

Block Pyramid Based Adaptive Quantization Watermarking for Multimodal Biometric Authentication

Bin Ma¹, Chunlei Li^{1,3}, Yunhong Wang¹, Zhaoxiang Zhang¹ and Yiding Wang²

¹*School of Computer Science and Engineering, Beihang University, China*

²*School of Information Engineering, North China University of Technology, China*

³*School of Electronic and Information Engineering, Zhongyuan University of Technology, China*
 {mabin, lichunlei1979}@cse.buaa.edu.cn, {yhwang, zxzhang}@buaa.edu.cn, ydwang1985@yahoo.cn

Abstract

This paper proposes a novel robust watermarking scheme to embed fingerprint minutiae into face images for multimodal biometric authentication. First, a block pyramid is layered according to the block-wise face region distinctiveness estimated by Adaboost; upper level indicates informative spacial regions. Then, we adopt a first-order statics QIM method to perform watermark embedding in each pyramid level. Numeric watermark bits with higher priority are embedded into upper pyramid level with a larger embedding strength. By joint differentiation of host image regions and watermark bits priority, our scheme achieves a trade-offs among watermarking robustness, capacity and fidelity. Experimental results demonstrate that our approach guarantees the robustness of hidden biometric data, while preserving the distinctiveness of host biometric images.

1. Introduction

Biometric authentication systems have inherent advantages over traditional identification techniques. However, while biometric data provide uniqueness, they do not provide secrecy themselves [4]. Thus, establishing the security and integrity of biometric data has become a critical issue. As cryptography is not fully capable to address this problem [4], digital watermarking has emerged to cover its shortages.

Embedding imperceptible watermark within the host content, digital watermarking can provide further protection even after decryption. Due to such advantages, numerous work has been done on biometric watermarking, and the existing schemes could be divided into three categories according to the role of biometric data in a watermarking system:

- **Embedding biometric:** Employing biometric as watermark to replace the unique identifier in traditional watermarking (*e.g.* embedding signature code in host image for copyright protection [6]);
- **Watermarking biometric:** Introducing traditional watermark to assist a biometric host (*e.g.* applying copyright symbol to indicate biometric owner, or hash sequence for integrity authentication);
- **Multi-biometrics watermarking:** Embedding one kind of biometric data into another biometric host (*e.g.* hiding face in fingerprint [4], voice in face [7]) to provide additional authentication.

However, rather less attention has been paid to the essential difference between traditional watermark and biometric watermark: the former is a binary stream without bit priority (*e.g.* binary logo, hash sequence) while the latter is numeric feature, whose bits have different importance. To our knowledge, only Hoang proposed a priority based numeric embedding method in [2], considering that high priority bits should be embedded at good positions in the image container to achieve low retrieval errors. In this paper, we will further discuss the numeric embedding topic.

2. Principles

As for biometric data, the most important quality metric is distinctiveness. In order to control the distortion introduced by watermarking, embedding position and strength should be chosen adaptively according to feature analysis.

Although much previous work [4, 7] has been devoted to preserve recognition quality by avoiding watermarking region-of-interest (ROI), we argue that ROI is more appropriate for watermark embedding for two

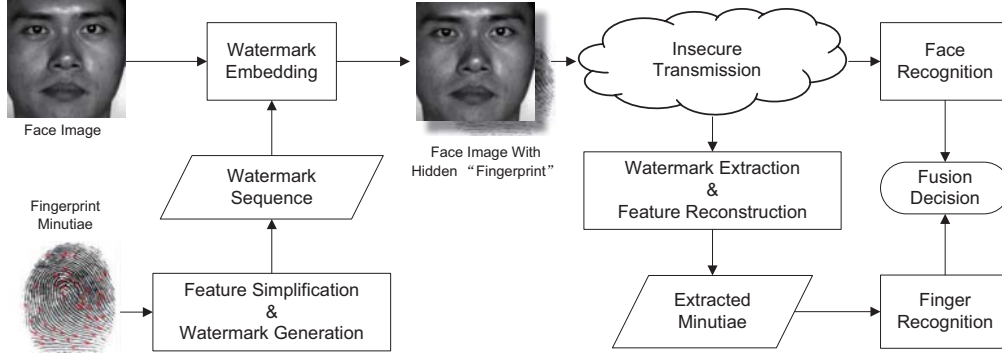


Figure 1. Framework of Watermarking Based Multimodal Biometric Authentication

reasons: First, prominent features have inherent robustness against noise, thus will be less affected by watermark. Second, regions with high information entropy have good masking effect to noise, therefore the watermarked host will be visually inconspicuous. In addition, watermark bits should be differentiated according to their priority. We embed important bits into critical face region (ROI) with large quantization step, with the following consideration: important bits should be extracted with high retrieval accuracy. Moreover, hiding critical information in significant face regions can resist cropping and tampering attacks.

