Improving biometric recognition accuracy and robustness using DWT and SVM watermarking

Mayank Vatsa, Richa Singh, and Afzel Noore[a)]

West Virginia University, Morgantown, WV, 26506

a) *noore@csee.wvu.edu*

Abstract: This paper presents a novel biometric watermarking algorithm for improving the recognition accuracy and protecting the face and fingerprint images from tampering. Multi-resolution Discrete Wavelet Transform is used for embedding the face image in a fingerprint image. An intelligent learning algorithm based on v-Support Vector Machine (SVM) is introduced to enhance the quality of the extracted face image. The performance of the watermarking algorithm is experimentally validated using existing fingerprint and face recognition algorithms. The results show that the extracted fingerprint and face images are of high quality. The use of SVM enhances the performance of face recognition by at least 10% even when the watermarked image is subjected to certain geometric and frequency attacks such as scaling, cropping, compression and filtering.

Keywords: watermarking, biometrics, support vector machine, DWT

Classification: Science and engineering for electronics

References

[1] A. K. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," *IEEE Trans. PAMI*, vol. 19, no. 4, pp. 302–314, 1997.

[2] Y.-H. Pang, A. Teoh B. J., and David Ngo C. L., "Enhanced pseudo Zernike moments in face recognition," *IEICE Electron. Express*, vol. 2, no. 3, pp. 70–75, 2005.

[3] A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Trans. PAMI*, vol. 25, no. 11, pp. 1494–1498, 2003.

[4] L. Shutao, T. K. James, W. T. Ivor, and W. Yaonan, "Fusing images with different focuses using support vector machines," *IEEE Trans. Neural Networks*, vol. 15, no. 6, pp. 1555–1561, 2004.

[5] B. Schölkopf, A. Smola, R. Williamson, and P. L. Bartlett, "New support vector algorithms," *Neural Comput.*, vol. 12, no. 5, pp. 1207–1245, 2000.

[6] O. de Vel and S. Aeberhard, "Line based face recognition under varying pose," *IEEE Trans. PAMI*, vol. 21, no. 10, pp. 1081–1088, 1999.

DOI: 10.1587/elex.2.362
Received April 15, 2005
Accepted May 18, 2005
Published June 25, 2005

1 Introduction

Biometric based personal authentication system is emerging as an attractive alternative to password based authentication. Fingerprint [1], face [2], iris and hand geometry are widely used as biometric features for authentication. A critical problem is to ensure the integrity and security of biometric data. Jain and Uludag [3] have discussed sources of attacks that are possible in a generic biometric system and have shown that watermarking can be effectively used to protect biometric templates. We propose a novel biometric image watermarking algorithm where the face image is embedded in the fingerprint using DWT and υ-SVM is used to enhance the quality of the extracted face image. We evaluate the performance of our proposed biometric watermarking algorithm using a database of face and fingerprint images from 150 individuals. Experimental results show that the integration of SVM approach in the proposed biometric watermarking algorithm improves the recognition accuracy and is resilient to different attacks.

2 Proposed Watermark Embedding and Extraction Algorithm

Let $FP_{original}$ be the original fingerprint image of size $n \times n$ and $FP_{dwt}(i,j)$ be the corresponding four level discrete wavelet transformed image, where $i = 1,2,3,4$ denotes the wavelet decomposition level and $j = a,h,v,d$ denotes the approximation, horizontal, vertical and diagonal sub-bands respectively. Let $FA_{original}$ be the original face image of size m x m, where $m \leq n$ and $FA_{dwt}(i,j)$ be the corresponding two level wavelet transformed image with $i = 1,2$. At level-2, the coefficients of approximation band of the face image are embedded into the detail sub-bands of the fingerprint image. A random key K_1 is used to embed the coefficients in the possible $3{*}N{*}N$ locations, where N is the length and width of the sub-bands. Embedding at level-2 is described in Equation (1a).

