRTIT), 2016.
[10] E. H. R. R. I. M. S. Christy Atika Sari, "Robust and imperceptible image watermarking by DC coefficients using singular value decomposition," in 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Yogyakarta, Indonesia, 2017.
[11] Mehta R, Rajpal N, Viswakarma VP," Adaptive image watermarking Scheme Using fuzzy Entropy and GA ELM Hybridization in DCT domain for copyright protection", J Signal process Syst 84,2016,265-281.
[12] Pooja Kulkarni, "Review of Digital watermarking techniques", International journal of computer applications, Vol 109, No 16, 2015
[13] Zhi-Hong Guan," Chaos based image encryption algorithm", Physics letters A, 2005,153-157.
[14] Rama Kishore, "Digital watermarking based on Visual cryptography and histogram", International journal of computer, Electrical, Automation, control and information engineering", Vol10, 2016.
[15] Pravin M, "DCT based Digital image watermarking, De watermarking and Authentication", International journal of latest trends in Engineering and technology, vol2, 2013.
[16] Rafael C Gonzalez, "Digital image processing using MATLAB", Mc Graw Hill Education, 2010,
[17] Rajesh Metha, "LWT-QR decomposition based robust and efficient image watermarking scheme using lagrangian SVR", Multimedia tools and application, Springer,2015.

R. Rama Kishore is currently working as an Associate Professor at University School of Information, Communication and Technology, G.G.S.Indraprastha University, Delhi. He received his PhD degree from G.G.S.Indra Prastaha University, Delhi and M. Tech from I.I.T. Delhi. His area of interests includes Computer Graphics, Multimedia technologies, Image processing etc.

Sunesh received B.E. degree in Computer Science and Engineering from Maharishi Dayanand University and the M.Tech degree from Chaudhary Devi Lal University, Haryana. She is currently an Assistant Professor with Maharaja Surajmal Institute of Technology, New Delhi, India and also working towards Ph.D. degree with University School of Information, Communication and Technology, Guru Gobind Singh Indraprastha University, New Delhi, India.