A Robust DHWT Based AES Encrypted Image Watermarking Scheme

Maheswari Sureshbabu[1], Rameshwaran Kalimuthu[2], and Chandra Vadivel[3]
[1]Department of Electrical and Electronics Engineering, Kongu Engineering College, India
[2]Department of Electronics and Communication Engineering, Shanmuganathan Engineering College, India
[3]Department of Electronics and Communication Engineering, Institute of Engineering and Technology, India

Abstract: *In this paper, we propose the blind watermarking algorithm based on Double Haar Wavelet Transform (DHWT) for copyright protection of encrypted images. Watermark embedding is performed in wavelet transform domain. DHWT is applied to the original cover image and binary watermark. Selected subband is encrypted by Advanced Encryption Standard (AES) encryption scheme. Singular Value Decomposition (SVD) is applied on selected subband of both the cover image and binary watermark. Eigen values of selected subband of cover image are modified by the Eigen values of the selected subband of binary watermark. Experimental results show that the proposed algorithm achieves very high imperceptibility which is evidenced by high Peak Signal to Noise Ratio (PSNR) value for various gray scale encrypted images. Also, it produces very high robustness against various types of image processing attacks.*

Keywords: *DHWT, AES encryption, SVD, digital watermarking.*

Received October 28, 2013; accepted May 15, 2014

1. Introduction

The availability of increased computational power and the proliferation of the internet have facilitated the production and distribution of unauthorized copies of multimedia information. As a result, the problem of multimedia copyright protection has attracted the interest of scientific and business communities worldwide. The most promising solution seems to be the watermarking process where the original data is marked with ownership information hidden in an imperceptible manner in the original signal. Media contents are often distributed in encrypted format and watermarking of these media need to be carried out in encrypted domain for copyright violation detection, proof of ownership or distributorship, media authentication etc. In an encrypted image, changing even a single bit may lead to a random decryption; therefore the encryption should be such that the distortion due to embedding can be controlled to maintain the image quality. It should also be possible to detect the watermark correctly even after the content is decrypted.

An encryption algorithm is classified into two types, a stream cipher algorithm and a block cipher algorithm. Wide numbers of papers are proposed to encrypt the digital images. Subramanyam and Emmanuel [19] proposed an algorithm to watermark JPEG2000 compressed and RC4 encrypted images to improve the overall security of the image. In this paper, a block cipher based Advanced Encryption Standard (AES) encryption algorithm [8, 9, 16] is proposed to encrypt the cover image.

Hiding the ownership information can be done in two ways, viz. spatial domain technique and transform domain technique. In spatial domain technique [12], pixel value is modified directly to embed the secret information. In transform domain technique, original image is transformed into transform coefficients by using various popular transforms Discrete Cosine Transform (DCT) [6], Discrete Fourier Transform (DFT) [18] and Discrete Wavelet Transform (DWT) [1, 2, 3, 4, 7, 10, 11, 13, 20, 21] etc. Then, transform coefficients are modified to embed the secret information. Transform domain techniques possess lot of advantages. It offers very high robustness against compression such as scaling, rotation, cropping, row and column removal, addition of noise, filtering, cryptographic and statistical attacks as well as insertion of other watermarks.

Robustness, imperceptibility and capacity are the three conflicting requirements of digital watermarking. The added binary bits should not degrade the quality of the image. At the same time, it should not be removed by the attacks. Different attacks are sensitive in different frequency bands. Modifications of the histogram, such as contrast/brightness adjustment, gamma correction, histogram equalization, and cropping are very sensitive in low pass band. But, attacks like filtering, lossy compression, geometrical distortions are less sensitive in low pass. Similarly

such characteristics are more sensitive in high frequency band. Noise adding, nonlinear deformations of the gray scale are less sensitive in high frequency band. Therefore, adding of extra bits in the mid frequency band, compromise these two characteristics of frequency bands [1, 2, 3, 4, 6, 10, 11, 13, 20, 21]. Designing of blind watermarking i.e., extracting the watermark without original image and original watermark is very difficult task. In this paper, blind watermarking scheme is employed. Watermark is extracted with the help of secret key only.

