Priority Watermarking-Based Face-Fingerprint Authentication System

Tuan Hoang
School of Computer Sciences and Engineering
International University
Ho Chi Minh City, Vietnam
htatuan@hcmiu.edu.vn

Dat Tran, Dharmendra Sharma, Trung Le
Faculty of Information Sciences and Engineering
University of Canberra
Canberra, Australia
dat.tran@canberra.edu.au

Bac H. Le
Faculty of Information Technology
University of Science
Ho Chi Minh City, Vietnam

***Abstract*— In this paper, we propose a multi-biometrics authentication system based on our proposed priority-based watermarking method. We investigate how watermarking techniques affect the container, which is facial image used in further authentication steps. We conduct experiments on facial and fingerprint features using both priority-based watermarking method and non-priority-based method. Results show that the proposed priority-based watermarking method has reduced data retrieval errors from the facial image after decoding, thus it has also reduced authentication error rates.**

***Keywords:* priority-based watermarking, fingerprint, multi-biometrics authentication**

I. INTRODUCTION

Biometric authentication has recently received great interest from computer science researchers. With its unique characteristics, biometric authentication is believed to be a reliable authentication method in the near future [9]. However, on the way it becomes true, Ratha et al [12] shows that impostors can do at least 8 types of attacks onto the biometrics authentication system. From that finding, researches have been proposing several ways to enhance authentication system's security. Among those, using digital watermarking to secure template stores and data communication between client and server is widely used, especially in network environment. Moreover, this method can be used for multi-biometrics authentication system in which one or more biometrics can be embedded into other biometrics for improving accuracy and reducing bandwidth. For robust watermarking, RDWT watermarking [4] is used to embed voice features of a person, MFCC, into the same person's face image; DWT and SVM watermarking [5] is used to embed face image into a fingerprint image of the same person; FFT-based watermarking [6] is used to embed iris features into a face image; and a non-uniform Discrete Fourier Transform-based watermarking [7] is used to embed fingerprint image into audio signals. For fragile watermarking, amplitude modulation watermarking proposed in [1] and then enhanced in [2, 3] to embed information into a color facial image.

The paper is the continuing work of [3] by using our proposed watermarking method called priority-based watermarking to embed one's fingerprint into his face for face-fingerprint authentication system. The paper is organized as follows. Section 1 reviews watermarking methods and its appliance into multi-biometrics. Section 2 introduces our framework for remote multimodal biometrics authentication system. Section 3 briefly presents the priority-based watermarking method. Section 4 presents experiments to conduct using real fingerprint and facial databases, comparing our proposed method and original amplitude modulation method. Finally, we conclude in Section 5.

II. FRAMEWORK FOR REMOTE MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM

We propose a new framework for remote multimodal biometric authentication system.

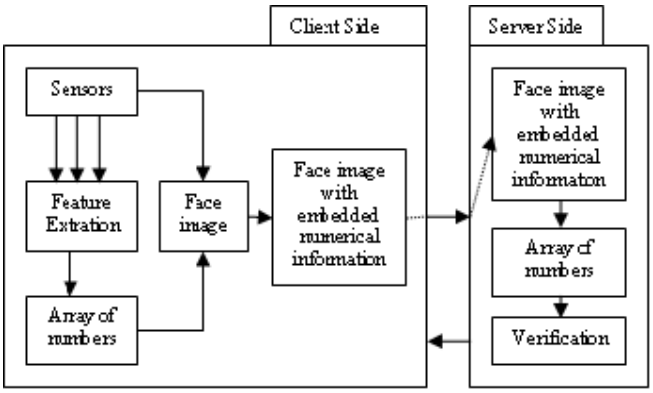

Figure 1. The proposed framework.

In our framework, at the client side, biometric features need to be extracted to numerical values and then embedded into a face image before securely transmitted to a verified server. At the server side, the watermarked face image is decoded to retrieve the biometric features for verification. The verification result is then sent back to the client side. This framework has some advantages as follows

- Facial image is the only biometric that is understandable by human-beings and watermarked face image is not sensible to human eyes so they can manually verify if needed.
- All other biometric features are numbers whose formats are not included, so attackers need to know numeric format to convert the retrieved bit sequence

978-0-7695-3922-5/09 $26.00 © 2009 IEEE
DOI 10.1109/ICIMT.2009.44

to the right sequence of numbers and to know from what biometric these numbers were extracted**.**

- The framework can be applied to any biometrics.
- Easier for encoding and decoding cause of uniform representation.

