RESEARCH ARTICLE OPEN ACCESS

A Novel Algorithm on Wavelet Based Robust Invisible Digital Image Watermarking for Multimedia Security

Mr.K.SRIDHAR, Dr.syed abdul sattar, Dr. M Chandra Mohan
*ASST PROF IN VREC, NIZAMABAD,
**Professor&dean of academics, Royal institute of technology sciences, Chevella,R.R.Dist,
***Computer Science & Engineering, JNTUH College of Engineering Hyderabad (Autonomous)

Abstract
This paper presents a new algorithm on waveletbased robust and invisible digital image watermarking for multimedia security. The proposed algorithm has been designed, implemented and verified using MATLAB R2014a simulation for both embedding and extraction of the watermark and the results of which shows significant improvement in performance metrics like PSNR, SSIM, Mean Correlation, MSE than the other existing algorithms in the current literature. The cover image considered here in our algorithm is of the size (256x256) and the binary watermark image size is taken as (16x16).
***Keywords**: Digital Image Watermarking Algorithm; Wavelet; MATLAB R2014a; Multimedia Security; Robust and Invisible; PSNR; SSIM; Mean Correlation; MSE

I. INTRODUCTION

In recent years there has been growing interest in developing effective techniques to discourage the unauthorized duplication of digital data. The technology designed to make electronic publishing feasible has also increased the threat of intellectual property theft. One approach to address the problem is called digital watermarking. Digital watermarking is the imperceptible marking of multimedia data to “brand” ownership. The process of digital watermarking involves the modification of the original multimedia data to embed a watermark containing key information such as authentication or copyright codes. The embedding method must leave the original data perceptually unchanged, yet should impose modifications which can be detected by using an appropriate extraction algorithm. Common types of signals to watermark are images, music clips and digital video. In this paper we concentrate on the application of digital watermarking to still images.[1]

We will only consider here invisible watermarks that protect rights by embedding ownership information into the digital image in an unnoticeable way. This imperceptibility constraint is attained by taking into account the properties of the human visual system (HVS), which in turn helps to make the watermark more robust to most types of attacks. In fact, robustness of the watermark is a capital issue, since it should be resilient to standard manipulations, both intentional and unintentional[2].There are two parts to building a strong watermark: the watermark structure and the insertion strategy.

In order for a watermark to be robust and secure, algorithm under different attacks. In [6], PSNR of thethese two components must be designed correctly [17].

We propose a transform domain technique which shows greater robustness to common signal distortions. The fundamental advantage of our wavelet-based technique lies in the method used to embed the watermark in each of the resolution levels. The approach provides the simultaneous spatial localization and frequency spread of the watermark within the host image to provide robustness against widely varying signal distortions such as cropping and filtering.

Section II describes literature survey. In section III wavelet preliminaries are explained and our selection of wavelet and corresponding Sub-bands for encoding is explained. In section IV, the proposed algorithm is described within which, in IV-A Encoding algorithm is explained and in IV-B Decoding algorithm is described. In section IV-C watermark encoding and decoding block is explained with figure. Next in section V performance evaluation is being explained. In V-A different performance metrics are described which we will be calculating for analyzing the performance of the algorithm. In V-B experimental results for the algorithm are given & are compared with previous works. During comparison it was found that there is a gap between the results given in previous works. Where attacks were performed has failed to give any satisfactory result for imperceptibility and vice versa. In most of the cases optimum performance metrics ware not found. In section IV-B we draw some inference from the experimental results and evaluate the quality & reliability of the algorithm. Section VI concludes about the new algorithm and shows light on further works that can be carried on with the work done.

