ELectronics EXpress

IEICE Electronics Express, Vol.3, No.2, 23–28

Robust biometric image watermarking for fingerprint and face template protection

Mayank Vatsa[1], Richa Singh[1], Afzel Noore[1a)], Max M. Houck[2], and Keith Morris[2]

[1] *West Virginia University, Morgantown, WV, 26506*

[2] *Forensic Science Initiative, West Virginia University, Morgantown, WV, 26506*

a) *noore@csee.wvu.edu*

Abstract: This paper presents a combined DWT and LSB based biometric watermarking algorithm that securely embeds a face template in a fingerprint image. The proposed algorithm is robust to geometric and frequency attacks and protects the integrity of both the face template and the fingerprint image. Experimental results performed on a database of 750 face and 750 fingerprint images show that the algorithm has the advantages of both the existing DWT and LSB based algorithms. A multimodal biometric algorithm is used as a metric to evaluate the combined performance of both face and fingerprint recognition.

Keywords: watermarking, biometrics, DWT

Classification: Science and engineering for electronics

References

[1] F. Petitcolas, R. Anderson, and M. Kuhn, "Information hiding - A Survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[2] A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 25, no. 11, pp. 1494–1498, 2003.

[3] M. Vatsa, R. Singh, and A. Noore, "Improving biometric recognition accuracy and robustness using DWT and SVM watermarking," *IEICE Electron. Express*, vol. 2, no. 12, pp. 362–367, 2005.

[4] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," *Int. Conf. on Acoustic, Speech and Signal Processing*, vol. 5, pp. 2969–2972, 1998.

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

[6] R. Singh, M. Vatsa, and A. Noore, "Textural feature based face recognition for single training images," *IEE Electron. Lett.*, vol. 41, no. 11, pp. 23–24, 2005.

[7] A. Ross and A. K. Jain, "Information Fusion in Biometrics," *Pattern Recogn. Lett.*, vol. 24, no. 13, pp. 2115–2125, 2003.

DOI: 10.1587/elex.3.23
Received December 08, 2005
Accepted December 19, 2005
Published January 25, 2006

ELectronics EXpress

IEICE Electronics Express, Vol.3, No.2, 23–28

1 Introduction

Biometrics based authentication systems have inherent advantage over traditional personal identification techniques. A critical problem is to ensure the security and integrity of biometric data. In [2] and [3], watermarking based approaches have been proposed to make the biometric system secure and resilient to deliberate manipulations and attacks. There has been limited performance study on the integrity and robustness of biometric data when subjected to different attacks. In this paper a novel biometric watermarking algorithm is designed to mitigate the vulnerabilities of a biometric system caused due to both geometric and frequency attacks. A watermarked fingerprint is created by embedding a template or face image in the fingerprint image using a combination of wavelet and LSB based watermarking techniques. Wavelet based watermarking techniques are resistant to frequency attacks but are susceptible to geometric attacks. On the other hand, LSB based watermarking algorithms are robust to geometric attacks but are vulnerable to frequency attacks. The proposed algorithm synergistically combines the advantages of wavelet and LSB based techniques such that it is robust to both geometric and frequency attacks [4].

The performance of the proposed algorithm is validated using biometric verification algorithms [5, 6] when the watermarked fingerprint is subjected to different types of attacks. The sum rule based multimodal algorithm [7] is further used as a metric to evaluate the combined performance of the fingerprint and face recognition system.

2 Proposed Watermarking Algorithm

For watermarking, the fingerprint image is used as the base or the cover image and the facial features are used as the watermark. These features are the face template [5] obtained by convolving the face image with 2D Gabor filter. The algorithm is divided into two parts, watermark embedding and watermark extraction.

2.1 Watermark Embedding Algorithm

Step 1: Two-level Discrete Wavelet Transform (DWT) is applied on the original fingerprint image I. The coefficients of the approximation band of the DWT image contain significant details of the fingerprint image. Hence the approximation band is not modified during embedding or extraction.

Step 2: The detailed sub-bands are divided into blocks $I_1, I_2, \ldots, I_r$ of size $M \times N$ and the coefficients in each block are numbered in raster scan order. From each block, the first wavelet coefficient that has a positive phase and whose value is less than threshold η is selected. The second LSB of the selected coefficient is replaced by one bit from the facial template. This process is written as follows:

DOI: 10.1587/elex.3.23
Received December 08, 2005
Accepted December 19, 2005
Published January 25, 2006

$$I'_w(i,j) = \begin{cases} LSB_2(I_w(i,j)) = F(x,y) \\ \qquad if\ Phase(I_w(i,j)) \geq 0 \quad \& \quad I_w(i,j) < \eta \\ I_w(i,j) \\ \qquad if\ Phase(I_w(i,j)) < 0 \end{cases} \tag{1}$$

where $I'_w(i,j)$ are the wavelet coefficients in block I_r. $F(x,y)$ is the face template, $I_w(i,j)$ is the wavelet decomposed fingerprint image, η is the threshold which decides whether the watermark bit is inserted or not, and LSB_2 denotes the second LSB.

