Offline Handwritten Signature based Blind Biometric Watermarking and Authentication Technique using Biorthogonal Wavelet Transform

Vandana S.Inamdar
College of Engineering
Pune, India

Priti. P. Rege
College of Engineering
Pune, India

Meenakshi S Arya
College of Engineering
Pune, India

ABSTRACT
A method for establishing the identity of an individual is essential in all transactions whether they are commercial or personal. The ability to establish identity with certainty can prevent fraud or forgery. In the midst of an electronic revolution, this remains a major concern in ecommerce, telecommunications, healthcare, and security. In this paper, we present a novel method for biometric image watermarking using the biorthogonal wavelet transform and authentication of the recovered signature from the image data. In proposed approach the offline signature, which is a biometric characteristics of owner is embedded in second level detailed coefficients of discrete wavelet transform of cover image. The novelty of the proposed scheme is that, it also goes a step further wherein it extracts the features of recovered signatures and does the template matching with features of signature data base.

GENERAL TERMS
Information hiding, Digital Right Managements

KEYWORDS
Biometric watermarking, Biorthogonal wavelets, discrete wavelet transform, template matching, Hough transform, Principal component analysis

1. INTRODUCTION

Watermarking is not a new phenomenon. For nearly one thousand years, watermarks on paper have been used to identify a particular brand and to discourage counterfeiting. In the modern era, proving authenticity is becoming increasingly important as more of the world's information is stored as readily transferable bits. Digital watermarking is a process whereby arbitrary information is encoded into an image in such a way that the additional payload is imperceptible to the image observer. Copyright abuse is the motivating factor in developing new encryption technologies.

Watermarks have a number of applications:

- Establishing ownership by embedding identifying data.
- Tracking the movement of authorized copies by embedding a unique serial number in each copy.
- Attaching meta-data that pertains to the image such as a time, date, and location stamp.

Digital watermarking is the process of possibly irreversibly embedding information into a digital signal. Typically, the watermark is text or a logo or pseudorandom sequence which identifies the owner of the media. The digital watermarking is intended to complement cryptographic process. Access control or authenticity verification has been addressed by digital watermarking as well as by biometric authentication [2,3].

Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, signatures, facial patterns and hand measurements for authentication purposes. Biometric watermarking is a special case of digital watermarking where the content of watermark or the host data (or both) are biometric entities. This imparts an additional layer of authentication to the underlying system [3].
Although lot of efforts have been made in the field of watermarking, yet most of them embed a character string or logo as a copyright information. There are some limitations to these watermarks:

1) Usually they are less meaningful and intuitive for easily identifying. 2) Low correlative to copyright holder. The information of the holder is not inherent and may change with time. Using these as a watermark may lead to imitation, tamper and repudiation. Traditional watermarking method does not convincingly validate the claimed identification of the person as the host might be fraudulently watermarked with a particular string pattern or logo by impersonators [4].

Recently biometrics is adaptively merged into watermarking technology to enhance the credibility of the conventional watermarking technique [20]. By embedding biometrics in the host, it formulates a reliable individual identification as biometrics possesses exclusive characteristics that can be hardly counterfeited. Hence, the conflicts related to the intellectual property rights protection can be potentially discouraged [4].
Watermarking algorithms fall into two categories.

- Spatial domain: Spatial-domain techniques work with the pixel values directly. Generally, spatial domain watermarking is easy to implement from a computational point of view, but too fragile to resist numerous attacks.
- Transform domain: Some of the transform based watermarking techniques used Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet transform, Singular Value Decomposition (SVD). Transform-domain techniques employ various transforms, either local or global. In order to have more promising techniques, researches were directed towards watermarking

in the transform domain, where the watermark is not added to the image intensities, but to the values of its transform coefficients. Then to get the watermarked image, one should perform the inverse transform.

Wavelet based transform gained popularity recently because of its multi resolution property. Wavelets can be orthogonal or biorthogonal. Most of the wavelets used in watermarking were orthogonal wavelet. The biorthogonal wavelet transform is an invertible transform. It has some favourable properties over the orthogonal wavelet transform, mainly, the property of perfect reconstruction and smoothness (vanishing points) [17,18] which is a desirable feature for information hiding.

2. REPRESENTATIVE WORK

A.K.Jain and his research team primarily proposed digital watermarking. Jain and Umut [5] proposed multimedia content protection framework that is based on biometric data of the users. M.Vasta[6] presented a novel biometric watermarking algorithm for improving the recognition accuracy and protecting the face and fingerprint images from tampering. He made use of multi resolution DWT to embed face image in a finger print image. V-Support Vector Machine is exploited to enhance the quality of the extracted face image. Low etc al. [4] proposed to adaptively fuse Least Significant Bit (LSB) and Discrete Wavelet Transform (DWT)-based approaches into a unison framework, which to be known as LSBDWT scheme. The performance of LSB-DWT scheme is validated against simulated frequency and geometric attacks.

Namboodiri, Jain [9] presented an LSB-based biometric watermarking scheme where a digital document was spatially watermarked with online handwritten signature.