Wavelet transform is a very popular technique in image transform, especially in watermarking of images. Various watermarking methods are proposed in wavelet domain due to their excellence of multi resolution property. Byun *et al.* [4] proposed a watermarking method using quantization and statistical characteristics of wavelet transform. Wang and Lin [21] proposed a wavelet tree based blind watermarking scheme. Jiang *et al.* [7] proposed a blind watermarking scheme based on 4-band wavelet transform. An integer wavelet based multiple logo-watermarking scheme was proposed by Yuan *et al*. [25]. Preprocessed watermark is embedded in the low and high frequency subbands. Mahmood and Selin [1] proposed a semi blind watermarking scheme using image de-noising based on DWT. Li *et al.* [11] proposed wavelet tree quantization based watermarking scheme robust to geometric attacks like rotation, scaling and cropping. Lein and Lin [10] proposed a blind image watermarking scheme using wavelet trees quantization. Wei *et al.* [13] proposed a blind watermarking algorithm based on the significant difference of wavelet coefficient quantization. Papakostas *et al.* [17] proposed a watermarking algorithm based on Krawtchouk moments, interms of locality**,** the zero-bit watermarking technique was proposed by Wen-ge and Lei [23] here watermark is generated by the features of the cover image and makes host image without any distortion. You *et al.* [24] proposes a blind watermarking method by using non-tensor product of wavelet filter banks.

However scalar wavelets are generated by one scaling function. It does not support, orthogonality and symmetry, simultaneously. Multiwavelets which have more than one scaling function can simultaneously provide better reconstruction while preserving length. Good performance at the boundaries and a high order of approximation are added features. Thus, multiwavelet provides superior performance for image processing applications, compared with scalar wavelets [23]. The Haar wavelet transform consistently outperform the more complex ones when using non-colored watermark [3]. In this paper we propose a Double Haar Wavelet Transform (DHWT) based watermarking scheme.

The Haar Wavelet based M-channel Filter (HWF) bank with M=3 called the DHWT [22]. It divides the original image into nine subimages at a first level. Each subimage in the first level is further divided into nine sub images at the second level. AES encryption is done in the low frequency subimage. Binary watermark is embedded in the selected mid frequency subimage. In this paper, section 2 discusses the DHWT from HWF. Section 3 discusses the AES encryption. Section 4 discusses the proposed embedding and extraction algorithms using DHWT. Section 5 discusses the experimental output for different gray scale images followed by conclusions in section 6.

2. M-Channel Filter Bank and Double Haar Wavelet Transform

Multiwavelet is developed from Multiresolution Analysis (MRA). The difference is that multiwavelets have several scaling functions whereas MRA have one scaling function. Multiwavelets offer superior performance for image processing applications compared with scalar wavelets [14, 25]. Multi wavelet offers short support, orthogonality, symmetry, and vanishing moments. A multiwavelet system can provide better reconstruction while preserving length, good performance at the boundaries and a high order of approximation. Each multiwavelet system is a matrix valued multirate filterbank. A multiwavelet filterbank has “taps” that are (NxN) matrices. A filter bank is a structure that decomposes a signal into a collection of subsignals. Depending upon the application, subsignals help to emphasize specific aspect of the original signal or may be easier to work with than of the original signal [14]. The structure of a classical filter bank is shown in Figure.1.

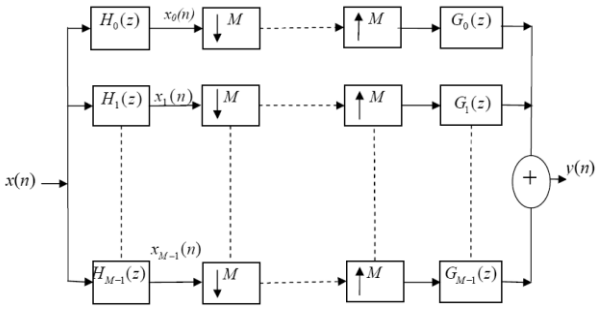


Figure 1. M-channel filter bank.

