Wavelet Based Blind Technique by Espousing Hankel Matrix for Robust Watermarking

Dr.M.Mohamed Sathik[1] , S.S.Sujatha[2]

[1] Associate Professor in Computer Science,
Sadakathullah Appa College, Tirunelveli, India
mmdsadiq@gmail.com

[2] Associate Professor in Computer Science,
S.T.Hindu College, Nagercoil, India
sujaajai@gmail.com

Abstract

The central idea of this paper is to propose an innovative watermarking scheme for digital image authentication which embeds watermark into the host image and provides qualities such as imperceptibility, robustness and security. A watermark signal is constructed from feature of original image instead of using external watermark. Several pixels are randomly selected from original image, so that all of them have a valid 3x3 neighborhoods. A binary sequence is constructed from those pixels by comparing them against average values of neighborhoods. The binary sequence is then converted into a watermark pattern in the form of a Hankel matrix to improve security of watermarking process and is then embedded within the host image. The operation of embedding and extraction of watermark is done in high frequency domain of Discrete Wavelet Transform since small modifications in this domain are not perceived by human eyes. This watermarking scheme deals with the extraction of the watermark information in the absence of original image, hence the blind scheme was obtained. The proposed algorithm was verified under common image processing attacks such as salt & pepper noise, Gaussian noise, median filtering, linear filtering, JPEG compression, blurring, scaling, intensity adjustment and histogram equalization. Peak Signal to Noise Ratio (PSNR) and Similarity Ratio (SR) are computed to measure imperceptibility and robustness of the watermark respectively.

Keywords: Digital watermarking, Discrete Wavelet Transform, Hankel Matrix, Image Authentication, Content based watermarking.

. Introduction

Due to the rapid growth of the internet and the extensive evolution of digital technologies, the distribution of digital multimedia content has sharply increased in a cost efficient way. Also the images can be readily shared, easily used, processed and transmitted which causes serious problems such as unauthorized use and manipulation of digital content. As a result, there is the need for authentication techniques to secure digital images. Digital watermarking is a technique which embeds additional information called digital signature or watermark into the digital content in order to secure it. A watermark is a hidden signal added to images that can be detected or extracted later to make some affirmation about the host image.

The major point of digital watermarking is to find the balance among the aspects such as robustness to various attacks, security and invisibility. The invisibleness of watermarking

technique is based on the intensity of embedding watermark. Better invisibleness is achieved for less intensity watermark. So we must select the optimum intensity to embed watermark. In general there is a little trade off between the embedding strength (the watermark robustness) and quality (the watermark invisibility). Increased robustness requires a stronger embedding, which in turn increases the visual degradation of the images. For a watermark to be effective, it should satisfy the following features.

- *Imperceptibility* - It should be perceptually invisible so that data quality is not degraded and attackers are prevented from finding and deleting it.
- *Readily Extractable* - The data owner or an independent control authority should easily extract it.
- *Unambiguous* - The watermark retrieval should unambiguously identify the data owner.
- *Robustness* – It should tolerate some of the common image processing attacks.

The digital image watermarking scheme can be divided into two categories. They are visible digital image watermarking and invisible image watermarking techniques. The commonly used watermarking applications include copyright protection, authentication, embedded and hidden information. Furthermore the invisible watermarks are categorized into watermarking techniques as fragile and robust. Generally, a robust mark is designed to resist attacks that attempt to remove or destroy the mark. These algorithms ensure that the image processing operations do not erase the embedded watermark signal. On the other hand a fragile mark is designed to detect slight changes to the watermarked image with high probability.

Several methods have been proposed and developed for digital watermarking. A survey is in [1]. The proposed methods can be classified according to the domain in which the embedding is performed. Two categories of Digital watermarking algorithms are spatial-domain techniques and frequency-domain techniques. Least Significant Bit (LSB) is the simplest technique in the spatial domain techniques [2] which directly modifies the intensities of some selected pixels. There are many variants of this technique. The data hiding capacity of these algorithms is high. However, these algorithms are prone to attacks by unauthorized users and hence are not robust.

The frequency domain technique transforms an image into a set of frequency domain coefficients [3]. The transform domain methods transform the original data into the frequency domain and then watermark is embedded in the frequency domain. Watermarking in transform domain is more secure and robust to various attacks. The transformation adopted may be discrete cosine transform (DCT), discrete Fourier transforms (DFT) and discrete wavelet transforms (DWT) etc. After applying transformation, watermark is embedded in the transformed coefficients of the image such that watermark is not visible. Finally, the watermarked image is obtained by acquiring inverse transformation of the coefficients.