In the guidance of above principles, we propose a biometric watermarking based multimodal authentication framework as Figure 1 illustrates.

3. Embedding Preparation

One critical issue for robust biometric watermarking is the trade-off between watermark robustness and data payload. In minutiae based fingerprint recognition system, each minutia is represented by an unsigned integer triple (X, Y, θ) , where (X, Y) indicates the the coordinate of minutia, and θ denotes the orientation. We employ Jean's method [5], and averagely get 45 minutiae from one single fingerprint in FVC2002 database. If conventional representation of one dimension (12-bit unsigned integer) is applied, the minutiae feature (about $45 \times 3 \times 12 = 1620$ bits) will be too large for quantization index modulation watermarking method.

To employ fingerprint minutiae as robust watermark, we simplify the minutiae feature by the following strategies: (1) randomly pick up 20 minutiae near the center of fingerprint, and discard the rest; (2) scale (X, Y) coordinate into $[1, 256]$, and decrease the accuracy of $\theta \in [0^\circ, 360^\circ]$ by 1-bit right shift, so that each dimension can be represented by an 8-bit unsigned integer. Finally, the simplified minutiae feature is $20 \times 3 \times 8 = 480$ bits.

While much smaller than the original one, it can still act as an effective assistant information for authentication (see "Original" and "Simplified" curves in Figure 3(c)). But note that, such result greatly relies on the performance of fingerprint recognition algorithm ([5] is adopted in our experiments).

To differentiate face regions for watermark embedding. We divide the host face image into 16 non-overlapped blocks in shape of 4×4 , and apply Zhang's Adaboost region selection method in [9] to acquire a *weighting mask* that indicates the discriminating power of each block.

Subsequently, a layer structure, which we named *block pyramid*, is constructed by grouping the most distinctive blocks into level 1, and so forth. Each level of the the pyramid could be regarded as "pieces of a jigsaw puzzle" formed by different face regions. Critical blocks in high pyramid level indicate the ROI of a face image. Numeric watermark bits are also separated into 4 groups according to the bit priority. The most important bits that weighted by 2^7 and 2^6 are embedded in the highest pyramid level as Figure 2 demonstrates.

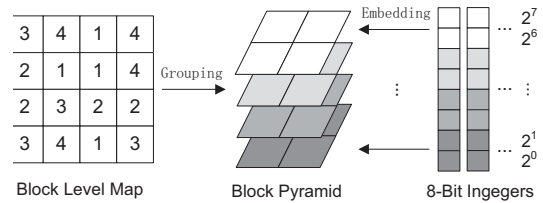


Figure 2. Block Pyramid Based Numeric Embedding

4. Watermark Embedding and Extraction

In this section, the quantization of first-order statics method in [1] is adopted for watermark bits embedding and extraction in each pyramid level.