Perfect reconstruction Quadrature mirror filters are used to split the input signal into M subbands which are decimated by M in signal decomposition [15]. During reconstruction, M subband signals are decoded, interpolated and recombined using synthesis filters. The HWF with M=3 is called the DHWT [22]. The decomposition and reconstruction filter banks are defined as:

$$H = \frac{1}{3}\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix} \qquad G = \begin{pmatrix} 2 & 1 & 1 \\ -1 & 1 & 1 \\ -1 & -2 & 1 \end{pmatrix}$$

Similar to the two dimensional orthogonal wavelet transform, the DHWT can be extended to 2-D signals. Let $x_0(m, n)$ be an image of NxN pixels. The steps of the 2-D discrete DHWT are defined by the following steps:

1. In the horizontal direction, the original image $x_0(m, n)$ is filtered by the filters $H_0(z)$, $H_1(z)$ and $H_2(z)$ respectively. Three images $x_{00}(m, n)$, $x_{01}(m, n)$ and $x_{02}(m, n)$ are produced.
2. In the vertical direction, the three images $x_{00}(m, n)$, $x_{01}(m, n)$ and $x_{02}(m, n)$ are filtered by the filters $H_0(z)$, $H_1(z)$ and $H_2(z)$ respectively. This gives nine images $x^{n}_{0j}(m,n)0 \le j \le 8$.
3. Down-sampling the images $x^{n}_{0j}(m,n)\,0 \le j \le 8$, with an interval of three, we obtain nine subimages $x^{n}_{0j}(m,n)0 \le j \le 8$.
4. Steps (1-3) can be repeated on the subimage $x_{00}(m, n)$, so as to get the other subimages in the next scale.

3. Encryption Standard Encryption

Cryptography has an important role in the security of data transmission and is the best method of data protection against passive and active fraud. The growing number of communication users has led to increasing demand for security measures to protect data transmitted over open channels. In cryptography, AES [8, 9, 16] is based on the block cipher and become the designated successor of the Data Encryption Standard (DES) which has been implemented in a tremendous number of cryptographic modules worldwide since 1977.

This standard comprises three block ciphers [9] AES-128, AES-192 and AES-256 i.e., it has a 128-bit block size, with key sizes of 128, 192 and 256 bits respectively. AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. AES-128 (a key length of 128 bits (16 bytes)) is proposed which has 10 rounds in order to minimize the number of if-then-else conditions. Figure 2 shows the AES encryption flowchart.

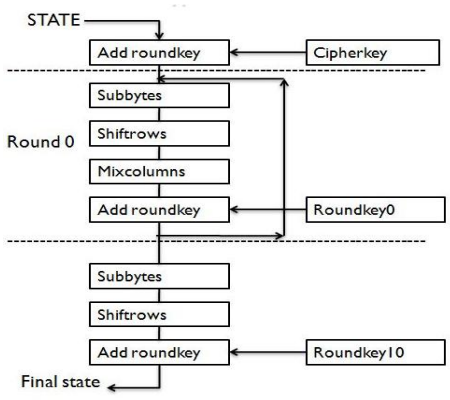


Figure 2. AES encryption flowchart.

The initial step of AES is converting the input plaintext matrix into state matrix. State matrix is the hexadecimal value of input matrix which is given as input to the forthcoming steps of encryption. The plaintext matrix is rearranged into state matrix and iteratively loops the state through 4 steps: Addroundkey, Subbytes, Shiftrows and Mixcolumns.

Decryption blocks step-by-step reverses the transformations of the encryption process. Input parameters of decryption block are the ciphertext to be decrypted (back) into plaintext, inverse Sbox, key schedule 'w' and inverse polynomial matrix. The first round key to be used here is the last one that has been used in encryption process. As in encryption process, but in the opposite order, it takes nine identical rounds of row shifting, byte substituting and column mixing and a final tenth round to end up with the reshaped plaintext matrix.

4. Proposed Scheme

DHWT based blind watermarking scheme is proposed. Watermark is extracted by using secret key only. DHWT is applied on both cover image and binary watermark. In two-dimensional DHWT, each level of decomposition produces nine bands of data. The low pass band can further be decomposed to obtain second level of decomposition. Figure 3 shows the first level of decomposition.

x_{11}	x_{12}	x_{10}
x_{21}	x_{22}	x_{20}
x_{01}	x_{02}	x_{00}

Figure 3. 1-level DHWT.