In feature based watermarking scheme, watermark is generated by applying some operations on the pixel value of host image rather than taking from external source. In the proposed watermarking scheme, discrete wavelet transform (DWT) is used for embedding watermarks, since it is an excellent time-frequency analysis method, which can be well adapted for extracting the information content of the image [4]. A detail survey on wavelet based watermarking techniques can be found in [5].

To improve the security, Wang et.al [6] adopt a key dependent wavelet transform. To take the advantage of localization and multiresolution property of the wavelet transform, Wang and Lin [8] proposed wavelet tree based watermarking algorithm. Tao et al.[6] put forward a

discrete-wavelet transform based multiple watermarking algorithm. The watermark is embedded into LL and HH subbands to improve the robustness. Luo et al.[9] introduced an integer wavelets based watermarking technique to protect the copyright of digital elevation mode data. The method utilized encryption technique to lift the security.

Yuan et al.[10] proposed an integer wavelet based Multiple logo watermarking scheme. The watermark is permuted using Arnold transform and is embedded by modifying the coefficients of the HH and LL subbands. Qiwei et al.[11] put forward a DWT based blind watermarking scheme by scrambling the watermark using chaos sequence. Many of the algorithms proposed meet the imperceptibility requirement quite easily but robustness to different image processing attacks is the key challenge and the algorithms in literature addressed only a subset of attacks.

This paper proposes a novel DWT based blind watermarking scheme, in which watermark is constructed from the spatial domain and is embedded in the high-frequency band. The security of the proposed method lies on the multifaceted procedure used to construct watermark. The watermark construction process selects pixels in a random method and adopts Hankel matrix and thereby offer better security. The extraction is done without using original image. This method is robust against many common image attacks and experimental results verify this.

The rest of this paper is organized as follows: Section 2 gives an overview of Discrete Wavelet Transform and Hankel matrix. The details of watermark generation, embedding and extraction process are explained in Section 3. Section 4 shows experimental results and discussion. Finally section 5 provides concluding remarks.

2. Related Background

This section briefly describes the techniques and methods that have been adopted by the proposed scheme, including DWT and watermark construction by Hankel matrix.

2. 1 Discrete Wavelet Transform

Wavelet is a multi-resolution function with the following properties:
- *Linear time complexity*: Transforming to and from a wavelet representation can generally accomplished in linear time, allowing a very fast algorithm.
- *Sparsity*: Many of the coefficients in a wavelet representation are either zero or small.
- *Adaptability*: Wavelets are very flexible as compared to Fourier techniques. They are suited to problems involving images.

The DWT decomposes input image into four components namely LL, HL, LH and HH where the first letter corresponds to applying either a low pass frequency operation or high pass frequency operation to the rows, and the second letter refers to the filter applied to the columns [12], which is shown in Figure 1. The lowest resolution level LL consists of the approximation part of the original image. The remaining three resolution levels consist of the detail parts and give the vertical high (LH), horizontal high (HL) and high (HH) frequencies. In the proposed algorithm, watermark is embedded into the host image by modifying the coefficients of high-frequency bands i.e. HH sub band.

DWT on rows   DWT on columns
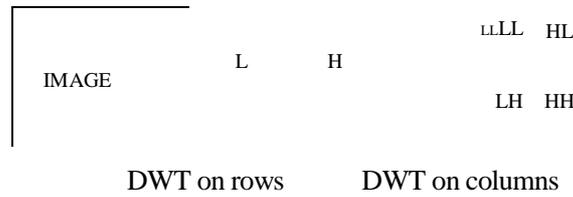
Figure. 1 DWT decomposition of image

For a one level decomposition, the discrete two-dimensional wavelet transform of the image function f(x, y) can be written as [13]

$$LL = [(f(x, y) * 0(-x)\, 0\,(-y))(\,2n,2m)]_{(n,m)\,\in Z^2}$$

$$LH = [(f(x, y) * 0(-x)\, \psi\,(-y))\,(2n\,,2m)]_{(n,m)\,\in Z^2}$$

$$HL = [(f(x, y) * \psi(-x)\, 0\,(-y))\,(2n\,,2m)]_{(n,m)\,\in Z^2}$$

$$HH = [(f(x, y) * \psi(-x)\psi\,(-y))\,(2n\,,2m)]_{(n,m)\,\in Z^2}$$

where 0 (t) is a low pass scaling function and ψ (t) is the associated band pass wavelet function.

The advantages of wavelet transform are as follows:

- Large numbers of the digital coefficients turn out to be very small in magnitude
- By truncating or removing the small coefficients introduces only small errors in the reconstructed image.

2.2 Hankel Matrix

Hankel matrices are frequently encountered in applications where matrix computation is exploited in order to devise very effective numerical solution algorithm. A Hankel matrix is defined as a matrix that is symmetric and constant across anti-diagonals, and has elements h(i, j) = p(i+j-1) where p is a vector represented as [col, row (2: end)] which completely determines the Hankel matrix. It is a square matrix with constant positive slopping skew diagonals and for constructing a Hankel matrix of order NxN, we need 2N-1 elements.