Kundur and Hatzinakos [10] were the pioneers in suggesting a watermarking model using biorthogonal wavelets based on embedding a watermark in detail wavelet coefficients of the host image. The model proposed was robust against numerous signal distortions, however it was non-blind. Yang [11] in his paper simulates under a spread-spectrum watermarking framework where a Gaussian distributed watermark is injected into the largest wavelet coefficients to find the best biorthogonal wavelet filter for multi resolution image watermarking. The performance of seven integer biorthogonal wavelet bases is evaluated and it is observed that the 917-F wavelet provides a substantial edge' when all detail sub bands are eligible for watermarking.

The effect of using even-length and odd length biorthogonal wavelets for watermarking have been discussed in [12] and [13] respectively. Both these techniques were robust against several attacks, but were presented for the sake of detecting the presence of a watermark not for extracting it.

The motivation of the present work arises from developing a watermarking algorithm which embeds offline signature as a biometric data. Signature is a socially accepted trait for authentication purpose. In this paper, a scheme is proposed which embeds offline signature of owner as a watermark in second level detailed coefficients of discrete wavelet transform of cover object. The cover image is decomposed using biorthogonal wavelet transform. We have borrowed the idea from [28] with significant modifications and improvements in implementation. The work also goes a step further wherein it extracts the features of recovered signatures and does the template matching with features of signature data base.

The paper is organized as follows: A brief review of biorthogonal wavelet transform is provided in section III. Section IV provides the outline of the method employed and the results are provided in the next section. The last section summarizes the work and future scope.

3.BIORTHOGONAL WAVELET TRANSFORM

Decomposition of a signal in terms of a wavelet basis is termed as wavelet transform. A biorthogonal wavelet is a wavelet where the associated wavelet transform is invertible but not necessarily orthogonal. Designing biorthogonal wavelets allows more degrees of freedoms than orthogonal wavelets. One additional degree of freedom is the possibility to construct symmetric wavelet functions.

The property of perfect reconstruction and symmetric wavelet functions exist in biorthogonal wavelets because they have two sets of low pass filters (for reconstruction), and high pass filters (for decomposition)[28]. One set is the dual of the other. On the contrary, there is only one set in orthogonal wavelets. In biorthogonal wavelets, the decomposition and reconstruction filters are obtained from two distinct scaling functions associated with two multiresolution analyses in duality. Another advantageous property of biorthogonal over orthogonal wavelets is that they have higher embedding capacity if they are used to decompose the image into different channels. All mentioned properties make biorthogonal wavelets promising in the watermarking domain [17].

In the biorthogonal case, there are two scaling functions, which may generate different multiresolution analyses, and accordingly two different wavelet functions. The scaling sequences must satisfy the following biorthogonality condition. For orthogonal wavelets, the scaling function φ and mother wavelet ψ are given by the recursion relations defined by following equations.

Their scaled translates are denoted by

$$\varphi(x) = \sqrt{2}\ \sum_k h_k\ \varphi(2x-k) \tag{1}$$

$$\Psi(x) = \sqrt{2}\ \sum_k g_k\ \varphi(2x-k) \tag{2}$$

In the case of biorthogonal wavelet, rather than a single scaling function there is a dual scaling function and mother wavelet.

$$\varphi_k^n(x) = 2^{\frac{n}{2}}\varphi(2^n x-k) \tag{3}$$

$$\Psi_k^n(x) = 2^{\frac{n}{2}}\Psi(2^n x-k) \tag{4}$$

When the image is decomposed using normal DWT, if the embedding rate becomes high, data imperceptibility becomes lower and robustness performance is also decreased. Interference may occur as different sets of spreading codes (used for different watermark messages) are added with the decomposed cover image signal using single scaling function. Moreover, the decomposition does not always yield low correlation with the code patterns and high robustness may not be achieved. This problem can be solved to a great extent, if image signal is decomposed properly in different directions, so that low correlation value with the code patterns can be satisfied. When the correlation between the code pattern and the image decomposition coefficients obtained using several DWT and biorthogonal DWT is calculated, it is observed that the biorthogonal DWT provides lower correlation with the code patterns. This is possibly due to the complementary information

present in two wavelet systems that offers better directional selectivity compared to classical wavelet transform [17].

4. PROPOSED SCHEME

Signature is a behavioral biometric that is developed over the course of a person's lifetime. Many people are very accustomed to the process of signing their name and having it matched for authentication. This process has been in practice for centuries and is well accepted among the general public to protect confidential information. The use of signature is prevalent in the legal, banking, and commercial domains. Each person has a unique handwritten signature. The way a person signs their name or writes a letter can be used to prove a person's identity. These important traits of the handwritten signature is a motivation in embedding it as a watermark in an image.

