Identity Verification System Using Data Hiding and Fingerprint Recognition

Guorong Xuan, Dan Jiang, Hongfei Ji
Dept. of Computer Science
Tongji University
Shanghai, China
grxuan@public1.sta.net.cn

Yun Q. Shi, Dekun Zou
Dept. of Electrical & Computer Engineering
New Jersey Insitute of Technology
New Jersey, USA
shi@njit.edu

Liansheng Liu, Heisheng Liu
Weichao Bai
Baojia Electronic Equipments, Co. Ltd
Shenzhen, China

***Abstract*—This paper proposes an identity verification system using data hiding and fingerprint recognition. At user's home, the client's account information is encrypted and embedded into the fingerprint image via data hiding method secretly. Then the fingerprint image with embedded data is transferred to the bank over Internet. At bank side, the client's account information is extracted. It is used to retrieve the client's registered fingerprint from central database, which is then matched with extracted fingerprint via fingerprint recognition method to verify user's identity. This system is more reliable and secure than transferring password alone. The data are embedded with quantization watermark in the JPEG 2000 coding pipeline. Compare to our previous proposed system, the interaction time can be reduced because less data will be transmitted. When the fingerprint image is compressed to 1/4~1/20 of its original size, the embedded watermark can still be recovered. This system has been used in a bank pension distribution system. It can also be used in other E-business applications.**

Keywords—integer wavelet lossless watermarking; JPEG 2000 real-time quantization watermarking; fingerprint recognition; identity verification

Topic area—4.a. data hiding

I. INTRODUCTION

In recent years, E-business and E-government applications become more and more popular. Many people begin to use Internet to deal with their daily affairs, such as banking service and online shopping. Technology gives us much convenience. It also brings security issues. Some smart criminals try to gain illegal benefits via feigning other person's identity. So how to verify a person's identity effectively becomes a key issue in secure online transactions.

In [1], Xuan et al. described an online pension distribution system, which use digital watermark in this field for the first time. At the client side, client's fingerprint image is captured and digested using SHA-256 algorithm. The encrypted account information and the hash value are embedded into the original fingerprint image as watermark. Then, the stego image might be transferred to bank server via Internet. Because lossless watermarking algorithm [2] is adopted, the fingerprint image and watermark can be recovered losslessly. Another SHA-256 digest is applied to fingerprint image after data extraction. It will be compared with the extracted hash to verify the integrity of the received fingerprint. If they match, the extracted account information is used to retrieve the registered fingerprint of this client from central database. If these two fingerprints match, the client identity is verified. The system is more reliable and secure than transferring password alone. However, it may not suit our needs sometimes. For example, the captured fingerprint image is a 75KBytes BMP file. If we use 56kbps dial-up service to connect the server, the interaction will last 30 or more seconds. The longtime waiting is annoying to clients. Therefore, we develop a new system suitable specific to narrow bandwidth situation.

In [3], Meerwald proposed a QIM (Quantization Index Modulation) based data hiding algorithm to insert watermark along the JPEG 2000 coding pipeline. We proposed a simplified and improved version of Meerwald's method, which results in a larger embedding payload. We adopt the new data hiding method into our identity verification system. Although the fingerprint image endures JPEG 2000 lossy compression, our experiments show it does not affect the recognition performance. Faster verification can be achieved because less data need to be transmitted. When the fingerprint image is compressed to 1/4~1/20 of its original size, the embedded watermark can be recovered without any error. Both the previous system and the proposed new JPEG 2000 based system discussed in this paper have been used in a bank pension distribution system, and are very promising in further E-business applications.

For the rest of this paper, Section II describes the proposed JPEG 2000 real-time quantization watermarking algorithm in detail. Section III describes the architecture of JPEG2000 based identity verification system. Section IV provides the performance analysis of the proposed system. Finally, Section V concludes.

II. JPEG 2000 REAL-TIME QUANTIZATION WATERMARKING ALGORITHM IN THE CODING PIPELINE

JPEG 2000 [4-6] is the next generation still image compression standard. The structure of JPEG 2000 encoder/decoder is shown in Fig.1. We simplify Meerwald's algorithm [3] to embed the client information in the JPEG2000 coding pipeline.

