Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2020) 28: 3235 – 3252

doi:10.3906/elk-2002-155

Analysis of biometric data using watermarking techniques

Foday JORH[1,2], **Barış ÖZYER**[1,*], **Claude FACHKHA**[3,4]

[1]Department of Computer Engineering, Faculty of Engineering, Atatürk University, Erzurum, Turkey
[2]Information and Communication Engineering, Beijing Institute of Technology, Beijing, China
[3]College of Engineering and IT, University of Dubai, Dubai, UAE
[4]Steppa Cyber Inc., Longueuil, QC, Canada

Received: 25.02.2020 • **Accepted/Published Online:** 10.07.2020 • **Final Version:** 30.11.2020

Abstract: This paper evaluates and analyses the discrete wavelet transform (DWT) frequency bands for embedding and extracting of the biometric data using DWT single level and multilevel watermarking approach with and without the use of alpha blending approach. In addition, singular value decomposition (SVD) combined with DWT is used to embed and extract the watermark image. The performance of compression and decompression approaches has been analyzed to examine the robustness and to check whether the compression function does destroy the integrity of the watermarked image. We investigate the proposed approach to understand how robust the watermarked on different sub-band is against the image processing and geometric attacks. The experimental results show that the DWT multilevel and SVD watermarking approach is more robust than the other watermarking methods implemented in this paper. The DWT bands dominate the approximate coefficient band (LL) in high-intensity alpha value. When the intensity is reduced, the coefficient standout to be very robust against the remaining bands.

Key words: Biometric data, security, watermarking, discrete wavelet transform (DWT)

1. Introduction

The rapid growth of the Internet has heightened concerns about the potential security threats associated with storing, processing, and reading sensitive data. Research within the technology industry is ongoing to discover and evaluate different methods and algorithms to detect security threats to copyrights, unauthorized access to information systems, and other types of security issues [1, 2]. Efficient methods are needed to protect the privacy of data employed by biometric applications against possible threats, i.e. hackers and social engineers, amongst others, and so research into such methods is ongoing [1, 3, 4]. Nonetheless, the exponential growth of cyber attacks that target data, including information theft and espionage, still constitutes a critical problem facing data providers, data holders, service providers, governments, and other entities. Watermarking, therefore, continues to be a viable option to verify ownership and maintain the authenticity and integrity of data. The invention of digital watermarking in place, it has been helping the organizations, governments, multimedia Institutions e.g., Hollywood etc. In protecting and monitoring data over the world wide web. Since the traditional old method i.e. the use of password cannot solve the security alone. Thus, the biometric authentication system is the right call for security. This is another reason why most companies are moving from the traditional system of security to biometric i.e. biometric system deter us against repudiation and detection of individuals with more than one identity (e.g., passport). Biometric systems have helped us detect individuals with more than passports using

*Correspondence: baris.ozyer@atauni.edu.tr

different identity. Therefore, protecting it is also necessary.

Although research into the means to protect the security of biometric data is ongoing, the efforts of those intending to violate the security of these data also continue, with the intent of attacking or bypassing any algorithms designed to ensure data security [5]. The aim of research in the field of watermarking and steganography is to achieve these qualities, which are imperceptibility and robustness [6, 7]. A watermarking approach can be implemented in two ways, a spatial domain and a frequency domain approach. In spatial domain watermarking, an image's pixel is manipulated to hide the actual content of pixel. The spatial domain watermarking approach is when a pixel of an image is manipulated to hide the secret image and to enable the efficient and easy to remove the secret [8]. Any attacks on the pixel ruins or distorts the secret. Due to this disadvantage, we selected the frequency domain approach. This paper investigates the domain frequency bands of discrete wavelet transform (DWT) to determine which of the bands is robust with respect to data integrity and the level of decomposition and embedding strength under which a particular band is robust. Furthermore, single and multilevel watermarking approaches are thoroughly examined using different embedding strengths. Finally, we describe the combination of the DWT and singular value decomposition (SVD) algorithm, and our tests of different alpha (embedding strength) intensities to determine the level of robustness and imperceptibility of alpha plays in the embedding process. In particular, we observed that the lesser the degree of embedding strength, the better and more imperceptible was the approximate coefficient. While the other bands irrespective of the strength, the eyes cannot notice the changes. All the tests mentioned above were conducted at different bands and different levels of decomposition. In this context, our research aimed to investigate, analyze, and then suggest the most efficient and most robust band to be used to protect and secure biometric data. Therefore, we explored the contribution using a single and multilevel discrete wavelet transform domain and then implemented the hybrid combination of multilevel DWT and SVD. In order to show the effectiveness of investigation embedded image with single and multilevel discrete wavelet transform and all the DWT band inclusive, the proposed approach is tested and compared with public data such as Lena and Baboon images.

This paper is organized as follows. Section 2 provides an overview of related works. Section 3 introduces our proposed scheme and describes its implementation. Section 4 presents our experimental results and compares them with those reported by other researchers. Finally, Section 5 discusses the limitations and challenges associated with implementing our proposal, summarizes our work and describes possible areas of future research.

2. Literature review

All researchers view the adequate securing of biometric data to be a key role of modern technology, and most have used different means of doing so—watermarking, steganography, encryption, and cryptography [1, 3, 4]. While some employ single methods to achieve this goal, others have used combinations of various methods—e.g., steganography with watermarking, steganography with cryptography, or even steganography with encryption. In [9], Zargar proposed a multilevel decomposition scheme using DWT in a hardware image compression architecture approach. The host image was then compressed using the JPEG compression algorithm before the watermark image was embedded in the cover image. In [10], Sharma et al., who provide the third level decomposition approach, focused on the low frequency subband. In this research, both the cover image and the watermark are decomposed equally, and the embedding and extraction of the watermark are performed in the LL subband. In [11], the watermark image was embedded in the high-level frequency subband using DWT. In [12], Rzouga et al. proposed a stronger reinforcement method in protecting biometric data. In other word, they used a combination of the same watermarking techniques twice, just to protect the secret (watermark). The

aim of the proposed system is to increase the security level of the authentication scheme, which the authors show is achieved. This increase in security level is, obtaining both the cover (host) image and the watermark without wrecking the watermark image meaning to retain the original characteristics and view of the image. In [13], an optimal DWT–SVD based image watermarking scheme using self-adaptive differential evolution (SDE) algorithm was proposed to eliminate mutation factor and crossover rate parameters.