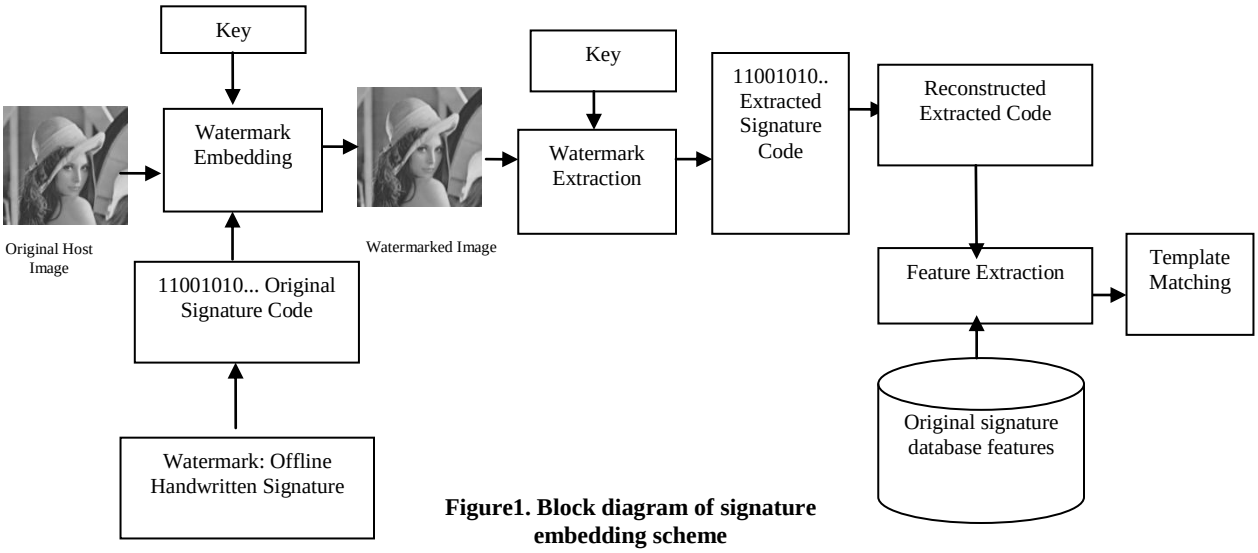


Figure1. Block diagram of signature embedding scheme

This section describes the proposed watermarking method which performs a 2-level DWT on the host image using biorthogonal wavelet. An offline hand written signature from the user is preprocessed and converted into a binary bit string before embedding.

The proposed scheme is carried out in four phases, watermark preparation from signature image, the signature embedding phase, the signature recovery phase and feature extraction and template matching phase. Figure 1 shows the block diagram of proposed watermarking scheme.

4.1 Watermark preparation

A binary bit string of the signature image selected by the user for embedding is generated. The signature image is converted to a 1-D binary string through vector division with values ranging between 0 and 1 only. This is essential as watermarking will be done based on these two values only.

4.2 Watermark Embedding

The following steps are followed for the watermark embedding.

1. A 2-level 2D DWT decomposition using biorthogonal filters is performed on the input image to generate the output image X. The host image is first subjected to the first level DWT to obtain one approximate (LL1) and three detailed (HL1, LH1 and HH1) sub-bands. The DWT approximate band represents the coarse region with significant low frequency coefficients. To obtain the next coarser domain, LL1 is further sub-sampled. In contrast, the detailed coefficients denote the finest domain that is occupied by middle and high frequency coefficients. Therefore, additional sub-sampling of the detailed coefficients is prohibited. In the proposed method, the sub-image was subdivided into 2-level DWT decomposition as shown in Figure 2. The detailed coefficients (HL2, LH2 and HH2) hence obtained are used for the process of embedding watermark. A secret key is used to generate pseudorandom sequences to ensure confidentiality and these sequences are used as a watermark depending upon the signature bit.
2. Generate number of PN sequences having mean 0 and variance 1 and the same dimension and structure of the image X using a secret key. Number of PN sequence generated will be equal to number of bands used for embedding. For embedding in HL2 band only, one PN sequence is generated, for embedding in HL2 and LH2 bands, two PN sequences are generated while for embedding in all the three bands, three PN sequences are generated.
3. To effectively differentiate between watermark bit '0' and '1', whenever the signature bit is zero, these pseudo-random sequences, are inserted into the horizontal detailed wavelet coefficients (or into HL2 and LH2 or in to all three bands) whenever the watermark bit is zero else the wavelet coefficients are left untouched. A large α (embedding factor) might be used to optimize the watermark robustness at the expense of host fidelity. Hence, a fine trade-off should be experimentally determined to strike a proper balance between the watermark imperceptibility and the watermark robustness. In proposed scheme, value of α is set in the range of 0.5 to 0.7 to obtain a balanced mix of robustness and fidelity.

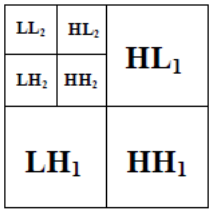


Figure 2. Second level decomposition LL represents the approximation sub-band, HL represents the horizontal sub-band, LH represents the vertical, and HH represents diagonal sub-band.

