A Novel Biometrics Triggered Watermarking Of Images Based On Wavelet Based Contourlet Transform

P.Tamije Selvy
Assistant Professor (SG)
Sri Krishna College of Technology

Dr.V.Palanisamy
Principal
Info Institute of Technology

S Elakkiya
PG Scholar
Sri Krishna College of Technology

ABSTRACT

The rapid development of network and digital technology has led to several issues to the digital content. The technical solution to provide law enforcement and copyright protection is achieved by digital watermarking Digital watermarking is the process of embedding information into a digital image in a way that is difficult to remove. The proposed method contains following phases (i) Pre-processing of biometric image (ii) key generation from the biometrics of the owner/user and randomization of the host image using Speeded-Up Robust Features (SURF) (iii) Wavelet-Based Contourlet Transform (WBCT) is applied on the host image. The WBCT can give the anisotropy optimal representation of the edges and contours in the image by virtue of the characteristics of multi-scale framework and multi-directionality (iv) Singular Value Decomposition (SVD) is enforced over the watermark image (v) Embedding of the host image with the watermark image. The comparative analysis confirms the efficiency and robustness of the proposed system

Keywords

Digital Watermarking, copyright, Pre-processing, wavelet, Speeded-Up Robust Features.

1. INTRODUCTION

The size of multimedia items are sharply decreasing by compression algorithms, increased internet connection speed helps to download much more data and the people connected to the net can share these types of data easily with peer-to-peer connection. Then, the protection of multimedia items gets more difficult day by day. Digital watermarking systems have been proposed to provide content protection, authentication and copyright protection [2], protection against unauthorized copying and distribution, etc.

In recent years, several watermarking algorithms have been proposed in the literature. These algorithms can be broadly classified in two categories, according to the embedding domain: the spatial domain and the transform domain. In the classification of watermarking schemes [1], an important criterion is the type of information needed by the detector which is shown in the Table 1:

Table 1. Type of Information Needed By Detector

Schemes	Requirement
Non-blind	The host image and The secret key(s)
Semi-blind	The secret key(s) and the watermark bit sequence.
Blind	secret key(s)

Spatial domain approaches [1] are the simplest, and the earliest algorithms were based on the modification of pixel intensities. These algorithms are generally fragile to numerous attacks. On the other hand, transform domain approaches insert the watermark into the transform coefficients.

Biometric authentication refers to verifying individuals based on their physiological and behavioral characteristics such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc. It is inherently more reliable than password-based authentication, as biometric characteristics cannot be lost or forgotten; they are extremely difficult to copy, share, and distribute and require the person being authenticated to be present.

2. RELATED WORKS

The iris is the annular region of the eye bounded by the pupil and the sclera. The visual texture of the iris is formed during fetal development. By the first two years of life it stabilizes. The complex iris texture carries very distinctive information useful for personal recognition [4]. The accuracy and speed of currently deployed iris-based recognition systems is promising and points to the feasibility of large-scale identification systems based on iris information. Each iris is believed to be distinctive and, like fingerprints, even the irises of identical twins are expected to be different. It is extremely difficult to surgically tamper the texture of the iris. Further, the ability to detect artificial irises (e.g., contact lenses) has been demonstrated in the literature. Although the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more users friendly and cost-effective.

Given its suitability to model the Human Visual System (HVS) behavior, the DWT has gained interest among watermarking researchers, as it is witnessed by the number of algorithms. Some methods directly take inspiration from the most popular Wavelet based compression algorithms. In [8], the binary logo and the image are hierarchically decomposed (the image through DWT), each detail subband of the logo is then embedded into the corresponding detail subband of the image (more b its of the binary logo are embedded into more active image locations), and the original image is required for watermark extraction. Image activity is estimated block wise through variance computation. The most widely used detector is probably the Harris corner detector [3], proposed. It is based on the Eigen values of the second moment matrix. However, Harris corners are not scale invariant. The SURF descriptor still seems the most appealing descriptor for practical uses, and hence also the most widely used nowadays. It is distinctive and relatively fast, which is crucial for on-line applications.

