A Novel Watermarking of Images Based on Wavelet Based Contourlet Transform Energized by Biometrics

P.TAMIJE SELVY[1], Dr.V.PALANISAMY[2], S.ELAKKIYA[3]
Computer Science and Engineering[1, 3]
Sri Krishna College of Technology[1,3], Info Institute of Engineering[2]
INDIA
[1]tamijeselvy@gmail.com,[3]elakkiya.soundar@gmail.com

Abstract: - The progress and the substantial procreation of web technologies have created an environment in which some crucial issues for digital media have become very easy. The phenomenon has led to an increasing need for developing some standard solutions to prevent these issues. One of the technical solutions is to provide law enforcement and copyright protection for digital media which can be achieved practically by Digital Watermarking. The proposed method contains following phases (i) Pre-processing of biometric image, (ii) Obtaining keys from the biometrics of the owner/user and Speeded-Up Robust Features (SURF) is used as the scale- and rotation-invariant detector for biometric images, (iii) Wavelet-Based Contourlet Transform (WBCT) is applied on the host image, (iv) Singular Value Decomposition (SVD) is enforced over the watermark image, (v) Embedding of the host image with the Watermark Image and (vi) Watermark Extraction and Attack Analysis. The implemented proposed system SURF provides execution time of 98% over SIFT. The comparative analysis confirms the efficiency and robustness of the proposed system.

Key-Words: - Digital Watermarking, Singular Value Decomposition (SVD), Speeded-Up Robust Features (SURF), Pre-processing, robustness.

1 Introduction

A Digital Watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of computer-aided information hiding in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermark may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Traditional Watermarks may be applied to visible media (like images or video), whereas in Digital Watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time[7]. Unlike metadata that is added to the carrier signal, a Digital Watermark does not change the size of the carrier signal.

1.1 Digital Watermarking Properties

Every watermarking system has some very important desirable properties. Some of these properties are often conflicting and forced to accept some trade-offs between these properties depending on the application of the watermarking system. The properties of Digital Watermarking are,

- Effectiveness.
- Fidelity of the images
- Payload size is an important property
- The false positive rate is also very important to watermarking systems
- Robustness is crucial for most watermarking systems

1.2 Embedding Domain

The Watermarking algorithms are classified based on the Embedding domain. To embed watermark information in host data, watermark embedding techniques apply minor modifications to the host data in a perceptually invisible manner, where the modifications are related to the watermark information[8]. The Watermark information [1] can be retrieved afterwards from the watermarked data by detecting the presence of these modifications. The two categories based on Embedding domain are: Spatial Domain and Transform Domain.Spatial Domain is method of manipulating or changing an image representing an object in space to enhance the image for a given application. Spatial Domain watermarking technologies change the intensity of original image or gray levels of its pixels. This kind

of watermarking is simple and has low computing complexity, because no frequency transform is needed. Transform Domain is a mathematical procedure that converts data from one domain to another domain. In the new Domain the data could be more easily handled, for lossy compression, de-noising, sharpening, etc. Data can be transformed back to its original domain. Transform domain approaches insert the watermark into the transform coefficients. Some of the examples are Fourier transform, Cosine transform, wavelet transform.

1.3 Feature Extraction

Feature Extraction is a special form of dimensionality reduction. When the input data to an algorithm is too large to be processed and it is suspected to be notoriously redundant then the input data will be transformed into a reduced representation set of features which is also named as features vector. Transforming the input data into the set of features is called feature extraction. If the features extracted are carefully chosen it is expected that the features set will extract the relevant information from the input data in order to perform the desired task using this reduced representation instead of the full size input. The Feature Extraction plays an import role in the image mining techniques and several other applications

1.3.1 Low Level Feature Extraction

Low level features are the basic features that are to be extracted automatically from an image without any shape information. Thresholding is a form of low-level feature extraction performed as a point operation. It mainly deals with the edge detection and it aims to produce a line drawing.

1.3.2 High Level Feature Extraction

High level feature extraction concerns finding shapes and objects in computer images. This feature extraction seeks the invariance properties so that the extraction result does not vary with specified conditions. This implies finding objects, regardless of their positions, orientation or size. That is, this technique should find shapes reliably and robustly independent of any parameter that can control the appearance of the shape.