4. The pseudo-random sequence thus generated during each pass is used to update the horizontal detailed coefficients using Cox's [27] algorithm only when the watermark bit is 0, in case it is one , the coefficients are unaltered.

$$HL2=HL2+\alpha PN\_sequence\_1 \quad (5)$$

If watermark is embedded in both bands then

$$LH2=LH2+\alpha PN\_sequence\_2 \quad (6)$$

If it is embedded in all three bands then

$$HH2=HH2+\alpha PN\_sequence\_3 \quad (7)$$

5. Finally, the watermarked image *I′* is reconstructed using the inverse DWT

4.3 Watermark extraction

1. The key shared between the embedder and the authenticator is used to re-generate pseudo-random sequences. Number of sequences generated equal to number of bands being used for embedding .
2. Another sequence 'W' consisting of only 1's equal to the length of the original watermark is also generated which is further used to generate/reconstruct the watermark.
3. The 2-level Biorthogonal DWT of the watermarked image is performed to obtain the detailed coefficient. Being a blind watermarking technique, for watermark recovery, original cover image is not required in this approach.
4. For each PN sequence generated, the correlation between this sequence and the horizontal detailed coefficient is calculated and stored in a 1-D sequence equal to the length of the watermark.

$$correlation\_HL2\ (i)=corr2(HL2, PN\_sequence\_1) \quad (8)$$

If watermark is embedded in both bands then

$$correlation\_LH2\ (i)=corr2(LH2, PN\_sequence\_2) \quad (9)$$

If watermark is embedded in all three bands then

$$correlation\_HH2\ (i)=corr2(HH2, PN\_sequence\_3) \quad (10)$$

5. In case the watermark is embedded in two or three bands, then finally the average of correlation sequences is found out. The standard deviation of this correlation sequence thus formed is calculated and then compared to each value of the correlation sequence to decide the watermark bit.
6. The decision for updating the watermark bit is taken depending upon the value obtained in the step above.

If correlation[i] > std(x)
set corresponding bit in 'W' to Zero
else
that particular bit is left unaltered.

7. The original signature image is reconstructed by reshaping the sequence 'W' thus obtained from step 6.

4.4. Template Matching Based Authentication

The signature pattern thus reconstructed is authenticated using template matching. The features of the entire signature database are extracted using the steps mentioned in the latter part of this section. The same steps are used to extract the features of the recovered signature and then using the euclidean distance as a measure, the features of recovered signature are matched with the features of signature from the database.

4.4.1 Feature Vector Generation

The flowchart in Figure 3 shows the process of feature vector generation. It consists of mainly two steps, preprocessing and feature extraction.

Preprocessing is done to the signature images from data base so as to prepare it for the process of feature extraction and to ensure that all the signature images are of the same dimensions so that it is easier and convenient to extract the features.

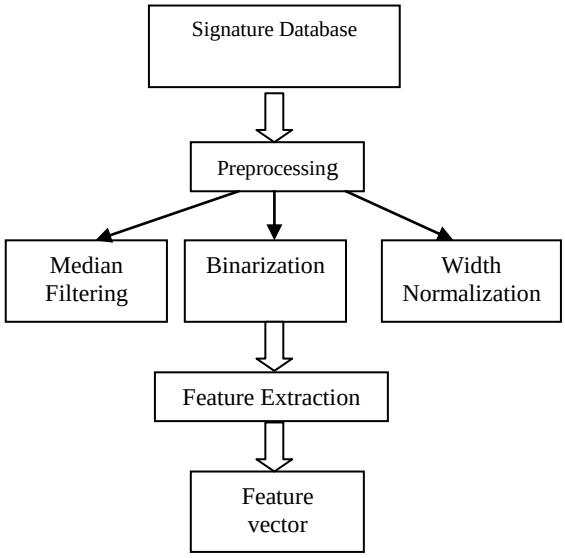


Figure 3 Feature Vector Generation Flowchart

Preprocessing is carried out in the following three steps.

- Median Filtering: Generally, digital image might contain speckles, smears, scratches or other forms of unwanted noise that might thwart feature extraction. Thus, median filtering is used to eliminate the existing noises.
- Binarization: The process by which the image is converted into black and white is called binarization. For a signature image X having dimensions m and n, the following equation is used to find out the level of Binarization [21].

$$P = (\sum\sum X\ (i,j))/(m*n)) \quad (11)$$

Where P = Average value of all pixels in the image.

The pixels are converted to black and white using the following criteria.

If $X(i, j) > P$ then $X(i, j) = 1$
Else if $X(i,j) < P$ then $X(i,j) = 0$

- Width normalization: All the signature images have been reduced to a standard size of 100 x 60 so as to ease the process of feature extraction.

4.4.2 Feature Extraction

Figure 4 depicts the process of feature extraction from the normalized signature images using Hough Transform and Principal component analysis.

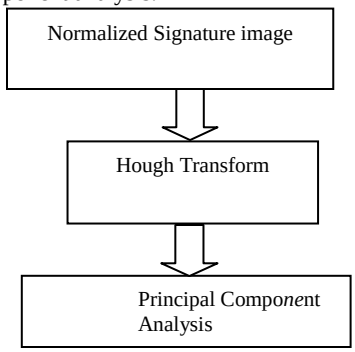


Figure 4 Signature Feature Extraction

4.4.2.1 Hough Transform

Hough transform is proposed for signature recognition by using Hough space parameter as a global feature [30]. The purpose of Hough transform is to find imperfect instances of objects within a certain class of shapes by a voting procedure.

This voting procedure is carried out in a parameter space, from which object candidates are obtained as local maxima in a so-called accumulator space that is explicitly constructed by the algorithm for computing the Hough transform [16]. This technique can be used to isolate features of a particular shape within an image. Because it requires that the desired features be specified in some parametric form, the classical Hough transform is most commonly used for the detection of regular curves such as lines, circles, ellipses, etc. A generalized Hough transform can be employed in applications where a simple analytic description of a feature(s) is not possible. The main advantage of the Hough transform technique is that it is tolerant of gaps in feature boundary descriptions and is relatively unaffected by image noise.