The proposed watermark embedding scheme shown in Figure 4 is summarized as follows:

1. The DHWT is applied on the original cover image $x_0(m, n)$ and binary watermark 'W'.
2. AES encryption is applied to the low frequency subimage $x_{00}(m, n)$.
3. Eigen values of the subimage $x_{11}(m, n)$ of the cover image (σ) and subimage $x_{11w}(p, q)$ of the watermark image (σ_w) are obtained by applying SVD [2].
4. Then the Eigen values (σ) of the subimage $x_{11}(m, n)$ are replaced by the Eigen values (σ_w) of the watermark image after multiplying with proper strength factor α.
5. Inverse SVD is applied on the new Eigen values σ^* in order to obtain the watermarked subimage $x^*_{11}(m, n)$.
6. Inverse DHWT is applied on x_{00}(m, n) and $x^*_{11}(m, n)$ to obtain the watermarked Image $x^*_w(m, n)$.

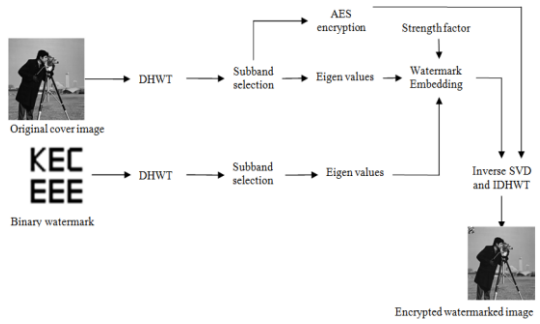


Figure 4. Watermark embedding algorithm.

The proposed watermark extraction scheme shown in Figure 5 is summarized as follows:

1. The DHWT is applied on the watermarked image $x_w^*(m, n)$.
2. The subimage $x_{11}^*(m, n)$is chosen in the first level DHWT. SVD is applied on the selected subimage to obtain the Eigen vales σ^*.
3. Then Eigen values of watermark are extracted by diving σ^* with the strength factor which is used in embedding process.
4. Inverse SVD and inverse DHWT is applied, in order to obtain the watermark.

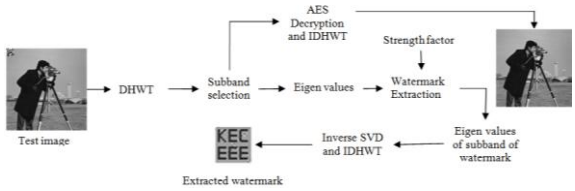


Figure 5. Watermark extraction algorithm.

5. Experimental Results

The experiments were performed on different gray scale images such as Lena, cameraman etc. Binary watermark image is of the size 33×33. We could obtain PSNR of 50.9 dB with no perceptibility problem on watermarked Lena image. Figure 6 shows the image results of the proposed watermarking scheme of the standard test image cameraman.

a) Cover image. b) Encrypted watermarked image. c) Decrypted watermarked image.

d) Original watermark image. e) Extracted watermark image.

Figure 6. Image results of the proposed scheme.

Any watermarking system should be robust against various image processing attacks. It should not be removable by unauthorized users and it should not degrade the quality of the images. There are many attacks against which image watermarking system could be judged. The attacks include average filtering, rotation, median filtering, salt and pepper noise, Gaussian noise, speckle noise and so on. These attacks are applied to the watermarked images to evaluate recovery process. Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Normalized Cross-correlation (NC) are used to estimate the quality of extracted watermark. *MSE*, *PSNR* and *NC* are defined as follows [5]:

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right) \quad (1)$$

Where *MSE* is defined as follow:

$$MSE = \frac{1}{MN}\sum_{x=1}\sum_{y=1}(f(x,y) - \bar{f}(x,y))^2 \quad (2)$$

Where *M* and *N* are size of images, $f(x, y)$ and $\bar{f}(x, y)$ are value at (x, y) location of host and watermarked image.

$$NC = \frac{\sum_i\sum_j p_{ij}\, p_{ij}^*}{\sum_i\sum_j (p_{ij})^2} \quad (3)$$

Where p_{ij} and p_{ij}^* are pixel value at i, j location of original watermark and recovered watermark pattern respectively. The obtained *PSNR* values for various gray scale images and normalized correlation of extracted watermark are shown in the Table 1 and also in Figure 7.