1.3.3 Object Description

Objects are represented as a collection of pixels in an image. Thus, for purposes of recognition we need to describe the properties of groups of pixels. The description is often a set of numbers – the object's descriptors. Thus, objects can be compared and recognized by simply matching the descriptors of object in an image against the descriptors of known objects.

1.4 Biometrics

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[3].

A number of biometric characteristics have been in use for different applications. 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[5]. 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.

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. The iris of the eye has a unique pattern, from eye to eye and from person to person . 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.

1.4.1 Iris

The iris is the elastic, pigmented, connective tissue that controls the pupil. The iris is formed in early life in a process called morphogenesis[13]. 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.

An iris scan analyses 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 thus an iris perfectly authenticate a person when compared with other biometrics such as face, fingerprints, and voiceprints.

2 Related Works

ETH Zurich et al. K.U. Leuven et al. proposed a novel scale- and rotation-invariant detector and descriptor, coined SURF. SURF approximates or even outperforms previously proposed schemes 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 and by simplifying these methods to the essential. This leads to a combination of novel detection, description, and matching steps. The search for the discrete image point correspondences can be divided into three main steps. 1) The 'interest points 'are selected. 2) The neighbourhood of every interest point is represented by a feature vector. The descriptor vectors are matched between different images

A novel watermarking algorithm based on Singular Value Decomposition (SVD) is used by Ruizhen Liu et al and Tieniu Tan et al. The Method is compared with the Spread Spectrum Communication method proposed by Cox in order to put the performance investigation of the algorithm in proper context[1]. This is because of the rapid growth of the Internet has made copyright protection of digital contents a critical issue. A Digital Rights Management (DRM) system is aimed at protecting the high-value digital assets and controlling the distribution and utilization of those digital assets. Watermarking technologies are being regarded as a vital mean to proffer copyright protection of digital images. Digital watermarking hides, in digital images, the information necessary for ownership identity to offer copyright protection.

The algorithm is tested on a variety of images results obtained using the gray scale image and test robustness under six practical conditions: adding noise, low-pass filtering, JPEG compression, scaling, image cropping, and rotation. The drawback of the method is that it suffers by ambiguity attacks. Yiwei Wang, John F. Doherty et al and Robert E. Van Dyck et al proposed the features that a practical digital watermarking system for ownership verification is required. Besides perceptual invisibility and robustness, they claim that the private control of the watermark is also very important . Second, they present a novel wavelet-based watermarking algorithm. The wavelet transform also finds its way into the field of signal analysis. A wavelet is a wave-like oscillation with amplitude that starts out at zero, increases, and then decreases back to zero.

Compared with the traditional transforms, the Fourier transform for instance, the wavelet transform has an advantage of achieving both spatial and frequency localization. In digital signal and image processing, the discrete wavelet is closely related to filter banks. A filter bank is an array of band-pass filters that separates the input signal into multiple components, each one carrying a single frequency subband of the original signal.

Umut Uludag et al, Sharath Pankanti et al, Salil Prabhakar et al, Anil k. Jain et al proposed User authentication is based on possession of secret keys , which falls apart if the keys are not kept secret which works on traditional systems. Further, keys can be forgotten, lost, or stolen and, thus, cannot provide non repudiation. Current authentication systems based on physiological and behavioral characteristics of persons (known as biometrics), such as fingerprints, inherently provide solutions to many of these problems and may replace the authentication component of the traditional cryptosystems. This paper proposes a binding of a cryptographic key with the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication.

2.1 Motivation

The challenges involved in biometric key generation primarily due to drastic acquisition variations in the representation of a biometric identifier and the imperfect nature of biometric feature extraction and

matching algorithms[12]. Thus, keys are generated using the Error calculation method.

3 Proposed Scheme

The goal of the proposed system is to have a robust watermarking technique. The Biometric images are scanned using optical biometric scanner. The first step is to pre-process the gray scaled biometric image for contrast adjustment. The Second stage is the feature extraction from the biometric images. The feature extraction is done using the SURF. The goal of feature extraction is to have land mark points using object descriptors. The keys from the biometric image are generated and embedded on the host image. The third step is to apply WBCT on the host image and the host image is embedded with the watermark image. The watermarked image is obtained from the embedding of the watermark image and the host image which is followed by the extraction of the host image. Finally, the attack analysis is performed. A major advantage of using Wavelet Based Contourlet Transform is that 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. Figure 1 represents the overall process of the proposed system. Singular value decomposition is used because SVD is in fact a one-way decomposition algorithm and is optimal matrix decomposition in a least square sense; the new method performs well both in resolving rightful ownership and in resisting common attacks.

