Enhancing Security of Fingerprints through Contextual Biometric Watermarking

Afzel Noore, Richa Singh, Mayank Vatsa, and Max M. Houck[†]

Lane Department of Computer Science and Electrical Engineering
[†]*Director, Forensic Science Initiative*
West Virginia University, Morgantown, WV 26506, USA.

Abstract

This paper presents a novel digital watermarking technique using face and demographic text data as multiple watermarks for verifying the chain of custody and protecting the integrity of a fingerprint image. The watermarks are embedded in selected texture regions of a fingerprint image using Discrete Wavelet Transform. Experimental results show that modifications in these locations are visually imperceptible and maintain the minutiae details. The integrity of the fingerprint image is verified through the high matching scores obtained from an Automatic Fingerprint Identification System. There is also a high degree of visual correlation between the embedded images, and the extracted images from the watermarked fingerprint. The degree of similarity is computed using pixel-based metrics and human visual system metrics. The results also show that the proposed watermarked fingerprint and the extracted images are resilient to common attacks such as compression, filtering, and noise.

Key words: Fingerprint identification, watermarking, wavelet transform.

* Corresponding author. Tel.: +1-304-293-0405 ext. 2547. Fax: +1-304-293-8602.
E-mail address: noore@csee.wvu.edu (A. Noore).

1 Introduction

Watermarking is used for hiding information imperceptibly in digital content for protecting its integrity. A number of watermarking techniques are available for embedding information securely in an image [1]. These can be broadly classified as transformation domain techniques [2]-[4] and spatial domain techniques [5]-[6]. Recently watermarking techniques have been used in conjunction with biometric identifiers [7]-[13]. Fingerprints are one of the reliable biometric identifiers that are extensively used for personal identification. Ratha, Connell, and Bolle proposed a blind data hiding method [12], which is applicable to fingerprint images compressed with WSQ (Wavelet-packet Scalar Quantization) standard. The watermark message is assumed to be very small compared to the fingerprint image. The quantizer integer indices are randomly selected and each watermark bit replaces the LSB of the selected coefficient. At the decoder, the LSB's of these coefficients are collected in the same random order to construct the watermark. Jain, Uludag, and Hsu used the facial information as watermark to authenticate the fingerprint image [13]. A bit stream of eigenface coefficients is embedded into selected fingerprint image pixels using a randomly generated secret key. The embedding process is in spatial domain and does not require the original image for extracting the watermark.

In this paper we propose a novel contextual digital watermarking technique using face and demographic text data as multiple watermarks for protecting the evidentiary integrity of fingerprint images. The following sections describe the process of embedding face and text images as watermarks into selected texture regions of the fingerprint image. We verify the matching ability of the watermarked fingerprint and the original fingerprint using an Automatic Fingerprint Identification System (AFIS) and study the resilience to various attacks during transmission.

2 Extraction of Fingerprint Texture Features

Texture is an important feature for the analysis of many types of images. Properties such as roughness, granulation and regularity which do not have smooth varying intensities can be determined through a set of local neighborhood properties of the gray levels of an image region. Multi-scale processing, which humans apply for texture perception is modeled using wavelet analysis [14]. The image features that represent the scale-dependent properties can be extracted from each sub-image separately. A non-linear function that produces the energy of the image when summed over a sub-image is widely used for texture computation. The feature set thus obtained consists of energies of different scales, which is an important characteristic for texture analysis.

A signal $f(x)$ when decomposed using a 1-dimensional wavelet transform into a basis of wavelet functions to obtain the transformed signal, $W_{p,q}$, is given by,

$$W_{p,q}(f(x)) = \int f(x)\psi_{p,q}(x)dx \tag{1}$$

where p and q are scale and position parameters respectively. The basis vectors are obtained by translating and dilating the mother wavelet,

$$\psi_{p,q}(x) = \frac{1}{p}\psi\left[\frac{x-q}{p}\right] \tag{2}$$

The mother wavelet ψ has to be localized in both spatial and frequency domains. A 2-dimensional wavelet transform is obtained by first applying a 1-dimensional transform along the rows and then along the columns. In this paper, a Daubechies filter bank is used to implement the Discrete Wavelet Transform (DWT) resulting in a pyramid structure of sub-bands shown in Fig. 1. The 2-level decomposition consists of seven sub-bands. The sub-bands labeled HH, HL and LH contain the diagonal, horizontal and vertical details of

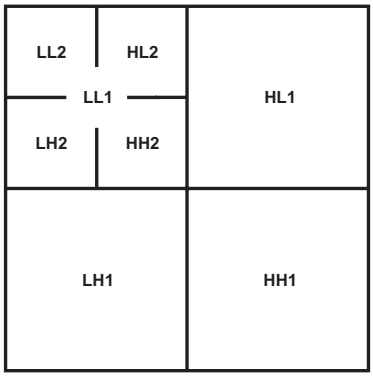

Fig. 1. Two level decomposition using DWT

the fingerprint image respectively, while the LL sub-band contains the coarse details of the image.

