Ferdowsi University of Mashhad

I C C K E

International Conference on Computer and Knowledge Engineering

CERTIFICATE OF PRESENTATION

It is certified that

Seyyed Hossein Soleymani, Amir Hossein Taherinia,

Presented a paper titled

Robust Image Watermarking Based on ICA-DCT and Noise Augmentation Technique

during the 5th International Conference on Computer and Knowledge Engineering (ICCKE 2015), held on October 29, 2015 at Ferdowsi University of Mashhad.

Saeid Abrishami, PhD

ICCKE 2015 Conference Chair

Robust Image Watermarking Based on ICA-DCT and Noise Augmentation Technique

Seyyed Hossein Soleymani
M.Sc. Student of Department of Computer Engineering
Ferdowsi University of Mashhad
Mashhad, Iran
seyyedhosein.soleymani@stu.um.ac.ir

Amir Hossein Taherinia
Assistant Professor of Department of Computer Engineering
Ferdowsi University of Mashhad
Mashhad, Iran
taherinia@um.ac.ir

***Abstract*— In this paper, We present a blind image watermarking method based on DCT domain and independent component analysis (ICA). First of all, an approximation of cover image is created using ICA. We divide approximation image to equal 8x8 blocks and then apply DCT transform to each block. We use spread spectrum (SS) method for embedding the watermark bits. In our method a group of random bits are generated and embedded into high frequency coefficients of each block using SS method. For finding the watermark bits, we denoise watermarked image in order to augment the noise that was embedded into cover image. Then similar to embedding process the approximation image is created from the augmented noise image using ICA, and two group of random bits are generated again, and correlation of high frequency coefficients of the watermarked approximation image with the groups of random bits is computed. We find that, higher robustness and better imperceptibility is obtained because of using approximation image and spread spectrum technique. We test our method against some attacks such as additive Gaussian noise, Salt and Pepper noise, Speckle noise, JPEG and JPEG2000 compression and Average filter. Results show that, our method have a high robustness against Gaussian noise and compression, and good imperceptibility measure like PSNR for the watermarked images. Sensitivity to geometric attacks and need to more times for calculating ICA are two limitations of this method.**

Keywords-component; Blind Watermarking, ICA, DCT, compression attack, Spread Spectrum technique

I. INTRODUCTION

In the last twenty years, copyright protection of digital image have been more attended and for solve this problem many digital watermarking techniques are proposed. Often, domains like spatial, Discrete Cosine Transform, Fourier transform, Wavelet and other X-let transform Domains are used in image watermarking. Between mentioned domains, DCT is most frequently used. It can decompose an image into frequency coefficients which each coefficient of this decomposition have different value in reconstructing spatial domain of image. So it is good choice for embedding of watermark bits in suitable coefficients of DCT domain. In this transformation low and middle frequencies are used for watermark embedding because of high frequencies are choice for most of compressors like JPEG [1-5]. One of watermarking methods is based on Independent Component Analysis (ICA). It can separate independent signals of image. Most of watermarking methods use ICA in extraction phase [6, 7].

II. RELATED WORKS

In this section we describe some of DCT and ICA based watermarking methods.

In [11], the watermark bits are embedded in low frequency of DCT coefficients by changing the least significant bit (LSB). Therefore, this method has low robustness against JPEG compression because information bits are lost after quantization of DCT coefficients. In [10] a blind watermarking algorithm in DCT domain is presented. In this method, inter block correlation of adjacent blocks is used to determine type of watermark bits. In order to make difference between two adjacent block, one DCT coefficient of each block is modified. Difference between median of a few low frequency AC coefficients and DC is calculated and normalized by DC coefficient and this value is used to modify one coefficient in each block.

In [6] method called WMicaD (watermarking by independent component analysis with dual watermark) is presented. Aim of using two watermark in this method is robustness and tamper detection. This method use ICA to extract watermark using an external template image. In [7] a method based on redundant discrete wavelet transform (RDWT) and independent component analysis (ICA) is presented. The watermarks are embedded into middle frequencies such as LH and HL sub bands and in order to extracts watermarks in spatial domain an ICA based detector is proposed.