Employing a hierarchical combination of both watermarking and steganography, Whitelam et al. represented a giant leap in securing biometric data [14]. First, the image of a fingerprint was embedded in the corresponding facial image, and the watermarked image was then inserted into a nonforensic-like image to hide the fingerprint/facial image. In the event that the biometric data of the watermarked image comes into contact with a man-in-the-middle attack, adversaries can suspect or investigate the image in contact. However, with the help of steganography, it would be very difficult to do so. In [15] Ouslim et al. described in detail how biometric data can be transferred onto a computer network without an attack or even without being detected. They also highlight the possible location of such an attack, a sensor location, where most of the fingerprint is left. In the section describing watermarking, the authors proposed a number of performance evaluations and robustness tests. The image compression type used in this paper is the JPEG extension, and the authors' algorithm is very efficient. The visual observation was also measured using the peak signal-to-noise-ratio (PSNR) comparing the original image and the watermarked image. Alkhathami et al. proposed an algorithm to secure fingerprint images with double watermarking using a discrete cosine transform [16]. On one hand, they compared and contrasted the watermark image before embedding and after extraction of the original image. The fingerprint image was then protected by inserting two watermarks simultaneously without necessarily destroying the structure of the fingerprint. Examination and analyses were done on the images to verify that the watermarking and its techniques had not affected the fingerprint. The DCT algorithm was developed to help embed the watermarked image into the fingerprint. The fingerprint image was then split with a DCT-based algorithm to easily enable the embedding of the watermark into the fingerprint. Implementing a system that mitigates security and privacy, Islam et al. employed a biometric authentication strategy that utilized two different biometric features with the combination of the watermark and a conceal/disguise password encryption that helped with the authentication process [17]. These authors' focus was how best to hinder many types of attacks and eavesdropping. In [18] Tareef and Al-Ani proposed a system that provides verification in case an attacker induced another watermark in an already existing watermark. Their system can provide a secure base of sparse coding together with SVD and DWT watermarking system. The system addresses serious security threats and attacks, i.e. robustness, in the event two or more individuals claim ownership of the same image, a nonauthorized to reader, detection of a false positive (FPD), and so on. The robust technique was proposed for the watermarking process using DWT together with the singular value decomposition (SVD) algorithm so as to hide the secret image into the cover image [19, 20]. Both the host and secret image are decomposed using the HAAR wavelet, and then the high-frequency subband (i.e. HH) is later decomposed using the SVD methodology. The HH subband is further decomposed into matrices. In addition, the authors employed a median filter function to smooth the image before decomposition took place. Siddiqui et al. proposed a hybrid DWT and SVD watermarking approach, in which the host image was decomposed into four bands: LL, LH, HL, and HH [7]. Then the LL subband was further decomposed into the fourth level. The HH subband was passed into the SVD. Then the watermark image was then passed into the SVD algorithm to generate the matrices. They also generated a unique signature that was later embedded in the host image using the already decomposed LL subband. The algorithm is thus able to withstand many of the implemented attacks using the same algorithm, i.e. the hybrid DWT and

SVD algorithm. The host image is disintegrated into second level, and the HH subband (high-frequency) is chosen. The additional value for this is that the decomposed HH band is divided into the block, and then each of the block SVDs is implemented [21]. Based on their findings, the second level watermarking schemes were apparently more robust with respect to implemented attacks [20].

3. Methodology

The overview of our proposed approach for securing biometric data is shown in Figure 1. In this diagram, we demonstrate all the steps including the finger enhancement, decomposition, embedding and extraction. The details for each steps are given as below.

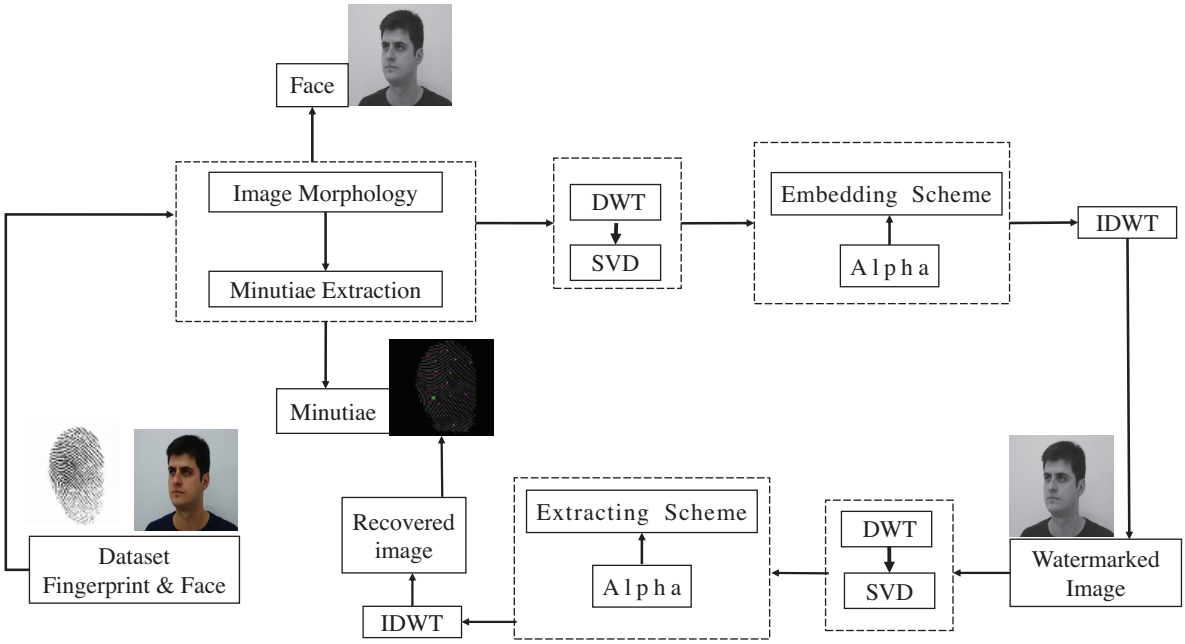


Figure 1. Overview of DWT Watermarking Process. The face image is the host image and the fingerprint image is the watermark image.