The process of obtaining texture features from an image was adopted from [15]. Let I be an N x N input grayscale image in the spatial domain. This image is transformed to frequency domain (W) using DWT. The decomposed image consists of sub-images from which the texture information of the input image at different scale resolution is obtained. The resulting texture feature matrix is of dimension N/r x N/r, where r is the level of decomposition.

The texture map, t_{W_r}, is computed for each input sub-image W_r. The energy of the coefficient combined with the variance of the corresponding coefficients in the lowest LL sub-image represents the texture of that coefficient.

$$t_{W_r}(i,j) = W_r(i,j)^2 + var([LL2(i+1,j+1), LL2(i+2,j+2)] \tag{3}$$

where var is the variance of the two coefficient block and W_r ϵ (HH2, HL2, LH2, HH1, HL1 and LH1).

The background pixels in the texture map have a higher magnitude compared to the pixels representing the actual fingerprint image. The locations in the texture map whose magnitude is less than a predefined threshold, T_{W_r}, compared to its adjacent locations are selected. These selected locations contain-

ing higher texture details are used in our proposed watermarking algorithm. Modification of these coefficients is imperceptible since the most significant coefficients act as a visual mask. The selected texture regions of HH1, HL1 and LH1 sub-bands are denoted by ST_{HH1}, ST_{HL1} and ST_{LH1} and are defined in equation 4.

$$\begin{aligned} ST_{HH1} &= min[t_{HH1}(i,j+1), t_{HH1}(i,j)] \quad if \ \ |t_{HH1}(i,j+1) - t_{HH1}(i,j)| > T_{HH1} \\ ST_{HL1} &= min[t_{HL1}(i,j+1), t_{HL1}(i,j)] \quad if \ \ |t_{HL1}(i,j+1) - t_{HL1}(i,j)| > T_{HL1} \\ ST_{LH1} &= min[t_{LH1}(i,j+1), t_{LH1}(i,j)] \quad if \ \ |t_{LH1}(i,j+1) - t_{LH1}(i,j)| > T_{LH1} \end{aligned} \tag{4}$$

where,

$$\begin{aligned} T_{HH1} &= max(t_{HH1}) - avg(t_{HH1}) \\ T_{HL1} &= max(t_{HL1}) - avg(t_{HL1}) \\ T_{LH1} &= max(t_{LH1}) - avg(t_{LH1}) \end{aligned}$$

The texture maps and the corresponding selected texture regions of HH1, HL1 and LH1 are shown in Fig. 2. The selection of texture regions in the remaining sub-bands are similarly computed.

3 Proposed Watermarking Algorithm

Fingerprint images collected by law enforcement agencies are stored in a database along with the demographic text data of the individual and a facial image. The different data types are usually stored under three different sub categories in a database. The collection, storage and analysis of disparate information introduces problems such as data mismatches and mishandling, high cost of storage, a longer time for retrieval, and unauthorized tampering of the files in the database. Furthermore, these images must be protected from possible network intrusion and manipulation. Maintaining the integrity of fingerprints and chain of custody is extremely impor-