Table 1. PSNR values of watermarked image.

Image Type	PSNR (dB) (Encrypted Image)	PSNR (dB) (Decrypted Image)	Normalized Correlation
Moon (500x375)	29.3695	51.4543	0.9912
Lena (512x512)	36.4909	50.9016	0.9842
Rohith (189x253)	27.7148	49.7872	0.9978
Rose (150x150)	22.3071	41.556	0.9948
Cameraman(256x256)	30.1393	42.9689	0.9765
Girl (131x131)	21.1622	40.1696	0.9970
Boat (131x131)	24.3433	41.3727	0.9942
Fruits (131x131)	22.0797	39.4920	0.9893
Baboon (131x131)	25.1141	36.3916	0.9812
Circles (300x320)	26.6858	34.2085	0.9248
Circuit (300x234)	27.7485	31.5071	0.8016

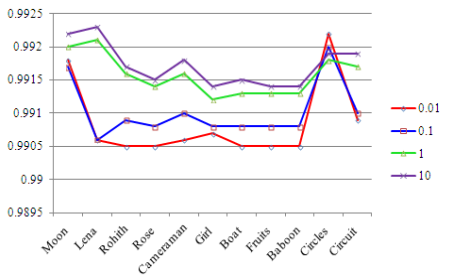
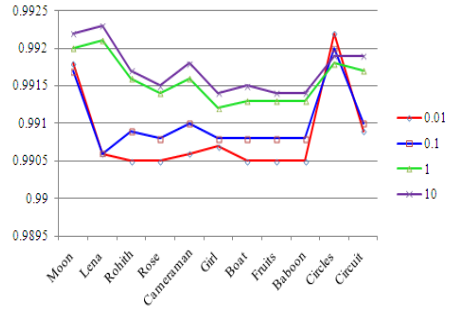


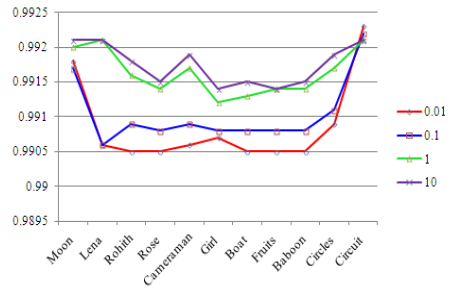
Figure 7. PSNR value of watermarked images.

5.1. Robustness to Noise

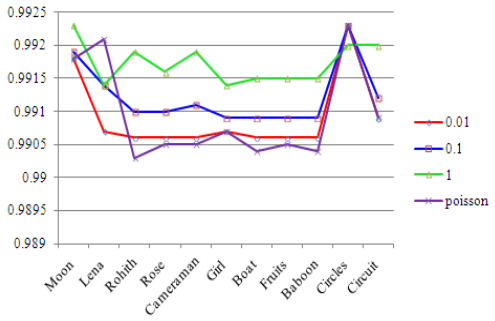
Robustness on noise is very important to watermarking algorithm. Proposed algorithm is tested against four kinds of noise. Zero mean Gaussian noise with variance 100, 1% salt and pepper noise, Poisson and speckle noise.



a) NC under Gaussian noise.



b) NC under speckle noise.



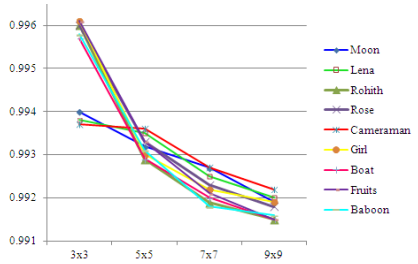
c) NC under salt and pepper and Poisson noise.

Figure 8. NC of extracted watermark under various addition of noises.

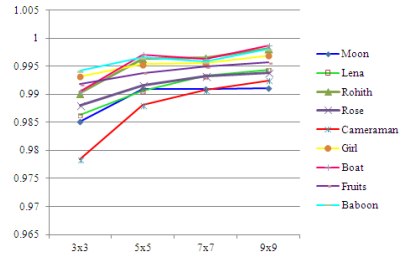
The simulated results of the normalized correlation under various noises are shown in Figure 8. And it demonstrates the robustness of this algorithm to various noises with different variances.