In [12], a non-blind and robust image watermarking is proposed that have robustness against geometric transformations and common image watermarking attacks like additive noises. In this method, Singular Value Decomposition of LL sub bands of Redundant-DWT transformation is computed and singular values of host image is manipulated by singular values of watermark image. Usually non-blind image watermarking methods are more robust than blind methods. We compare our proposed method with this paper.

III. MAIN TOOLS USED IN THIS METHOD

In this section we describe main tools that is used in this method of watermarking. We describe ICA, Spread Spectrum and DCT in the following subsections.

978-1-4673-9280-8/15/$31.00 ©2015 IEEE

Elearnica Downloaded from http://www.elearnica.ir

A. Independent Component Analysis

One of the most important methods in signal processing for separating independent components which are hidden in mixed signals is Independent component analysis (ICA). ICA is presented as a method for solving Blind Source Separation (BSS). Suppose observation signals be mixed of unknown independent sources. Aim of ICA is to find a transformation on observation signals such that output of this transformation be signals that are as possible as independent.

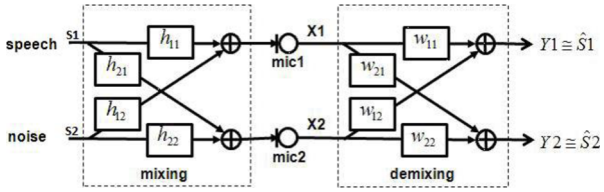

Fig 1: Process of Mixing and Demixing of two signals [13]

In the system of Fig 1 the observation signals is created using a linear unknown mixing transformation of sources. Mixing transformation can be shown as below:

$$x(t) = A\,s(t) \quad (1)$$
$$x(t) = [x_1(t), \dots, x_N(t)]^T \quad (2)$$
$$s(t) = [s_1(t), \dots, s_N(t)]^T \quad (3)$$

Equation (2) is observation signals vector and (3) is unknown source signals vector. Also, A is an unknown mixing matrix so each one of observation signals can be shown as (4):

$$x_i(t) = a_{i1}s_1(t) + a_{i2}s_2(t) + \cdots + a_{iN}s_N(t) \quad (4)$$

In (4), a_{ij} are elements of matrix A. Aim of ICA is to find matrix A using independent component analysis. It means that ICA must find coefficients of matrix A in a way that the separated components have the most statistical independence. FastICA is one of methods that find independent components using finding maximum Non-Gaussian signals [8]. In this paper we use FastICA to make an approximation image of cover and watermarked image.

DWT can decompose cover image to four decompositions in vertical, horizontal and diagonal directions. We can using ICA decompose cover image to more than four decompositions, although in this paper we decompose image into just four decompositions. In order to have more decompositions we must reshape more rows and give them to FastICA algorithm as input.

B. DCT & Spread Spectrum Watermarking

Discrete cosine transform (DCT) is one of transformations that map an image from spatial domain to frequency domain. In [11] Low frequency coefficients of a DCT based transformed image is used for producing robust watermarking systems, because in compressions like JPEG, high frequency of transformations will change.

In some cases, spread spectrum technique (SS) is used for watermarking in DCT domain. Using SS technique for each bit of watermark we embed a group of random bits which is much larger than one bit in count. In this case, in front of embed one bit of watermark with creating large change in just one coefficient of cover image, SS technique embed more bits with smaller change in much more coefficients of cover image. So, changes which is viewed in image using SS technique is much smoother. As a result, we select Spread Spectrum method because we can using it have a blind watermarking method and have more security in embedding watermark. Also, we want to embed watermark bits in high frequency coefficients of blocks of approximation image. So, SS method can be better choice than quantization methods [1, 14].

IV. PREPOSED METHOD

A. Watermark Embedding

In order to embed the watermark into the cover image we first create an approximation image using ICA and then we embed the watermark bits in high frequency coefficients of DCT approximation image using spread spectrum method.