3. PROPOSED METHOD

In this section, some of the motivating factors in the design of our approach to the biometrics trigged Randomization of Images Based On Wavelet-Based Contourlet Transform

technique are discussed shown in Fig. 1. Without loss of generality, assume that Image I represent the original host and of size M × N respectively. The core idea is to capture the appropriate biometrics of the owner/user followed by the transform order generation using SURF and biometrics images. Now, the host image is randomized with the help of a nonlinear chaotic map and Hessenberg decomposition followed by embedding in the WBCT.

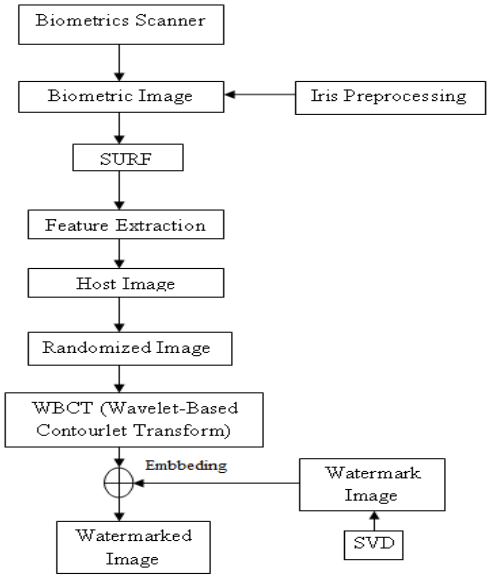

Fig 1: Block Diagram of Proposed Method

3.1 Biometrics

Thus, a biometrics-based authentication scheme is a powerful alternative to traditional authentication schemes. In some instances, biometrics can be used along with passwords to enhance the security offered by the authentication system. In the context of a digital rights management (DRM) system, biometrics can be used 1) to facilitate the entire authentication mechanism, or 2) secure the cryptographic keys that protect a specific multimedia file.

A number of biometric characteristics have been in use for different applications [10]. Each biometric trait has its strengths and weaknesses, and the choice depends on the application. A biometric feature cannot effectively meet all requirements. In other words, no biometric is "optimal" although a number of them are "admissible." The suitability of a specific biometric for a particular application is determined depending upon the requirements of the application and the properties of the biometric characteristic. It must be noted that traits, such as voice and keystroke, lend themselves more easily to a challenge-response mechanism that may be necessary in some applications. Table 2 shows the comparison on different biometric identifier.

Before the key generation, two biometrics iris images of the user are captured by the biometrics scanner. After capturing the biometrics images, the features are extracted followed by the key generation. The iris is the elastic, pigmented, connective tissue that controls the pupil. The iris is formed in early life in a process called morphogenesis. Once fully formed, the texture is stable throughout life [13]. The iris of the eye has a unique pattern, from eye to eye and from person to person [13]. An iris scan analyzes over 200 points of the iris, such as rings, furrows, freckles, and the corona, and compares it with a previously recorded template. Glasses, contact lenses, and even eye surgery do not change the characteristics of the iris [13, 14]. The iris will not be forgotten or stolen, and this suggests that an iris perfectly authenticates a person when compared with other biometrics such as face, fingerprints, and voiceprints.

Table 2. Comparison of different Biometric identifier

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Finger Print	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

3.2 Image Pre-processing

Image pre-processing can significantly increase the reliability of an optical inspection. Biometric images are increased with the contrast by mapping the values of the input intensity image to new values such that, by default, 1% of the data is saturated at low and high intensities of the input data.