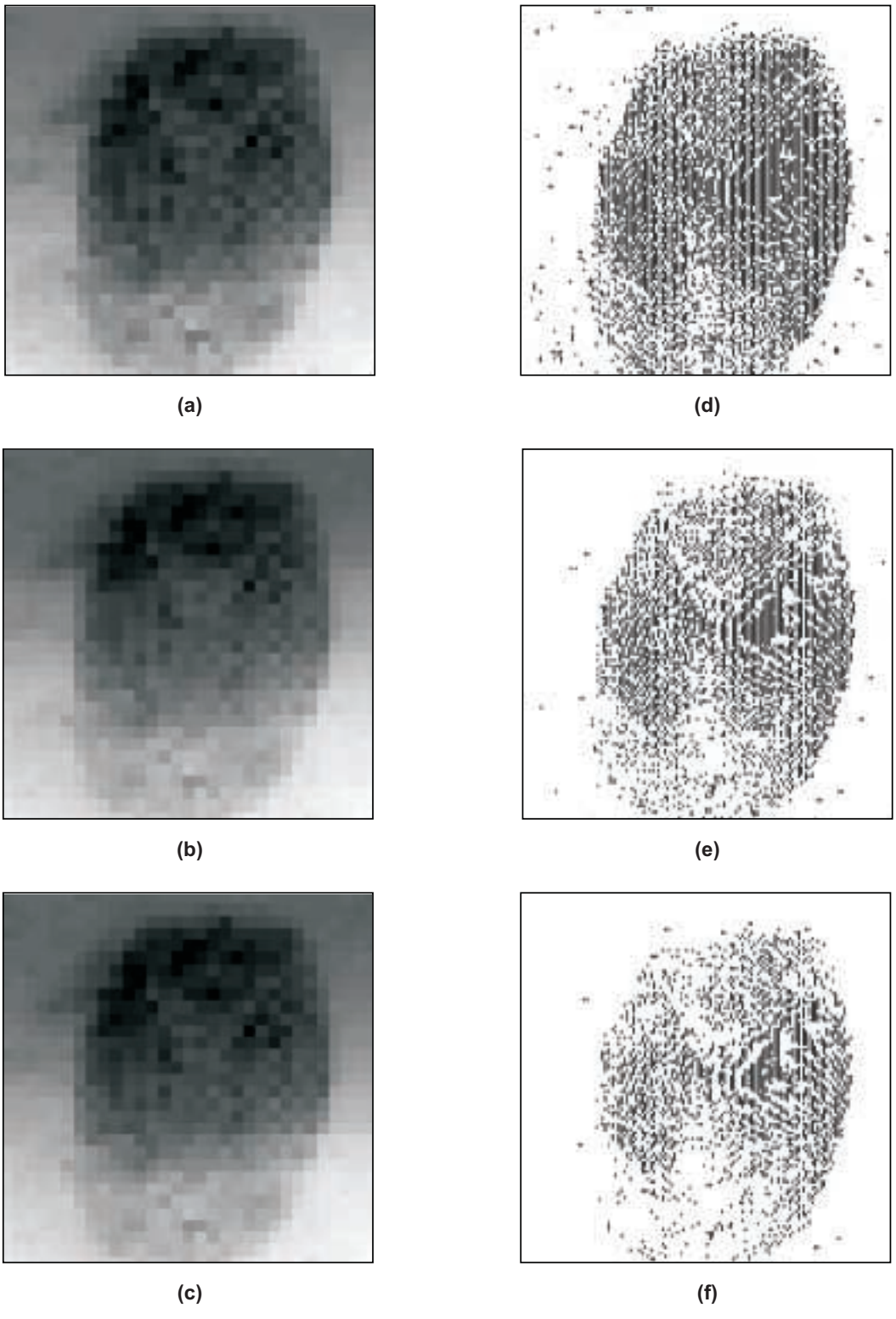

Fig. 2. (a), (b) and (c) are texture maps of LH1, HL1 and HH1 respectively, (d), (e) and (f) are corresponding texture representation

tant especially when it is used in court as evidence. In this paper, the face and text data are used as contextual watermarks and are embedded in the fingerprint image to be authenticated. The grayscale fingerprint image is decomposed using a 2-level Discrete Wavelet Transform to obtain seven sub-bands as shown in Fig. 1. The text and face watermark images are embedded into the wavelet coefficients of the fingerprint image that represent the locations of the selected texture regions. The facial image is in grayscale while the text image is in binary. The sub-image selection for watermarking depends on several factors. The modification of the low frequency sub-image LL2 will impose severe degradation of the reconstructed image as most of the energy is concentrated in this band. During filtering and compression some of the information will be lost in the high frequency bands. One way of overcoming this information loss is by redundantly embedding information in all the high frequency bands (LH1, HL1 and HH1). The three mid-frequency bands (LH2, HL2 and HH2) are good choices for embedding. We embed the grayscale face image into the mid-frequency bands and the binary text image is redundantly embedded into the high frequency bands for increased robustness.

3.1 Embedding the Face Image

The face image is embedded into the wavelet coefficients, Wav^{ST}_{LH2}, Wav^{ST}_{HL2} and Wav^{ST}_{HH2}, which represent the locations of the selected texture regions of LH2, HL2 and HH2 respectively. The size of the facial image is adjusted to be one third of the total number of available embedding locations. Let the face image watermark, w_f, be of size p x q. The grayscale values of the facial watermark image are divided into three bit-streams, L, I, and M, representing the least-significant, the intermediate, and the most-significant integer values respectively as described in equation 5.

$$w_f(i,j) = \sum_{i=1}^{p}\sum_{j=1}^{q} 100 * M(i,j) + 10 * I(i,j) + L(i,j) \tag{5}$$

where, $0 \leq (L, I) \leq 9$ and $0 \leq M \leq 2$. The bit-streams L, I and M are inserted into the lowest order integer of Wav^{ST}_{LH2}, Wav^{ST}_{HL2} and Wav^{ST}_{HH2} respectively. The

embedding of facial integer bit-streams into the wavelet coefficients is described in equation 6.