3.1 Image Enhancement (Pre-processing)

Image enhancement is one of the image preprocessing techniques. The aim of image enhancement is to improve the interpretability or perception of information in images for human viewers, or to provide `better' input for other automated image processing techniques. It consists of collection of techniques that seek to improve the visual appearance of an image or to convert the image to a form better suited for analysis by a human or machine. Contrast adjustment processes adjust the relative brightness and darkness of objects in the scene to improve their visibility. The contrast and tone of the image can be changed by mapping the gray levels in the image to new values through a gray-level transform. It is the image enhancement technique that is commonly used for scanned images. Contrast Adjustment process plays an important role in enhancing the quality and contrast of images. Different types of Contrast Adjustment techniques include local contrast adjustment, global contrast adjustment, partial contrast adjustment, bright and dark contrast adjustment.

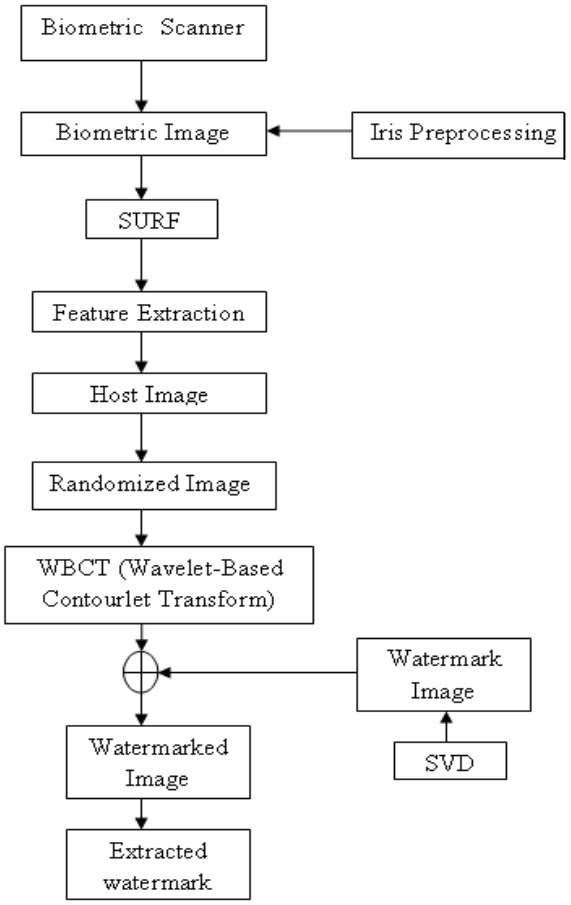

Figure 1 Overall Process of the Proposed System

3.3 Feature Extraction (SURF)

The Speeded-up Robust Features (SURF) technique has been developed for both the detection and description of local features[2]. The main advantages are repeatability, distinctiveness, and robustness with less computation time and SURF is also referred as 'Fast-Hessian' detector. The whole SURF technique is summarized into following steps.

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

$$H = \begin{bmatrix} L_{xx}(x,y,\sigma) & L_{xy}(x,y,\sigma) \\ L_{xy}(x,y,\sigma) & L_{yy}(x,y,\sigma) \end{bmatrix} \quad (1)$$

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

2 Interest Point Descriptors (SURF Descriptors): SURF descriptors are calculated in the square regions centered 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 (d_x) and vertical (d_y) directions are calculated. Therefore, the underlying descriptor of each square is described by the vector $\vec{v}$ as

$$\vec{v} = (\Sigma d_x, \Sigma d_y, \Sigma|d_x|, \Sigma|d_y|) \quad (2)$$

Due to the division into 4 × 4 sub regions, each feature point has 64 descriptors. Finally, the SURF descriptor is formed by normalizing the 64 descriptors to guarantee invariance to scale.