4.4.2.2 Principal Component Analysis

Dimensionality reduction of a feature set is a common preprocessing step used for pattern recognition and classification applications [29]. Principal Component Analysis (PCA) is one of the popular methods used, and can be shown to be optimal using different optimality criteria. PCA involves a mathematical procedure that transforms a number of possibly correlated variables into a smaller number of uncorrelated variables called principal components. It takes the cloud of data points and rotates it in such a way that maximum variability is visible.

4.4.3 Template matching

Initially all the above mentioned steps are applied on the entire signature database to generate a feature vector comprising the feature vectors corresponding to each signature image. Then after the watermarking has been done and the signature image extracted from the watermarked image, these steps are applied to the recovered signature image to extract it's features. The euclidean distance between the feature vector of the recovered signature and the feature vectors of all the signatures in the database is calculated according to the Euclidean distance formula,

$$\text{dist}((x, y), (a, b)) = \sqrt{(x - a)^2 + (y - b)^2} \qquad (12)$$

The signature image from the database having the minimum euclidean distance with the recovered watermark is chosen to verify and authenticate the signature watermark.

5. EXPERIMENTAL OUTCOMES

5.1 Experimental Setup

This paper focuses on invisible watermark data. Watermark data size is variable depending upon the size of the signature image however the general range is between 60×30 to 120×120.

Apart from the perceptual quality of the watermarked image and recovered watermark, the quantitative metrics used to evaluate the quality of watermarked image are PSNR and SNR, while that of recovered signature is Structural Similarity Index Measure (SSIM) [26].

Standard images used for watermarking are leena, baboon, pepper, cameraman etc, while fourteen different signatures are taken as a watermark. Figure 5 indicates some of the samples of cover images and signatures used in the experiments.

Figure 5 Sample images used for experiments

Figure 6 shows the original and watermarked image and also original and recovered signature and it's template matching.

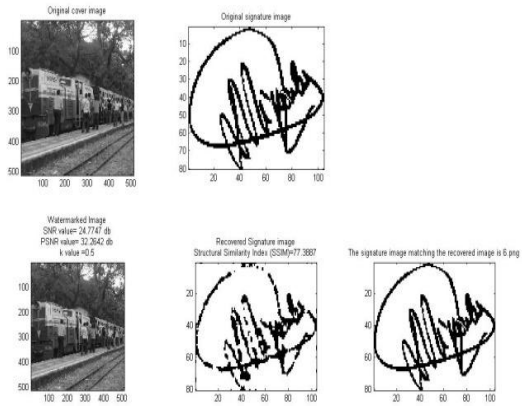


Figure 6 Top – original image and signature watermark Down- watermarked image with embedding strength 0.5, PSNR 32.26db, recovered signature with SSIM 77.38, template matched signature (rightmost), when watermark is embedded in all 3 bands

5.2 The Decomposition Level Effect

In order to embed the watermark into the host image, one should perform DWT to the host image and obtain the required coefficients for embedding. The coefficients needed for embedding can be obtained from one level (scale) of DWT or more. In this experimentation, tests are performed that include one-level DWT, and other tests that include two-level DWT.

To show the effect of the level, a gain factor of 0.5 was selected in embedding and the tests were performed on different host image. The effect of the decomposition level is shown in Table I. The table shows the results of two tests, the first test embeds in the horizontal detail sub-band of the first level decomposition, and the second embeds in the horizontal detail (second level) that is obtained from the first level decomposition.

It has been observed that embedding in 1st level results in a failure of template matching as the recovered watermark is not very clear whereas in case of 2nd level, the recovered watermark is absolutely matched with the correct template. The same is depicted in Figure 7.

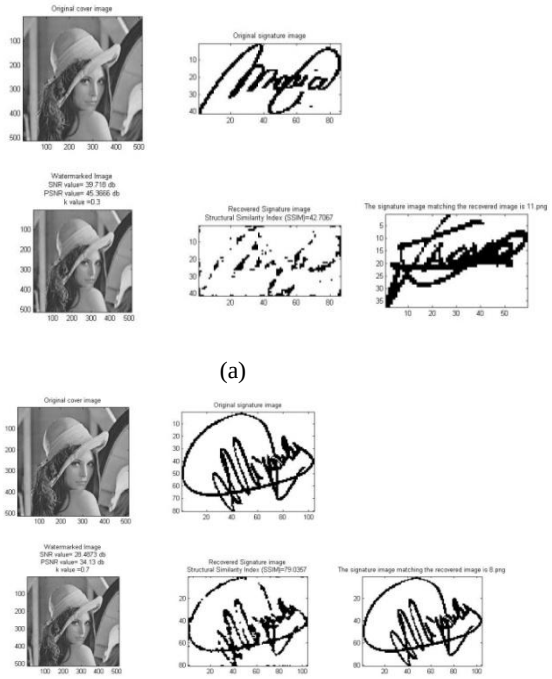
TABLE I Effect of decomposition level

Level	signature no.	PSNR(db)	SNR(db)	SSIM
2	3.png	40.92	35.28	90.03
1	3.png	34.8	39.15	70.55

5.3 The Gain Factor Effect

In the embedding process, the PN sequences are multiplied by a gain factor, and then embedded in the host image coefficients. Therefore, changing the value of the gain factor has an obvious effect on both, the watermarked image, and the watermark extracted from it.