II. LITERATURE SURVEY

In 1997 cox.et.al [16] proposed spread spectrum watermarking using DCT and different attacks were made to verify the sustainability of the algorithm to attacks. In 2000 changedal[5] used pyramid transform for spatial-frequency domain embedding and PSNR was found to be 45.2 but lacked in analysis of other performance metrics and attack sustainability. In 2007 yang et al [6] proposed HVS based watermarking. In 2008 Yusuf et al [7] focused to analyze DWT based watermarking and evaluated performance of the watermarking algorithm varies from 50dB to 21dB but this drastic variation is occurring for a small change in embedding strength (0.01- 2.0) whereas in [7] the variation of the gain factor is between 2 to 8 , hence not very much controllable for adjusting imperceptibility with robustness. We analyzed [3], [5], [7], [9], [16], [18], [19], [23] and every schemes are using different processes like SVD, HVS, DCT, DWT and others but the PSNR value ranges from 35dB to 45dB at an average and most of them have not provided SSIM and CORRELATION after attack.

Where attacks were performed has failed to give any satisfactory result for imperceptibility and vice versa. In most of the cases optimum performance metrics were not found. In 2008 Maity et al[18] proposed a different spread spectrum watermarking algorithm using wavelet based Hilbert transform and also incorporated QCM for capacity improvement but average PSNR in this algorithm is 35 dB and average SSIM is 0.95 for single watermark embedding. In 2012 Rivet al [4] proposed an algorithm using 4 level DWT and SVD with shared secret key and average PSNR is found to be 47 and correlation is around 0.9988. Thereafter different attacks were performed and correlation for each of the decoded watermark from the attacked image is analyzed.

III. WAVELET PRELIMINARIES

A wavelet basis set starts with two orthogonal functions, which are Scaling function and Wavelet function . By scaling and translation of the above two functions we obtain a complete basis set. In a wavelet basis set consists of one scaling function and the rest of the elements are the wavelet functions. The scaling function captures the average part of the signal whereas the wavelet function captures thedifferences. The Wavelet Transform of a function f (t) isdefined

$$f(t) = \sum_{k=-\infty}^{\infty} c_k \varphi_k(t) + \sum_{j=-\infty}^{\infty}\sum_{k=-\infty}^{\infty} d_{jk}\psi_{jk}(t)$$

The coefficients c_k, d_{jk} represent the DWT of the function f(t), where c_k represent the average parts (LL) and the d_{jk} represent the variations at different scales (LH,HL,HH) and these features are common to all wavelets.

$$c_k = \int f(t)\Phi_k(t)\, dt \text{.........} (2)$$
$$d_{jk} = \int f(t)\psi_{jk}(t)\, dt \text{.......} (3)$$

Within each family of wavelets, wavelet subclasses are distinguished by number of coefficients and by the level of iteration.

Bi-orthogonal Wavelet

The L2(R) inner product <f, g >= Rf(x) ÷ (x) introduces an identification of L2(R) with its dual space. An important generalization is a bi-orthogonal wavelet system in which one replaces a function satisfying quadratic equations with pairs of functions satisfying bilinear equations and since the bilinear conditions generalize the usual orthogonality equations, these biorthogonal equations and the corresponding functions are called biorthogonal wavelets and are defined as follows:

$$\phi(t) = \sqrt{2}\sum_{n=-\infty}^{\infty} h[n]\phi(2t-n) \text{.......} (4)$$
$$\hat{\phi}(t) = \sqrt{2}\sum_{n=-\infty}^{\infty} h[n]\hat{\phi}(2t-n) \text{.......} (5)$$
$$\psi(t) = \sqrt{2}\sum_{n=-\infty}^{\infty} g[n]\phi(2t-n) \text{......} (6)$$
$$\hat{\psi}(t) = \sqrt{2}\sum_{n=-\infty}^{\infty} g[n]\hat{\phi}(2t-n) \text{......} (7)$$

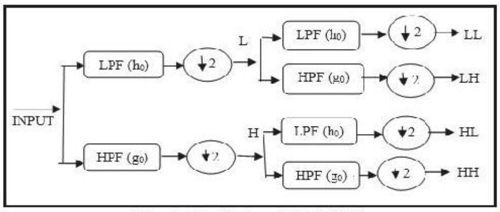


Fig. 1:Single level 2D DWT

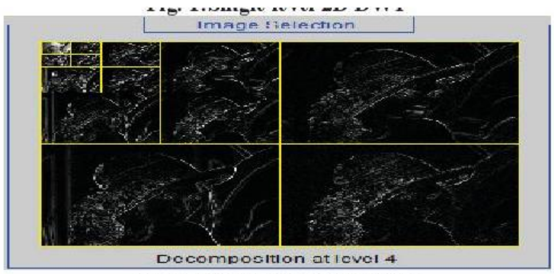


Fig. 2: 4 level 2D DWT of lena

In this paper we use **Bi-orthogonal1.1** wavelet for transformation both in analysis & synthesis part.

