Remote Multimodal Biometric Authentication Using Bit Priority-Based Fragile Watermarking

Tuan Hoang, Dat Tran, Dharmendra Sharma
University of Canberra, Faculty of Information Sciences and Engineering, Australia
{tuan.hoang, dat.tran, dharmendra.sharma}@canberra.edu.au

Abstract

We propose a new remote multimodal biometric authentication framework based on fragile watermarking for transferring multi-biometrics over networks to server for authentication. A facial image is used as a container to embed other numeric biometrics features. The proposed framework enhances security and reduces bandwidths. In order to reduce error rates from embedding numeric information, we also propose a new method to determine bit priority level in a bit sequence representing the numerical information to be embedded and combine with the current amplitude modulation watermarking method.

1. Introduction

A number of watermarking techniques, including both robust and fragile watermarking, have been applied to remote multimodal biometric verification to enhance security and to reduce bandwidths. For example, RDWT [4], DWT and SVM [5], FFT-based watermarking [6], and a non-uniform Discrete Fourier Transform-based watermarking [7]. All of the above watermarking methods are classified as robust watermarking, which are proved to be resistant to possible attacks, such as compression or transformation. Meanwhile, some authors have tried to use another watermarking method which is called fragile watermarking and is more efficient but less assistant to attacks than robust watermarking to hide information. The most popular fragile watermarking method is amplitude modulation watermarking proposed in [1] and then enhanced in [2] to embed information into a color facial image. To combine strengths of robust and fragile watermarking, dual watermarking [8] is used to protect fingerprint features in a remote verification.

Most of the above-mentioned watermarking methods are used to embed non-numerical information, such as images or sequence of bits [5, 6, 7, 1, 2] and do not emphasize on embedding numerical information [4]. There is a need for embedding numerical information in biometrics authentication applications for security reasons and bandwidth reduction. For example, voice, fingerprint, and iris features are numeric.

In this paper, we propose a new framework for transferring multi-biometrics over fixed or remote networks in which facial image is used as a container to embed other biometrics converted to numeric features before they are sent to server for authentication. The proposed framework can enhance security of communicating on remote verification because attackers need to know numeric format to convert the retrieved bit sequence to the right sequence of numbers and to know from what biometric these numbers were extracted**.** Moreover, because current watermarking methods cannot handle the numerical information, we also propose a new method to determine bit priority level in the bit sequence representing the numerical information to be embedded. High priority bits should be embedded at good positions in the image container to achieve low retrieval errors. We then compare the proposed method with the current amplitude modulation watermarking method. We performed a number of experiments to evaluate the proposed framework and method in both simulated numbers and a real fingerprint database. Experimental results show a significant error reduction.

978-1-4244-2175-6/08/$25.00 ©2008 IEEE

2. Proposed framework for remote multimodal biometric authentication

We propose a new framework for remote multimodal biometric authentication system. In our framework, at the client side, biometric features are extracted to numerical values and then embed into a face image before securely transmit to a server. At the server side, the watermarked face image is decoded to retrieve the biometric features for verification. The result is 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 hidden format numbers, so attackers cannot convert the retrieved bit sequence to the right number sequence and know from what biometric these numbers were extracted**.**
- The framework can be applied to any biometrics.
- Easier for encoding and decoding because of uniform representation.

3. Amplitude modulation and bit priority level-based digital watermarking

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 $B''_{i,j}$. It can be seen that the closer $B''_{i,j}$ and $B_{i,j}$, the more accurate the bit retrieval. In other words, the more accurate the linear combination approximation of $B_{i,j}$, the lower error of bit retrieval, and so is the better the position (i,j). 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 is used. We propose to use Pewit operator because of its efficiency and fast computation.

The lower the gradient at a position, the better the position. 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 the above condition, our experiments show that in facial images, the blue channel has high and positive correlations with the two other channels, especially the correlation between blue and green channels as shown in Table 1. The bits whose priority levels are from high to low will be embedded sequentially.

Table 1. Correlation between channels in facial images of CVL face database [11] and AR Face database[12].

	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

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.

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

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

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

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 to retrieve information are conducted as follows

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

$$\delta_{i,j} = B'_{i,j} - B''_{i,j} \tag{8}$$

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

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

4. Experimental results

We conducted two experiments to compare the original amplitude modulation method and our proposed one. In the first experiment, a random array of numbers was generated and then embeded into a well-known image of Mona Lisa. In the second experiment, we embedbed fingerprint features into face images and then retrieved fingerprint features for authentication. Both non-priority and priority-based methods were applied.

In the first experiment, we generated several arrays of the same random 32-bit integers. We used the same random integer value for all experiments for easily comparing results. The integer was repeated in those arrays m times, where $m \in \{100, 150, 200, \ldots, 400\}$. Each bit was embedded at different d positions. In our experiments, d took the three values 5, 10, and 15. Table 2 shows the ratios of embedded pixels over total pixels for each experiment. Some experiments had ratios greater than 100%. We used them to find out whether or not that embedding one bit at several positions could enhance the quality of retrieval even the image size was small. The simplest priority function value for the i-th bit in the bit sequence S representing an integer would be of the form $Pri(s_i) = i$. We represented these integers as sequences of 4 bytes, i.e. 32 bits, therefore i would be from 1 to 32.

To eliminate its dependence on the random sequence of positions, for each experiment, we embedded the array 5 times in 5 different random sequences of positions in the image and then took the average of their error results.