Table II shows the effect of changing the gain factor on both the Peak Signal-To-Noise Ratio (PSNR) of the watermarked image, and the structural similarity index (SSIM) between the original and extracted watermark.



(a)

(b)

Figure 7 Watermarks extracted from the watermarked image of Lena from (a) 1st level DWT- Template matching not done. (b) 2nd level DWT, perfect template matching

TABLE II: The Effect of Gain Factor for embedding in various coefficients

Embedding band	K value			
Horizontal	**0.3**	**0.5**	**0.7**	**1**
PSNR	45.36	40.92	38	35.90
SNR	39.7	35.2	32.3	29.2
SSIM	42.7	70.5	81.9	86.2
Horizontal And Vertical				
PSNR	42.1	37.77	34.85	26.11
SNR	36.56	32.12	29.2	31.75
SSIM	59.52	80.88	84.71	88.44
Horizontal, vertical and diagonal				
PSNR	40.46	36.3	33.1	24.37
SNR	34.82	30.38	27.46	30.01
SSIM	78.82	86.57	89.06	89.63

5.4 The Sub- Band Effect

Initially the horizontal detail sub-band is chosen for embedding since embedding in the approximation sub-band produces perceptible artifacts in the watermarked image, then we graduate to embedding in horizontal and vertical band and finally into all the three detailed sub- bands. The set of tests presented examines different sub-bands for embedding. Figure 8 shows

watermarks extracted from embedding in three different ways while Table III shows the effect on the quality metrics.

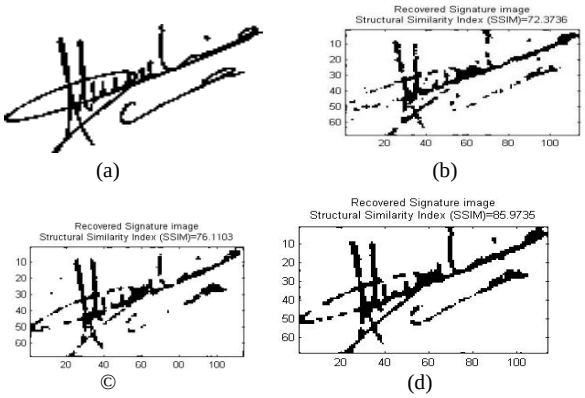


Figure 8 The effect of the sub-band on quality of extracted watermark (a) Original signature (b) Horizontal, SSIM=72.23 © Horizontal and vertical sub-band,SSIM =76.11 (d) Horizontal vertical and diagonal sub band, SSIM=85.97

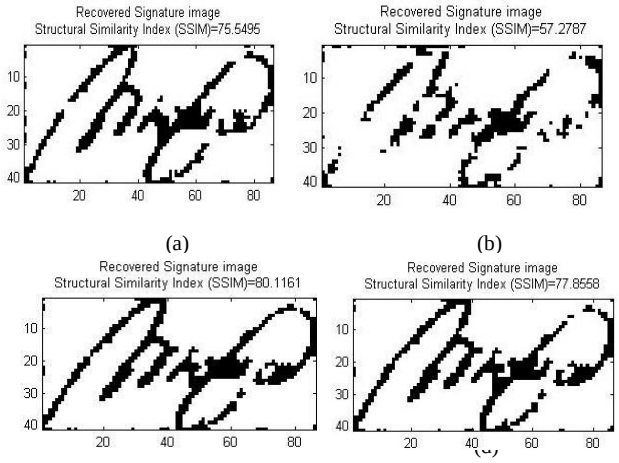
TABLE III The Effect of Decomposition Level on HL2, LH2, HH2 Sub-Bands

Sub band	PSNR(db)	SNR(db)	SSIM
Horizontal	38	32.36	81.9
Horizontal and Vertical	34.85	29.2	84.71
Horizontal, Vertical and Diagonal	33.1	27.46	89.06

5.5 Robustness against attacks:

Watermarking scheme discussed here is tested against different attacks for robustness for all three methods. The results are shown Figure 9 and are tabulated in Table IV.

The proposed scheme shows robustness against all attacks except rotation when watermark is embedded in all three bands. However for lower values gain factor the scheme does not survive weiner and median filtering attacks when watermark is embedded only in horizontal details.