Step 3: If the number of bits in the face template $F(x,y)$ is less than the number of blocks in the fingerprint image, then all bits of the face template can be embedded. Otherwise, the following procedure is used to embed the remaining bits of the face template:

(a) For each block I_r, a message block MB_r is formed by selecting few high order bits from each pixel of I_r. A key K is appended to message block MB_r. The value K is sufficiently large to prevent an attacker from using brute force to remove the watermark.

(b) The key K is used to compute a cryptographic hash of the message block

$$H_r = H(MB_r)K \tag{2}$$

(c) The value of $[H_r \bmod (M \times N)]$ gives the pixel position for embedding the watermark bit. The watermark bit is embedded depending on the value of the most significant bit (MSB) of the hash value H_r.. If the MSB of H_r is 0 then the facial bit is inserted unchanged; otherwise the complement of the facial bit is inserted.

Step 4: After embedding all the bits from the face template, Inverse Discrete Wavelet Transformation (IDWT) is applied on the watermarked fingerprint coefficients to generate the final secure watermarked fingerprint image. Fig. 1 shows the watermark embedding process.

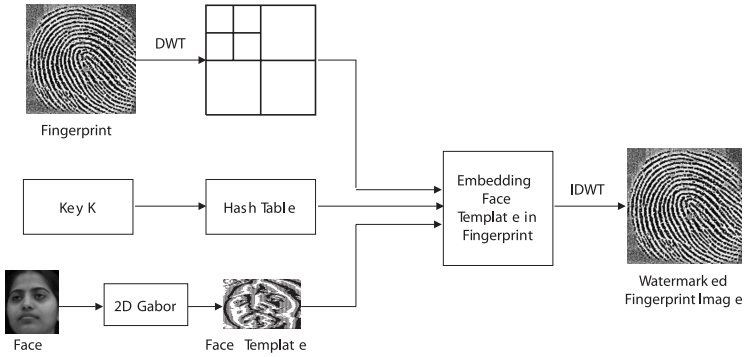

Fig. 1. Watermark Embedding Process

DOI: 10.1587/elex.3.23
Received December 08, 2005
Accepted December 19, 2005
Published January 25, 2006

Any change in the value of I_r produces an entirely different hash and can make the watermark undetectable. Since the attacker does not know the key K, it is not possible to compute the hash value H_r. Also, high order bits are chosen for watermark insertion because any change in these values will degrade the quality of the image and hence the biometric verification performance.

2.2 Watermark Extraction Algorithm

Step 1: The image is first synchronized with the block boundaries. The synchronization is performed corresponding to the blocks of size $M \times N$ formed during the embedding process. DWT is first applied on the image and the detailed sub-bands are divided into blocks of size $(2M-1) \times (2N-1)$.

Step 2: For each block of size $M \times N$, the following steps are performed for synchronization of block boundaries:

(a) Similar to the embedding process, a corresponding message block MB_r is formed by selecting few high order bits from each pixel of that block and a key K is appended to it.

(b) The cryptographic hash of MB_r is computed as before using Equation 2.

(c) The synchronized block boundaries are identified by comparing the last few bits of the hash value H_r with the LSBs of pixels in every block and its neighboring blocks.

Step 3: From each synchronized block, the first coefficient with positive phase and whose value is less than the threshold η is identified. The watermark bit is extracted from this coefficient.

Step 4: The remaining bits of the watermark are extracted by computing the pixel position for each block where the bit was embedded. The pixel positions are calculated using the expression $[H_r \bmod (M \times N)]$. The MSB of H_r is analyzed to determine if the actual value or its complement was inserted and the bit is extracted.

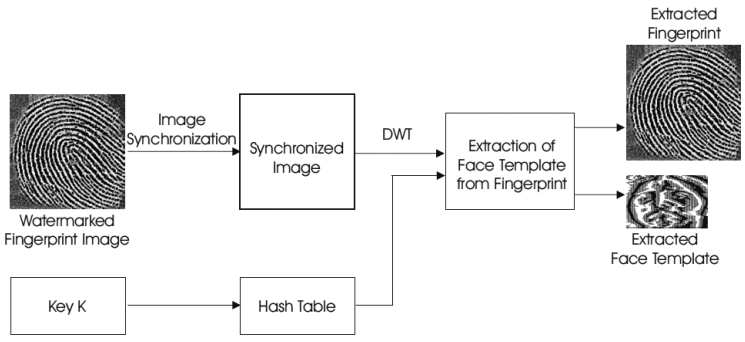

Fig. 2. Watermark Extraction Process

DOI: 10.1587/elex.3.23
Received December 08, 2005
Accepted December 19, 2005
Published January 25, 2006

Step 5: These extracted bits are arranged to form the facial template and IDWT is applied on the fingerprint image to generate the watermark extracted fingerprint image. Fig. 2 shows the extraction process of the fingerprint and the face template from the watermarked fingerprint image.