3.3.1 Feature Extraction Algorithm

1 Pre-processed Biometrics images is taken as Input
2 Apply SURF on the Pre-processed iris images using equation (1)
3 The robust matching point vectors ($\vec{}$v1 and $\vec{}$v2) along with position vectors (X1, Y1) and (X2, Y2) is obtained using equation (2)
4 The interest points are obtained

3.4 Embedding Process

3.4.1 Singular Value Decomposition (SVD)

Singular value decomposition (SVD), one of the most useful tools of linear algebra, is a factorization and approximation technique which effectively reduces any real or complex matrix into smaller and invertible matrices [11]. Mathematically, SVD of a rectangular matrix A is expressed as in equation 3

$$A = USV^T \quad (3)$$

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. On the other hand, U and V are unitary matrices. The columns of U are left singular vectors whereas the columns of V are right singular vectors of A. It is important to note that the singular values specify the luminance of the matrix whereas the corresponding pair of singular vectors specifies the geometry of the matrix.

3.4.2 Wavelet-Based Contourlet Transform (WBCT)

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) 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[6].

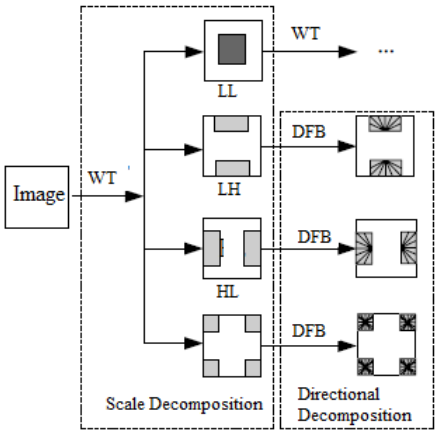

Figure 2 Decomposition of WBCT (First Level)

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. Figure 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.

By analyzing, we find that WBCT can capture image structure features more efficiently than Discrete Wavelet Transform (DWT) 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[10]. 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.

3.4.3 Embedding Algorithm

1 Perform L-level order decomposition using WBCT on 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
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

3.4.4 Watermark Extraction

The objective of watermark extraction is to obtain the estimate of the original watermark. The Watermark image is extracted from the watermarked image.

1 Perform L-level order decomposition using WBCT on image
2 Perform SVD on all the subbands of the randomized host image and the gray scale watermark
3 Extract the singular values of the watermark from each subband
4 Perform inverse SVD to construct the extracted watermarks from each subband

3.5 Attack Analysis

The transmission of the images over insecure communication channels introduces degradation in the images. Such degradation also affects the hidden information (watermarks) in the images. Therefore, the robustness of the proposed technique against degradation incurred by various intentional and unintentional attacks is studied. Generally, a good watermarking technique should be sufficiently robust against all these attacks[4]. To investigate the robustness, the watermarked image is verified and then attacked by; Median filtering the median filter is a nonlinear digital filtering technique, often used to remove noise. Such noise reduction is a typical pre-processing step to improve the results of later processing. Gaussian noise addition is properly defined as the noise with a Gaussian amplitude distribution. This says nothing of the correlation of the noise in time or of the spectral density of the noise. Salt and pepper noise addition is a form of noise typically seen on images. It represents itself as randomly occurring white and black pixels

4 Experimental Results

The performance of the proposed biometrics inspired watermarking framework is demonstrated using a MATLAB platform. A number of experiments are performed on different gray-scale images of size 256 × 256, namely Building, Lena and Mandrill. Also, three different gray-scale images of size 64×64, namely Logo1, Logo2 and Logo3 respectively, are used as the watermark images. Watermarks Logo1, Logo2 and Logo3 are embedded into Building, Lena and Mandrill images, respectively. The keys are obtained with the help of biometrics of the owner/user. Since biometrics are the unique and permanent characteristics of the individuals.

Therefore, biometrics inspired keys are unique and can only be generated by the owner/user. For the image watermark embedding, the 2-level of WBCT decomposition is used. Therefore, the watermark is embedded more than once in the host image. The watermarked image quality is measured using the peak signal to noise ratio (PSNR) which indicates the similarity between the host and the watermarked images[15]. To evaluate the similarity between the

original and extracted watermarks; the correlation coefficient (ρ) is used as the similarity measure between the original and extracted watermarks show in the Equation 4. Mathematically, ρ is defined as

$$\rho = \frac{\sum_{i=1}^{M_1}\sum_{i=1}^{N_1}(w(i)-m_w)(\overline{w}(i)-m_{\overline{w}})}{\sqrt{\sum_{i=1}^{M_1}\sum_{i=1}^{N_1}(w(i)-m_w)^2}\sqrt{\sum_{i=1}^{M_1}\sum_{i=1}^{N_1}(\overline{w}(i)-m_{\overline{w}})^2}} \quad (4)$$

where w, $\overline{w}$, m_w and $m_{\overline{w}}$ are the original, extracted, mean of original, and mean of extracted watermarks respectively. ρ is a number that lies in the range [−1, 1].