We use LL sub-band for lower levels of transforms and embed data in the mid-band of the corresponding transformed LL sub-band i.e. if 2 level transform is done, then first the image is transformed and again wavelet transform is done in LL1 band. That LL1 will have LL2, LH2, HL2& HH2. We will select LH2 & HL2 for watermark encoding. The reason behind this is LL band consists of low frequency parts of the image and most of the information is present over there. Higher frequency regions have fewer details and are very prone to attack. That's why we select LL band for further transform. On the other hand since most of the information is present in LL band, it will have impact in perceptual quality of the image. Hence for watermark encoding mid band i.e. LH & HL of transformed LL of lower level is selected.

IV. PROPOSED WATERMARKING ALGORITHM

We propose an algorithm for watermarking which will embed a binary watermark (16x16) in a gray scale cover image of size (256 x 256). The basic sequence is as below.

A. Encoding Algorithm

Step 1: Take a grayscale cover image of size (256 x 256).

Step 2: Apply 2D Bi-orthogonal DWT in 4 levels & get wavelet coeff matrices defining approx, horizontal, vertical & diagonal details as LL4, LH4, HL4 & HH4 suands(m x m).

Step 3: Take a PN-sequence of equal size of that of wavelet transformed coefficient matrix (m x m).

Step 4: Take a binary watermark of size (m x m)

Step 5: Sum the PN-sequence and the watermark element by element. This is the final data to be embedded.

Step 6 : If the binary watermark =1 then , new wavelet coeff matrix is sum of the old one with the embedding data multiplied by some constant factor & if it is 0, the new coeff matrix is old coeff matrix minus the embedding data multiplied by the same constant factor.

Step 7: Change the mid-bands i.e. LH & HL sub-bands by the above method for better imperceptibility. Thus the LH & HL bands will have watermarked coefficients.

Step 8: Perform inverse 2D-DWT for 4 levels using same wavelet but with the new wavelet coefficients. Generate the watermarked image.

Reason behind addition of the PN-sequence and watermark information:

Suppose we have a wavelet transformed coefficient of value 15. Following are the possibilities that can happen without addition:

TABLE I. PN SEQUENCE CASE STUDY

PN-sequence	Watermark	Result(k=2)
0	0	15-0=15
0	1	15+0=15
1	0	15-2=13
1	1	15+2=17

Here we see that if the PN-sequence is 0 then whatever be the watermark, there will be no change of the coefficient which will pose great unreliability during decoding. Thus we sum the PN-sequence and the watermark which eliminate this problem.

TABLE II. PN SEQUENCE CASE STUDY

PN-seq(p)	Watermark(w)	Embedding data(p+k*w)	Result (k=2)
0	0	0+2*0	15
0	1	0+2*1	17
1	0	1+2*1	13
1	1	1+2*2	19

Thus if the new coefficient is less than or equal to old one, we get (w) =0 & if it is greater than the old one we get (w) =1 & hence we get perfect reconstruction.

B. Decoding Algorithm

- We take the original cover image and perform wavelet transform using the same wavelet as we used in the encoder.
- We take the watermarked image or its possibly distorted version and perform the same wavelet transform.
- We now compare the wavelet transform coefficients of the above two, both having same length.
- If the transformed watermarked image coefficient is less than or equal to the transformed original cover image coefficient, we get 0 & if it is greater, we get 1.

Though this algorithm is a non-blind one but it retains imperceptibility as well as robustness (including immunity to distortions) to a high degree (will be discussed in details in performance evaluation section). The non-blind method of extraction is outperforming the blind method because of the availability of original image and has been proved much more robust [3].