$$
\begin{aligned}
lowest\_order\_integer(Wav^{ST}_{LH2}(i,j)) &= \sum_{i=1}^{p}\sum_{j=1}^{q} L(i,j) \\
lowest\_order\_integer(Wav^{ST}_{HL2}(i,j)) &= \sum_{i=1}^{p}\sum_{j=1}^{q} I(i,j) \\
lowest\_order\_integer(Wav^{ST}_{HH2}(i,j)) &= \sum_{i=1}^{p}\sum_{j=1}^{q} M(i,j)
\end{aligned}
\tag{6}
$$

3.2 Embedding the Text Image

Next, the binary text image is embedded into the wavelet coefficients, Wav^{ST}_{LH1}, Wav^{ST}_{HL1} and Wav^{ST}_{HH1}, which represent the locations of the selected texture regions of LH1, HL1 and HH1 respectively. The size of the text watermark is made equal to the size of the smallest of three selected texture represented sub-images. The lowest order integers of Wav^{ST}_{LH1}, Wav^{ST}_{HL1} and Wav^{ST}_{HH1} are replaced by the text watermark bits.

Let the size of the text watermark image, w_t, be r x s. The embedding of binary text image into the wavelet coefficients is given by,

$$
\begin{aligned}
lowest\_order\_integer(Wav^{ST}_{LH1}(i,j)) &= \sum_{i=1}^{r}\sum_{j=1}^{s} w_t(i,j) \\
lowest\_order\_integer(Wav^{ST}_{HL1}(i,j)) &= \sum_{i=1}^{r}\sum_{j=1}^{s} w_t(i,j) \\
lowest\_order\_integer(Wav^{ST}_{HH1}(i,j)) &= \sum_{i=1}^{r}\sum_{j=1}^{s} w_t(i,j)
\end{aligned}
\tag{7}
$$

3.3 Generating the Watermarked Fingerprint with Multiple Watermarks

The final watermarked fingerprint image is obtained when the embedded sub-bands are reconstructed using a two-level Inverse Discrete Wavelet Transform (IDWT). A secret key is used to select the embedding locations randomly to secure the original fingerprint and the embedded face and text watermarks from tampering. As part of the implementation of the algorithm we use the perceptual model for varying the watermark images based on the fingerprint image content [16], [17]. An amplifying factor, α, is computed which varies the watermarks such that maximum amount of information can be hidden in the host fingerprint image depending on luminance and contrast properties of the embedding region. In other words, the correlation between the original watermark, w_m, and the embedded watermark, w_a, is made maximum, while keeping the perceptual distance between the original fingerprint and watermarked fingerprint images constant. The best value of α is found by iteratively computing the just noticeable difference for the watermarked fingerprint and reducing this difference to a target value. The embedded watermark is finally obtained using the best value of α defined in equation 8.

$$w_a = \alpha w_m \tag{8}$$

Fig. 3 shows the proposed watermarking algorithm used for embedding the face and the text images in the fingerprint. Our proposed embedding algorithm is implemented using a 512 x 512 fingerprint image as the host image shown in Fig. 4a. Figs. 4b and 4c are the original face image and the original text image used as contextual watermarks. The resulting watermarked fingerprint image is shown in Fig. 4d. This fingerprint image is securely protected and can be used to verify if the chain of custody is maintained or if the fingerprint has been compromised by tampering.