3.3 Speeded-Up Robust Feature

SURF approximates or even outperforms Scale Invariant Feature Transform (SIFT) [3] with respect to repeatability, distinctiveness, and robustness, yet can be computed and compared much faster. This is achieved by relying on integral images for image convolutions; by building on the strengths of the leading existing detectors and descriptors (specifically, using a Hessian matrix-based measure for the detector, and a distribution-based descriptor); and by simplifying these methods to the essential. This leads to a combination of novel detection, description, and matching steps. The whole SURF technique is summarized into following steps.

1. Interest Points Localization: The interest points (their locations and sizes) are chosen automatically using a Fast-Hessian detector (1) that is based on the determent of the Hessian matrix, i.e.,

$$H = \begin{pmatrix} Lxx(x,y,\sigma) & Lxy(x,y,\sigma) \\ Lxy(x,y,\sigma) & Lyy(x,y,\sigma) \end{pmatrix} \quad (1)$$

where Lxx is the convolution of the Gaussian second-order derivative with an image I at the point (x, y).

2. Interest Point Descriptors: SURF descriptors are calculated in the square regions centred on each interest point. The region is divided into 4×4 equal sub regions. In each sub region, the Harr wavelet responses in the horizontal (dx) and vertical (dy) directions are calculated.

3.4 The Wavelet Based Contourlet Transform

The contourlet transform based on a multiscale and multidirectional filter bank developed by Do and Vetterli is one of the new geometrical image transforms, which can capture nearly arbitrarily directional information of the natural images. It has been shown to be a better alternative choice than wavelets for image denoising. This transform consists of two major stages: the subband decomposition and the directional transform. At the first stage, Laplacian pyramid (LP) is employed, while directional filter banks (DFB) are used for the second stage. But, the contourlet transform is a redundant image transforms due to LP. The Wavelet-Based Contourlet Transform (WBCT) [6] developed by Eslami and Radha, with a construction similar to the contourlet is a new non-redundant image transform. It also consists of two filter bank stages: the first stage provides subband decomposition using wavelet transform rather than the Laplacian pyramid; the second stage of the WBCT is a directional filter bank (DFB), which provides angular decomposition. At each level in the wavelet transform of the first stage, the image is decomposed into LF subband and three HF subband(corresponding to the LH, HL, and HH) by wavelet transform; Then, each HF subband is decomposed into the number of direction subbands by the DFB in a given level. Start from the desired maximum number of directions on the finest level of the wavelet transform, and decrease the number of directions at every other dyadic scale when preceded through the coarser levels. By means of this way, the anisotropy scaling law is achieved. Moreover the wavelet filters are not perfect in splitting the frequency space to the low pass and high pass components, the scheme using fully DFB decomposition on each band could compensate for the drawbacks of the wavelet filters [12]. Fig.2 shows the flowchart of first level decomposition of WBCT on an image. The HF subband images from the WT are processed by the DFB so that the directional information can be captured. The scheme can be iterated the LF subband image over. The WBCT decomposes the image into directional subbands at multiple scales.

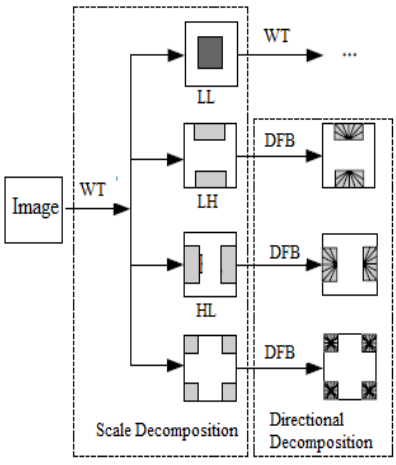

Fig 1: First Level Decomposition of WBCT

By analyzing, we find that WBCT can capture image structure features more efficiently than Discrete Wavelet Transform (DWT) [7] and be more suitable to identify the subbands in the host image where a watermark can be embedded effectively. Considering a watermarking scheme that embeds watermark into HF subbands, which watermark will be removed easily when the watermarked image is attacked by image processing methods destroying the HF information of the image; while watermark is embedded in LF subbands which may make the scheme easily perceptible. In order to ensure the visual quality and robustness of the image which watermark is embedded into, the watermark should be embedded into the low-middle frequency subbands in our scheme.