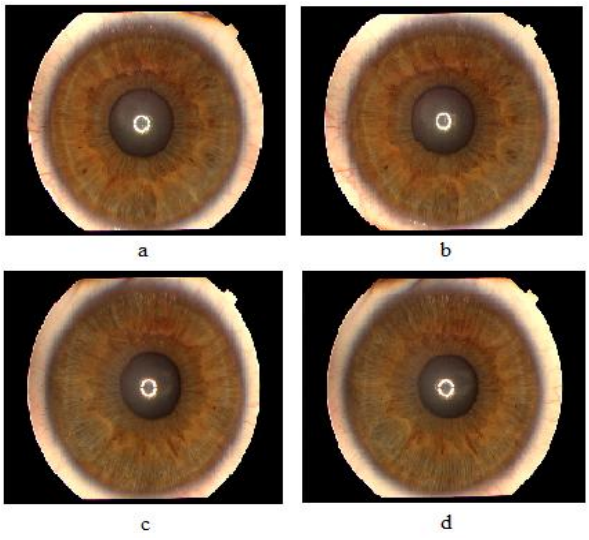

Figure 3 Iris images (a, b) Left Eye; (c, d) Right Eye

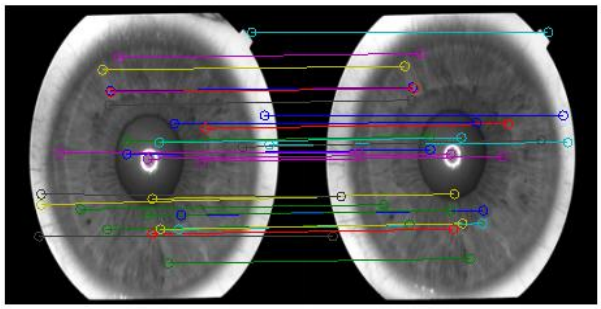

Figure 4 Interest Points Matching

The input Biometric Iris images of a person captured over a short period of a few seconds. Figure 3 depicts the iris images. The Figure 4 depicts Interest points matching. The input host image of size 256 × 256 is taken[9].

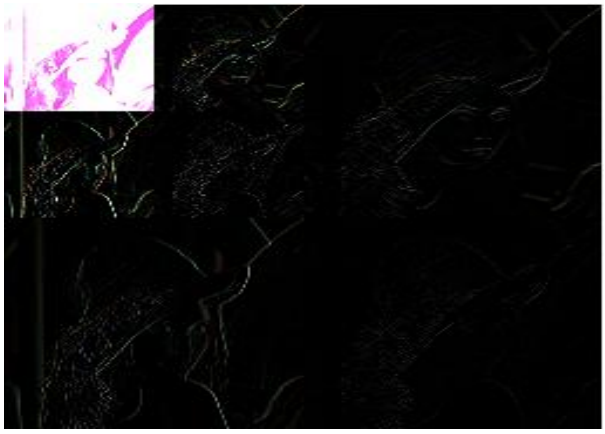

Figure 5 Applying Two Levels of WBCT Decomposition

Figure 6 (a, b, c) Original Host Images

Figure 6 depicts the original host images used for watermarking. Figure 5 depicts the two levels of WBCT Decomposition on the input host image. The Embedding of the watermark image with the host image to obtain the watermarked image is depicted in Figure 7. The most common manipulation in digital image processing is filtering. The attacked watermark image and extracted watermark, after applying 3 × 3 median filtering respectively, are shown in Figure 8 (a) and Figure 9 (a). Robustness against additive noise is estimated by degrading the watermark image by randomly adding Gaussian and salt and pepper noise. The attacked watermark images and extracted watermarks from the attacked images are shown in Figure 8 (b), Figure 9 (b) and Figure 8 (c), Figure 9 (c).