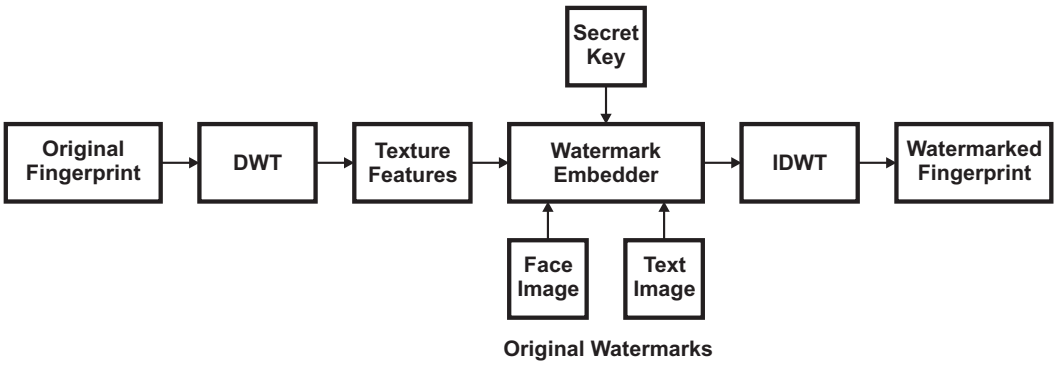

Fig. 3. Proposed face and text watermark embedding algorithm

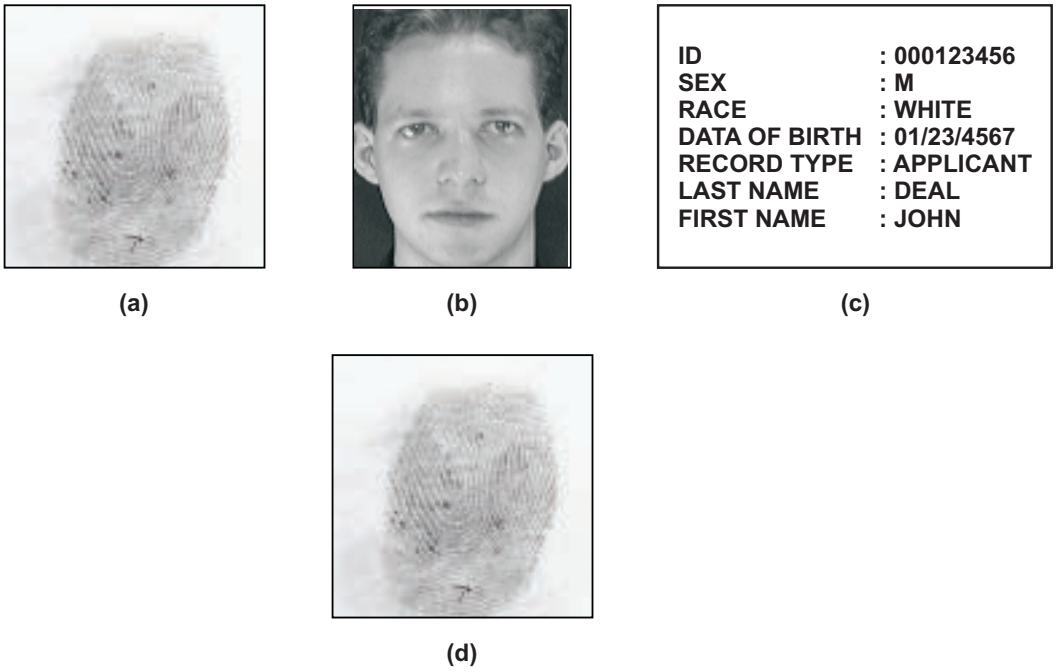

Fig. 4. (a) Original fingerprint, (b) Original face image, (c) Original text image, (d) Watermarked fingerprint

3.4 Matching Performance of the Watermarked Fingerprint

Embedding the facial and demographic text data into the individuals fingerprint image eliminates data mismatch, reduces the high cost of storage, speeds the retrieval of related data, establishes a digital chain of custody, and detects tampering. It is important to ensure that the embedded text and face watermarks do not alter the

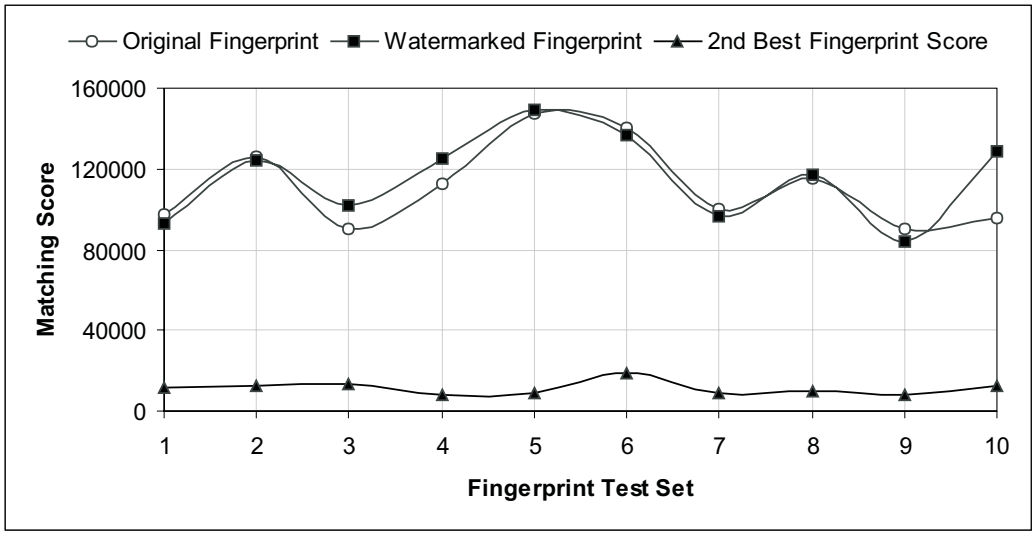

Fig. 5. Matching watermarked fingerprint images on AFIS system [18]

functional integrity of the fingerprint and its ability to detect possible matches. To verify the effect of watermarking on matching fingerprint images, an AFIS system is used [18]. A set of fingerprint images are watermarked with face image and demographic text data using the proposed algorithm. The fingerprint database consists of 2,800,000 prints collected by law enforcement agency and the face images are obtained from AT&T database [19]. The results of the matching scores obtained from the AFIS system are shown in Fig. 5. The high matching scores of the original fingerprint image and the watermarked fingerprint image validate that the fingerprint features such as the ridge bifurcations and ridge endings used for matching purposes have not been altered. The matching score of the next closest fingerprint or the second best fingerprint from the database is so low that it would not be classified as a possible match in the AFIS system.