Let P= {a, b, c, d, e, f, g, h, i}. Since there are 9 elements in this vector, a Hankel matrix of size 5x5 may be constructed so that its first column is first 5 elements and last row except the first element is last 4 elements of P, which is given in equation (1).

$$H = \begin{matrix} a & b & c & d & e \\ b & c & d & e & f \\ c & d & e & f & g \\ d & e & f & g & h \\ e & f & g & h & i \end{matrix} \qquad (1)$$

2.3 Neighbors

Consider a pixel P at coordinates (x, y) has two horizontal and two vertical neighbors whose coordinates are (x+1, y), (x-1, y), (x, y-1), (x, y+1).
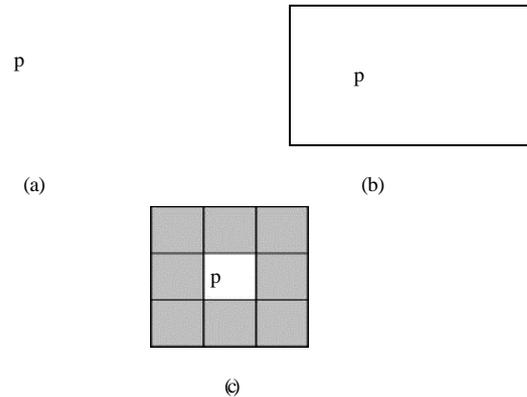
Figure 2 (a) 4-neighbors (b) Diagonal -neighbors
(c) 8-neighbors

This set of 4-neighbors of P is denoted as N_4 (P) and is shaded in Figure 2(a). The four diagonal neighbors of P have coordinates (x+1, y+1). (x+1,y-1),(x-1,y+1) and (x-1, y-1). These neighbors are denoted as N_D(P) and is shaded in Figure 2(b). The union of N_4(P) and N_D(P) form the 8-neighbors of P and is denoted as N_8(P) and is given in Figure 2(c).

3. Proposed Method

In the proposed scheme, there are three significant phases: Watermark generation, Watermark embedding and Watermark Detection. The watermark is generated from pixel value of original image and so there is no need of external image or logo. Hence it is necessary to devise a method to generate watermark. The resolution of watermark is assumed to be half of that of original image.

For embedding the watermark, a 1-level discrete Wavelet Transform is performed. Watermark information is embedded in the high frequency bands (HH1) since it is robust against various normal image processing and malicious attacks. The resultant image is called watermarked image. In detection phase, watermark is once again generated from watermarked image and also extracted the embedded watermark from HH1 sub band. Comparison is made between those watermarks to decide authenticity.

3. 1 Watermark generation

`The watermark pattern is generated from the spatial domain information and so it is referred as content based watermarking. The term spatial domain refers to the image plane itself, and methods in this category are based on direct manipulation of pixels in an image. The procedure for generating watermark is presented in Figure 3.
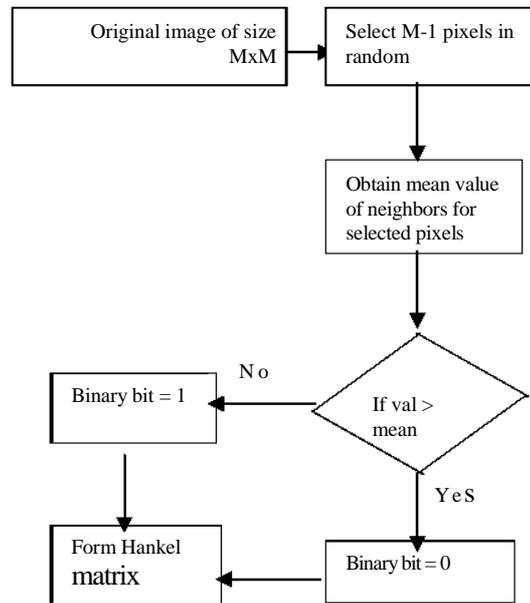
Figure 3 Watermark generation Procedure

Watermark generation procedure includes the following steps:
- Consider the original image P of size M x M.
- Randomly select M-1 elements from P so that all the pixels have valid 3x3 neighborhoods.
- Let P(x-1, y-1), P(x-1, y), P(x-1, y+1), P(x, y+1), P(x+1, y+1), P(x+1, y), P(x+1, y1), P(x, y-1) are the neighborhoods of the selected pixel P(x, y).
- Find average value of those neighborhoods. Let it be $P_a(x, y)$.
- A binary sequence 'B' can be obtained by applying the following constraint.

$$B = \begin{cases} P_a(x, Y) & \\ 0 & \\ 1 & otherwise \end{cases}$$

where i=1,2,3,...M-1

- A Hankel matrix of size M/2 x M/2 is constructed from the binary sequence B_i as
  H (i, j) = B (i + j – 1)
  where $1 \le i \le M/2$, and $1 \le \le N/2$
  which is the watermark pattern to be embedded in to the host image.