3.1. Fingerprint enhancement

The minutiae-based fingerprint matching algorithm is used to extract minutiae from the fingerprints that helps in the alignment and in the retrieval of minutiae between the fingerprint sets. The minutiae-based is common due to its unique proportion with the way forensic experts and security agencies compare fingerprints to proof individual's identification several countries. Fingerprint feature extraction, minutiae representation and registration are among the most important component in fingerprint algorithm matching. Based on the fingerprint algorithm, there are basic feature necessary to extract the minutiae. These are image tones, image enhancement processing, pre- and postprocessing and the feature set extraction algorithm. In the image-enhancement algorithm, the Fourier domain is applied with prefiltered image. The reason is that it gives us permission to convolve the fingerprint image with filter accessibility of full size image as in [22, 23]. These involves the ridges segmentation, the ridges orientation, ridges frequency and the ridges filter. We apply a

global threshold value to every fingerprint pixel. In the fingerprint extraction process the images are converted to grayscale and then to binary image. The binarization of the grayscale image is the main approach before any step is taken. The binary image is passed via the morphological operation. In the case of the ridges structure of the fingerprint is deduced to a pixel thick. This is also known as skeleton and it helps in the detection of minutiae. The minutiae-base extraction algorithm on this paper follows the methodology in [24] using the the formula:

$$Cn(P) = \frac{1}{2} \sum_{i=1...8} |Val[P_{[1 mod 8]}] - ValP_{[i-1]}| \tag{1}$$

where P is the resulting value of the thinned image, val is a member of 0,1 that is the binary pixel value, $C(n)$ is the cross number that aid in the identification of the ridges and bifuracations. If the values of $C(n)$ is calculated as 1, then it is a ridges and if $C(n)$ is equal to 3, it is a bifuracation. After the extraction of the minutiae, the similarity score of the extracted minutiae is calculated using the other fingerprint in datasets. The two variables such as distance threshold and angular threshold and the use of Euclidean distance between these two fingerprints are created to achieve the similarity index as shown in Figure 2.

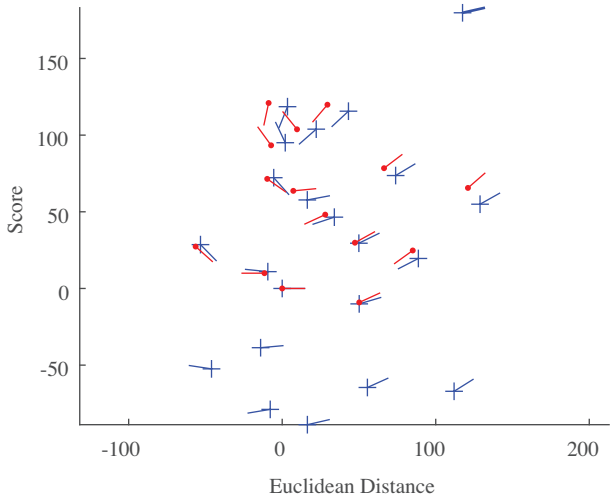


Figure 2. Similarity measure is obtained as 0.77067. The red arrows represent the first fingerprint image and the blue arrows represent the second fingerprint image in the database.

3.2. Decomposition scheme

The host face and secret fingerprint images are decomposed into frequency bands using the DWT which is an important process for our embedding procedures. Approximate coefficient (CA), horizontal coefficient (CH), vertical coefficient (CV) and diagonal coefficient (CD) of DWT are used separately in hiding the watermark image. This process is repeated for all the approaches, including the single level and multilevel DWT. In addition, in the DWT and SVD watermarking approach, after DWT decomposition is attained, the targeted band is also decomposed using the SVD algorithm. The reason is that finding all the contradictory requirements in a technique is quite difficult and achieving both robustness and imperceptibility is difficult too. These two algorithms are combined to achieve an efficient result. In most cases, LL (i.e. CA) and HL are decomposed

[7, 10]. So, we also started our decomposition with the LL band, and we further decomposed the other DWT frequency band i.e. LH, HL and HH. In all decomposition the mother wavelet is used as HAAR wavelet domain. The block diagram of the DWT and SVD decomposition scheme is shown in Figure 3. The original host and watermark (i.e. minutiae extraction) are shown in Figure 4.

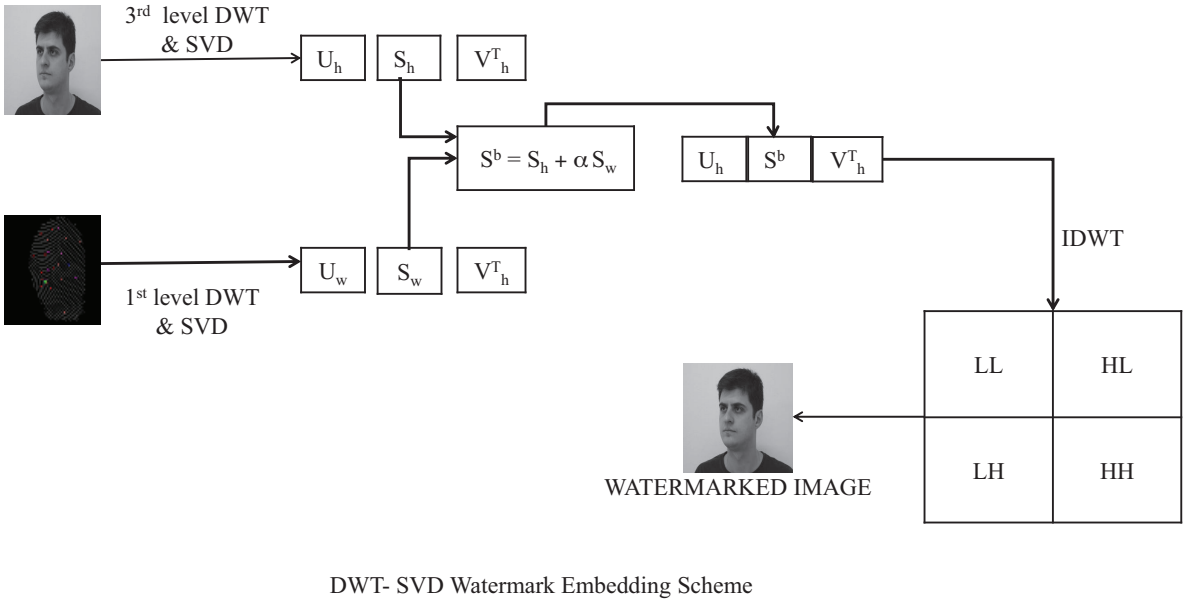


Figure 3. Block diagram DWT and SVD decomposition scheme. The representation of this block diagram demonstrates the decomposition and embedding the host and the watermark image using the DWT and SVD watermark approach.

Figure 4. A sample of the original binarized host face image and the extracted watermark fingerprint image.

3.3. Embedding process

In this process, the secret (i.e. watermark) image is inserted into the host image. First, single level, multilevel without alpha blending are applied to the LL band and then remaining DWT bands, respectively. The

watermarked is calculated from the equation given as below:

$$Watermarked = \mu + (WM \times \alpha\times) \tag{2}$$

where μ represents the decomposed intended frequency band of the host image, WM represents the intended frequency band of the watermark image ready to be inserted into the host image and α is the embedding strength. Then, alpha blending watermarking approach is applied in single level and multilevel for all bands in the embedding process. In embedding process, the LL band of the secret watermark is multiplied with the embedding strength then added to the host to generate the watermarked image. The process is that the LL of the host image is passed via the key K and the secret (watermark) LL band together with embedding strength to generate the watermarked image calculated by the following equation:

$$Watermarkedalpha = K \times \mu + (WM \times \alpha) \tag{3}$$

The last, the combination of DWT and singular value decomposition techniques are applied on all bands. The fourth decomposition frequency band is taken and then passed to the SVD algorithm. The singular value of both the host LL and the secret LL are multiplied by embedding strength *alpha* to generate the secret image. This is in turn embedded into the host image to achieve the watermarked image. SVD generates the orthogonal matrix from the DWT decomposed band to rebuild the original secret subband that is inserted into the host image. The Algorithm 1 represents the embedding process of DWT and SVD.