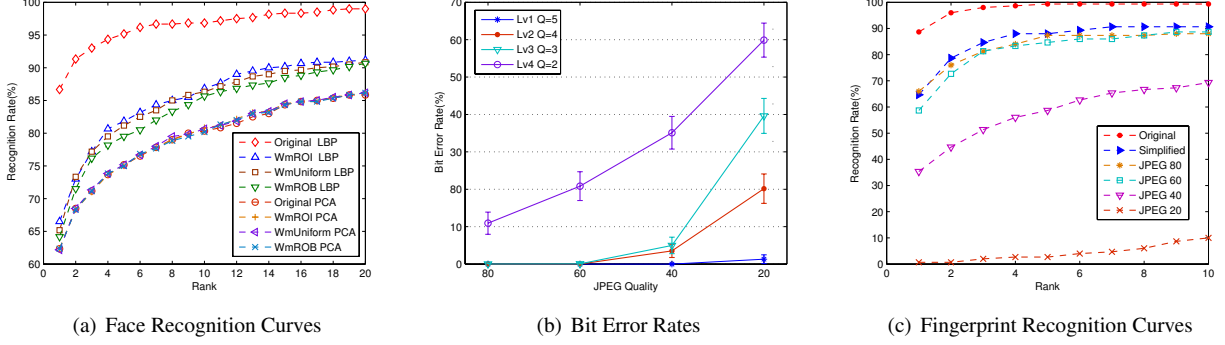


Figure 3. Evaluation of Face Distortion and Fingerprint Robustness

Let I indicate one single block pyramid level, and b the corresponding watermark bits. Sub-block of I denoted as Λ_i , is aligned to each watermark bit b_i according to the secret key. To perform watermark bit embedding, the mean value of Λ_i , μ_i is quantized to an even multiple of Q if $b_i = 0$, or odd multiple if $b_i = 1$ as Equation (1), where μ'_i is the mean value of Λ_i after watermark embedding, and Q is the quantization step that controls the overall embedding strength of current pyramid level. Evidently, higher value of Q brings better robustness together with larger distortion.

$$\mu'_i = \left\lfloor \frac{\mu_i + Qb_i}{2Q} + 0.5 \right\rfloor \times 2Q - Qb_i \quad (1)$$

The total change of Λ_i will be $\Delta_i = (\mu'_i - \mu_i) \cdot N_p$ where N_p denotes the number of pixels in Λ_i . Finally, the modification is distributed to each pixel $p \in \Lambda_i$ by Equation (2).

$$\Delta_{p(j)} = \Delta_i \cdot \frac{QM(j)}{\sum_{j \in \Lambda_i} QM(j)} \quad (2)$$

Here, QM is a *quantization map* generated through Equation (3), which employs noise visibility function (NVF) [8] to get a better visual quality.

$$QM = 1 - NVF(i, j) = \frac{\theta \cdot \sigma_x^2(i, j)}{1 + \theta \cdot \sigma_x^2(i, j)} \quad (3)$$

$\sigma_x^2(i, j)$ denotes the local variance of image window centered at pixel (i, j) , and θ is a scaling constant.

In the extraction stage, the extractor uses the secret key to identify the sub-block corresponding to each watermark bit, from which the mean value $\hat{\mu}'_i$ is calculated. Since the watermarked image may endure both incidental distortion and malicious attacks during transmission, we use $\hat{\mu}'_i$ as the estimated value of μ'_i . The quantization step parameter Q is assumed to be shared by watermark

embedder and extractor, so that watermark bit \hat{b}_i can be extracted by Equation (4).

$$\hat{b}_i = \text{mod} \left\{ \left\lfloor \frac{\hat{\mu}'_i}{2Q} + 0.5 \right\rfloor, 2 \right\} \quad (4)$$

5. Experimental Results

In this section, we design numerous experiments to verify our hypotheses in Section 2 and discuss the benefits of differentiating face regions and numeric bits.

We construct three watermarking strategies to evaluate the advantages of differentiating face regions: Uniformly watermarking each pyramid level with the same quantization step Q (Uniform [3, 3, 3, 3]), watermarking region of background with larger strength (ROB [2, 2, 4, 4]), and ROI [4, 4, 2, 2] inversely. The quality of watermarked sets are shown in Table 1, where PSNR represents pixel-wise errors, WPSNR takes visual masking effect into consideration, and SSIM focuses on the overall structure information. Through comparison, we can draw the conclusions: (1) ROI presents better perceptual masking than ROB; (2) Uniformly distribute the watermark energy into each pyramid level causes lower distortion.

Table 1. Quality of Watermarked Images

	PSNR↑	WPSNR↑	SSIM↑
Uniform	42.95	46.20	0.9877
ROI	41.26	45.07	0.9823
ROB	41.28	43.16	0.9823

The influences of different watermarking strategies to LBP and PCA face recognition methods are illustrated in Figure 3(a). We can observe that PCA method, which is based on global appearance, only has been slightly affected; while local feature based LBP scheme suffers a great loss, since watermark is one kind of

pseudo random noise to local texture information. One suggestion for preserving LBP feature is not to involve perceptual masking when quantization the mean value of blocks in embedding process (the method we use in "WmLBP", Figure 4). Moreover, the recognition performance that "WmROI > WmUniform > WmROB" verifies our previous statement.