Specifically, in this paper, at the client side, we extract one's fingerprint features and then embed them, which are numerical values, into the same person's face image by using priority-based watermarking before transmitting the watermarked facial image to server. At server side, one fingerprint and two facial images of each registered user are stored for later authentication. We also use other non-error watermarking algorithm to securely store them

III. PRIORITY-BASED WATERMARKING METHOD

Let $I(m, n)$ be a color image of size $m \times n$. If the RGB color system is used, then $I(m, n) = \{R(m, n), G(m, n), B(m, n)\}$. Let $S = (s_1, s_2, \ldots, s_k)$ be the bit sequence of size k to be embedded in the image I, and $I'(m, n) = \{R'(m, n), G'(m, n), B'(m, n)\}$ be the image obtained after embedding S into the image I. Let $Pri(S)$ be the bit priority function in S. The original amplitude modulation-based digital watermarking method embeds bits by modifying the blue channel in the color image I. Each bit in S will be embedded d times at different positions in the image I. The blue channel is chosen because human eyes are least sensitive to it comparing with the red or the green ones. Therefore

$$I'(m, n) = \{R(m, n), G(m, n), B'(m, n)\} \quad (1)$$

Encoding Process: A pseudo-random position sequence $p = (p_1, p_2, \ldots, p_{d\times k})$, where $p_{(t-1)*d+h} = (i, j)$ representing row and column indices at which bit s_t is embedded the h-th time, is chosen to embed the bit sequence S. The sequence p is randomly generated by a pseudo-random generator based on a given secret key K, which is used as a seed to the generator. The t-th bit in the bit sequence S will be embedded in the blue channel of the image I at d positions $p_{(t-1)*d+h}$, …, p_{t*d} according to the following equation

$$B'_{i,j} = B_{i,j} + s_t q L_{i,j} \quad (2)$$

where $L_{i,j}$ is luminance at the position (i, j) and can be calculated as follows

$$L_{i,j} = 0.299R_{i,j} + 0.587G_{i,j} + 0.144B_{i,j} \quad (3)$$

and q is a tradeoff between robustness and invisibility.

At decoding step, $B'_{i,j}$ will be estimated by its neighbour pixels, which is called $B''_{i,j}$, *as Formula 4*. It can be seen that the closer $B''_{i,j}$ and $B_{i,j}$ are, the more accurate the bit retrieval is. In other words, the more accurate the linear combination approximation of $B_{i,j}$ is, the lower error of bit retrieval is, and so the better the position (i, j) is. In our proposed method, we will embed high priority level bits at the best positions to guarantee that we can retrieve them later with the lowest error. To determine goodness of positions, a gradient should be used. We propose to use Pewit operator cause of its efficiency and fast computation.

–1	–1	–1
0	0	0
1	1	1

Pewitt op. Px for Gx

–1	0	1
–1	0	1
–1	0	1

Pewitt op. Py for Gy

The lower the gradient at a position is, the better the position is. The values Gx and Gy are calculated as

$$Gx_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} B_{i+di,j+dj} Px_{di+2,dj+2} \right)$$
$$Gy_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} B_{i+di,j+dj} Py_{di+2,dj+2} \right)$$
$$G_{i,j} = \sqrt{Gx_{i,j}^2 + Gy_{i,j}^2} \quad (4)$$

If the difference between the pixels in a small neighbor block of the pixel (i, j) is small enough, we can replace the blue channel by another channel for gradient calculation. In this paper, we choose the green channel.

$$Gx_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} G_{i+di,j+dj} Px_{di+2,dj+2} \right)$$
$$Gy_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} G_{i+di,j+dj} Py_{di+2,dj+2} \right)$$
$$G_{i,j} = \sqrt{Gx_{i,j}^2 + Gy_{i,j}^2} \quad (5)$$

Not all types of image satisfy above condition, but our experiments in Table 1 on facial images show that in facial images the blue channel has high and positive correlations with the two other channels, especially between blue and green channels.

TABLE I. CORRELATION BETWEEN CHANNELS IN FACIAL IMAGES OF CVL FACE DATABASE [10] AND AR FACE DATABASE[8]. (R: RED, B:BLUE, G:GREEN)

	CVL			**AR**		
	R-G	R-B	B-G	R-G	R-B	B-G
min	0.81	0.74	0.92	0.32	0.40	0.65
max	0.99	0.98	1.00	1.00	0.99	1.00
mean	0.95	0.92	0.99	0.96	0.89	0.97

The position sequence p will be rearranged according to the increasing of gradient. The bits whose priority level is from high to low will be embedded sequentially.