Algorithm 1 Embedding process for DWT and SVD.

procedure INPUT(CImg,WImg)
    InputA = CoverImage
    InputB = WatermarkImage
    Binarize (InputA, InputB)
    if $Input = 512$ **then**
        [ll,lh,hl,hh] = DWT(InputA)
    else if $InputA \neq 512$ **then**
        $InputA == 512$
        $[ll, lh, hl, hh] = DWT(InputA)$;
        $DoSVD$
        $[U_h, S_h, V_h] = SVD(ll)$
    if InputB = 64 **then**
        [ll,lh,hl,hh] = DWT(InputB)
    else if $InputB \neq 64$ **then**
        $WM_{IMG} == 64$
        $DoSVD$
        $[U_{wm}, S_{wm}, V_{wm}] = SVD(ll_{wm})$
        $S_{mark} = S_h + alpha \times (S_{wm})$;
        $Watermarked = U_h \times S_{mark} \times V_h$;

3.4. Extraction

The watermarked images in the dataset are extracted using the blind watermarking method, in which the original image is not required in detecting the secret image. The watermarked images are passed via image processing and geometric attacks. In this point, it is necessary to extract the watermark image from the attacked

Algorithm 2 Extraction process for DWT and SVD.

System Initialization
$InputC$ = watermarkedIMG;
watermarkedIMG = 512×512
$[ll, lh, hl, hh] = DWT(InputC)$ ▷ //decompose the watermarked
repeatDecomposition
until 3-level
$[U_{wmll}, S_{wmll}, V_{wmll}] = SVD(ll)$
$S_{rec} = (S_{wmll} - S_y)/\alpha$ ▷ //use the Singular Value of the Host and Watermarked image
$ExtImg = U_{wm} \times S_{rec} \times V_{wm}$
$Rec_{wmark} = ExtImg$;

watermarked image [8, 21]. The general DWT watermarking-extraction is calculated by following equations:

$$Extimage = (watermarked - WM)\alpha \tag{4}$$

where $Extimage$ is the extracted image. In order verify the accuracy of the watermarked image, MSE , the PSNR , normalized correlation (NC) and the bit error ratio (BER) are calculated against the original secret and the recovered secret, given as the equations below. The extraction algorithm is illustrated in Algorithm 2.

$$MSE = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \frac{[I1(i,j) - I2(i,j)]^2}{N \times N} \tag{5}$$

$$PSNR = 10 \log 10 \frac{255^2}{MSE} \tag{6}$$

$$NC = \frac{\sum_{i=1}^{N1} \sum_{j=1}^{N2} (W(i,j) \times W^*(i,j))}{\sum_{i=1}^{N1} \sum_{j=1}^{N2} (i,j)^2} \tag{7}$$

$$BER = \frac{\sum_{i=1}^{N1} \sum_{j=1}^{N2} (W(i,j) \bigoplus W^*(i,j))}{N1 \times N2} \tag{8}$$

4. Dataset whereabouts

Fingerprint [25] and facial images [26] are two types of biometric dataset carried out in this paper. The face dataset comprise of 702 images. The size of each image is640×480 pixel and the image type is JPEG. The fingerprint dataset is comprised of four databases and each database contain 80 fingerprint images. The size of each fingerprint is 388×374 pixel of type TIFF. The fingerprint and the face images are both passed via an image enhancement algorithm to convert them from RGB to grayscale, and we worked with the gray scaled images throughout our experiment. These are the two databases FVC2002DB1-B and FCV2002DB2-B used in this paper [25] as these were the sources of the data used in [12]. Specifically, we tested and worked with the dataset name DB1-B that contains 80 fingerprint images of size 388×374 pixels and employs image format BMP. We normalized them into different sizes ranging from 64×64, 128×128, and 256×256 pixels as in [19] and facial image [26]. The reason for the normalization is to check whether the size of the watermark matters. The value of the PSNR decreases with reference to the size of the watermark shown in Table 1. Figure 5 depicts as an example of the original fingerprint and its associated minutiae.

Table 1. Single level DWT with normalised images.

No.	Host (capacity) face	Watermark (capacity) minutiae	PSNR	Correlation
1	480 × 640	64 × 64	61.38	1
1	480 × 640	128 × 128	58.58	1
1	480 × 640	256 × 256	56.88	1

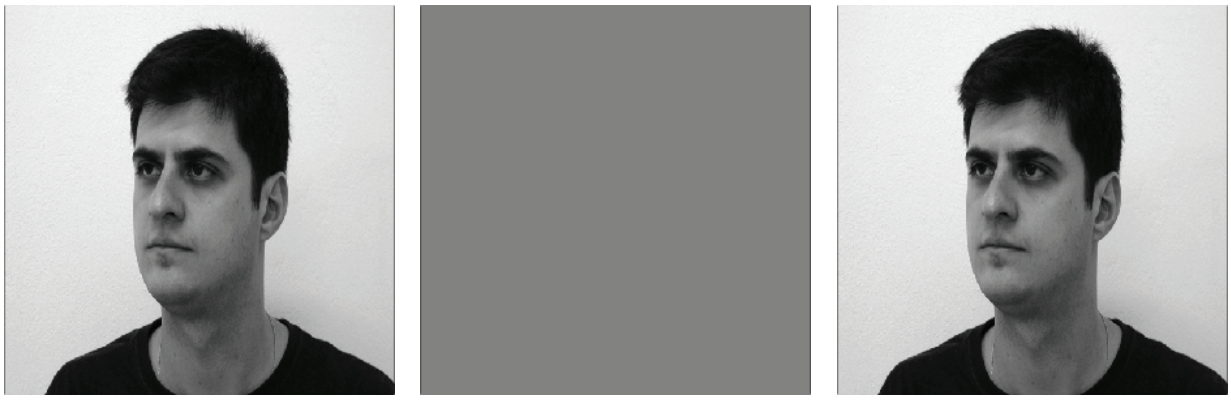
(a) Original Image (b) Minutiae

Figure 5. A sample of (a) original fingerprint image and (b) corresponding minutiae image. The extracted minutiae image is used as the watermark image defined as the secret image.