Next, the approximation band in the second level of the face image is further decomposed to the third level. At level-3, the coefficients of the approximation band of the face image are embedded into the detail sub-bands of the fingerprint image using another random key K_2 whose upper bound is $3{*}M{*}M$. M is the height and width of sub-bands at level-3. Equation (1b) describes the watermark embedding process at level-3.

The inverse wavelet transformation is performed on the modified $FP_{dwt}(i,j)$ to obtain the final watermarked fingerprint image FP_{wm}. Figure 1 shows the process of embedding face image in the fingerprint image.

$$FP_{dwt}(2,j) = \begin{cases} FA_{dwt}(2,a) & \textit{according to } K_1 \\ FP_{dwt}(2,j) & \textit{elsewhere} \end{cases} \tag{1a}$$

$$FP_{dwt}(3,j) = \begin{cases} FA_{dwt}(3,a) & \textit{according to } K_2 \\ FP_{dwt}(3,j) & \textit{elsewhere} \end{cases} \tag{1b}$$

Two face images are extracted from the watermarked fingerprint image FP_{wm}, by applying discrete wavelet transform to three levels. At level-2 using

DOI: 10.1587/elex.2.362
Received April 15, 2005
Accepted May 18, 2005
Published June 25, 2005

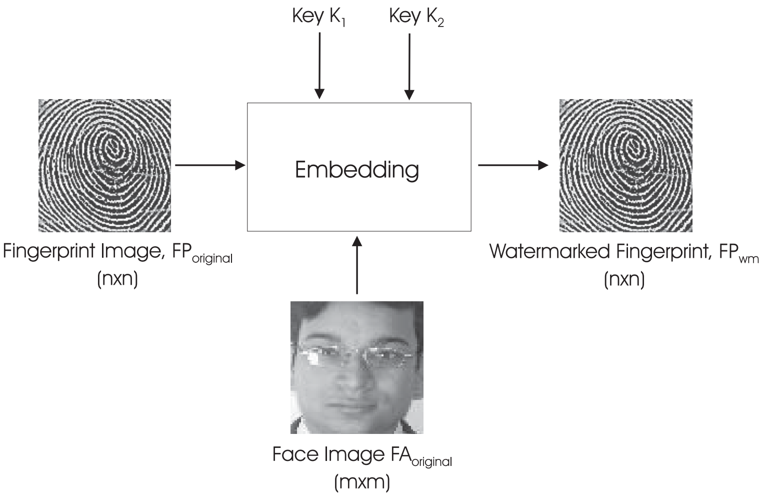
Key K_1
Key K_2
Embedding
Fingerprint Image, $FP_{original}$ (nxn)
Watermarked Fingerprint, FP_{wm} (nxn)
Face Image $FA_{original}$ (mxm)

Fig. 1. Embedding face image in fingerprint

key K_1 the embedded face coefficients are first located and the inverse Discrete Wavelet Transform (IDWT) is applied linearly to obtain the extracted face, $FA1_{extracted}$. Similarly, at level-3 using key K_2 the embedded face coefficients are located and the inverse Discrete Wavelet Transform (IDWT) is applied to obtain the extracted face, $FA2_{extracted}$. The fingerprint image is extracted by applying nonlinear IDWT to get $FP_{extracted}$. Figure 2 shows the extraction process.