Following example illustrates how a Hankel matrix is constructed from the host image. Suppose the original matrix is:

63	72	79	76	75	20	66	70
39	54	66	50	79	29	20	29
67	45	51	42	46	31	39	23
55	47	59	70	26	47	90	23
2	8	59	56	83	40	13	10
5	4	73	47	59	58	35	37
6	6	49	40	40	32	35	62
8	44	72	77	78	80	67	62

Since a 1-level DWT is performed on the matrix for embedding watermark, a binary signal of 4x4 is to be created. To construct a Hankel matrix of order 4x4, number of elements needed are 7. So a set of seven elements are randomly selected with valid 3x3 neighborhoods. Let $P(x, y) = 54$, the first element selected from 2nd row 2nd column. Its neighborhoods are 63, 72,79,66,51,45,67,39. The average of those numbers $Pa(x, y)$ is 60.25. Since $P(x, y)$ is less than $Pa(x, y)$, the binary bit $Bi = 1$.

Let $P(x, y) =83$, the 5th row 5th column element. Its neighborhoods are 70, 26,47,40,58,59,47,56. In this case, $Pa(x, y) =50.375$. Since $P(x, y)$ is greater than $Pa(x, y)$, the binary bit is 0. Proceeding in this way, let the binary pattern obtained is (1, 0, 0, 1, 0, 1, 1). Now the Hankel matrix is constructed so that its first column is first 4 elements and last row except the first element is last 3 elements of binary pattern. The created watermark pattern is given below:
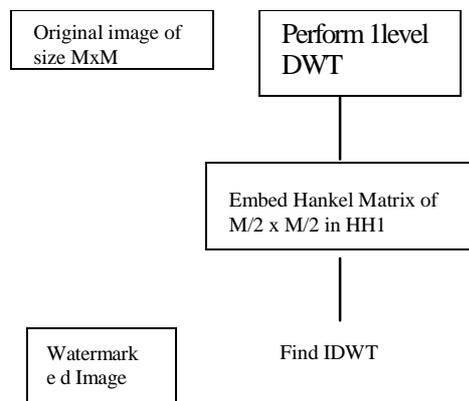
$$
\begin{array}{cccc}
1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1
\end{array}
$$

In the proposed technique, watermark is embedded in the host image by performing 1-level DWT, and so, for the 512x512 given image matrix, a 256x256 watermark pattern is generated.

3.2 Watermark embedding

The watermark is embedded in the high frequency subband of DWT as given in Figure 4.
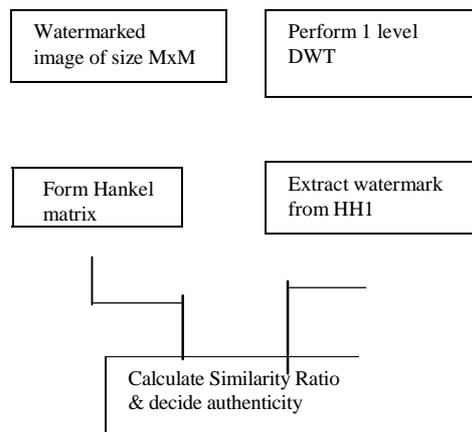- Apply 1-level DWT to original image.
- The watermark is embedded in the high frequency component HH1 of DWT.
- Perform inverse wavelet transform to obtain the watermarked image.

Original image of size MxM → Perform 1level DWT

Embed Hankel Matrix of M/2 x M/2 in HH1

Watermarke d Image — Find IDWT

Figure 4 Watermark embedding process

3.3 Watermark Detection

Proposed watermarking scheme extracts and generates watermark information from watermarked image and so original image is not essential. So it can be referred as blind watermarking. The procedure for watermark detection is shown in Figure 5.

Watermarked image of size MxM — Perform 1 level DWT

Form Hankel matrix — Extract watermark from HH1

Calculate Similarity Ratio & decide authenticity

Figure 5 Authentication Process

The authentication process shown in Figure 5 includes the following steps:
- Watermark is derived form the content of watermarked image using the steps described under watermark generation in section 3.1.
- Apply 1-level DWT to the watermarked image and extract the embedded watermark from HH1 sub band.
- Compare the two watermarks (derived and extracted). If two values match, authenticity is preserved. Otherwise the authenticity is suspected.
- Quality of watermarked image and the watermark is found out according to equation (2) and (4).