5. Experimental results

All the experiments are carried out on MATLAB 2018a on a 64-bit Window 8.1 operating system executed on Inter(R) Pentium(R) CPU 2.20 GHz Processor with 8GB RAM. In the experiment, we implemented the single level and multilevel watermarking embedding system in this paper using the discrete wavelet transform domain with and without the use of alpha blending. We combined two algorithms: DWT and SVD. In this process, all secret images are hidden in all the DWT bands, i.e. LL, LH, HL, and HH. When we calculated the normalized correlation Eq. (7) and bit error rate Eq. (8), in all analyses, the approximate coefficient band produced the least values compare to those produced in the other bands. The reason is that the approximate coefficient contains the most important credentials of the image, video, audio, etc.[8–11, 20, 21, 23]. Thus, any manipulation on the LL band can affect the image drastically. In addition, we performed a number of attacks on the watermarked image, i.e. salt and pepper, Poisson, speckle noise, Gaussian noise, cropping, JPEG compression, Gaussian filter, average filter, median filter, sharpening, rotation, and soft and hard threshold as shown in Figure 6. Before the attacks are tested on the watermarked image, we also compared the relationship of the original watermarked and decompressed image using the NC formula Eq. (7). The correlation value is 1, showing that the compression function did not destroy our watermarked image.

After attacks are implemented and the secret extracted from the attacked watermarked image, we compared the original watermark and the recovered watermark image using the BER Eq. (8) and normalized correlation Eq. (7). The highest BER was approximately 2%, and others were equals to 0%. The correlation calculations between the original watermark and the recovered watermark image after the watermarked image



(a) Original Image (b) Compressed Image (c) Decompressed Image

Figure 6. Samples of different types attacks applied on the watermarked image.

passed via the implemented attacks yielded values of 1 and close to 1 (i.e. 0.9). The combination approaches thus produced an efficient means of protecting the secret image from being affected by the attacks. We also compare our results with the findings reported in [12]. We used the PSNR Eq. (6) and MSE Eq. (5) matrices respectively, to calculate the signal-to-noise ratio between the two images. The higher the PSNR is, the better is the imperceptibility. We also implemented the other remaining bands and calculated the corresponding PSNR and MSE values for these bands also. The NC (normalized correlation) given by Eq. (7) was used to calculate the relationships between the watermarked and host and between the watermark and recovered watermark images.

Table 2 presents the results of the extracted images after having undergone some image processing attacks. According to our observations, in most attacks implemented with the low frequency (i.e. percentage intensity of the attack), the LL band is more robust than the other bands. However, when the percentage intensity is high, we noticed that the LH and HL frequency bands are more robust than was the LL band. On the other hand, the reason we chose the SVD technique is that it has the capability to examine and analyze the object (e.g., image, audio, etc.) from one edge to another. Moreover, the singular value is not affected by the desynchronization, and so, due to its stability against many types of attacks, we decided to employ the singular value method.

Although space constraints limited our ability to present all of our results in this paper, we were able to confirm that the multilevel watermarking approach is more robust than the single level approach. With the exception of median filters and JPEG compression, the implemented attacks listed herein were able to easily destroy or ruin the watermark (secret) image in the single level watermarking approach, whereas the multilevel approach was able to withstand many of these attacks. However, its major problem was that it could not withstand the geometric attacks (e.g., cropping, rotation, etc.) In all our approaches, we tested all the DWT frequency bands, and the results are represented below.

5.1. Experimental result of SVD and DWT

In this approach, in order to achieve the complete biometric modality of a database system, we randomly selected 80 facial images and 80 fingerprint images from each dataset to simulate matching fingerprint facial image sets belonging to 80 individuals. We adopted the facial image of size 512×512 pixels as the cover and the watermark image of size (i.e. 64×64, 128×128 pixels). We used the abovementioned two dimensions in nearly

Table 2. General results from DWT & SVD of the extracted images on biometric datase.

DWT-SVD	LL		HL		LH		HH	
	NC	BER	NC	BER	NC	BER	NC	BER
Attack Free	1	0	1	0	1	0	1	0
Salt and pepper noise(0,01)	1	0.0245	1	0.0179	1	0.0186	1	0.175
Poisson noise	1	0.0197	1	0.076	1	0.0185	1	0.0167
Speckle noise (0.001)	1	0.0149	1	0.0143	1	0.0152	1	0.0131
Speckle noise (0.005)	1	0.0201	1	0.0172	1	0.0169	1	0.0154
Speckle noise (0.009)	1	0.0207	1	0.0183	1	0.0189	1	0.0169
Gaussian noise(0.001)	1	0.0171	1	0.0202	1	0.0209	1	0.0206
Gaussian noise(0.005)	0.9973	0.0164	1	0.203	1	0.0215	1	0.0203
Gaussian noise(0.009)	0.9963	0.0158	1	0.0211	1	0.0207	1	0.0206
Cropping top left	0.9960	0.0156	1	0.0036	1	0.0008	1	0.0016
Cropping center	NaN	0.1094	1	0.0041	1	0.0009	1	0.0016
Cropping bottom right	NaN	0.1012	1	0.0038	1	0.0011	1	0.0014
Compression 80	0.9998	0.0091	1	0.0097	1	0.0124	1	0.0002
Compression 75	0.9999	0.0093	1	0.0100	1	0.0126	1	0.0009
Compression 50	1	0.0136	1	0.0013	1	0.0013	1	0.0017
Gaussian filter 5×5	1	0.0203	0.9999	0.0002	1	0.0000	1	0.0003
Gaussian filter 3×3	1	0.0208	0.9999	0.0002	1	0.0000	1	0.0003

all of our implementation. However, all the results in this paper is based on the 64×64 pixel. The results of this watermark image size 128×128 where lesser than the 64×64. The cover watermark images are all gray scaled. Figure 7 depicts the compressed and decompressed watermarked image. In [21] state "that the combination of multialgorithms in watermarking can really prevail over the potential problem of the other approaches," and the results of our experiment confirmed this assertion. The result of the single level, multilevel watermarking, and the DWT and SVD approach can be our reference. The paper examined and analyzed the entire DWT band in hiding our watermark image. In addition, the watermarked image underwent various signal processing and geometric attacks to help us evaluate the robustness and imperceptibility of the algorithm and watermark, respectively. The attacks also indicate the intensity of the attacks. Figure 6 represents samples of watermarked image after implementing the attacks. Using the normalized correlation, PSNR and MSE in Eqs.(5)–(7) above, we analyzed the differences between our proposed algorithm (SVD and DWT) and [12] shown in Table 3. We used the same types of attacks reported in [12]. Based on our use of multilevel DWT decomposition and SVD, our result generated a higher PSNR value, and our correlation very closely approximated or equaled 1 in other bands. In addition, our proposed method implements the blind extraction approach. We also compared the results of our proposed method with those reported by [7, 13, 18, 23] shown in Table 4. The normalized correlation were calculated between the watermark image and recovered image. NC values should be very large compared to other coefficients in order to obtain distinct identifications. As in Table 4, we observed that DWT LL band is robust again salt and pepper noise, median filter, average filter and JPEG compression as indicated in the result based on the normalized correlation. Less robust against gaussian noise, geometric attack such as cropping. Even though the result of the normalized correlation is least compare to the other DWT band (LH,

HL and HH), these other bands have shown great robustness in all our implementation using multilevel DWT and SVD watermarking approach. We observed that our results were more robust against the median filters and average filtering using the DWT and SVD methodology.