Table 2. Ratios (%) of embedded pixels over total pixels

Size of Array	Number of positions for embedding		
	5	10	15
100	13.89%	27.78%	41.67%
150	20.83%	41.67%	62.50%
200	27.78%	55.56%	83.33%
250	34.72%	69.44%	104.17%
300	41.67%	83.33%	125.00%
350	48.61%	97.22%	145.83%
400	55.56%	111.11%	166.67%

The error was calculated as the absolute difference between the embedded integer and retrieved integer. As other experiments in amplitude modulation-based watermarking, the tradeoff q was set to 0.1.

$$AbsoluteError = \sum \left| RA_i - OA_i \right| \tag{11}$$

where RA was the retrieved array and OA was the original array (embedded array).

We also computed the distributed error over all element of the array as follows

$$DErr(\%) = \frac{AbsoluteError}{ArraySize * Value} * 100 \tag{12}$$

It is seen from Figure 1 that the error obtained from the proposed method is not quite different from the original method if the array size is less than 150, but it is significantly better when the array size increases.

Table 3 shows *DErr* for all experiments. It is seen that all *DErr* is acceptable and practical in the case the ratios of embedded pixels and total pixels of the image is less than 100%. When the ratios of embedded pixels and total pixels of the image are greater than 100%, the average error is not stable and unpredictable.

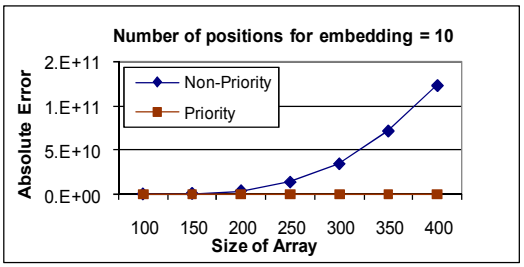

Figure 1. Comparisons on absolute error (Eq. 11) between original and priority-based methods with integer v = 814724.

Table 3. Distributed error (%) over all array elements

Size of Array	Number of positions for embedding		
	5	10	15
100	0.0670%	0.0001%	0.0000%
150	0.0055%	0.0000%	0.0000%
200	0.1315%	0.0000%	0.0000%
250	0.0542%	0.0000%	0.1030%
300	0.0032%	0.0007%	0.0862%
350	0.0932%	0.2419%	18.8278%
400	0.0315%	0.0003%	2.2405%

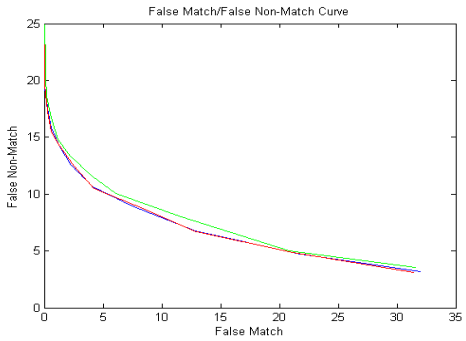

Figure 2. FM/FNM curves (blue: no watermarking, red: priority watermarking, green: non-priority watermarking)

In the second experiment, we used fingerprint database of VeriFinger company and AR-Face database. Verifinger fingerprint database consists of 51 fingers and each finger has 8 samples, so there are 408 fingerprint samples. In the first stage, all fingerprint minutiaes were extracted using method in [9]. Each minutiae consisted of coordinates and angle, in the form of (x, y, θ) and was embedded into a random image from DBF2 of AR-Face database. To improve watermarking accuracy for both methods, we used 12-bit unsigned integer to represent x, y and θ. In the second stage, we retrieved minutiae information and used them for fingerprint authentication using the method proposed in [10]. We embeded each fingerprint's minutiaes into each face image 5 times to eliminate the dependence on random positions sequence.

Figure 2 shows False Match / False Non-Match (FM/FNM) curves after performing verification in three different ways: 1) no watermarking (blue curve), 2) watermarking with priority-based method (red curve) and 3) watermarking with non-priority method (green curve). It is seen that our proposed method does not increase the verification error rate while the non-priority method does.

5. Conclusion

We have proposed a new framework for remote multimodal biometric verification system, and a new digital watermarking method based on amplitude modulation and priority level of bits for numerical information hiding problems. While inheriting security characteristics such as anti-attack from the original method, and reducing the bandwidths for transferring over networks, the proposed method also significantly reduces error comparing with the non-priority method.

6. References

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

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

[3] S. Voloshynovskiy et al, *Attacks on digital watermarks: classification, estimation based attacks, and benchmarks*, IEEE Comm Magazine, 39(8), 118 – 126, 2001

[4] Vatsa, M. et al., *Feature based RDWT watermarking for multimodal biometric system*, Image Vis. Comput., 2007

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

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

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

[8] T. Kim et al, *Secure remote fingerprint verification using dual watermarks*, LNCS 3919, pp.217 – 227, 2006

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

[10] N. Ratha, K. Karu, S. Chen, A. Jain, *A Real-time Matching System for Large Fingerprint Databases*. IEEE Trans. PAMI, 18(8):799-813, 1996

[11] F. Solina, P. Peer, B. Batagelj, S. Juvan, J. Kovac, *Color-based face detection in the "15 seconds of fame" art installation*, Proc. Conf Comp Vision, INRIA, 38-47, 2003