3.5 Embedding of watermark images

The watermark image (W) is embedded into the randomized host image

1. Perform L-level order decomposition using WBCT on randomized image
2. Perform SVD on all the subbands of the randomized host image and the gray scale watermark
3. Modify the Singular values of all subbands with the help of singular values of the watermark

   $$A = USV^T \quad (1)$$

   Where S is a diagonal matrix with non-negative real numbers on the diagonal arranged in decreasing order. The diagonal entries of S are known as the singular values of A
4. Perform inverse SVD to construct all modified subbands
5. Perform inverse L-level order decomposition of WBCT
6. Perform the inverse randomization to obtain the watermarked image

4. RESULTS AND DISSCUSION

4.1 Experimental Setup

The performance of the proposed biometrics inspired watermarking framework is demonstrated using a MATLAB platform. Experiments are performed on different gray-scale images of size 256 × 256, namely Boat, Mandril and Lady. Therefore, biometrics inspired keys are unique and can only be generated by the owner/user. Here, the iris biometrics are used in all simulations. The iris is the elastic, pigmented, connective tissue that controls the pupil. The iris is formed in early life in a process called morphogenesis. Once fully formed, the texture is stable throughout life. The iris of the eye has a unique pattern, from eye to eye and from person to person [13]. An iris scan analyzes over 200 points of the iris, such as rings, furrows, freckles, and the corona, and compares it with a previously recorded template. Glasses, contact lenses, and even eye surgery do not change the characteristics of the iris. The iris will not be forgotten or stolen, and this suggests that an iris perfectly authenticates a person when compared with other biometrics such as face, fingerprints, and voiceprints. For instance, Fig 4. Shows two iris images of both eyes of a person captured over a short period of a few seconds, and it can be seen that the pattern obtained is different and gray value distribution is changed due to the eye movement and other factors. The two iris images are randomly selected from the Palacky University iris database [9] for key generation. The database contains 256 iris images (2 × 64 of left and 2 × 64 of right eye) of size 576 × 768 pixels. These irises were scanned by a TOPCON TRC50IA optical device connected to a SONY DXC-950P 3CCD camera.

The input biometric image is taken which is converted into the gray scale image Fig.3. The input is pre-processed [11]. The pre-processing is done for the significantly increase the reliability of an optical inspection shown in Fig. 5. Then interest points are matched on the biometric gray scale images which are done using SURF. Fig. 6. The Host image (Mandrill) is randomized which is then decomposed using the WBCT. Two level decomposition is used in Fig 7 and Fig 8. Thus the image quality is measured using the peak signal to noise ratio (PSNR) shown in equation 2. The PSNR values are 44.6582, 45.6658 and 44.0178, respectively for Boat, Mandrill and Lady Images. The visual results are given only for the Mandrill image because it has maximum PSNR among all experimental images. The transformed applied image quality is measured using the peak signal to noise ratio (PSNR) which indicates the similarity between the host and the transformed image is shown between DWT and WBCT with SVD where the comparative analysis is Fig.11 and Fig.12. PSNR represents a measure of the peak error. To compute the PSNR, the block first calculates the mean-squared error using the following equation:

$$MSE = \sum_{M,N} \frac{[I_1(m,n) - I_2(m.n)]^2}{M * N} \qquad (2)$$

In the previous equation, *M* and *N* are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right) \qquad (3)$$

In the previous equation, *R* is the maximum fluctuation in the input image data type. In Table 3 performance analysis is been shown on SURF and SIFT, which is based on feature extraction rate and the time of extraction visually shown in Fig. 9 and Fig. 10.