Table 3. Comparision of extracted images of LL, LH, HL, HH with [12].

Attacks	LL		LH		HL		HH		WPD [12]	
K	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC
Attack free	Inf.	1	Inf.	1	Inf.	1	Inf.	1	34.48	1
Compression 70%	50.62	0.99	52.79	1	48.05	1	35.20	1	33.92	0.81
Compression 80%	53.22	0.99	53.13	1	48.02	1	36.78	1	34.14	0.94
Salt and pepper noise 0.5%	37.94	1	36.24	1	37.88	1	33.29	1	27.44	0.98
Salt and pepper noise 0.5%	38.584	1	36.24	1	36.94	1	32.58	1	82.82	0.98

Table 4. Comparison of all DWT bands with [7], [13], [18] and [23].

BAND	LL	LH	HL	HH	[18]	[23]	[13]	[7]
	NC	NC	NC	NC	NC	NC	NC	NC
Attack free	1	1	1	1	-	-	-	-
Salt and pepper (0.01)	1	1	1	1	0.9470	0.9823	-	-
Salt and pepper (0.1)	1	1	1	1	0.7978	0.9113	-	-
Gaussian noise (0.01)	0.9963	1	1	1	0.8736	0.9681	0.8589	-
Gaussian noise (0.1)	0.9960	1	1	1	0.8000	0.8619	-	-
Speckle noise (0.01)	1	1	1	1	0.9762	0.9838	-	-
Speckle noise (0.1)	0.9596	1	1	1	0.8219	0.9541	-	-
JPEG comp. 50%	1	1	1	1	0.9841	0.9852	0.9607	-
Average filter 3×3	1	1	1	1	0.9402	0.9757	0.9191	0.881
Median filter 3×3	1	1	1	1	0.9702	0.9817	0.9495	0.881
Cropping top left	0.9960	1	-	1	-	-	-	-
Cropping center	NaN	1	1	1	-	-	-	0.947
Cropping bottom right	NaN	1	1	1	-	-	-	-
Rotation 45°	NaN	1	1	1	0.8717	0.9763	-	0.881
Rotation 270°	1	1	1	1	0.9727	0.9867	-	-
Soft threshold (0.4)	1	1	1	1	0.9491	0.9297	-	-
Hard threshold (0.4)	1	1	1	1	0.9450	0.9490	-	-
Sharpening	1	1	1	1	0.9663	0.9769	0.8893	-

In order to show the effectiveness of embedding the watermark into the other bands for biometric images, the proposed approach is tested and compared with public data available in a variety of images that embedded with single and multilevel discrete wavelet transform and all the DWT band inclusive. The Lena and Baboon images are used as cover and watermark image, respectively. Table 5 represents the result generated from the watermark image and the extracted image after undergoing the attacks. When it is compared the result from the biometric data with the public dataset, we observed that the biometric data produces better result with different of 0.01, 0.001 and so on. The reason is that the biometric dataset e.g. the fingerprint has many black

and white bits making it very difficult to spot the changes. The same test (i.e. the increment of embedding strength from several ranges) was also test on the public dataset. In our experiment with the biometric dataset we observed that the embedding strength (alpha) when it increased the imperceptibility reduces. We did reduce the alpha to 0.1 and 0.01 respectively in all our experiment. In the public dataset implementation, we observed the same issue. Counter the same problem we also applied the same method that is the reduction of the alpha intensity as mentioned in the paper. We have also observed that, the result given by the normalized correlation (NC) is higher in the other bands (i.e. HH, HL, LH) compared to the LL. We also test the attack from NC and the result in Table 5 shows that all the value are 1 before any attacks are implemented and after the attacks the values changes base on the type of attack and the intensity of the attacks. Figure 8 showcase the different attacks on the maximum NC values of extracted watermark image with their respective intensity and attack type indicating the host, watermark, stego image and the extracted secret images.