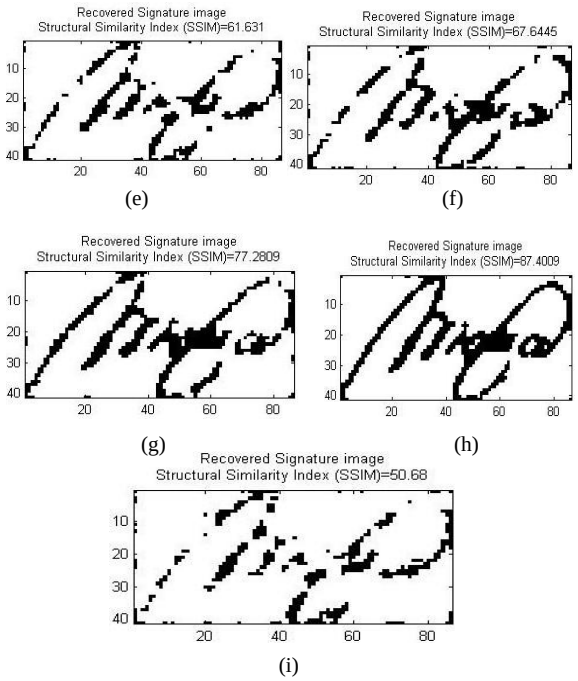


Figure 9: Extracted watermarks against different attacks(a) cropping (b) Gaussian (c) Histogram Equalization (d) JPEG compression (e) 3×3 median filter (f) 5% salt and pepper noise (g) Scaling (h) Sharpening (i) 3×3 weiner filter

TABLE IV Effects of attacks on recovery and template matching when watermark is embedded in different bands

Attack /Transform	Options	Horizontal coefficients only	Horizontal and vertical coefficient	Horizontal, vertical and diagonal coefficient
Cropping	% of original image	YES	YES	YES
Histogram Equalization		YES	YES	YES
Median Filtering	Filter size 3 × 3	NO	YES	YES
Salt n pepper	Filter size 3 × 3	YES	YES	YES
Sharpening	Filter size 3 × 3	YES	YES	YES
Scaling	Downscaling by 0.5 and up scaling by 0,5	YES	YES	YES
Weiner Filtering	Noise density: 0.02 to 0.05	NO	NO	YES
Gaussian noise	Gaussian white noise of mean 0 and variance 0.01	YES	YES	YES
JPEG Compression	Quality: 10, 30, , 50, 75, 90	YES	YES	YES

Though the idea is borrowed from [28], there are significant differences and performance improvements of proposed

implementation compared with Hajjara [28]. It is tabulated in Table V. In the implemented work discussed here, second level decomposition is obtained from approximation band, while that in [28] it is obtained from horizontal details. In the presented scheme three PN sequence are embedded at a time, PSNR of covered image is pretty high compared to Hajjra [28] scheme.

TABLE V
Comparison of Presented scheme with Hajjara scheme[28]

	Presented scheme	**Hajjara scheme [28]**
Second level decomposition	Approximation details	Horizontal details
PSNR range	30 to 38 db	3 to 5 db
Number of PN sequences	Three PN sequences are embedded at a time in all detail bands	Only one PN sequence is embedded in either of bands
Watermark	Signature which is more related for authentication	Logo
Authentication through template matching	Features of recovered signatures are extracted and matched	No such scope

6 DISCUSSION OF RESULTS AND SUMMARY

The technique employed has many factors that may affect the resulting watermarked image and the extracted watermark and its template matching with the signature database.

Table 1 show that when watermark is embedded in the second level of DWT, PSNR, SNR and SSIM were greater than when watermark is embedded in first level of DWT. When watermark is embedded in first level decomposition, as coefficients are significant image gets more distorted and SNR and PSNR values are less compared to when embedded in second level. The level of decomposition not only affects the quality of the watermarked image, but also affects the extracted watermark. SSIM factor is more when embedded in second level.

The gain factor has an important influence on both the marked image and the extracted watermark. Table II shows that as the gain factor increases, the PSNR decreases. This is because the payload is multiplied to the gain factor before embedding, cover image is more distorted. On the other hand, increasing the gain factor increases the robustness of the method, meaning that the correlation between the extracted and the original watermark is almost near or equals to 1. Trade off has to be achieved among these two factors.

Table III shows the improvement in quality metrics SSIM, when signature is embedded only in horizontal band and gradually it is embedded in both and finally in all three bands. When recovering the signature from multiple bands, average of correlation sequences is taken for decision. It gives drastic improvement in performance parameters and also show strong robustness against different attacks.

The technique was tested on several signature images. It is observed that the larger the size of signature image, the more distorted the marked image, and the more time it takes to embed the watermark. This is due to the fact that larger PN sequences were be added to the image equal to the size of the watermark. Therefore, the technique works better with watermarks that include fewer black areas since we embed only the foreground of the watermark.

The approach is robust against several attacks, except for the geometric attacks like rotation. The robustness of the watermarking methods has been quantitatively measured by comparing the extracted watermark with the original watermark. The threshold value for SSIM is 45, which gives better perceptual quality of recovered signature as well as template matching.

7 CONCLUSION

The study proposes a novel biometric watermarking and authentication technique using an amalgamation of Biorthogonal wavelets and template matching. The technique combines the field of biometric watermarking and signature verification. The technique is highly robust against numerous non- geometric attacks like cropping, median and weiner filtering, Gaussian and salt and pepper noise, histogram equalization and JPEG compression.

The current study can be extended to include those attacks and measure the robustness of the algorithms against them by using RST invariant transform like Complex wavelet transform and Zernike moments.