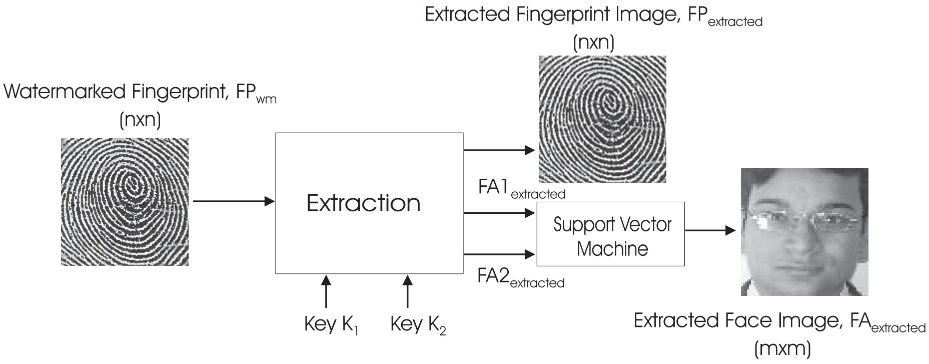
Extracted Fingerprint Image, $FP_{extracted}$ (nxn)
Watermarked Fingerprint, FP_{wm} (nxn)
Extraction
$FA1_{extracted}$
Support Vector Machine
$FA2_{extracted}$
Key K_1
Key K_2
Extracted Face Image, $FA_{extracted}$ (mxm)

Fig. 2. Extraction of fingerprint image and generation of face image from two face images obtained at level-2 and level-3

3 Proposed Image Quality Enhancement Using SVM

Attacks on the watermarked fingerprint image FP_{wm} causes various degrees of distortion in the two extracted face images, $FA1_{extracted}$ and $FA2_{extracted}$. We propose using an intelligent learning algorithm based on Support Vector Machine to train and classify the pixel quality from corresponding locations of extracted multi-resolution face images when subject to attacks such as filtering, compression, cropping, noise and nonlinear deformations of the gray scale. The fusion algorithm [4] uses face image $FA1_{extracted}$ obtained from

DOI: 10.1587/elex.2.362
Received April 15, 2005
Accepted May 18, 2005
Published June 25, 2005

level-2 and face image $FA2_{extracted}$ obtained from level-3 to generate a higher quality face image, $FA_{extracted}$. The fusion algorithm uses υ-SVM which is expressed as:

$$f(x) = \operatorname{sgn}\left(\sum_{i=1}^{m} \alpha_i y_i k(x, x_i) + b\right) \tag{2}$$

$$\sum_{i=1}^{m} \alpha_i y_i = 0 \quad \text{and} \quad \sum_{i=1}^{m} \alpha_i \geq \upsilon$$

where $\upsilon \in [0,1]$, x_i is the input to the υ-SVM, y_i is the corresponding output, m is the number of tuples, α_i is the dual variable and k is the RBF kernel [5]. The fusion algorithm that selects pixels from two multi-level redundant face images to generate a higher quality image is described as follows:

1. Face images, $FA1_{extracted}$ and $FA2_{extracted}$, are decomposed to three levels using discrete wavelet frame transform [4].

2. Higher coefficients of both the wavelet transformed images are used to calculate the weighted average window based activity, which is given as input to the υ-SVM. A total of 18 activity levels are computed and provided as input to the υ-SVM.

3. The SVM is trained to determine if the coefficients from image $FA1_{extracted}$ or image $FA2_{extracted}$ should be used. At any position (p, q) the output $O(p, q)$ of υ-SVM is 1 if $FA1_{extracted}$ is less distorted than $FA2_{extracted}$; otherwise the output $O(p, q)$ of υ-SVM is -1.

4. Testing is performed over the whole image using the trained υ-SVM. If the υ-SVM output $O(p, q)$ is positive, the coefficients for the detail and approximation sub-bands of the fused image at this pixel location are selected from image $FA1_{extracted}$, otherwise the pixel location from image $FA2_{extracted}$ is used. The final extracted face image $FA_{extracted}$ is calculated as:

$$FA_{extracted} = \begin{cases} coeff\,(FA1_{extracted}) & if \quad O(p,q) > 0 \\ coeff\,(FA2_{extracted}) & if \quad O(p,q) < 0 \end{cases} \tag{3}$$

5. The final extracted fused image, $FA_{extracted}$, is reconstructed using inverse DWT.

4 Experimental Results and Performance Validation

The performance of a watermarking algorithm, in general, is computed based on measures such as peak signal-to-noise ratio, mean square error, normalized cross correlation, and histogram similarity. However, for a biometric watermarking algorithm, the most important performance metric is the recognition accuracy. Fingerprint recognition algorithm [1] and face recognition algorithm [6] are used to calculate the verification accuracy, V, at every stage.