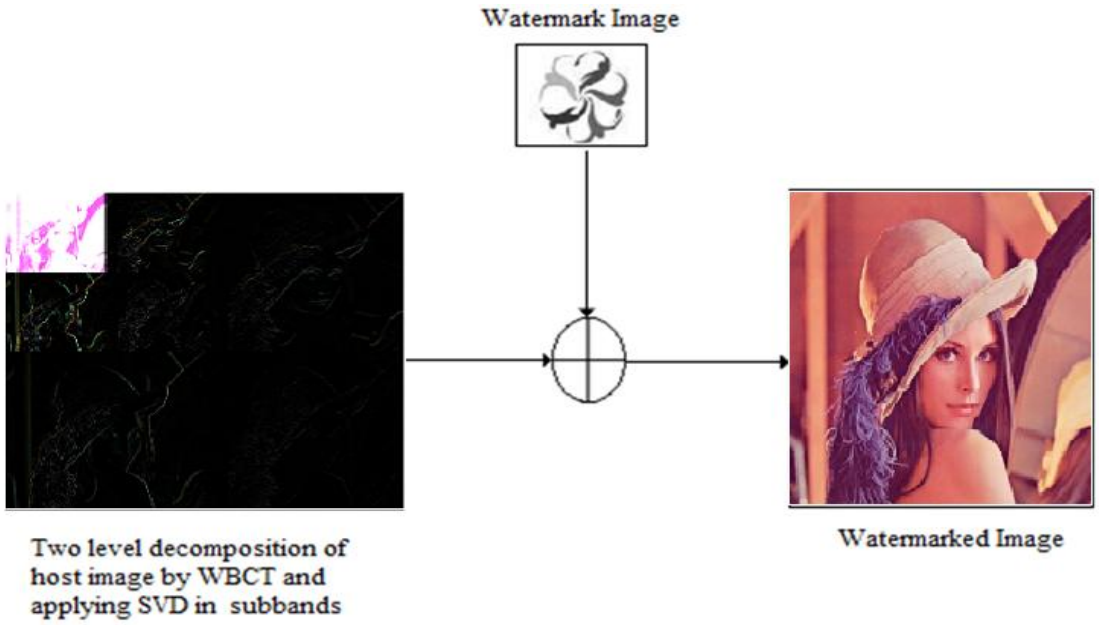

Figure 7 Watermark Embedding

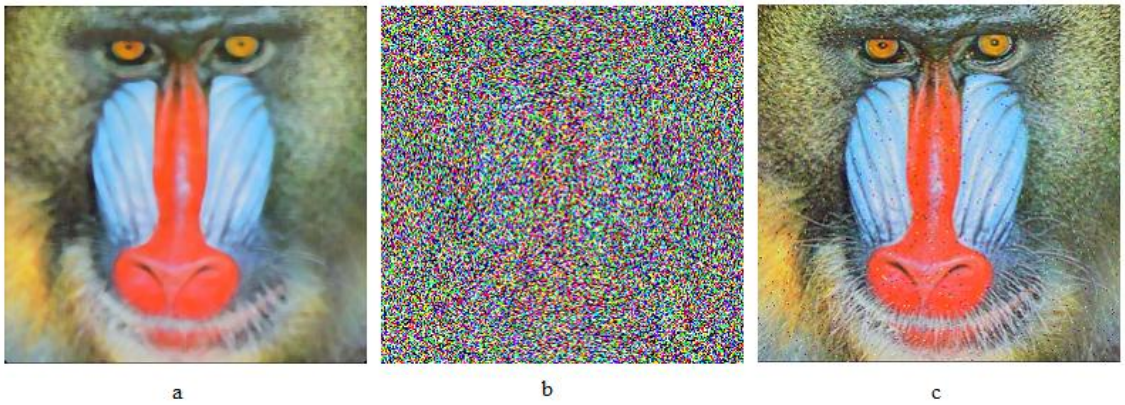

Figure 8 Watermarked Images after Attack (a) Median Filtering (b) Gaussian Noise Addition (c) Salt and Pepper Noise Addition

Figure 9 Extracted Watermark Images after (a) Median Filtering (b) Gaussian Noise Addition (c) Salt and Pepper Noise Addition

The Speeded-Up Robust Features (SURF) technique has been developed for both the detection and description of local features. The SIFT and SURF Techniques are applied on a dataset of 256 iris images. Table 1 represents the comparison rates of Sensitivity, Specificity and Execution Time.