Now the k (constant factor) is a very important value which is often called modulation index and it determines the degree robustness and imperceptibility. More the value of k, more the wavelet coefficients will change which results in two situations

- Having more change in coefficient, it will be easier to reconstruct and will be much more immune to noise or distortions.
- Since the coefficients are highly different than the original ones, there will be high visual quality degradation and imperceptibility will be compromised.

Hence we propose a model for encoding and its corresponding decoding.

C. Watermark Encoding & Decoding Model

We summarize the significant parts of this model.

- We take 16 different PN-sequences, each of length 16 and rearrange to form 16x16 matrixes.
- 4 level wavelet transform is performed in LL

sub-band and watermark is embedded in the mid-band (LH4 & HL4) after wavelet transforming LL3 sub-band. Both LH4 & HL4 are 16x16 matrixes.

The total encoder block and decoder block is given in **Fig. 3**&**Fig. 4** respectively.

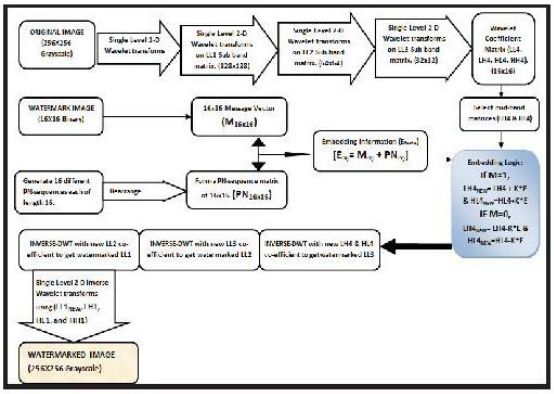


Fig. 3: Encoder Flow Chart

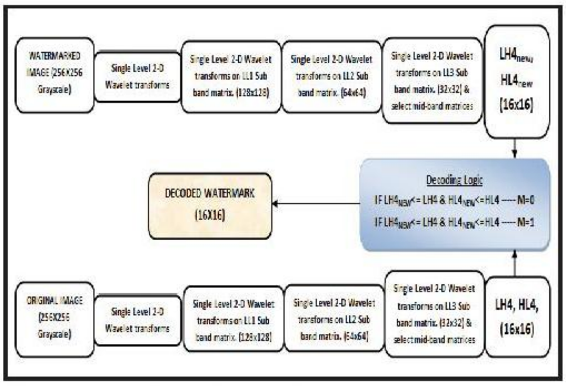


Fig. 4: Decoder Flow Chart

V. PERFORMANCE EVALUATION

The performance evaluation of image watermarking algorithm mainly includes imperceptibility, robustness, the hidden capability and security [7]. These evaluations are different according to different situations [4] [5] [6] [7].

A. Performance Metrics

*1) **Imperceptibility**(namely transparency, invisibility) isthat neither the carrier has the perceptibility change and nor does the perceptibility distortion on quality occur after the watermarking information is embedded [8].*

*Two commonly used measures are the **MeanSquared Error(MSE)** function and the **Peak Signal to Noise Ratio (PSNR).***

The MSE between the original image (I_0) and watermarked image, (I_W)

$$\mathbf{MSE=1/N\sum\ (I_0\ [j,\ k]\ -\ I_W\ [j,\ k])^{\ 2}}$$

where N=number of pixels in each image sum over j, k =sum over all pixels in the image.

The PSNR which is usually expressed in decibel scale (dB) is defined as:

$$\mathbf{PSNR=20\ log_{20}\ (MAX_I/\sqrt{MSE})}$$

Typical range for PSNR values is between 30 to 50 dB, with notion that higher is better where the differences are visually indistinguishable by human eyes [12]. Thus for conformity, both visual inspections and distortion measures (i.e. MSE and PSNR) are used together to determine imperceptibility [9].

*2) **Robustness***

In this paper we analyze two different performance metrics for robustness calculation.