Table 4. Comparison between SURF and SIFT

S.NO	Method	Total matches	Processing Time(in sec)
1	SURF	379	0.8
2	SIFT	362	1

Table 5. Comparison between SVD and WBCT

S.NO	Image quality Measurement	SVD	WBCT+SVD
1	PSNR	44.5703	48.0992
2	MSE	0.0409	0.0282

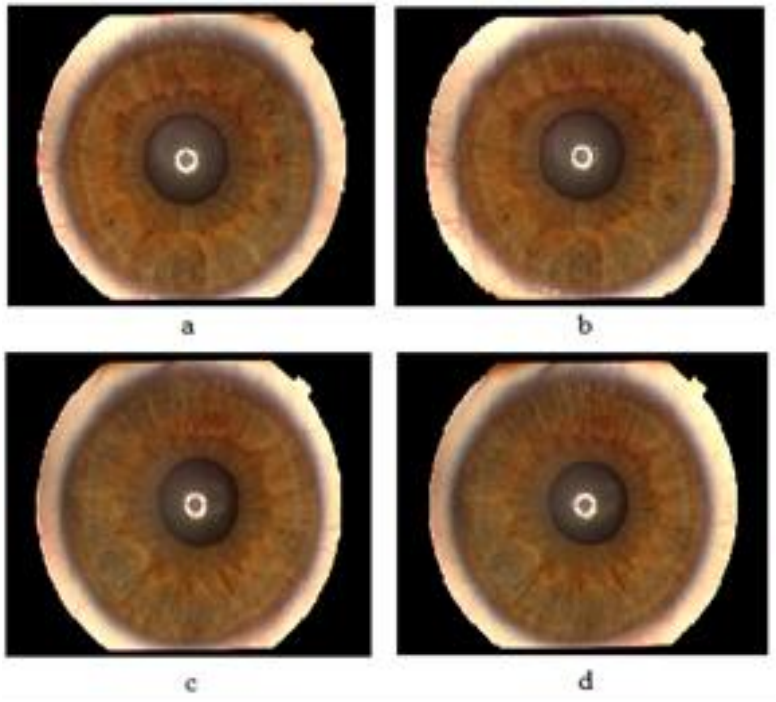

Figure 3. Iris images of a person captured over a short period of a few seconds. (a, b) left eye; (c,d) right eye.