5.2. Robustness to Image Processing Attacks

The watermarking algorithm is also robust to image processing techniques. The most popular method in this branch is histogram equalization. The correlation computed from histogram equalized images is shown in Table 3. Another popular image processing tool is filter. Two types of filters are tested. Low pass filter and median filter, which can be considered as case of pixel permutation. The simulated results of the NC for the above mentioned two filtering conditions are shown in Figure 9.



a) NC under average filtering.



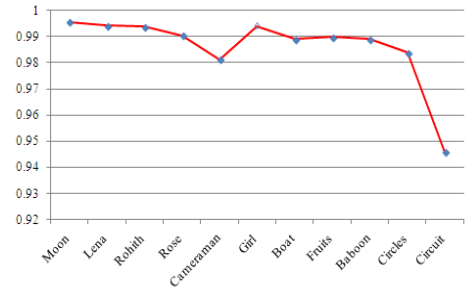
b) NC under median filtering.

Figure 9. NC of extracted watermark under filtering attack.

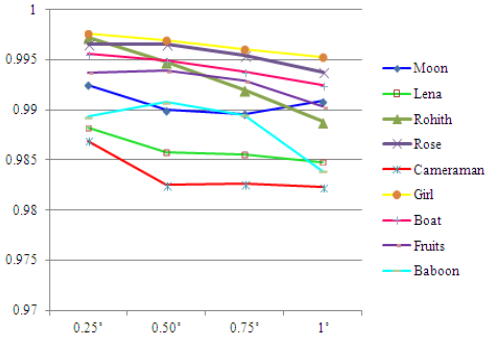
Figure 9 gives the experimental results of various gray scale images under filter attacks. We can see that this scheme can resist filter attacks under different window size.

6. Robustness to Geometric Attacks

Digital watermarking robust to geometric attacks is a difficult problem that constrains the practical value of watermarking technique. Geometric attacks include rotation, cropping and scaling etc., the simulated results of the normalized correlation under cropping attack and various angles of rotation are shown in the Figure 10.



a) NC under cropping.



b) NC under various angles of rotation.

Figure 10. NC of extracted watermark under geometrical attacks.

It may be noted that this scheme can resists cropping attacks and rotational attacks under various angles of rotation. From the results shown in Figure 10 the proposed algorithm is robust to geometric attacks.

The proposed watermarking scheme is compared with existing recently published papers by Byun *et al.* [4], Wang and Lin [21], Jiang *et al.* [7], Yuan *et al.* [25], Mahmood and Selin [1], Li *et al.* [11], Lein and Lin [10], Wei *et al.* [13], Papakostas *et al.* [17], Wenge and Lei [23] and You *et al.* [24] based on Lena image, the results are shown in Tables 2 and 3.

Table 2. Comparison of PSNR value of watermarked image in proposed method and existing methods.

Methods	PSNR in db
Byun *et al.*	41.95
Wang *et al.*	38.20
Jiang *et al.*	40.26
Mahmood *et al.*	45.10
Li *et al,*	40.60
Wei *et al.*	44.25
Papakostas et al.	58.28
Proposed method	51.45

Table 3. Comparison on NC of extracted watermark of proposed method and existing methods under various attacks.

Methods	Median Filtering 3x3	Gaussian Noise	Histogram Equalization	Cropping	Angle of Rotation			
					0.25°	0.50°	0.75°	1°
Wang *et al.*	0.51	0.64	-	-	0.31	0.29	0.26	0.24
Jiang *et al.*	0.99	0.9596	-	0.678	-	-	-	-
Mahmood *et al.*	0.92	1	-	-	-	-	-	-
Li *et al.*	0.35	0.7	-	0.61	0.46	0.38	0.36	0.33
Lein and Lin	0.89	0.768	0.935	0.88	0.88	0.859	0.808	0.79
Wei *et al.*	0.88	0.91	0.77	0.7	-	-	-	-
Yuan *et al.*	-	0.546	0.616	0.943	-	-	-	-
Papakostas *et al.*	0.83	0.5016	-	-	-	-	-	-
Feng *et al.*	0.93	0.6	-	-	-	-	-	-
Xinge *et al.*	-	-	-	-	0.79	-	-	-

From Tables 2 and 3, we can see the PSNR of the watermarked image and the robustness of watermark is far better than those existing methods. The authors claim their method can effectively resist image processing attacks like median filtering, histogram equalization, addition of noise and geometric attacks like rotation, cropping and can obtain a higher PSNR of the watermarked image.