4. Experimental Results

Experiments are performed to evaluate the effectiveness of the method using host images with number of rows and columns are of equal size since the embedded Hankel matrix is a square matrix. For testing, the size of the original image is taken as 512x512. Figure 6(a) shows original image. A 256x256 Hankel matrix (binary watermark signal) is constructed from original image and is embedded within itself. The proposed method is tested using MATLAB.

Watermark embedding and extraction phases make use of the MATLAB commands dwt2 and idwt2. The command dwt2 performs single level two dimensional wavelet decomposition with respect to particular wavelet. The Inverse Discrete Wavelet Transform idwt2 command performs a single level two dimensional reconstruction with respect to the specified wavelet. The wavelet 'haar' is used in the proposed method. It is the simplest wavelet and is discontinuous and resembles a step function.

After embedding the watermark, there was no visual difference between the original and watermarked images. Figure 6(b) shows watermarked image. The absolute difference of the pixel intensities of the watermarked image and the original image is shown in Figure 6(c). The difference image shows that the technique ensures high degree of fidelity.

(a)   (b)   (c)
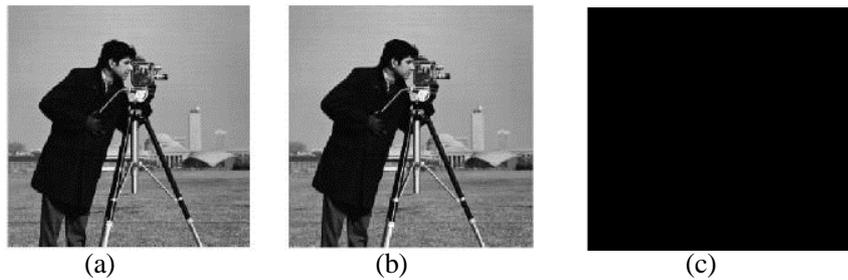
Figure 6 (a) Original Image b) Watermarked Image
(c) Difference Image

The visual quality of watermarked and attacked images is measured using the Peak Signal to Noise Ratio, which is defined in equation (2). The PSNR value of watermarked image is 56.2083, which indicates that there is very little deterioration in the quality of original image.

$$PSNR = 10\log_{10}\left[\frac{255^2}{MSE}\right] \tag{2}$$

where MSE is Mean Squared Error between original and distorted images, which is defined in equation (3).

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[OI(i,j) - DI(i,j)]^2 \tag{3}$$

where OI is original image and DI is the distorted image.

The extracted watermark sequence is compared to the originally embedded watermark using the similarity ratio between the sequences. Similarity Ratio (SR) between these

extracted and original patterns is calculated according to equation (4).

$$R \quad D \qquad\qquad (4)$$
$$+$$

where S denotes number of matching pixel values and D denotes number of different pixel values. In the proposed scheme, similarity ratio evaluated between extracted and calculated watermark is 0.9933 which indicates that the number of matching pixels are high and hence authenticity is preserved.

To evaluate the performance of the proposed watermarking scheme, experiments have been conducted on various images with different textures and various common image processing attacks. Watermark invisibility is evaluated on images provided in Figure 7. The PSNR values of these watermarked images are all tabulated in Table 1. The calculated PSNR values all are greater than 35.00 db, which is the empirical value for the image without perceivable degradation.
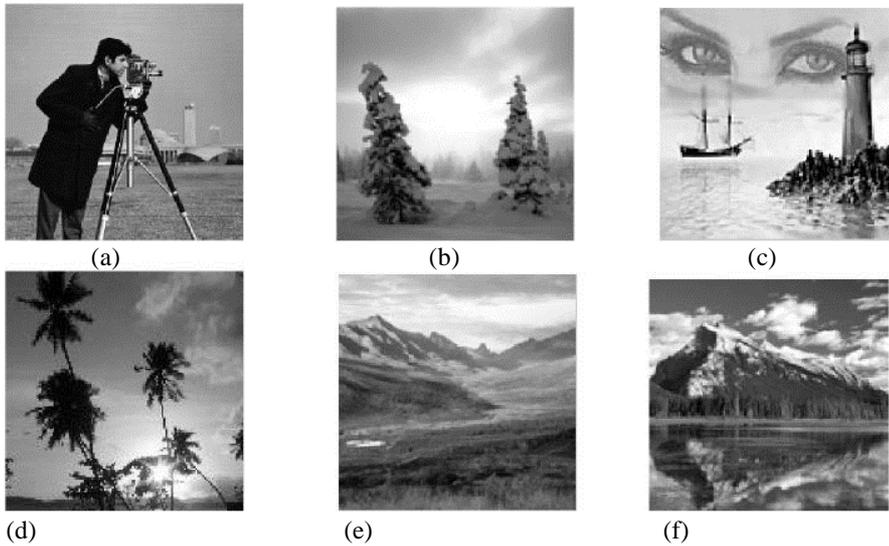
Figure 7. Original Pictures with different textures

Similarity Ratio are computed for watermarks of different images provided in Figure 7 and are tabulated in Table 1. A comparison between extracted and original watermarks show better authentication since the similarity ratio computed is greater than 0.8789 in all cases.