The **Correlation Coefficient** is a measure association

$$Corr = \frac{\sum_m \sum_n (A_{mn}-\bar{A})(B_{mn}-\bar{B})}{\sqrt{[\sum_m \sum_n (A_{mn}-\bar{A})^2][\sum_m \sum_n (B_{mn}-\bar{B})^2]}} \ldots$$

The value of correlation coefficient lie betweení1and+1. If two watermarks are identical, then its value will be+1, if they are completely opposite (i.e., one is negative of other) then its value will be í1 and it will be 0 if watermarks are completely uncorrelated. T he correlation coefficient value from 0.4 to 0.9 indicates significant similarity between two watermarks [4].

The robustness evaluation c an also be determined by using **Structural Similarity (SSIM) index**, a new promisingmethod for measuring the similarity between two images [10]. The SSIM index can be viewed as a quality measure of one of the images being compared provided the other image is regarded as of perfect quality [11].

These three factors are actually interrelated and can be expressed as:

$$\mathbf{PSNR=\ 20\ log\ (MAX_I/\ [\sigma\ \sqrt{C}\ ((1/p)\text{-}2)])\ \ldots}$$

*B. **Experimental Results***

All the experimentation and testing is performed on Windows-7 platform. MATL AB version R2014a is used for the implementation of the proposed algorithm. Table III gives performance metrics change with increasing gain.

Time Complexity: Since weare using nested for-loop in thealgorithm, the number of operations increases in a quadratic manner. For doubling N, the number of operation increases N*N. Hence the time-complexity of the proposed algorithm (both encoding and decoding) is **O ($\mathbf{n^2}$)** where **n** is the number of pixels processed per unit time.

TABLE III. PERFORMANCE METRIC FOR VARIOUS MODULATION INDEX

Quality Metric	GAIN/MODULATION INDEX				
	K=1	K=5	K=8	K=15	K=20
MSE	0	0.3965	0.8066	3.2266	5.1058
PSNR	Inf	52.1485	49.0640	43.0434	41.0502
SSIM	1	0.9989	0.9978	0.9914	0.9867

Table IV provides information about correlation value of recovered watermark with the original one when the watermarked image is attacked.

TABLE IV. CORRELATION OF RECOVERED WATERMARK FOR DIFFERENT ATTACKS

Distortions	GAIN/MODULATION INDEX				
	K=1	K=5	K=8	K=15	K=20
No noise	NAN	1	1	1	1
Gaussian noise	NAN	0.25	0.25	0.46	0.609
Poisson noise	NAN	0.56	0.625	0.74	0.831
Salt & pepper noise	NAN	0.24	0.22	0.45	0.586
Speckle noise	NAN	0.323	0.30	0.53	0.674
Median filtering	NAN	0.63	0.67	0.80	0.804
Histogram equalization	NAN	0.07	0.09	0.16	0.21

Table V & VI provides a detailed performance metrics and watermarked image for different cover images at maximum and minimum allowable gain values. Figure 5 & 6 provides the graphical representation of PSNR & SSIM variation.

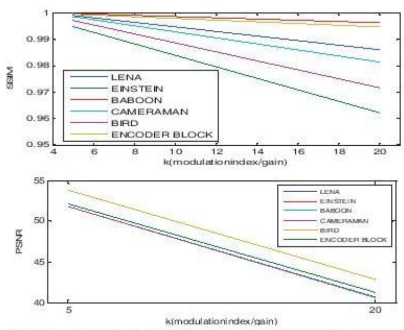


Fig. 5 & 6 : SSIM & PSNR Vs. K(gain) [K= 5 & 20] for various cover images

As we implement the Model, the imperceptibility increases by a considerable extent and by the proposed algorithm, there is no significant visual quality distortion. At gain 20, average PSNR for different cover images is 41.05dB & average SSIM value of 0.9867. For gain 5, average PSNR is 52dB & average SSIM is 0.9989.

When we intentionally distort the watermarked image we get a fine correlation value between original watermark and decoded watermark ranging from 0.6 to 0.8 even after attack.