The electronic transmission of fingerprints over the communication channel introduces degradations in the image data. For example, images are compressed when transmitting large image files over low bandwidth channel; a median filter is used to smooth the image and reduce the data to be transferred by eliminating noise and insignificant structures; and during transmission, some noise is introduced. These effects on the watermarked fingerprint are studied by using various image process-

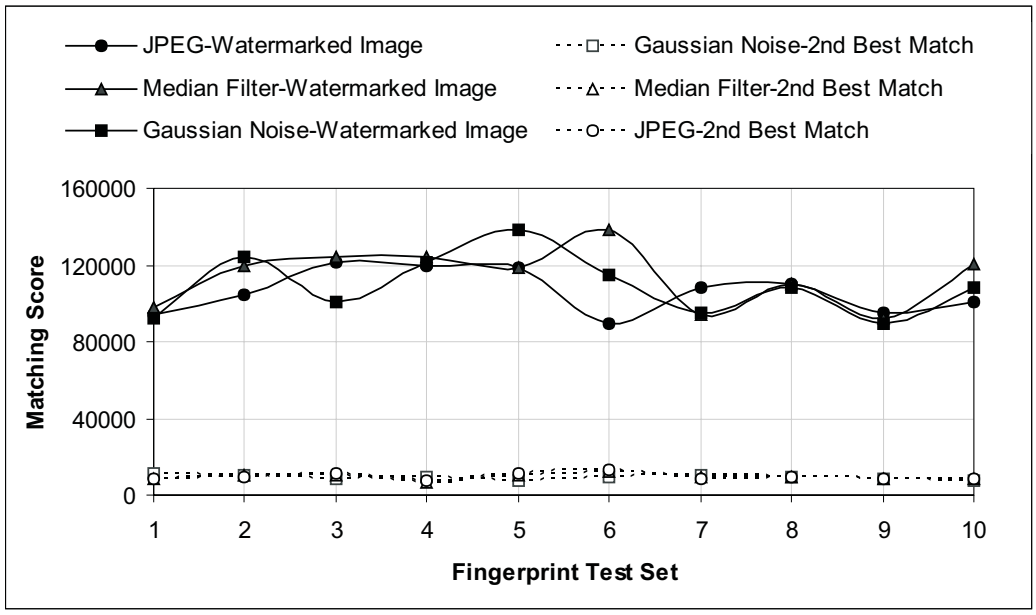

Fig. 6. Matching watermarked fingerprints subjected to various attacks

ing attacks such as JPEG compression at 80%, median filtering with 3 x 3 filter mask, and the addition of Gaussian noise. For each type of attack, the matching score of the watermarked fingerprint image is compared with the matching score of the original fingerprint image and the remaining images in the AFIS database. The results of the attacks are shown in Fig. 6. The results indicate that the watermarked fingerprint is resilient to various attacks and is able to successfully match the original fingerprint. The matching score of the next best fingerprint is so low that the AFIS system would not classify this as a possible match. The results also validate that the proposed embedding technique does not alter the key fingerprint features used in level-2 matching when attacked.

4 Verifying the Integrity of the Watermarked Fingerprint

The watermarked fingerprint has several advantages. One of the main advantages is that the fingerprint, the demographic text information of the individual and the facial image need not be stored in separate databases. The contextual digital watermarking allows all related data to be stored and retrieved at the same time.

From the extracted watermarks, the integrity of the fingerprint can be verified against possible tampering. The retrieval of the facial image and the text data also helps with identification of an individual. The procedure to extract the text and face image is shown in Fig. 7a. The extraction process is the reverse of the embedding process. The same secret key used during embedding is now used to determine the order of extracting the bits. The selected texture region is obtained for all six sub-images and the watermarks are extracted from the lowest order integer of the corresponding sub-images. The spatial redundancy introduced in the high frequency channel during embedding the text watermark ensures reliable extraction when at least two of the three values are the same. Using the same technique, the facial image is extracted from the lower frequency channel. Figs. 7c and 7d show the extracted face and the extracted text images from the watermarked fingerprint image of Fig. 7b. Neither the original fingerprint image nor the original watermark images are required for extraction. The extracted text and face image are of good quality and closely resemble the original images shown in Figs. 4b and 4c.

We next quantitatively determine the degree of similarity between the original watermark images and the extracted watermark images using two different types of metrics. The peak signal to noise ratio (PSNR), mean square error (MSE), and correlation between the original and modified images give the pixel-based similarity between the images. The structural similarity measure (SSIM) [20] and universal image quality index (UIQI) [21] compare the images based on human visual system (HVS). Table 1 shows the degree of similarity between the original images and the extracted images. The similarity values using both the pixel based approach and the human visual system approach show a high level of correlation between the images.