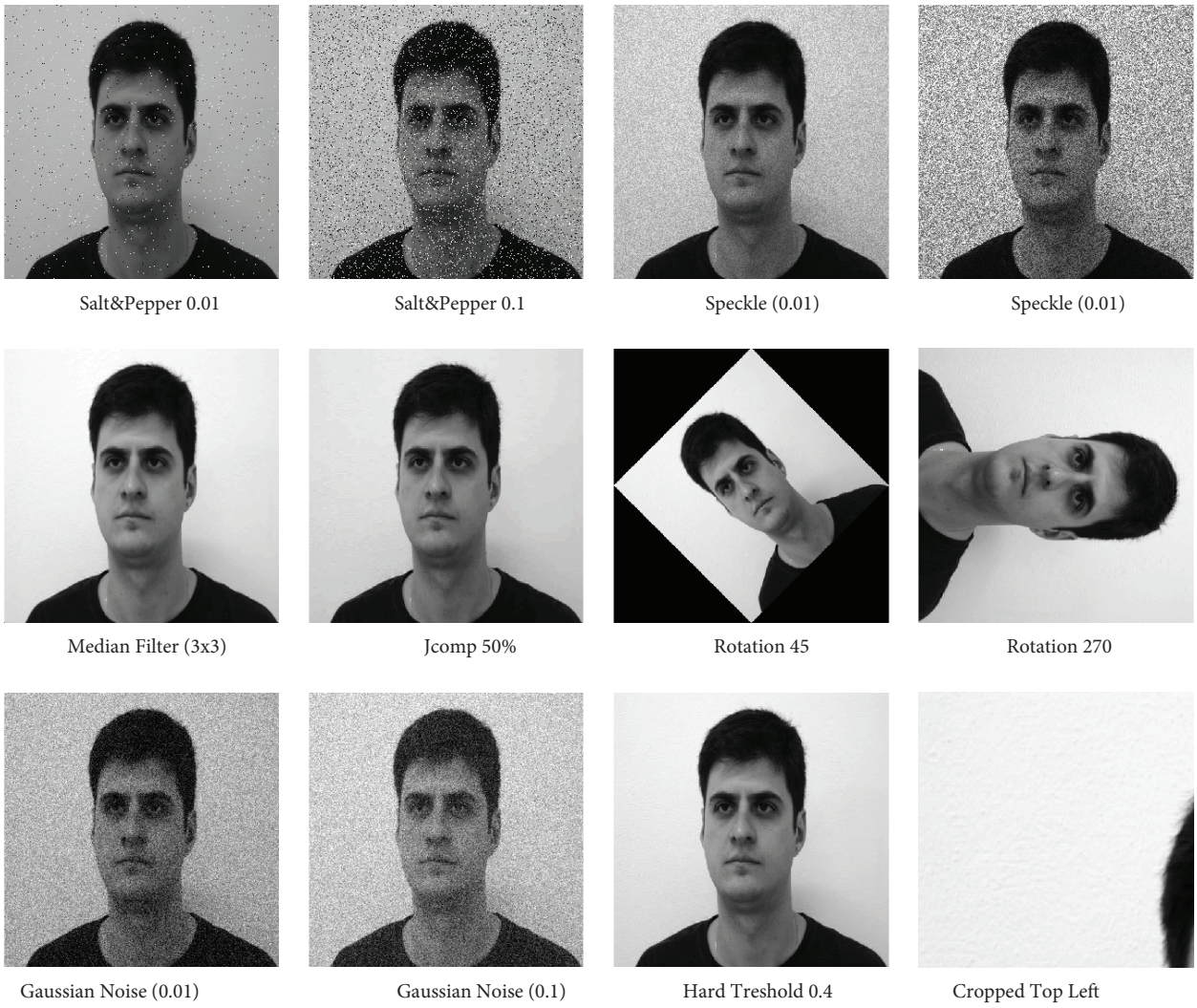


Figure 7. A sample of (a) compressed and (c) decompressed image watermarked image. The watermarked image image is also defined as the stego image. (b) represents the tick grayed image which is compressed image of the watermarked image.

Table 5. General results using public data set (Lena and Baboon) on DWT bands.

BAND	LL	LH	HL	HH
	NC	NC	NC	NC
Attack free	1	1	1	1
Salt and pepper (0.01)	0.9982	0.9985	0.9987	0.9966
Salt and pepper(0.1)	0.8172	0.9582	0.9563	0.9431
Gaussian noise (0.01)	0.9608	0.9896	0.9896	0.9826
Gaussian noise (0.1)	0.6299	0.9903	0.9901	0.9821
Speckle noise (0.01)	1	0.9986	0.9987	0.9966
Speckle noise (0.1)	0.8595	0.9623	0.9608	0.9471
JPEG comp. 50%	1	1	1	1
Average filter 3×3	0.9972	1	1	1
Median filter 3×3	0.9994	1	1	1
Cropping top left	0.6907	0.9986	0.9608	1
Cropping center	0.8889	0.9997	0.9992	1
Cropping bottom right	0.6201	0.9985	1	1
Rotation 45°	0.7107	0.9943	1	1
Rotation 270°	0.9989	1	1	1
Soft threshold (0.4)	1	1	1	1
Hard threshold (0.4)	1	1	1	1
Sharpening	0.9979	1	1	1

Table 6. Comparison of alpha blending result with [11].

		LL BAND		HL BAND		HH BAND		[11]	
K	Q	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
0.2	0.009	6.95	3215.89	38.61	8.95	50.07	0.64	8.06	10167.720
0.5	0.009	11.04	5151.97	38.98	8.22	50.51	0.58	12.22	3900.448
0.75	0.009	17.07	1287.42	39.17	7.87	50.73	0.55	18.45	928.642
0.85	0.009	21.51	462.37	39.22	7.79	50.78	0.54	23.18	312.882
0.99	0.009	45.36	1.91	9.24	7.75	50.81	0.54	48.78	0.860
1.25	0.009	17.02	5177.67	39.17	7.86	50.73	0.55	17.62	1123.906
1.5	0.009	11.02	5177.67	38.98	8.22	50.50	0.58	11.81	4290.97
2.0	0.009	5.01	20691.89	38.30	9.62	49.69	0.70	5.89	16763.99

5.2. Alpha blending result

In another approach, we implemented the alpha blending as in [11] where the value of K varies from 0.2 to 2.0 and the Q (embedding strength) remains constant throughout the experiment and Q is 0.009. Here, we employed both the multilevel and single watermarking approach in order to compare our results with theirs. According to their result from the watermarking implementation, K = 0.99 and q = 0.009 generate the best result for the PSNR between the watermark and the host. A comparison of the LL band and their HL band reveals that their result is a bit higher than the result of the approximate coefficient. In comparing the other

Figure 8. Different attacks on the watermarked image and their corresponding extracted watermarks including the maximum NC values and the bands. The attacks are cropped center noise, gaussian noise with zero mean and 0.01 variance, rotation 270 and salt and pepper noise with 0.01 corruption.

bands (i.e. HL and HH), our proposed method results are higher than that of [11]. We show only a few diagrams of our implemented alpha blending approach due to spacing constraints, and Table 6 shows the result of the alpha blending.

Based on the results from normalized correlation, watermarked images, and histograms, we have noticed that the key K really affects the watermarked image. This makes us understand the fact that the LL frequency band contains the most valuable features of the image. Comparing the results of the LL frequency band with the HL band, the key K has not really affected the watermarked image. The PSNR value is in the range of

38dB and 39dB. This shows a good imperceptibility result for watermarking. With alpha blending on the HH frequency band we noticed that the PSNR values is the highest amongst all other bands. The results are in the range of 49dB and 50dB. This is demonstrating that the HH band is the most imperceptible with regards to alpha blending watermarking approach.

Knowing the secret (watermark) is hidden in the cover image but not knowing the exact position, especially after undergoing geometric attacks (such as rotation, cropping, etc.). These are the two types of attacks that the single and multilevel DWT decomposition could not solve. However, with the multilevel DWT and SVD could solve most geometric attacks implemented in this paper. All the bands are robust against median filter and noise attacks. However, concerning the geometric attacks, our experiment cannot withstand especially effected by rotation attack.