3 Experimental Results

The proposed algorithm is validated on a database containing 750 frontal face images and 750 fingerprint images from 150 individuals. The size of face images is 128 × 128 and the size of fingerprint images is 512 × 512. Two face and two fingerprint images per person are used for training the recognition algorithm and the rest of the three face and three fingerprint images are used for testing. The performance of the proposed watermarking algorithm is evaluated using fingerprint, face, and multimodal biometrics verification algorithms. The fingerprint verification algorithm is based on minutiae matching as described in [5], and the face templates are matched using the texture based face verification algorithm described in [6]. Sum rule based multimodal biometric verification algorithm described in [7] is used to obtain the combined matching score of face and fingerprint.

We tested the fingerprint and face recognition performance when the watermarked fingerprint image is subjected to different frequency attacks such as JPEG and JPEG 2000 compression, gaussian noise, median filtering, blur-

Table I. Verification accuracy of extracted biometric images when the watermarked fingerprint image is attacked

Algorithm / Attacks	LSB Algorithm [1]			DWT Algorithm [4]			Proposed Algorithm (DWT+LSB)		
	Finger -print	Face	Multi modal	Finger -print	Face	Multi modal	Finger -print	Face	Multi modal
No Attack	98.94	94.78	99.57	98.94	92.16	99.41	98.94	94.16	99.48
JPEG (50 %)	98.94	0.00	0.00	98.94	90.87	99.10	98.94	91.42	99.25
JPEG 2000 (50 %)	98.94	0.00	0.00	98.94	91.41	99.39	98.94	92.89	99.36
Gaussian Noise (3 x 3)	96.56	0.00	0.00	98.10	91.22	99.18	98.10	91.67	99.21
Median Filter (3 x 3)	94.23	0.00	0.00	94.12	47.63	64.81	94.12	69.21	85.33
Blurring (3 x 3)	97.11	42.32	61.22	97.02	89.65	97.99	97.11	91.45	99.02
Gamma (0.5)	98.94	86.47	92.19	98.94	92.16	99.36	98.94	92.16	99.48
Cropping (10 pixels)	98.94	91.92	99.01	97. 99	53.69	80.28	97.99	89.65	98.83
Resize (90 %)	98.94	89.01	97.34	95.13	51.77	76.91	98.06	88.90	98.59
Rotation (10^0)	98.94	98.99	98.10	94.66	45.23	74.08	98.70	89.41	98.25
Affine Transform	91.76	74.31	88.29	91.20	25.62	67.45	92.13	75.29	90.68

DOI: 10.1587/elex.3.23
Received December 08, 2005
Accepted December 19, 2005
Published January 25, 2006

ring and gamma correction. The watermarked fingerprint is also subjected to geometric attacks such as cropping, resizing, rotation, and affine transformation. Table I summarizes the verification performance of LSB-based watermarking, DWT-based watermarking, and the proposed watermarking algorithm. For each algorithm, experiments are performed to determine the recognition accuracy of fingerprint, face, and multimodal combination of fingerprint and face. Under normal conditions, when there is no attack, the verification accuracy using all three algorithms for fingerprint, face and the multimodal approach yielded high performance. The multimodal verification performance gives a comprehensive metric that combines the performance of both fingerprint recognition and face recognition.

Using this metric, Table I shows that for geometric attacks such as cropping, resizing, rotation, and affine transformation, the LSB-based algorithm performs at least 18% better than the DWT algorithm. However, for frequency based attacks such as JPEG, JPEG 2000 compression, gaussian noise, median filtering, and blurring, the DWT-based algorithm outperforms the LSB algorithm. The LSB-based algorithm is sensitive to frequency attacks. As a consequence, the experimental results show the poor face recognition performance. The biometric verification accuracy of the proposed watermarking algorithm shows that the performance is more robust and resilient to a comprehensive set of attacks compared to either DWT or LSB based algorithms. Table I also shows that the multimodal performance of the proposed algorithm is comparable to or exceeds the performance of DWT or LSB based algorithms for both frequency and geometric attacks.

4 Conclusion

DWT watermarking is resilient to frequency attacks whereas LSB based watermarking is resilient to geometric attacks. This paper presents a novel biometric image watermarking algorithm which synergistically combines the DWT and LSB based algorithms for improved robustness and resiliency when subjected to both geometric and frequency attacks. We use a biometric multimodal algorithm as a metric to evaluate the combined performance of both fingerprint and face recognition. Experimental results show that the proposed watermarking algorithm is more robust to geometric and frequency attacks compared to either the LSB or DWT based techniques. The proposed algorithm also protects the integrity of both the face template and the fingerprint image.

Acknowledgments

This research is supported through a grant (Award No. 2003-RC-CX-K001) from the Office of Science and Technology, National Institute of Justice, Office of Justice Programs, United States Department of Justice.

DOI: 10.1587/elex.3.23
Received December 08, 2005
Accepted December 19, 2005
Published January 25, 2006