Table 1 Comparison between SURF and SIFT

S.NO	Method	Sensitivity (%)	Specificity (%)	Accuracy (%)	Execution Time(in sec)
1	SIFT	71.1	93	72.7	1
2	SURF	98	72.7	89.4	0.8

The figures 10 describe the Execution Time Comparison of SURF and SIFT Techniques. The graph depicts that SURF provides less execution time than SIFT. In this paper, the SURF and SIFT techniques are evaluated in terms of Sensitivity (Se), Specificity (Sp) and Accuracy (Acc) as shown in the Equation 5, 6, 7. The comparison graph is shown in the Figure 11. Here TP-True Positive, FN-False Negative, TN-True Negative, FP- False Positive.

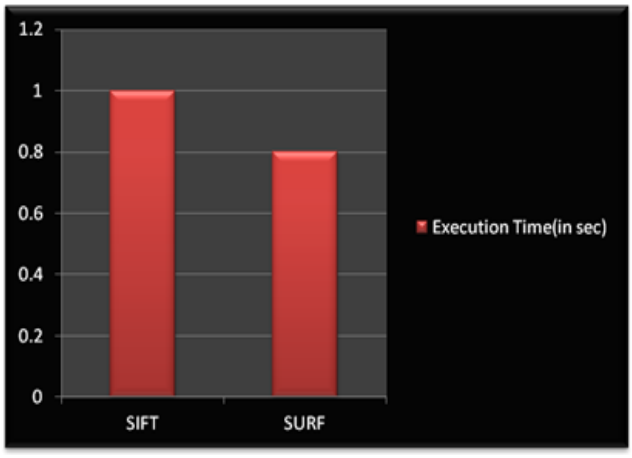

Figure 10 Execution Time Comparison of SURF and SIFT

The performance results [14] show the sensitivity (Se) of 98%. The correlation coefficients for all extracted watermarks are compared with other existing methods are depicted in Table 2 and Figure 12.

$$Se = TP/(TP+FN) \quad (5)$$

$$Sp = TP/(TN+FP) \quad (6)$$

$$Acc = TP+TN/(TP+FN+TN+FP) \quad (7)$$

Table 2 Comparison of Correlation Coefficients of Extracted Watermarks after Attack Analysis

Attacks	Multi-Band Wavelet	Contourlet	WBCT	WBCT+SVD
Median Filtering (3 × 3)	0.3557	0.4302	0.5545	0.8583
Salt and Pepper noise (0.01)	0.9193	0.9745	0.9807	0.9954
Gaussian Noise (10)	0.9087	0.9491	0.9657	0.9969