We compare the significant performance parameters for imperceptibility and robustness in Table VII.From the above results we notice some very interesting phenomena.

Since only 256 elements are being changed according to the Message Vector, by a PN-sequence out of 65536 elements and that too in fourth level of frequency domain, it has been highly imperceptible and the non-blind decoding has proved to be of great robustness. Unlike other works proposed in the existing literature we have analyzed the algorithm for large variety of cover images and proved successful in each of the cases.

In the comparative study of different performance metrics for different cover images, it is evident that for gain 20 also a satisfactory PSNR & SSIM value is achieved. We also took a practical example- the encoder block diagram. Since it is being developed by us, we implant a watermark within it. The result is giving PSNR of 53.79 and Similarity with the cover image is 99.95% for a gain of 5.

VI. CONCLUSION

This paper proposes a new improved algorithm & it is noticed that the proposed algorithm has good imperceptibility and retains robustness and immunity to attacks. Since we implemented non-blind watermarking, we have exploited its robustness at a high level and had perfect reconstruction every time in case no attack has been made, but if more Imperceptibility is required, gain can be fine-tuned according to the requirement. Thebi-orthogonalwavelettransformwithitsnoise/distortion for various modulation index unique time-frequency localization property helped watermark to get embedded in a very secure and invisible manner.

TABLE V. PERFORMANCE METRICS AND WATERMARKED IMAGES FOR DIFFERENT COVER IMAGES WITH LOWEST AND HIGHEST ALLOWABLE GAIN (K=5 & 20)

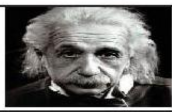
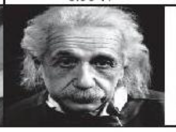
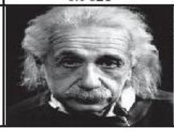
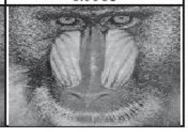
ORIGINAL IMAGE→						
	LENA		EINSTEIN		BABOON	
WATERMARK						
K→	5	20	5	20	5	20
MSE	0.4316	5.6233	0.4019	4.86	0.4316	5.62
PSNR	51.77	40.63	52.09	41.25	51.77	40.63
SSIM	0.9989	0.9860	0.9947	0.9621	0.9997	0.9961
WATERMARKE-D IMAGE						

TABLE VI. PERFORMANCE METRICS AND WATERMARKED IMAGES FOR DIFFERENT COVER IMAGES WITH LOWEST AND HIGHEST ALLOWABLE GAIN (K=5 & 20)

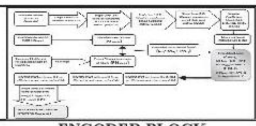
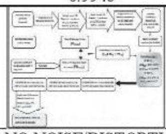
ORIGINAL IMAGE→						
	CAMERAMAN		BIRD		ENCODER BLOCK	
WATERMARK						
K→	5	20	5	20	5	20
MSE	0.4316	5.62	0.4316	5.62	0.2714	3.34
PSNR	51.77	40.60	51.77	40.63	53.79	42.89
SSIM	0.9985	0.9814	0.9981	0.9767	0.9995	0.9946
WATERMA-RKED IMAGE						
CORRELATION BETWEEN ORIGINAL WATERMARK & RECOVERED WATERMARK AT DECODER IN ALL ABOVE CASES UNDER NO NOISE/DISTORTION = 1						

TABLE VII. COMPARATIVE STUDY OF PERFORMANCE PARAMETERS WITH THE RESULT OF THE PROPOSED ALGORITHM

REFERENCE WORK →	[3]	[5]	[6]	[7]	[9]	[4]	[17]	[18]	[19]	[20]	PROPOSED WORK
PSNR (Max/Avg)	44	45	50/25	45	43/35	47/45	33/25	36/35	40/39	44	**53.79/46**
SSIM (Max/Avg)	NA	NA	NA	NA	NA	0.9994/ 0.9977	NA	0.9645 - 0.95	0.97	NA	**0.9997/ 0.9900**
CORRELATION (ATTACK)	NA	NA	NA	NA	NA	0.4-0.7	NA	NA	NA	NA	**0.60-0.85**

REFERENCES

[1] Deepa Kundur and Dimitrios Hatzinakos "Digital watermarking using multiresolution wavelet decomposition" ICASP, Vol 5, pp 2969-2972,IEEE,Washington,U.S.A,1998.