First of all, cover image is divided into 2×2 blocks. Then each 2×2 block reshaped as a 4×1 vector. If cover image be a $N \times N$ matrix in this case we have $(\frac{N}{2}) \times (\frac{N}{2})$ blocks with 2×2 size that each block is presented as a 4×1 vector. If we put together this 4×1 columns, a matrix with size $4 \times \left((\frac{N}{2}) \times (\frac{N}{2})\right)$ will be make. Then this $4 \times \left((\frac{N}{2}) \times (\frac{N}{2})\right)$ matrix is given to FastICA method as input in order to separate independent components. Output of FastICA method can be 1, 2, 3 or 4 signals with size $1 \times \left((\frac{N}{2}) \times (\frac{N}{2})\right)$ according to input image. Also, two 4×4 matrix for mixing and demixing operations is created using FastICA that is used for reconstruct watermarked image using output signals. One of output signals of FastICA is approximation of main image that have half of size of main image. If we two times again do above method to create approximation image, an image with size $(\frac{N}{2^3}) \times (\frac{N}{2^3})$ is obtain that we give it to second steps for embedding. Above operations can be seen in Fig 2. Size of approximation image after three times using FastICA is $\frac{1}{64}$ smaller than main image. In other words if main image have 512×512 pixels, approximation image will be 64×64 pixels. Steps of first phase is presented in Fig 2.

After creating approximation image from cover image, we divide it to 8×8 blocks and do DCT on each block. After blocking of approximation image, according to the bit (0 or 1) value of watermark we make a group of random bits as noise and add them to high frequency coefficients of each block using below equation:

$$DCTBlock^w(u,v) = \begin{cases} DCTBlock(u,v) + k \times W_x^i(u,v), & u,v \in F_H, i \in \{0,1\} \\ DCTBlock(u,v), & u,v \notin F_H \end{cases} \quad (5)$$

As shown in (5), just high frequency coefficients of each block is used. In this equation $DCTBlock$ represent DCT transformation of blocks of approximation image, and K represent gain coefficient. If we increase the gain, robustness of watermarking will be increase but

imperceptibility of watermarked image will be decrease. Also, x is one bit of group of random bits and (u, v) is coordinate of DCT coefficient corresponding to x in approximation image. Result of above equation is $DCTBlock^w$ which it is watermarked approximation image and W^i is a group of random bits according to the bit (0 or 1) value of watermark that we want to embed in each block. As well as, F_H shows high frequency coefficients of each block that is selected to be embedding. Embedding in high frequency coefficients led to good imperceptibility of watermarked image. For a cover image with size 512×512, maximum number of bits of watermark can be 8×8. In robust watermarking have a binary sequence with size 70(bit) is sufficient for proof of ownership [18].

After embedding of watermark in suitable DCT coefficients, we must do inverse transform of DCT (I-DCT) on embedded blocks in order to make approximation image. Last step for creating final watermarked image is use of non-approximation signals of ICA and watermarked approximation image. We must use mix matrix that is output of FastICA to mix signals and create an image in original size. Because we have used three times of FastICA for creating approximation image, then we must do three times reverse operations as demixing to create final watermarked image. In this method we use two different groups of random bits for each zero and one bits of watermark. If the groups of random bits be created with carefully and they have low correlation then error rate will be low in detector. Steps of second phase is presented in Fig 3.

B. Watermark Extraction

As described in embedding section, for embedding of watermark we used SS method, such a way each bit of watermark is embedded into high frequency coefficients of DCT of approximation image like a group of random bits. For extraction of watermark we can use method described in [9] that it use denoising technique for extract noise added to cover image in watermark embedding step. In this technique first we denoise watermarked image A and create $\acute{A}$ and compute $A - \acute{A}$ that shows noise added to cover image then create an approximation of image from the noise image using ICA, and the same group of random bits is generated. Then DCT of 8×8 blocks of approximation image is created and correlation between groups of random bits with high frequency coefficients of the watermarked approximation image is computed. In this time we can find bit that is embedded in each block. We do this work for all 64 blocks in approximation image to extract embedded hidden watermark.