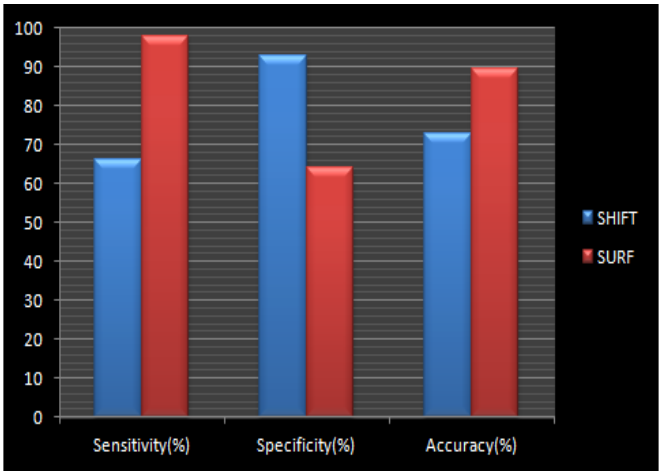

Figure 11 Comparison of Sensitivity, Specificity and Accuracy of SURF and SIFT

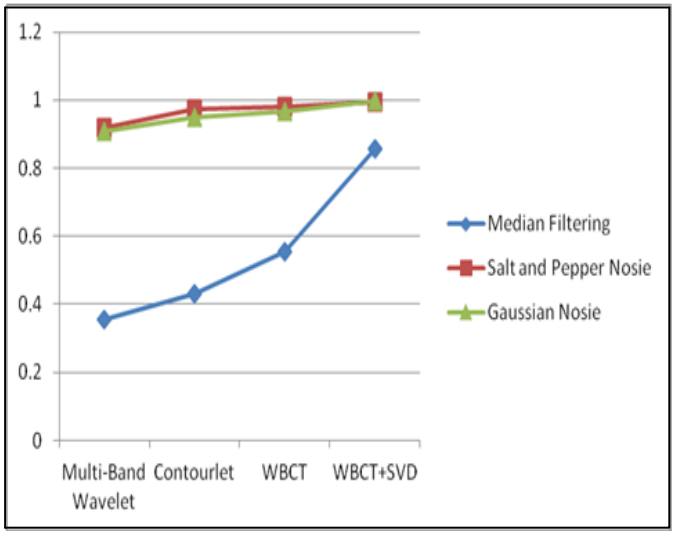

Figure 12 Correlation Coefficient Comparisons of Extracted Watermarks

5 Conclusion

The Biometrics trigged watermarking of images based on WBCT is proposed in which the key concept is introduced with biometric security. The original image has been improved by optical inspection. An Efficient method SURF is used for the feature extraction and interest points matching. The SURF performance is shown in the comparative

analysis which is efficient in both retrieval time and feature extraction. Two 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. The watermarked image is obtained by embedding the host image and the watermark image. The proposed technique meets the requirements of Digital Watermarking. As our experimental results have shown, the proposed algorithm achieves invisibility and robustness.

References:

[1] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science, Vol. 3, No. 9, 2001, pp. 740-746.

[2] H. Bay, T. Tuytelaars, L. Van Gool, "SURF: Speeded Up Robust Features", in:Proc. Computer Vision and Image Understanding,Vol.110, No.3, 2008, pp. 346-359.

[3] Gaurav Bhatnagar, Q.M Jonathan Wu, "Biometrics Inspired Watermarking Based on a Fractional Dual Tree Complex Wavelet Transform", Future Generation Computer Systems, Vol. 29, 2013, pp. 182-195.

[4] A.K. Jain, "A. Ross: A Tool for Information Security", IEEE transactions on Information Forensic and security, Vol.1, No. 2, 2006, pp. 125-143.

[5] A.k. Jain, R. Bolle, S. Pankanti, "Biometrics: Personal Identification in a Networked Society", Kluwer Academic Publishers, 1999.

[6] Jing Liu, Gang Liu, "A New Digital Watermarking Algorithm Based on WBCT", International Workshop on Information and Electronics Engineering (IWIEE), 2012, pp. 1559 – 1564.

[7] G.C. Langelaar, I. Setyawan, R.I. Lagendijik, "Watermarking Digital Image and Video Data", IEEE Signal Processing Magazine, Vol. 17, No. 5, 2000, pp. 20-46.

[8] Z.M. Lu, D.J. Xu and S.H Sun, "Multipurpose Image Watermarking Algorithm Based on Multistage Vector Quantization", IEEE Transactions on Image Processing, Vol. 14, No. 5, 2005, pp. 3271-84.

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

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

[11] Yavuz E, Telatar Z,"Improved SVD–DWT Based Digital Image Watermarking Against Watermark Ambiguity" in: Proc. ACM Symposium on Applied Computing, pp. 1051 – 1055, 2007.

[12] Chang-Doo Lee, Bong-Jun Choi, Kyoo-Seok Park, "Design and Evaluation of a block Encryption algorithm using dynamic-key mechanism", Future Gener. Comput. Syst., Vol. 20, No. 2, 2004, 327-338.

[13] Fabian Monrose, Aviel D. Rubin, "Keystroke dynamics as a biometric for authentication", Future Gener. Comput. Syst., Vol. 16, No.4, 2000, pp.351-359.

[14] A. Tefas, A. Nikolaidis, V. Solachidis, S. Tsekeridou, I. Pitas, "Performance analysis of correalation-based watermarking schemes employ markov chatic sequences", IEEE trans. Signal Process, Vol.51,2003, pp. 1979-1994.

[15] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, "Image quality assessment: from error visibility to structural similarity", IEEE trans. Image Process", Vol.13, 2004, pp. 600-612.