8 REFERENCES

[1] A. K.Jain, L. Hong and S. Pankanti ,"Biometric Identification", *Comm. ACM*, vol. 43, no. 2, pp. 91-98, Feb. 2000

[2] Hartung F, Kutter M ,"Multimedia watermarking Technique", IEEE proceeding on Signal Processing," vol 87, no.7, pp.1079-1107, July 1999

[3] Anil K. Jain, Stan Z. Li**,** "Encyclopedia of Biometrics," Springer (2009)

[4] Cheng-Yaw Low, Andrew Beng-Jin Teoh, Connie Tea, " Fusion of LSB and DWT Biometric watermarking for offline handwritten signature," 2008 Congress on Image and signal processing , IEEE Computer Society, pp.702-708, 2008.

[5] Anil K Jain, Umut Uludag, " Multimedia Content protection via Biometric based encryption," IEEE international conference on Multimedia and Expo", July 2003.

[6] Mayank Vasta, Richa Singh, Afzel noore ,"Improving Biometric recognition accuracy and robustness using DWT and SVM watermarking," IEICE Electronics Express, vol 2 , no.12, pp.362-367, June 2005

[7] W. Zhu et al, "Multi resolution Watermarking for Images and Video," IEEE Transaction On Circuits & Systems for Video Technology, vol.9, no.4, June 1999, pp.545-550

[8] W. Zhu et al ,"Multi resolution Watermarking for Images and Video : A Unified Approach," Proc. IEEE International Conference on Image Processing, ICIP-98, vol.1, pp.465-468.

[9] A. M. Namboodiri , A. K. Jain, "Multimedia Document Authentication using On-line Signature as Watermarks," Proc. of the International Society for Optical Engineering

(SPIE), 2004.

[10] Kundur D. and D. Hatzinakos ,"Digital watermarking using multi resolution wavelet decomposition," Technical report, Dept. of Electrical and Computer Engineering, University of Toronto, 1998

[11] Yang S.H. ,"Wavelet filter evaluation for image watermarking," Technical report, Dept. of Computer Science and Information Engineering, National Taipei University of Technology, China, 2002

[12] Marusic S., D.B. Tay, G. Deng, and M. Palaniswami ,"Even-length biorthogonal wavelets for digital watermarking", Technical Report School of Electrical Engineering and Telecommunication, University of South Wales, Australia, 2004

[13] Pla O.G., E.T. Lin, and E.J. Delp ,"A wavelet watermarking algorithm based on a tree structure," Technical report Polytechnic University of Catalonia, Spain, 2004

[14] Huang Z.Q., and Z. Jiang ,"Watermarking Still Images Using Parameterized Wavelet Systems," Technical report School of Computing and IT, University of Western Sydney, Australia, 2003

[15] Fritz Keinert, "Biorthogonal wavelets for fast matrix computations," Mathematics subject classification, 1991.

[16] Mark Nixon, Alberto Aguado, "Feature Extraction and image Processing ," Elsevier, 2005.

[17] Santi P. Maity, Malay K. Kundu, Mrinal Kr. Mandal ,"Capacity Improvement in Spread Spectrum Watermarking using Biorthogonal Wavelet," 2005 IEEE proceedings, pp.1426-1429.

[18] Nikolaidis N., and I. Pitas, "Copyright protection of images using robust digital signatures," in Proc. IEEE ICASSP'96, pp. 2168–2171.

[19] Shih-Hsuan Yang, "Wavelet filter evaluation for image watermarking," ICASSP 2003.

[20] Anil K Jain, Umut Uludag, " Hiding Biometric data," IEEE transaction on pattern analysis and Machine intelligence, vol. 25, no.11, pp.1494-1498, November 2003.

[21] Piotr Porwik, "The compact three stages method of the signature recognition," 6th International Conference on Computer Information Systems and Industrial Management Applications (CISIM'07).

[22] Hernandez J.R, F.P. Gonzalez, and M., Amado, "DCT-domain image watermarking and generalized Gaussian models," Technical report University de Vigo, Spain,1998

[23] Nino D., M. Abdallah, and B. Hammo ,"Dual domain watermarking in the biological colour model," ICIA International Conference , Sri Lanka, Colombo, 2006, pp. 407-411.

[24] Yuehua Z., C. Guixian and D. Yunhai, "An image watermark algorithm based on discrete cosine transform block classifying," ACM International Conference , 2004 , pp. 234-235

[25] Wu X., J. Hu, Z. Gu, and J Huang, "A Secure Semi-Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters," Technical Report School of Information Science and Technology, Sun Yat-Sen University, 2005, China.

[26] Zohu Wang, Alan Bovik, Hamid sheikh, Eero Simoncelli, " Image Quality Assessment From Error visibility to Structural Similarity ", IEEE transaction on Image Processing, vol 13, no. 4, April 2004

[27] Cox J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for multimedia," IEEE Transaction on Image Processing, vol. 6, pp. 1673–1687, Dec. 1997

[28] Suhad Hajjara, Moussa abdallah, Amjad Hudaib ," Digital Image Watermarking Using Localized Biorthogonal wavelets," European journal of scientific research, vol. 26, no.4 (2009),pp. 594-608

[29] Lindsay I Smith ," A tutorial on Principal Component Analysis" Feb.26, 2002

[30] Tonphone Kaewkongka, Kosin C , Bundit T ,"Offline Signature Recognition using Parameterized Hough Transform," 5th international symposium on Signal Processing and Applications, ISSPA 99,Brisbane, Australia, August 1999