Table
Performance of the proposed scheme

Picture	PSNR	SR
3.a	56.2083	0.9933
3.b	52.9225	0.9558
3.c	54.2661	0.9992
3.d	53.4041	0.8876
3.e	53.9632	0.8789
3.f	57.7024	0.9854

4. 1. Various Attacks

The proposed algorithm was tested using several attacks. The attacks chosen were adding noises such as Gaussian and salt & pepper noises, median filtering, linear filtering, image compression, blurring, scaling, intensity adjustment and histogram equalization. Table 2 gives the performance of proposed watermarking scheme under various attacks. The attacked watermarked images are presented in Figure 8 with the tools and parameters used for the attacks. Figure 9 depicts the difference between watermarked and attacked images.

4.1.1 Additive noises

The watermarked image is attacked by introducing white Gaussian and salt & pepper noises. Gaussian noise is added with a mean 'm' and variance 'n'. The simulation results show that increase in mean or variance affects the imperceptibility of watermarked image since the PSNR values decreases. But the robustness of watermark is high against this attack with a constant variance 0. With the increasing variance of Gaussian, the robustness gets affected.

Salt & pepper noise is added to the image with a noise density 'd'. The watermarked image is attacked with salt & pepper noise with noise densities 0.001, 0.002, 0.005 and 0.01. The simulation results after addition of salt& pepper noise shows that the watermark is highly robust. In both types of additive noises, the PSNR values are greater than 25.

Table 2
Quality Evaluation of Proposed Scheme under various attacks

Attacks		PSNR(dB)	SR
No		56.2083	0.9933
Adding Gaussian noise (mean, variance)	0.001, 0	56.2083	0.9933
	0.005, 0	46.4663	0.9933
	0.01,0	38.0920	0.9933
	0.05,0	25.7482	0.9931
	0, 0.001	30.0890	0.5229
	0,0.002	27.1712	0.5145
Adding Salt & Pepper noise	0.001	35.1261	0.9900
	0.002	32.0256	0.9859
	0.005	28.2018	0.9737
	0.01	25.0211	0.9595
Median filtering	3x3	29.5542	0.5789
	5x5	26.9883	0.5981
Linear filtering	3x3	27.7822	0.5909
	5x5	25.5281	0.5475
JPEG compression	90%	43.0983	0.5732
	70%	37.4635	0.5917
	50%	35.2171	0.6028
	30%	33.1944	0.6149
	10%	29.1840	0.7002
Blurring (sigma)	0.5	37.8601	0.6385

Rescaling (512-256-512)		53.1980	0.6913
Image adjustment		18.4945	0.8988
Histogram Equalization		19.0277	0.7049

4.1.2 Filtering

The performance of watermarking scheme is analyzed against filtering such as median filtering and linear filtering. Median filtering is performed on the watermarked image using 3x3 and 5x5 neighborhoods. Linear filtering performs multidimensional filtering using convolution. Experimental results show that the robustness of watermark is distorted moderately since more number of coefficients will be modified during the filtering process.

4.1.3 JPEG compression

The watermarked image is compressed with lossy JPEG compression by applying the quality factor ranges from 0 to 100. Higher number means less degradation due to compression but the resulting file size is larger. Simulation results show that a decrease in quality factor decreases the imperceptibility of watermarked image but increases the robustness of watermark.
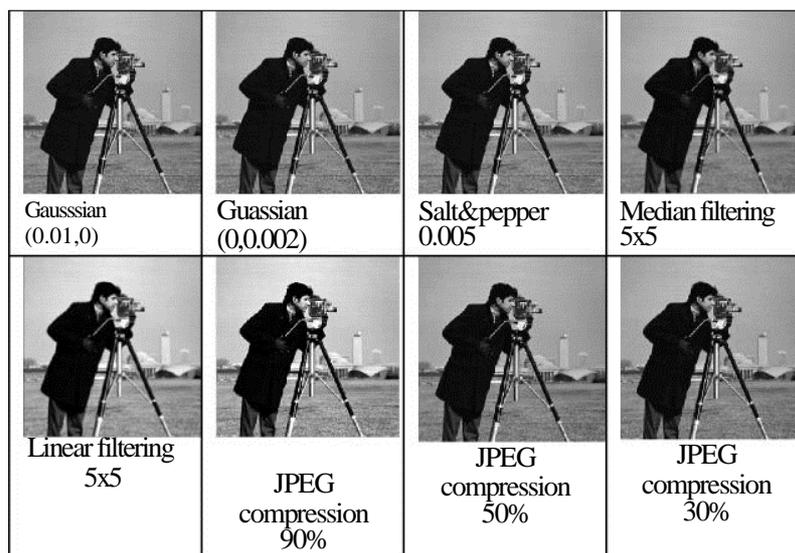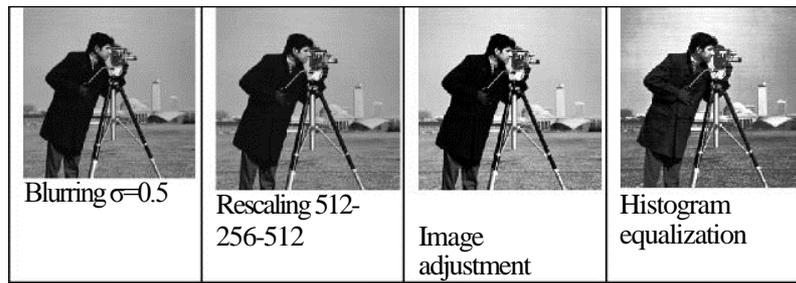
Figure 8. Watermarked images under various attacks