After extracting of embedded watermark in watermarked image, we can compute mean of correlation of extracted bits using NC similarity criterion and if this value is greater than an experimental threshold we can announce existing of watermark in image.

In Figs 4 and 5 Lena cover image and original watermark is viewed. Watermarking in this method, in no attack state, make very small change in cover image and PSNR of watermarked image and cover image is greater than 40 dB and NC value of watermark is equal to 1.

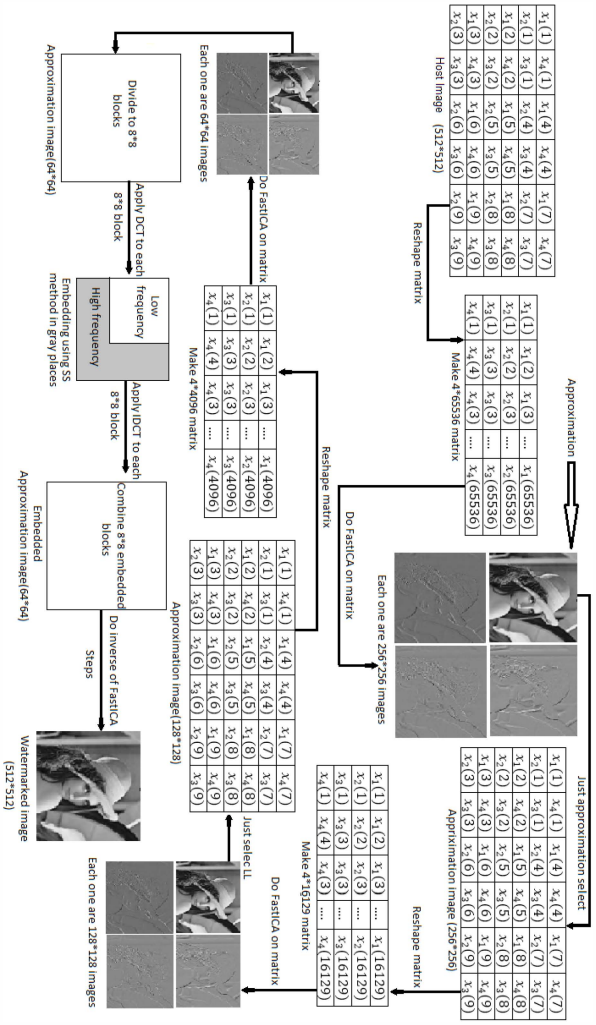

Fig 2: First phase of embedding process

Fig 4: Lena cover image

Fig 5: Original watermark

V. EXPERIMENTAL RESULTS AND DISCUSSIONS

We test our method on about forty different test image of size 512×512 with different level of details. For evaluation of robustness we apply JPEG and JPEG2000 compression attacks, Gaussian noise attacks from Stirmark [17] benchmark and Average filter attack, Salt and Pepper noise and Speckle noise attacks using Matlab. An 8x8 block of bits as watermark matrix is shown in Fig 5 which is created for embedding in the cover images.

In this paper for evaluation of visual quality we calculate PSNR criterion between cover image and watermarked image. The PSNR criterion shows peak signal to noise ration and is defined as (7):

$$PSNR(f,w) = 10log_{10}\left[\frac{max_{\forall(m,n)}f^2(m,n)}{\frac{1}{N_f}\sum_{\forall(m,n)}\left(f_w(m,n)-f(m,n)\right)^2}\right] \quad (6)$$

In (6), $f(m,n)$ is the original cover image, $f_w(m,n)$ is the watermarked or attacked watermarked image and N_f is number of pixels in image. Unit of PSNR is decibel (dB).

Also, we used Normalized Cross Correlation (NC) in order to have a measure for evaluation of robustness of watermark against attacks. NC formulation is as (7):

$$NC = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W(i,j)\times \acute{W}(i,j)}{\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W(i,j)]^2}\times\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}\left[\acute{W}(i,j)\right]^2}} \quad (7)$$

In (7), M_1 and M_2 are dimensions of watermark image or watermark pattern, and $\acute{W}$ and W are the extracted and original the watermark. Value of NC is between 0 to 1. According to our experiments ideal value of gain factor in order to receive psnr value more than 40 dB is 0.09.