7. Conclusions

In this paper, a new watermarking algorithm has been proposed based on DHWT for encrypted images. This algorithm guarantees a satisfactory level of robustness against different types of image processing distortions. Thus, the proposed algorithm qualifies itself to be highly image adaptive and provide best solution to protect the media contents are often distributed in encrypted format. Multiple watermarking and different forms of secret messages such as gray scale image, text, signature and pseudo-random binary sequence are suggested to be used in future.

References

[1] Al khassaweneh M. and Aviyente S., "Spatially Adaptive Wavelet Thresholding for Image Watermarking," *in Proceeding of IEEE Multimedia and Expo, 2006 IEEE International Conference*, Toronto, pp. 1597-1600, 2006.

[2] Bhatnagar G. and Raman B., "A New Robust Reference Watermarking Scheme Based DWT-SVD," *Computer Standards and Interfaces*, vol. 31, no. 5, pp. 1002-1013, 2009.

[3] Brannock E., Weeks M., and Harrisonm R., "The Effect of Wavelet Families on Watermarking," *Journal of Computers*, vol. 4, no. 6, pp. 554-566, 2009.

[4] Byun K., Lee S., and Kim H., "A Watermarking Method Using Quantization and Statistical Characteristics of Wavelet Transform," *in Proceeding of IEEE Parallel and Distributed Computing, Applications and Technologies*, Dalian, pp. 689-693, 2005.

[5] Hameed K., Mumtaz A., and Gilani S., "Digital Image Watermarking in the Wavelet Transform Domain," *in Proceeding of World Academy of Science, Engineering and Technology*, pp. 86-89, 2006.

[6] Hernandez J., Amado M., and Gonazalez F., "DCT Domain Watermarking Techniques for Still Images: Detector performance Analysis and a New Structure," *IEEE Transactions on Image Processing*, vol. 9, no. 1, pp. 55-68, 2000.

[7] Jiang M., Xu G., and Yuan D., "A Novel Blind Watermarking Algorithm Based on Multiband Wavelet Transform," *in Proceeding of IEEE International Conference on Signal Processing*, Beijing, pp. 857-860, 2004.

[8] Kun Y. and Zhaohui Li., "An Improved AES Algorithm Based on Chaos," *in Proceeding of International Conference on Multimedia Information Networking and Security*, Hubei, pp. 326-329, 2009.

[9] Kn M. and Karunavathi R., "Secured High Throughput Implementation of AES Algorithm," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 5, pp. 1193-1198, 2013.

[10] Lien B. and Lin W., "A Watermarking Method Based on Maximum Distance Wavelet Tree Quantization," *in Proceeding of 19th Computer, Vision, Graphics and Image Processing*, India, pp. 269-276, 2006.

[11] Li E., Liang H., and Niu X., "Blind Image Watermarking Scheme Based on Wavelet Tree Quantization Robust to Geometric Attacks," *in Proceeding of IEEE Intelligent Control and Automation*, Dalian, pp. 10256-10260, 2006.

[12] Li L. and Guo B., "Localised Image Watermarking in Spatial Ddomain Resistant to

Geometric Attacks," *International journal of Electronics and Communication*, vol. 63, no. 2, pp. 123-131, 2009.

[13] Lin W., Horng S., Kao T., Fan P., Lee C., and Pan Y., "An Efficient Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization," *IEEE Transactions on Multimedia*, vol. 10, no. 5, pp. 746-757, 2008.

[14] Mallat S., *A Wavelet Tour of Signal Processing*, Academic Press, 1999.

[15] Nguyen T. and Vaidyananthan P., "Structures for M-Channel Prefect-Reconstruction FIR QMF Banks Which Yield Linear-Phase Analysis Filters," *IEEE Transactions on Acoustics, Speech, Signal Procesing*, vol. 38, no. 3, pp. 433-446, 1990.