4.1.4 Blurring and scaling operations

A Gaussian lowpass filter of size 3x3 and a standard deviation sigma 0.5 is applied on the image. The quality of watermarked image is high in this case. The high value of Similarity Ratio indicates that the proposed method is able to withstand against blurring. In addition, the experimental result conveys that the proposed method is robust against scaling operation.

4.1.4 Image Adjustment

The intensity values of watermarked image are adjusted to new values such that 1% of data are saturated at low and high intensities. This attack increases the contrast of image which in turn degrades the imperceptibility of watermarked image. But the robustness of watermark is high.

4.1.5 Histogram Equalization

This attack enhances contrast of the watermarked image. In this case, the similarity ratio is 0.7049 which specifies that the robustness of watermark is better. The low PSNR value 19.0277 indicates that the imperceptibility of watermarked image gets affected.

| Blurring (σ=0.5) | Rescaling (512-256-512) | Image adjustment | Histogram equalization |
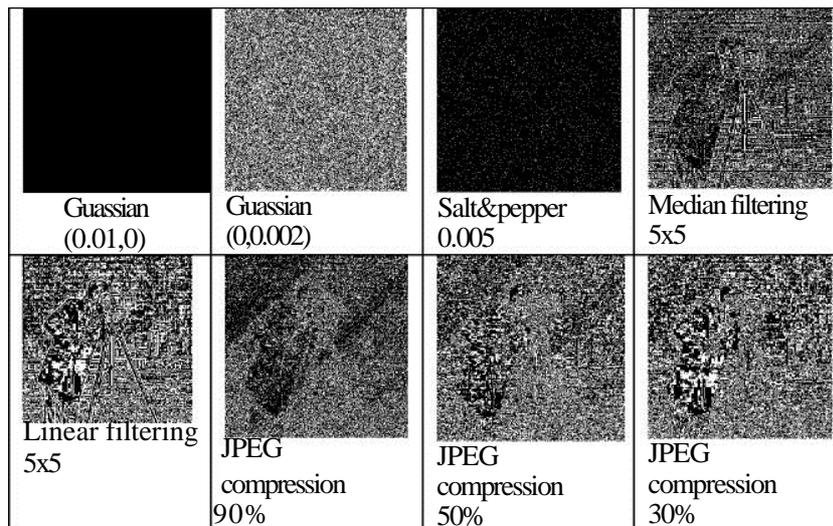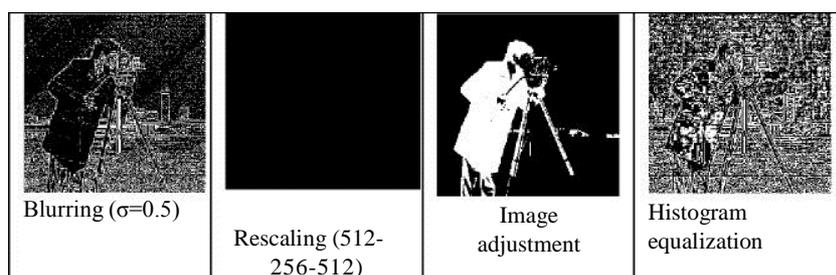
Figure 9. Disparity Images

5. Conclusion

This study has proposed a robust watermarking which provides a complete algorithm that embeds and extracts the watermark information effectively. In this method, a watermark pattern is constructed from host image with the help of statistical measure such as mean and security is enhanced by selecting random pixels and building Hankel matrix. The designed method makes use of the Discrete Wavelet Transform which provides a way for robustly hiding watermark within the host image. Moreover the authentication process provides qualities like imperceptibility, robustness and security.