Some of experimental results on Lena image is presented on Fig 6-11. As we see in Figs 8 and 9, even after JPEG compression with applying quality factor QF=1%, extracted watermark just have 6 error bit; this improvement in compression is one of the most benefits of this method. In Fig 10 Lena image is showed after adding 10% of Gaussian noise to watermarked image with gain factor 0.09 and extracted watermark is showed in Fig 11. Even after this attack that PSNR of watermarked image is 7.87, NC is 0.75 and is a good result.

Fig 6: Lena image after embedding with gain factor 0.09 and after compression 10% that have PSNR=8.96 dB

Fig 7: Extracted watermark with NC=0.96, Error=1 bit

Fig 8: Lena image after embedding with gain factor 0.09 and after compression 1% that have PSNR=11.16 dB

Fig 9: Extracted watermark with NC=0.81, Error=6 bit

Fig 10: Lena image after embedding with gain factor 0.09 and after adding 10 % Gaussian noise that have PSNR=7.87 dB

Fig 11: Extracted watermark with NC=0.75, Error=8 bit

In Figs 12-16 results of applying JPEG and JPEG2000 compression, adding Gaussian noise, Salt and Pepper noise and Speckle noise over watermarked Lena image with different gain factors is showed. As can be seen from Figs increasing gain factor let to increase of NC of extracted watermark.

In Figs 17 and 18 we can see results of testing proposed method over 40 different images. Results in Fig 17 shows that for less than 10 percent Gaussian noise, NC is greater than 0.66. And results in Fig 18 shows that for 1% JPEG compression the NC value is greater than 0.72 that it is a good result. We represent simultaneously PSNR of watermarked image in other vertical axis to have better mind of current situation of watermarked image in Figs 17-20.

In Figs 19 and 20 we can see comparison of proposed method and RDWT-SVD method. We test Gaussian noise and Average filter over watermarked image. Results show that proposed method has a better robustness than RDWT-SVD method.

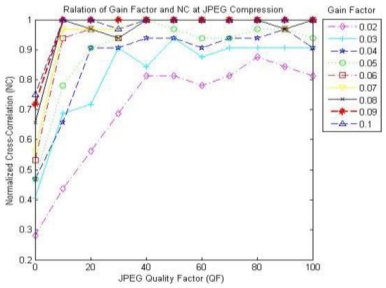

Fig 12: Comparison between gain factor and NC in case of JPEG compression over Lena watermarked image

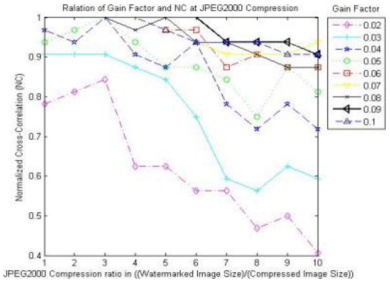

Fig 13: Comparison between gain factor and NC in case of JPEG2000 compression over Lena watermarked image

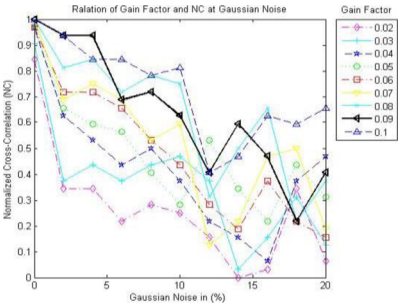

Fig 14: Comparison between gain factor and NC in case of Gaussian noise over Lena watermarked image

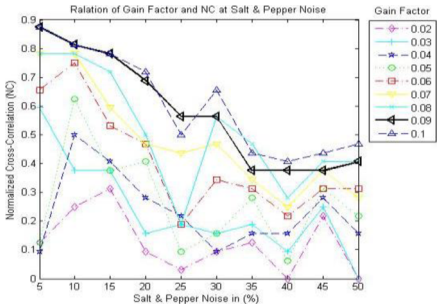

Fig 15: Comparison between gain factor and NC in case of Salt and Pepper over Lena watermarked image