Decoding Process: Based on the secret key K, the sequence p will be regenerated as shown in the encoding process. The gradient at each position needs to be calculated and depending on these gradient values, the sequence p will be rearranged.

$$Gx'_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} R'_{i+di,j+dj} \, Px_{di+2,dj+2} \right)$$

$$Gy'_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} R'_{i+di,j+dj} \, Py_{di+2,dj+2} \right)$$

$$G'_{i,j} = \sqrt{Gx'^{2}_{i,j} + Gy'^{2}_{i,j}} \quad (6)$$

As $G = G'$, we have $G'_{i,j} = G_{i,j}$ at all position (i, j). Therefore the sequence p after rearranging is the same in both the encoding and decoding processes. After rearranging the position sequence, further steps are conducted as the original method represented by the equations (7), (8), (9), and (10). The embedded information is retrieved.

$$B''_{i,j} = \frac{1}{8} \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} B'_{i+di,j+dj} - B'_{i,j} \right) \quad (7)$$

$$\delta_{i,j} = B'_{i,j} - B''_{i,j} \quad (8)$$

$$\bar{\delta}_t = \frac{1}{d} \sum_{t=1}^{d} (B'_{p(t-1)d+i} - B''_{p(t-1)*d+i}) \quad (9)$$

$$s'_t = sign(\bar{\delta}_t) \quad (10)$$

IV. Experimental Results

We conducted two experiments to compare the original amplitude modulation method and our proposed one. In the first experiment, we embedded fingerprint features into face images and then retrieved fingerprint features for uni-modal authentication based on fingerprint recognition. In the second experiment, we do the same thing by embedding fingerprint features into face images but use both fingerprint features and facial features after decoding for face-fingerprint multi-modal authentication. The first experiment shows us how watermarking technique affects original fingerprint features in authenticating result, by discarding face, the container. The second experiment shows how accuracy a combined face-fingerprint authentication system is. We conducted both two experiments based on AR Face Dataset and VeriFinger Company's fingerprint database. We assumed that there is no relation between face and fingerprint of one person so that we can create one multi-modal database from two distinct single-modal databases: AR Face database and VeriFinger's fingerprint database.

For the first experiment, we use all 51 fingers in Verifinger fingerprint database. Each finger has 8 samples. Totally, it has 408 fingerprint samples. Firstly, all fingerprint minutiaes are extracted by using method in [11]. Each minutiae consisting of coordinates and angle, in form (x, y, θ) then be embedded into a random image from DBF2 of AR-Face database. We can see that the more bits we use to represent a minutiae feature, the worse performance decoding phase has. In order to improve watermarking accuracy for both methods, we used 12-bit unsigned integer to represent x, y, and θ. A 12-bit unsigned integer is enough for covering all values of x, y, and θ. Secondly, we decode to retrieve minutiae information and use them for fingerprint authentication proposed by Ratha et al [12]. Then they are retrieved to do fingerprint authentication. We also embed each fingerprint's minutiaes into each face image 5 times to eliminate dependence on random sequence of positions.

TABLE II. Errors For Priority and Non-Priority Methods

	Priority		*Non-Priority*	
Bin	*Frequency*	*Cumulative*	*Frequency*	*Cumulative*
0	0	0.00%	15	3.68%
1	101	24.75%	1	3.92%
2	100	49.26%	0	3.92%
3	41	59.31%	1	4.17%
4	16	63.24%	1	4.41%
5	13	66.42%	1	4.66%
6	10	68.87%	0	4.66%
7	8	70.83%	0	4.66%
8	9	73.04%	4	5.64%
9	13	76.23%	0	5.64%
10	9	78.43%	0	5.64%
More	88	100.00%	385	100.00%

It is seen from Table 2 that when applying the priority-based method, above 78% errors produce error value less than or equal to 10, whereas only nearly 6% errors produce the same error value when applying the non-priority one.

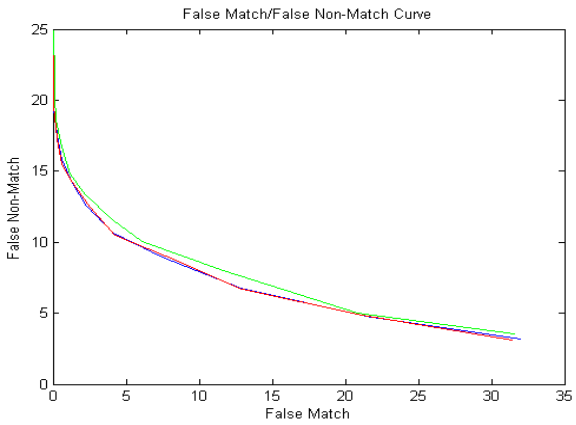

Figure 2. FM/FNM curves (blue: no watermarking, red: priority watermarking, green: non-priority watermarking).

Figure 2 shows FM/FNM curves after doing verification at three different ways: 1) no watermarking, 2) watermarking with priority-based method and 3) watermarking with non-priority method. It is seen that the curves of the first and the second methods are nearly identical whereas the third has higher FNM rate compared with the two others. It proves that our proposed method produce verification accuracy as good as no watermarking and better than non-priority method.