[2] Juan R. Hernández "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 9, NO. 1, JANUARY 2000, Pp 55-68

[3] V. Senthil , R. Bhaskaran, "Robustness Analysis of Blind and Non-Blind Multiple Watermarking using Edge Detection and Wavelet Transforms." IEEE ADCOM-2008 ,pp 106-111

[4] Gupta, Raval "A robust and secure watermarking scheme based on singular values replacement." Indian Academy of Sciences Vol. 37, Part 4, August 2012, pp. 425–440.(Masters Thesis)

[5] Q.Cheng and T.S.Huang, "Blind digital watermarking for images and videos and performance analysis." In 2000 IEEE International Conference on Multimedia and Expo, Vol. 1, pp. 389-392.

[6] Hongmei Yang, Yongquan Liang, Lianshan Liu, Haibin Sun "HVS-based Imperceptibility Measure of Watermark in Watermarked Color Image" 8th ACIS International Conference on Software Engineering,Artificial Intelligence,Networking, and Parallel/Distributed Computing. Pp.722-727

[7] Yusof,Khalifa "Imperceptibility and Robustness Analysis of DWT-based Digital Image Watermarking" Proceedings of the International Conference on Computer and

Communication Engineering 2008. pp.1325-1330

[8] XIE Qing “Performance Test and Analysis of Image Watermarking Algorithm Based on Singular Value Decomposition”2nd International Conference on Computer Engineering and Technology,2010 pp.282-286

[9] OthmanO.Khalifa et. al “Performance Evaluations of Digital Watermarking Systems” 8th International Conference on ICIDT, Vol.3, 2012 pp 533-536

[10] Wang, Z., Bovik, A. C., Sheikh, H. R. & Simoncelli, E. P. “The SSIM index for image quality assessment”. December 17, 2007.

[12] K. J. Kim K. H. Jung K. Y. Yoo. “A high capacity data hiding method using PVD and LSB[A]”. 2008 International Conference on Computer Science and Software Engineering (CSSE 2008)[C] Hubei, China Dec. 2008, pp 876-879.

[13] TONG Ming, YAN Tao, J I Hongbing. “Strong anti-robust watermarking algorithm”. Journal of Xidian Un iversity,2009,40(1): pp 22-27.

[14] Jiang Nan, Wang Jian, Niu Xinxin, Yang Yixian “ The Quantificational Relation of Imperceptibility, Robustness and Hi ding Rate in Digital Watermarking”. In International conference on Communications,Circuits& systems proc.2006, V ol-1, pp 11-14

[15] Meerwald & Uhl “A Survey Of Wavelet-do main Watermarking Algorithms” In Proceedings of SPIE, Electroni c Imaging, Security and Watermarking of Multimedia Contents III, vol. 4314, 2001.

[16] Ingemar J. Cox “Secure Spread Spectrum Watermarking for Multimedia”. IEEE Trans. Image Processing, vol. 6, no. 12, 1997.

[17] R. Grosbois & T. Ebrahimi “Watermarking in the JPEG 2000 domain”. 4th workshop on Mu ltimedia Signal Processing,IEEE, 2001 pp 339-344

[18] Santi Prasad MAITY et. al “ Wavelet Based Hilbert Transform with Digital Design and Application to QCM-SS Watermarking”. RADIOENGINEERING, VO L. 17, NO. 1, APRIL 2008, pp 64-72

[19] Santi P. Maity et. al “Design Of A Robust Spread Spectrum Image Watermarking Scheme”. ICV GIP, 2011.pp 145-150.

[20] Joachim J. Eggers, Jonathan K. Su and B.Girod “Robustness of a blind image watermarking scheme ” in proc. ICIP 2000Special Session on WM Vancouver, Canada2000.