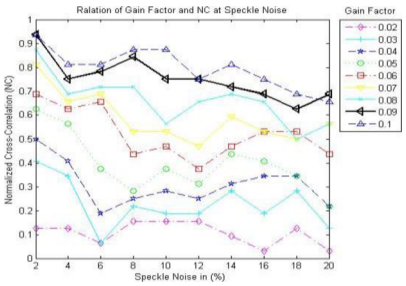

Fig 16: Comparison between gain factor and NC in case of Speckle noise over Lena watermarked image

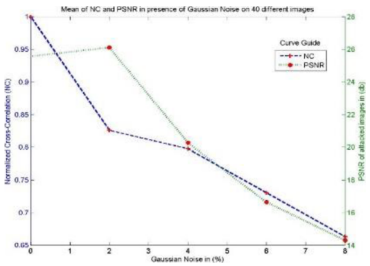

Fig 17: Average of test 40 different image in presence of Gaussian Noise in (%)

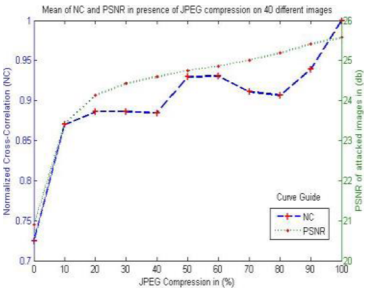

Fig 18: Average of test 40 different image in presence of JPEG Compression in (%)

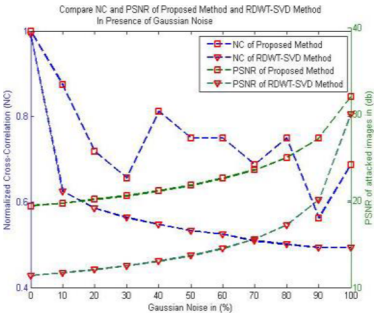

Fig 19: Compare result of proposed method and RDWT-SVD method in presence of Gaussian Noise with sigma(x) and zero mean

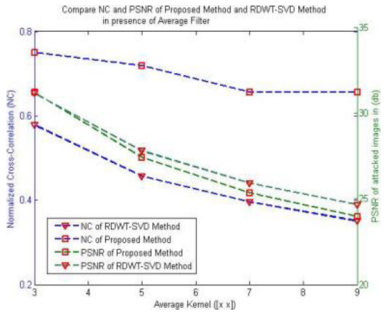

Fig 20: Compare result of proposed method and RDWT-SVD method in presence of Average Filter with different kernels([x x])

VI. RESULT AND FUTURE WORK

In this paper a blind image watermarking based on ICA technique and Spread Spectrum method in DCT domain is presented. First an approximation of cover image is created using ICA and then we embed the watermark in high frequency coefficients of DCT of 8×8 blocks of it. With determining coefficients which have been changed in compressors we can receive better robustness in front of compression. With this reality we propose a method based on creating approximation image using ICA and embedding in DCT domain that is robust even against JPEG compression with QF=1% while watermarked image PSNR is good.

Attacks on image watermarking can be divided to two main category: Intentional attacks and Unintentional attacks. In real world usually attacks are unintentional but there are some methods that their goal is to produce intentional attacks without loss of PSNR of watermarked images [15, 16]. Our proposed method have a good robustness in high JPEG and JPEG2000 compression and adding noise attacks; Although, in this situations PSNR of watermarked images can be highly decreased. We can claim that if an attacker apply such intentional attacks using JPEG compression and adding noise, our proposed method can extract watermark with acceptable NC.

Usually non-blind image watermarking methods are more robust than blind methods. We compare our proposed method with this RDWT-SVD method [12] that is a non-blind robust image watermarking. With Compare of Experiments, We see that in presence of Gaussian noise and Average filter that we tested, proposed method is more robust.