For the second experiment, in enrollment step, each user was asked to submit two face images and one fingerprint. We randomly chose 36 fingerprints from VeriFinger's finger print database and 36 pairs of face of the same user from DBF2 of AR Face dataset. From face images, we trained face recognition system by using a PCA-based method. In authenticating step, each user was asked to provide his face image in which his fingerprint features are embedded.

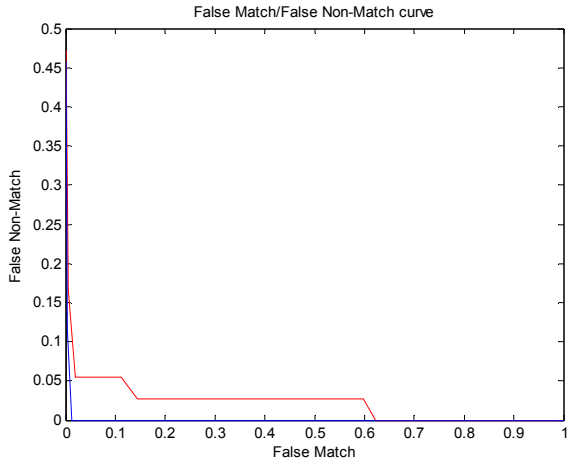

Figure 3. False Match/False Non-Match curves (red: original method; blue: priority-based method).

There are two fragile watermarking methods we need to make comparisons: 1) original amplitude modulation watermarking method and 2) our proposed priority-based amplitude modulation one. Firstly, we extracted users' fingerprint features from fingerprint image by using a Gabor filter-based method. Then each user's fingerprint features were embedded into his face image accordingly by each of testing watermarking methods. The watermarked image then was sent to the server where we retrieved embedded fingerprint features. As a result, it made the original face image changed. We then did face recognition based on PCA with two face images: one image retrieved by original amplitude modulation technique and one image retrieved by our proposed priority-based technique. To compare their performance we calculate False Match versus False Non-Match curve (Figure 3).

It can be seen that our proposed method nearly preserve the original face image and far better than the original amplitude modulation method.

V. CONCLUSION

We have proposed a new framework for securing multimodal biometrics authentication system in which a new digital watermarking method based on amplitude modulation and priority level of bits plays a key role. Following significant error reduction on embedded features by using our proposed priority-based fragile watermarking method, we now prove that it can preserve the original container, in this case the face image. The face image after retrieving embedded finger features is nearly the same with the original face image before embedding in aspect of recognition result by using a popular PCA-based face recognition method.

REFERENCES

[1] Kutter, M., Jordan, F. and Bossen, F.: "Digital Watermarking of Color Images Using Amplitude Modulation," *Journal of Electronic Imaging*, 7(2), 326 – 332 (1998)

[2] Amornraksa, T. and Janthawongwilai, K.: "Enhanced images watermarking based on amplitude modulation," *Image and Vision Computing*, 24(2), 111 – 119 (2006)

[3] Tuan Hoang, Dat Tran, and Dharmendra Sharma, **"**Remote Multimodal Biometric Authentication Using Bit Priority-Based Fragile Watermarking", *International Conference of Pattern Recognition 2008*, Tampa, Florida, USA, 12/2008.

[4] Vatsa, M. et al.: "Feature based RDWT watermarking for multimodal biometric system," *Image Vis. Comput. (2007)*, doi:10.1016/j.imavis.2007.05.003

[5] Vatsa, M.; Singh, R.; Noore, A.: "Improving biometric recognition accuracy and robustness using DWT and SVM watermarking," *IEICE Electronics Express*, Vol. 2, No. 12, 362 – 367 (2005)

[6] Park, K. R. et al; "A study on iris feature watermarking on face data," *ICANNGA 2007*, Part II, LNCS 4432, pp. 415 – 423, 2007.

[7] Khan, M. K. et al: "Robust hiding of fingerprint-biometric data into audio signals," *ICB 2007*, LNCS 4642, pp. 702 – 712, 2007.

[8] A.M. Martinez and R. Benavente, "The AR face database," CVC Tech. Report #24, 1998.

[9] A. K. *Jain*, L. Hong, and. S. Pankanti, "*Biometrics Identification,*". *Communications of the ACM*, Vo1.43, No.2, pp.91-98, February 2000.

[10] Peter Peer, CVL Face Database, http://lrv.fri.uni-lj.si/facedb.html.

[11] P. D. Kovesi. The University of Western Australia. http://www.csse.uwa.edu.au/~pk/research/matlabfns/.

[12] Nalini K. Ratha , Jonathan H. Connell , Ruud M. Bolle, "An Analysis of Minutiae Matching Strength", *Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication*, p.223-228, June 06-08, 2001.