To discuss the advantage of differentiating bit priority. We embed watermark bits in block pyramid with the Q_s of [5, 4, 3, 2], and use JPEG compression to evaluate the robustness of fingerprint watermark. Figure 3(b) illustrates the bit error rate (BER) of each level, and Figure 3(c) shows the fingerprint recognition curves using minutiae feature extracted from face images of different JPEG quality. From the results we can conclude that, larger Q brings better robustness, and higher extraction accuracy of more important bits can guarantee recognition performance to a great extent. Besides, quantization scheme itself can provide better robustness than amplitude modulation method that involved in [2, 4].

In multimodal recognition stage, we employ the fusion strategy of min-max normalization followed by the sum of scores method suggested by Jain et al. in [3]. From the results demonstrated in Figure 4, we may observe that both high accurate LBP and low accurate PCA can achieve a great additional performance through fusion with the extracted fingerprint minutiae.

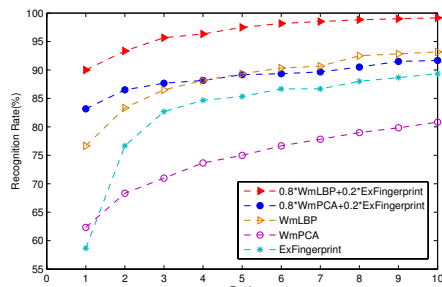


Figure 4. Multimodal Recognition Curves

Finally, a demonstration of face image authentication is shown in Figure 5. Since high priority bits of minutiae feature are embedded in critical face regions. Both impostor image containing no fingerprint and tampered image with seriously damaged fingerprint can be identified through fingerprint authentication.

6. Conclusions

In this paper, we propose a novel biometric watermarking scheme, which differentiates numeric bit priority and host face regions to enhance the security of biometric system. Experimental results demonstrate the

advantages of our approach. Furthermore, since our block pyramid based scheme allows different embedding strategy in distinct levels, various watermarking methods (either robust or fragile) can be combined according to the application requirements.

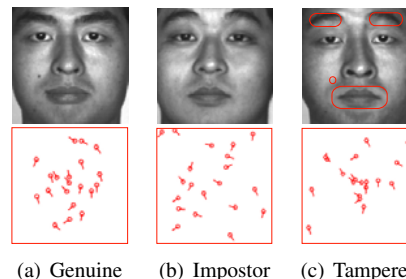


Figure 5. Minutiae Extracted From Valid(a) and Fake(b,c) Face Images

Acknowledgements

This work is funded by the National Natural Science Foundation of China (No. 60873158), the National Basic Research Program of China (No. 2010CB327902), the Fundamental Research Funds for the Central Universities, and the Opening Funding of the State Key Laboratory of Virtual Reality Technology and Systems.

References

- [1] S. He, D. Kirovski, and M. Wu. High-fidelity data embedding for image annotation. *IEEE Trans. on Image Processing*, 18:429–435, 2009.
- [2] T. Hoang, D. Tran, and D. Sharma. Remote multimodal biometric authentication using bit priority-based fragile watermarking. In *Proc. of ICPR'08*.
- [3] A. K. Jain, K. Nandakumar, and A. Ross. Score normalization in multimodal biometric systems. *Pattern Recognition*, pages 2270–2285, 2005.
- [4] A. K. Jain and U. Uludag. Hiding biometric data. *IEEE Trans. on PAMI.*, 25:1494–1498, 2003.
- [5] T. Y. Jea and V. Govindaraju. A minutia-based partial fingerprint recognition system. *Pattern Recognition*, 38:1672–1684, 2005.
- [6] C. Y. Low, A. B. J. Teoh, and T. Connie. Fusion of LSB and DWT biometric watermarking using offline handwritten signature for copyright protection. In *Proc. of ICB'09*, pages 786–795.
- [7] M. Vatsaa, R. Singha, and A. Noore. Feature based RDWT watermarking for multimodal biometric system. *Image and Vision Computing*, 27:293–304, 2009.
- [8] S. Voloshynovskiy, A. Herrigel, N. Baumgaertner, and T. Pun. A stochastic approach to content adaptive digital image watermarking. In *IHW'99*, pages 211–236.
- [9] G. Zhang and Y. Wang. Multimodal 2D and 3D facial ethnicity classification. In *Proc. of ICIG'09*, pp. 928-932.