Figure 4. (a, b, c) original host

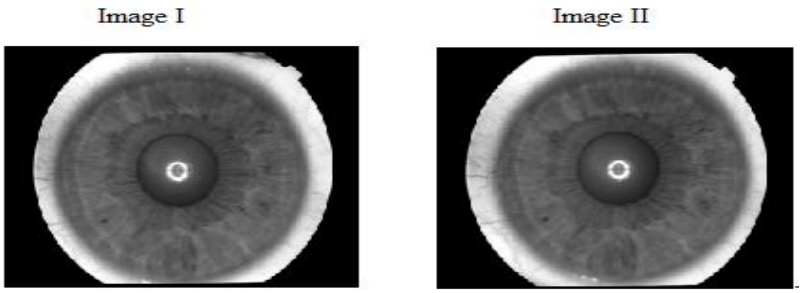

Figure 5. Pre-processed Input

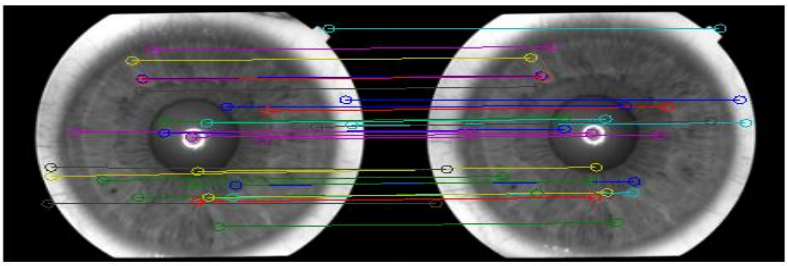

Figure 6. Interest points Matching

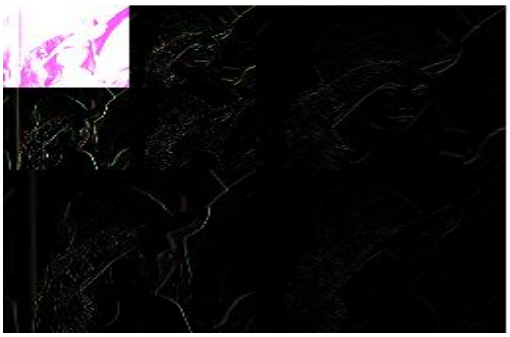

Figure 7. Applying two level WBCT Decomposition

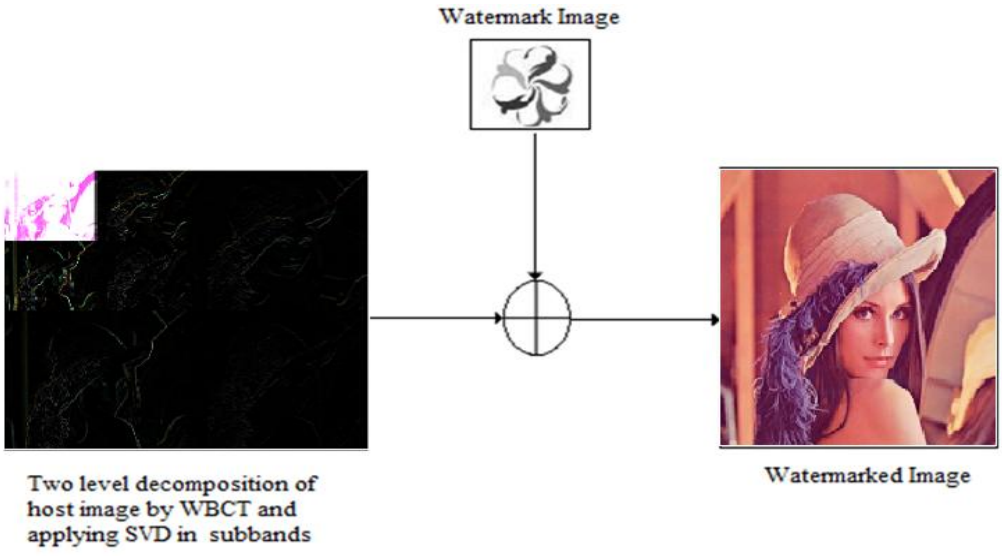

Figure 8. Watermark Embedding

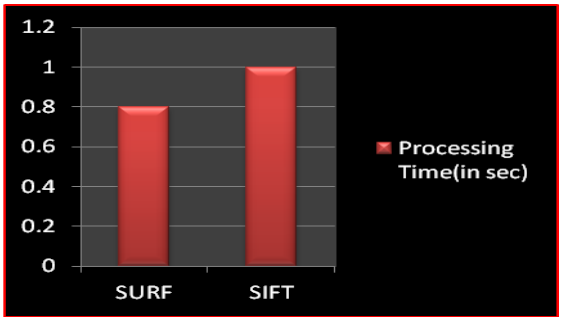

FIGURE 9. EXECUTION TIME COMPARISON

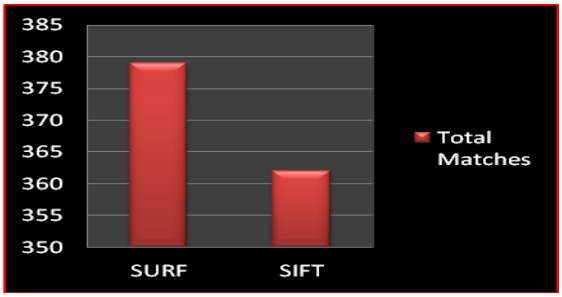

Figure 10.Total matches Comparison

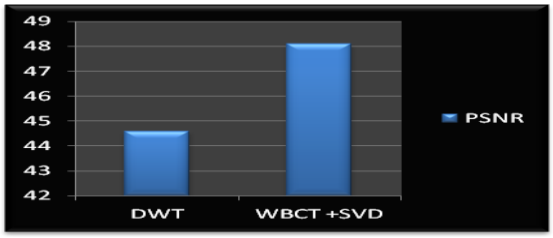

Figure 11. Comparison of PSNR value

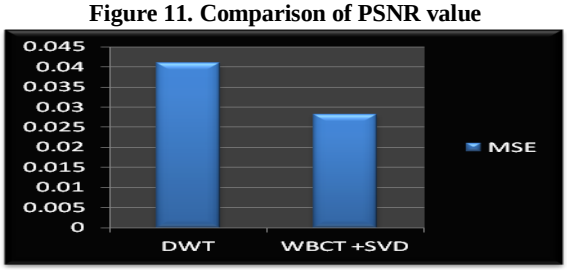

Figure 12. Comparison of MSE value

5. CONCLUSION

In this paper, biometrics trigged randomization of images based on WBCT is proposed in which the key concept is introduced with biometric security. By pre-processing of the original image it improves the optical inspection. Efficient method is used for the feature extraction and interest matching points are found using the SURF. The SURF performance is shown in the performance analysis which is efficient in both retrieval time and feature extraction. A single level decomposition of the image is performed with the WBCT which is embedded with the biometric keys. Thus, the WBCT can give the anisotropy optimal representation of the edges and contours.

6. REFERENCES

[1] G.C. Langelaar, I. Setyawan, R.I. Lagendijik, Watermarking digital image and video data, IEEE Signal Processing Magazine 17 (5) (2000) 20–46.

[2] A.K. Jain, A. Ross: a tool for information security, IEEE transactions on Information Forensic and security (2006).