© IEICE 2005
DOI: 10.1587/elex.2.362
Received April 15, 2005
Accepted May 18, 2005
Published June 25, 2005

The verification accuracy of the fingerprint and the face are calculated using Equations 4 and 5 respectively.

$$V(FP) = \frac{V(FP_{original}) + V(FP_{wm}) + V(FP_{extracted})}{3 * V(FP_{original})} \tag{4}$$

$$V(FA) = \frac{V(FA_{original}) + V(FA_{extracted})}{2 * V(FA_{original})} \tag{5}$$

The value of the verification accuracy for face, $V(FA)$, and the verification accuracy for fingerprint, $V(FP)$, ranges from 0 to 1. Higher values denote that the integrity of the biometric data is not compromised due to watermarking or subsequent attacks.

The proposed watermarking algorithm is tested on the face and the fingerprint database. This database contains 750 frontal face (512 × 512) and 750 fingerprint (512×512) images from 150 individuals. Images of each individual are collected during three different sessions. Images from the first session are used for training while images from the other two sessions are used for testing. Table I shows the verification accuracy of the fingerprint $V(FP)$, the verification accuracy of the extracted face image $V(FA1_{extracted})$ from level-2, the verification accuracy of the extracted face image $V(FA2_{extracted})$ from level-3, and the verification accuracy of the combined fused image $V(FA_{extracted})$ generated using υ-SVM.

The results show that the verification accuracy, $V(FA_{extracted})$, of the proposed biometric watermarking algorithm closely matches the verification accuracy of the images when there are no attacks. For blurring, scaling, and rotation, $V(FA1_{extracted})$ performs better than $V(FA2_{extracted})$; while for

Table I. Performance of the Proposed Biometric Watermarking Algorithm

Attack	Verification Accuracy			
	$V(FP)$	$V(FA1_{extracted})$	$V(FA2_{extracted})$	$V(FA_{extracted})$ using υ-SVM
No Attack	1.00	0.91	0.90	1.00
Blurring (3 × 3)	1.00	0.86	0.83	0.99
Scaling (1:1.5)	1.00	0.89	0.82	0.98
Rotation (10^0)	1.00	0.88	0.83	0.98
JPEG 2000 (50%)	1.00	0.87	0.86	0.99
JPEG (50%)	1.00	0.79	0.85	0.97
Distortion (20^0)	0.99	0.86	0.88	0.96
Filtering (3 × 3)	1.00	0.84	0.89	0.99

DOI: 10.1587/elex.2.362
Received April 15, 2005
Accepted May 18, 2005
Published June 25, 2005

compression, distortion, and filtering, $V(FA2_{extracted})$ performs better than $V(FA1_{extracted})$. However, $V(FA_{extracted})$ generated with υ-SVM performs the best among the three face images on all attacks.

5 Conclusion

In this paper, we propose a novel algorithm for protecting biometric fingerprint and face images from tampering. We use Discrete Wavelet Transform to robustly hide the face image in the fingerprint image using watermarking techniques. We also propose using a SVM-based learning algorithm to select the best quality pixels from two extracted face images to generate a high quality image. The results show that the proposed algorithm is resilient to geometric and frequency attacks and the integration of SVM before the final face extraction improves the face recognition accuracy by at least 10%.

Acknowledgments

This research (Award No. 003-RC-CX-K001) was supported by the Office of Science and Technology, National Institute of Justice, United States Department of Justice.

DOI: 10.1587/elex.2.362
Received April 15, 2005
Accepted May 18, 2005
Published June 25, 2005