[16] Prasad V. and Maheswari S., "Robust Watermarking of AES Encrypted Images for DRM Systems," *in Proceeding of IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology*, Tirunelveli, pp. 189-193, 2013.

[17] Papakostas G., Tsougenis E., and Koulouriotis D., "Near Optimum Local Image Watermarking Using Krawtchouk Moments," *in Proceeding of IEEE International Conference on Imaging Systems and Techniques*, pp. 464-467, 2010.

[18] Solachidis V. and Pitas I., "Circularly Symmetric Watermark Embedding in 2-D DFT," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741-1753, 2001.

[19] Subramanyam A. and Emmanuel S., "Robust Watermarking of Compressed and Encrypted JPEG2000 IMAGES," *IEEE Transaction on Multimedia*, vol. 14, no. 3, pp 130-142, 2012.

[20] Vundela P. and Sourirajan V., "A Robust Multiwavelet-Based Watermarking Scheme for Copyright Protection of Digital Images Using Human Visual System," *The International Arab Journal of Information Technology*, vol. 10, no. 6, pp. 527-535, 2013.

[21] Wang S. and Lin Y., "Wavelet Tree Quantization for Copyright Protection Watermarking," *IEEE Transactions on Image Processing*, vol. 13, no. 2, pp. 154-165, 2004.

[22] Wang X., "Moving Window-Based Double Haar Wavelet Transform for Image Processing," *IEEE Transactions on Image Processing*, vol. 15, no. 9, pp. 2771-2779, 2006.

[23] Wen-ge F. and Lei L., "SVD and DWT Zero-Bit Watermarking Algorithm," *in Proceeding of IEEE International Conference on Informatics in Control, Automation and Robotics*, China, pp. 361-364, 2010.

[24] You X., Du L., Cheung Y., and Chen Q., "A Blind Watermarking Scheme Using New Non-Tensor Product Wavelet Filter Banks," *IEEE Transactions on Image Processing*, vol. 19, no. 12, pp. 3271-328, 2010.

[25] Yuan Y., Huang D., and Liu D., "An Integer wavelet Based Multiple Logo-Watermarking Scheme," *in Proceeding of IEEE 1st International Multi-Symposiums on*, Hanzhou, pp. 175-179, 2006.

Maheswari Sureshbabu Received B.E degree in Electrical and Electronics Engineering from the University of Madras on 2001 and M.E degree in Applied Electronics in Anna University Chennai on 2005. She has received Ph.D in the faculty of information and communication engineering in Anna University, Chennai on November 2013. She has teaching experience of 10 years. She is presently working as an assistant professor in the department of electrical and electronics engineering at Kongu engineering college, Perundurai, Tamilnadu, India. She has presented 14 papers in international conferences and six papers in national conferences and she has published 8 papers in international journals. Her current research interests are in the areas of Wavelets, Watermarking and Image processing.

Rameshwaran Kalimuthu obtained his B.E. Degree in Electronics and Communi-cation Engineering from the University of Madras in 1980. He obtained his M.E. degree in Electronics Engineering from Anna University, Chennai in 1982 and his Ph.D. degree from I.I.T.Madras, Chennai. He started his professional career with a brief stint at I.I.T. Madras during 1982-1983 as a Project Engineer. He joined the department of Electrical Engineering at the Thiagarajar College of Engineering, Madurai as an Associate Lecturer in July 1983. Later, he joined the department of Electronics and Communication Engineering at the National Institute of Technology, Tiruchirappalli in 1987. Presently he is working as a professor in shanmuganathan engineering college, Pudukottai, Tamilnadu. He has published several research papers in International and National Journals. He has also presented research papers in National and International conferences. His areas of interest are: Digital system and Microprocessors, Digital Filters and Control theory.

Vadivel Chandra Received B.E degree in Electronics and communication Engineering from Anna University on 2011 and M.E degree in Applied Electronics in Anna university Chennai on 2013. Presently he is working as an assistant professor in the department of Electronics and communication Engineering at K.P.R Institute of Engineering and Technology, Coimbatore, Tamilnadu, India. He has presented four papers in international conferences and two papers in national conferences. His area of research is Cryptography and Watermarking.