[3] H. Bay, T. Tuytelaars, L. Van Gool, SURF: speeded up robust features, in:Proc. European Conference on Computer Vision, Graz, Austria, vol. 1, 2006,pp. 404–417.

[4] A.K. Jain, A. Ross, S. Pankanti, Biometrics: a tool for information security,IEEE Transactions on Information Forensics and Security 1 (2) (2006) 125–143.

[5] Z.M. Lu, D.G. Xu, and S.H. Sun.Multipurpose image watermarking algorithm based on multistage vector quantization.IEEE Transactions on Image Processing, 14:5(2005), 822-831.

[6] Jing Liu, Gang Liu A New Digital Watermarking Algorithm Based On WBCT in 2012 International Workshop on Information and Electronics Engineering (IWIEE)

[7] Ali Al-Haj. Combined DWT-DCT digital image watermarking. Journal of Computer Science,3: 9 (2007),740-746.

[8] E. Yavuz, Z. Telatar, Improved SVD–DWT based digital image watermarking against watermark ambiguity, in: Proc. ACM Symposium on Applied Computing, 2007, pp. 1051–1055.

[9] Michal Dobeš, Libor Machala, Iris database. http://www.inf.upol.cz/iris/.

[10] Biometrics inspired watermarking based on a fractional dual tree complex wavelet transform Gaurav Bhatnagar, Q.M. Jonathan Wu Department of Electrical and Computer Engineering, University of Windsor, Windsor, Ontario, ON, N9B 3P4, Canada(2012)

[11] www.mathworks.com.

[12] Gang Liu, The Translation Invariant Wavelet-based Contourlet Transform for Image Denoising journal of multimedia, vol. 7, no. 3, June 2011

[13] K. Roy, P. Bhattacharya, Iris Recognition: A Machine Learning Approach, VDM Verlag Saarbrücken, Germany, 2008.

[14] John Daugman, The importance of being random: statistical principles of iris recognition, Pattern Recognition 36 (2) (2003) 279–291.