The watermarked fingerprint was shown to be robust and resilient when subjected to various attacks. We next determine the effect of these attacks on the extracted face and text images for identification purposes. Unauthorized tampering or substitution of the fingerprint data can be detected by extracting the watermarks. Since the visual quality of the text and the face images are commonly used for personal identification, it is appropriate to use the human visual metrics for comparison purposes.

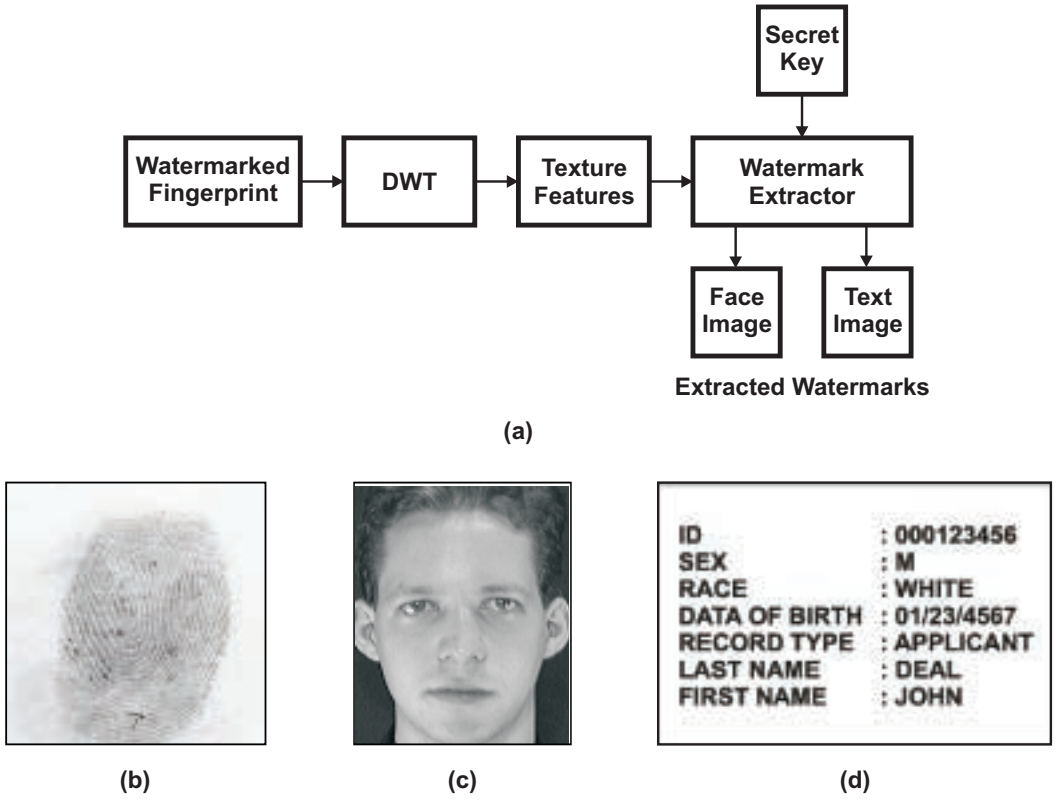

Fig. 7. (a) Extraction process, (b) Watermarked fingerprint, (c) Extracted facial image, and (d) Extracted text image

Table 1
Average image quality metrics

Test Images	PSNR	MSE	Correlation	SSIM	UIQI
Face	70.45	58	0.9861	0.9259	0.9134
Text	58.99	40	0.8641	0.9758	0.9241

Table 2 shows the human visual metrics of the extracted face and text images when the watermarked fingerprint image is subjected to various attacks. Numerical results show that the image quality is high and is suitable for personal identification and verifying the chain of custody. The proposed contextual watermarking approach using face and text images to watermark a fingerprint is useful for authenticating the integrity of the fingerprint. The contextual watermarking is novel because the watermarked fingerprint image is compact and takes less memory space compared to the space occupied by individual images. Furthermore, the time taken to search

different databases to obtain all pertinent information corresponding to an individual in greatly minimized since each fingerprint image has the demographic text and face image embedded as watermarks and can be easily extracted.

5 Conclusion

In this paper, a contextual fingerprint image watermarking algorithm is proposed. Two watermarks, a facial image and the corresponding demographic text data of an individual are embedded into selected texture regions of fingerprint image using Discrete Wavelet Transform. The watermarked fingerprint provides added protection from tampering and the fingerprint matching ability is not affected even when subjected to common attacks. For extracting the embedded face and text images, the original images are not required. Quantitative results show that the extracted face and text images are of high quality and provide additional information for identification purposes. Using the proposed approach, the absence of watermarks or visual distortions in the extracted watermarks would reveal that the integrity of the fingerprint image has been compromised.