6. Conclusion

In this study, we propose a multilevel watermarking approach using the discrete wavelet transform domain and singular value decomposition. All the DWT frequency bands is used to embed the watermark image ranging from single level, multilevel watermarking and alpha blending watermarking to evaluate and analyse the discrete wavelet transform bands in embedding the secret. In summary, we came to observe that watermarking using multilevel DWT with the combination of more than one algorithm in embedding the secret is more robust compared to a single algorithm. Our proposed method can withstand nearly all the attacks tested in this paper except for the rotation attack on the LL band. Then, LH, HL, and HH withstand the attacks in all the experiments carried out. We have noticed crucial facts that can enhance excellent and efficient watermarking are the size of the watermark image and tone (i.e. smoothness, roughness etc.). We test all our images in different hues. We observe that the rough or noisy images generate a watermarked image with less PSNR value when compare with the noiseless image. At the course of our experiment, we noticed that on the LL band, if the embedding strength is of high power, it affects the imperceptibility of the watermarked image. It is thereby making the watermarked image less robust. As we reduced the intensity (i.e. embedding strength) to 0.01, 0.001 and 0.0001, we noticed that the imperceptibility is excellent. The PSNR value is high as well. With this band, we can conclude that it would be better to do the manipulation within this range of alpha. In addition, we noticed that even though multilevel watermarking using DWT generate good result compare to the single level watermarking. However, DWT combined with other algorithm produces a practical effect. The experimental results show how robust the watermarked image is when combined with more than an algorithm.

References

[1] Jain AK, Nandakumar. Biometric authentication: system security and user privacy. IEEE Computer 2012; 45 (11): 87-92. doi: 10.1109/MC.2012.364

[2] Khan MK, Zhang J, Tian L. Protecting biometric data for personal identification. In: Li SZ, Lai J, Tan T, Feng G, Wang Y (editors). Advances in Biometric Person Authentication. Lecture Notes in Computer Science Berlin. Heidelberg, Germany: Springer, 2004, pp. 629-638. doi: 10.1007/978-3-540-30548-472

[3] Jain AK, Nandakumar K, Nagar A. Biometric template security. Eurasip Journal on Advances in Signal Processing 2008; 113: 1-17. doi: 10.1155/2008/579416

[4] Prabhakar S, Pankanti S, Jain AK. Biometric recognition: Security and privacy concerns. IEEE Security & Privacy 2003; 1 (2): 33-42. doi: 10.1109/MSECP.2003.1193209

[5] Anil KJ, Umut U. Hiding biometric data. IEEE Transactions on Pattern Analysis and Machine Intelligence 2003; 25 (11): 1494-1498.

[6] Douglas M, Bailey K, Leeney M, Curran K. An overview of steganography techniques applied to the protection of biometric data. Multimedia Tools and Applications 2018; 77 (13): 17333–17373. doi: 10.1007/s11042-017-5308-3

[7] Siddiqui A, Kaur A. A secure and robust image watermarking system using wavelet domain. In: IEEE 7th International Conference on Cloud Computing, Data Science and Engineering Confluence; Noida, India; 2017. pp. 599-604.

[8] Hasan KK, Ngah UK, Salleh MFM. Multilevel decomposition discrete wavelet transform for hardware image compression architectures applications. In: IEEE International Conference on Control System, Computing and Engineering; Mindeb, Malaysia; 2013. pp. 315-320.

[9] Zargar AJ. Digital watermarking using discrete wavelet techniques with the help of multilevel decomposition technique. International Journal of Computer Applications 2014; 101 (2): 25-29.

[10] Sharma P, Swami S. Digital image watermarking using 3 level discrete wavelet transform. In: Xun L (editor). Advances in Intelligent Systems Research. Tianjin, China: Atlantis Press, 2013, pp. 129-133.

[11] Yang W, Hu J, Wang S, Yang J, Shu L. Biometrics for securing mobile payments: benefits, challenges and solutions. In: Proceedings of the 6th International Congress on Image and Signal Processing; Hangzhou, China; 2013. pp. 1699-1704.

[12] Rzouga HL, Dorizzi B, Essoukri BAN. A combined watermarking approach for securing biometric data. Signal Processing: Image Communication 2017; 55: 23-31. doi: 10.1016/j.image.2017.03.008

[13] Ali M, Ahn CW. An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain. Signal Processing 2014; 94: 545-556. doi: 10.1016/j.sigpro.2013.07.024

[14] Whitelam C, Osia N, Bourlai T. Securing multimodal biometric data through watermarking and steganography. In: IEEE International Conference on Technologies for Homeland Security (HST); Waltham, MA, USA; 2013. pp. 61-66.

[15] Ouslim M, Sabri A, Mouhadjer H. Securing biometric data by combining watermarking and cryptography. In: 2nd International Conference on Advances in Biomedical Engineering; Tripoli, Lebanon; 2013. pp. 179-182.

[16] Alkhathami M, Han F, Van SR. Fingerprint image protection using two watermarks without corrupting minutiae. In: IEEE 8th Conference on Industrial Electronics and Applications; Melbourne, VIC, Australia; 2013. pp. 1151-1155.

[17] Islam MR, Sayeed MS, Samraj A. Biometric template protection using watermarking with hidden password encryption. In: Proceedings International Symposium on Information Technology; Kuala Lumpur, Malaysia; 2008. pp. 1-5.

[18] Tareef A, Al-Ani A. A highly secure oblivious sparse coding-based watermarking system for ownership verification. Expert Systems with Applications 2014; 42 (4): 2224-2233. doi: 10.1016/j.eswa.2014.09.055

[19] Kaur R, Jindal S. Robust digital image watermarking in high frequency band using median filter function based on DWT-SVD. In: International Conference on Advanced Computing and Communication Technologies; Rohtak, India; 2014. pp. 47-52.

[20] Araghi TK, Manaf AA, Araghi SK. A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. Expert Systems with Applications 2018; 112: 208-228. doi: 10.1016/j.eswa.2018.06.024

[21] Chakraborty S, Rao KR. Fingerprint enhancement by directional filtering. International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology; Phetchaburi, Thailand; 2012. pp. 1-4.

[22] Tao H, Chongmin L, Zain JM, Abdalla AN. Robust image watermarking theories and techniques: a review. Journal of Applied Research and Technology 2014; 12 (1): 122-138. doi: 10.1016/S1665-6423(14)71612-8

[23] Lai C, Tsai C. Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Transactions on Instrumentation and Measurement 2010; 59 (11): 3060-3063.

[24] Abraham J, Kwan P, Gao J. Fingerprint matching using a hybrid shape and orientation descriptor. In: Jucheng Y, Norman P (editors). State of the Art in Biometrics. Rijeka, Crotia: Intech Press, 2011, pp. 25-56.

[25] Dorizzi B, Cappelli R, Ferrara M, Maio D, Maltoni D et al. Fingerprint and on-line signature verification competitions. In: Proceedings of the International Conference on Biometrics (ICB); Alghero, Italy; 2009. pp. 725-732.

[26] Thomaz CE, Giraldi GA. A new ranking method for principal components analysis and its application to face image analysis. Image and Vision Computing 2010; 28 (6): 902-913.