The performance of the watermarking scheme is evaluated with image processing attacks such as adding noises, filtering, image compression, blurring, scaling, intensity adjustment and histogram equalization. Experimental results demonstrated that watermark is robust against those attacks. However the imperceptibility of watermarked image is degraded in cases of attacks such as Histogram Equalization and Image adjustment. Future work will aim at making suitable enhancements and considering attacks such as rotation, and translation.

References

[1] C.Rey, J.Dugelay. "A survey of watermarking algorithm for Image authentication", Journal on Applied Signal Processing, Vol.6, pp.613-621, 2002.

[2] C.I.Podilchuk, E.J.Delp. "Digital watermarking: algorithms and applications" IEEE Signal Processing Magazine, pp. 33-46, July 2001.

[3] Arvind kumar Parthasarathy, Subhash Kak. "An Improved Method of Content Based Image Watermarking", IEEE Transaction on broadcasting, Vol.53, no.2, June 2007, pp.468 -479.

[4] Ramana Reddy, Munaga V.N.Prasad, D.Sreenivasa Rao. "Robust Digital Watermarking of Color Images under Noise Attacks", International Journal of Recent Trends in Engineering, Vol.1, No. 1, May 2009.

[5] Q.Ying, W.Ying. "A survey of wavelet-domain based digital image watermarking algorithm", Computer Engineering and Applications, Vol.11, pp.46-49, 2004.

[6] Y.Wang, J.F.Doherty, R.E.Van Dyck. "A wavelet-based watermarking algorithm for ownership verification of digital images", IEEE Trans. Image Process, 11, pp.77-88,2002.

[7] S.H.Wang , Y.P.Lin. "Wavelet Tree quantization for copyright protection for watermarking", IEEE Trans. Image Process, pp.154-165, 2002.

[8] P.Tao, A.M.Eskicioglu. "A robust multiple watermarking scheme in the discrete wavelet transform domain", Proceedings of the SPIE, Vol.5601, pp.133-144, 2004.

[9] Y.Luo, L.Z.Cheng, B.Chen, Y.Wu. "Study on digital elevation mode data watermark via integer wavelets", Journal of software, 16(6), pp.1096-1103, 2005

[10] Yuan Yuan, Decai Huang, Duanyang Liu: An Integer Wavelet Based Multiple Logo-watermarking Scheme. In IEEE, Vol.2 pp.175-179, 2006.

[11] Qiwei Lin, Zhenhui Liu, Gui Feng. "DWT based on watermarking algorihthm and its implementing with DSP", IEEE Xplore, pp. 131-134, 2009.

[12] Xiang-Gen Xia, Charles G.Boncelet, Gonzalo. "Wavelet Transform based watermark for digital images", OPTICS EXPRESS, 1998 Vol.3, No.12, pp 497-511.

[13] Sanjeev Kumar, Balasubramanian Raman, Manoj Thakur. "Real Coded Genetic Algorithm based Stereo image Watermarking", IJSDIA, 2009, Vol. 1 No.1 pp 23-33.

[14] Hongmei Liu, Junhui Rao, Xinzhi Yao. "Feature Based Watermarking Scheme for Image Authentication", IEEE, 2008, pp 229-232.

[15] J.Dittmann. "Content-fragile Watermarking for Image Authentication", Proc. of SPIE, Security and Watermarking of Multimedia Contents III, vol.4314, pp.175-184, 2001.

[16] Suliman Al-Homidan, "Solving Hankel matrix approximation problem using semidefinite programming", Journal of Computational and Applied Mathematics, Vol.2 Issue 2 pp.304-314, May 2007

[17] Rafael C.Gonzalez, R.E.Woods, , Steven L. Eddins "Digital image processing", 2009.

Author Biographies

M.Mohamed Sathik received the M.Sc(Mathematics) degree from Bharathidhasan University in 1986, and the M.Phil and Ph.D. in Computer Science degrees from Manonmanium Sundaranar University in 1997 and 2006 respectively. He was also awarded the degrees M.Tech(CS&IT), MBA(Project Management) and M.S(Psycho Therapy). Currently he is an Associate Professor in Computer Science department at Sadakathullah Appa College, Tirunelveli since 1988. His research interest is Virtual Reality Techniques. He had presented number of papers in national and international conferences and Journals.

S.S.Sujatha received the M.C.A degree from Alagappa University in 1993 and M.Phil degree from Manonmanium Sundaranar University in 2003. She is working as an Associate Professor in Computer Science Department at S.T.Hindu College, Nagercoil since 1994. She has presented and published eight papers in national and international conferences and Journals. Her current research interest focuses on digital watermarking and Authentication.