Table 2
Average visual metrics for extracted images when the watermarked fingerprint is attacked

Attacks	Extracted Face Image		Extracted Text Image	
	SSIM	UIQI	SSIM	UIQI
Cropping	0.7223	0.6597	0.7320	0.7017
Rotation	0.8365	0.8106	0.7843	0.7539
JPEG Compression	0.8944	0.8831	0.9374	0.8840
Gaussian Noise	0.8831	0.8799	0.9469	0.8713
Median Filtering	0.8802	0.8705	0.9407	0.8345

Acknowledgements

This research (Award No. 2003-RC-CX-K001) was supported by the Office of Science and Technology, National Institute of Justice, Office of Justice Programs, US Department of Justice. The authors thank Sagem Morpho for donating the AFIS system and 2,800,000 fingerprints used in performing this research.

References

[1] T. Liu, Z.-D. Qiu, The survey of digital watermarking-based image authentication techniques, *6th International Conference on Signal Processing*, Vol. 2, 2002, pp. 1556-1559.

[2] Y. Wang, J.F. Doherty, R.E. Van Dyck, A wavelet-based watermarking algorithm for ownership verification of digital images, *IEEE Transactions on Image Processing*, 11(2) (2002) 77-88.

[3] R. Tay, J.P. Havlicek, Image watermarking using wavelets, *45th Midwest Symposium on Circuits and Systems*, Vol. 3, 2002, pp. 258-261.

[4] M.-S. Hsieh, D.-C. Tseng, Y.-H. Huang, Hiding digital watermarks using multiresolution wavelet transform, *IEEE Transactions on Industrial Electronics*, 48(5) (2001) 875-882.

[5] R. Bangaleea, H.C.S. Rughooputh, Performance improvement of spread spectrum spatial-domain watermarking scheme through diversity and attack characterization, *IEEE 6th Africon Conference*, Vol. 1, 2002, pp. 293-298.

[6] D.P. Mukherjee, S. Maitra, S.T. Acton, Spatial domain digital watermarking of multimedia objects for buyer authentication, *IEEE Transactions on Multimedia*, 6(1) (2004) 1-15.

[7] A.K. Jain and U. Uludag, Hiding fingerprint minutiae in images, *Proceedings of Third Workshop on Automatic Identification Advanced Technologies (AutoID)*, 2002, pp. 97-102.

[8] V. Claus, S. Ralf, Approaches to biometric watermarks for owner authentication, *Proceedings of SPIE*, Vol. 43, No. 14, 2001, pp. 209-219.

[9] A.K. Jain, U. Uludag, Hiding biometric data, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(11) (2003) 1494-1498.

[10] M. Vatsa, R. Singh, A. Noore, Improving biometric recognition accuracy and robustness using DWT and SVM watermarking, *IEICE Electronics Express*, 2(12) (2005) 362-367.

[11] M. Vatsa, R. Singh, A. Noore, M.M. Houck, K. Morris, Robust biometric image watermarking for fingerprint and face template protection, *IEICE Electronics Express*, 3(2) (2006) 23-28.

[12] N.K. Ratha, J.H. Connell, R.M. Bolle, Secure data hiding in wavelet compressed fingerprint images, *International Multimedia Conference, Proceedings of the 2000 ACM workshop on Multimedia*, 2000, pp. 127-130.

[13] A.K. Jain, U. Uludag, R.-L. Hsu, Hiding a face in a fingerprint image, *Proceedings of International Conference on Pattern Recognition*, Vol. 3, 2002, pp. 756-759.

[14] M. Kociolek, A. Materka, M. Strzelecki, P. Szczypinski, Discrete wavelet transform - derived features for digital image texture analysis, *Proceedings of International Conference on Signals and Electronic Systems*, 2001, pp. 163-168.

[15] A.S. Lewis, G. Knowles, Image compression using the 2-D wavelet transform, *IEEE Transaction on Image Processing*, 1(2) (1992) 244-250.

[16] A. Noore, N. Tungala, M.M. Houck, Embedding biometric identifiers in 2D barcodes for improved security, *Journal of Computers and Security*, 23(82) (2004) 679-686.

[17] C.I. Podilchuk, W. Zeng, Image-adaptive watermarking using visual models, *IEEE Journal on Selected Areas in Communications*, 16(4) (1998) 525-539.

[18] www.morpho.com

[19] www.uk.research.att.com/facedatabse.html

[20] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, Image quality assessment: From error measurement to structural similarity, *IEEE Transactions on Image Processing*, 13(4) (2004) 600-612.

[21] Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, A universal image quality index, *IEEE Signal Processing Letters*, 9(3) (2002) 81-84.