One of main steps of proposed method is creating approximation image using ICA. For future work anyone can test DWT, DCT or other domains to create approximation image. We can use wavelet transform to create approximation image in order to obtain good robustness against JPEG2000 compression. In our work we use gray images for watermarking and size of watermark for a 512x512 image is 64 (8x8) bits. In future, anyone can use color images and benefit of their color systems like RGB and CMYK in order to have more space and recognize more robust places for embedding. Sensitivity to geometric attacks and need to more times for calculating ICA are two limitations of this method. So, as future works we can robust this method against geometric attacks such as rotation and

scaling and apply preprocessing works to reduce the time processing of this method.

REFERENCES

[1] I Cox, Miller M., Bloom J., " Digital Watermarking and Steganography " Artech House, January 2008, ISBN: 0123725852.

[2] P Wayner, " Disappearing cryptography: information hiding: steganography & watermarking ", International Journal of Image and Graphics, 2008, ISBN: 0123744792.

[3] M Ramaraj, S Raghavan, "A survey of wavelet techniques and multiresolution analysis for cancer diagnosis." Computer, Communication and Electrical Technology (ICCCET), 2011 International Conference on. IEEE, 2011..

[4] Khan, Asifullah. "A recent survey of reversible watermarking techniques." Information Sciences 279 (2014): 251-272.

[5] Hai T., Chongmin L. "Robust image watermarking theories and techniques: A review." Journal of applied research and technology 12.1 (2014): 122-138.

[6] T.V. NGUYEN, J.C. PATRA, and P.K. MEHER, "WMicaD: A New Digital Watermarking Technique Using Independent Component Analysis," EURASIP Journal on Advances in Signal Processing, vol. 2008, no. 2, 2008.

[7] Hien, Thai Duy, Z Nakao, and Yen-Wei Chen. "Robust multi-logo watermarking by RDWT and ICA." Signal Processing 86.10 (2006): 2981-2993.

[8] Comon, Pierre, and Christian Jutten, eds. Handbook of Blind Source Separation: Independent component analysis and applications. Academic press, 2010.

[9] Kasmani, Saied Amirgholipour, Meysam Mahfouzi, and Mohsen Asfia. "A new pre-processing approach to improve DCT-based watermarkings extraction." Computer Science and Information Technology-Spring Conference, 2009. IACSITSC'09. International Association of. IEEE, 2009

[10] Das, Chinmayee, "A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation." AEU-International Journal of Electronics and Communications 68.3 (2014): 244-253.

[11] Lin, Shinfeng D., and Chin-Feng Chen. "A robust DCT-based watermarking for copyright protection." IEEE Transactions on Consumer Electronics 46.3 (2000): 415-421.

[12] Lagzian, Samira, Mohsen Soryani, and Mahmood Fathy. "A new robust watermarking scheme based on RDWT-SVD." International Journal of Intelligent Information Processing 2.1 (2011): 22-29.

[13] Lee, Heungkyu. "Simultaneous Blind Separation and Recognition of Speech Mixtures Using Two Microphones to Control a Robot Cleaner." Int J Adv Robotic Sy 10.103 (2013).

[14] Golikeri, Adarsh, and Panos Nasiopoulos. "A robust DCT energy based watermarking scheme for images." Journal of Proceedings of IEEE (2005).

[15] Taherinia, Amir H., and Mansour Jamzad. "A two-step watermarking attack using long-range correlation image restoration." Security and Communication Networks 5.6 (2012): 625-635.

[16] Taherinia A.H. and Jamzad M., "A New DWT-Based Watermarking Robustness Evaluation Method", Optical Engineering, Vol. 50(5), Pages 057006-1:057006-9 (May 2011).

[17] Peticolas A.-P., Anderson R.-J., and Kuhn M.-G., "Attacks on copyright marking systems", In 2nd Workshop on InformationHiding, Portland, Oregon, April 1998.

[18] F.A.P. Petitcolas , R.J. Anderson, and M.G. Kuhn,"Information Hiding-A Survey." Proceedings of the IEEE,Vol. 87, No.7, 1999, pp.1062-1078.