Watermark Embedding Algorithm The watermark is embedded after quantization and prior to entropy encoding in the JPEG 2000 coding pipeline. Suppose *R*-level wavelet decomposition is adopted. The watermark is embedded into the last low-frequency band LL_R to ensure the robustness in the low bit rate situation. Suppose watermark data is $w = w_1, \dots, w_m$ in binary format, where m is watermark length. Let Δ denote quantization step size.

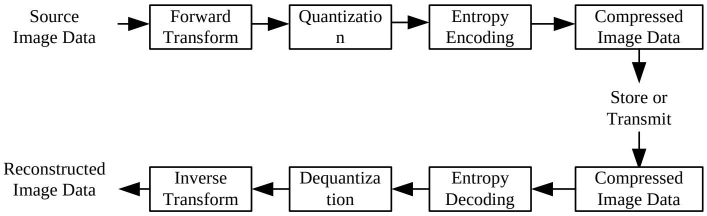

Fig.1 Structure of JPEG 2000 encoder/decoder [6]

We select certain amount of code blocks of LL_R depending on watermark length. Each coefficient c in the code block is embedded with one bit of watermark via Even-Odd Scalar Quantization method. Embedding equation is (1).

$$c = \begin{cases} \text{the nearest even value with quantization step size } \Delta, \text{ if } w_i = 0 \\ \text{the nearest odd value with quantization step size } \Delta, \text{ if } w_i = 1 \end{cases} \tag{1}$$

If embedded watermark bit w_i equals zero, c is quantized to the nearest even value with quantization step size Δ . If embedded watermark bit w_i equals one, c is quantized to the nearest odd value. We scramble the embedding positions in the code block via hashing method. The hash equation is $y = (k_0 + k_1 \times x) \bmod s$, where x and y is the position before and after hashing, k_0 and k_1 is hashing key. We can estimate the embedding capacity of an $M \times N$ image in (2).

$$C = (M \times N) / 2^{2R} \tag{2}$$

Watermark Extracting Algorithm The watermark is extracted between entropy decoding and de-quantization in the JPEG 2000 decoding pipeline. Below is the extracting method.

$$r = round(c/\Delta),$$

$$watermark\_bit = \begin{cases} 0, & if \;\; r \text{ is even} \\ 1, & if \;\; r \text{ is odd} \end{cases} \tag{3}$$

where round is Integer Round operation

The flowchart of this algorithm is shown in Fig.2.

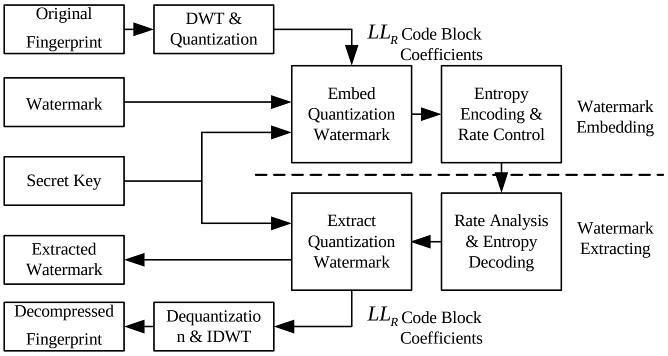
Original Fingerprint
DWT & Quantization
LL_R Code Block Coefficients
Watermark
Embed Quantization Watermark
Entropy Encoding & Rate Control
Watermark Embedding
Secret Key
Extract Quantization Watermark
Rate Analysis & Entropy Decoding
Watermark Extracting
Extracted Watermark
Decompressed Fingerprint
Dequantizatio n & IDWT
LL_R Code Block Coefficients

Fig.2 Embedding/Extracting flowchart of JPEG 2000 real-time quantization watermarking algorithm

III. Architecture of Poposed System

The architecture of the new proposed system is described in Fig. 3.

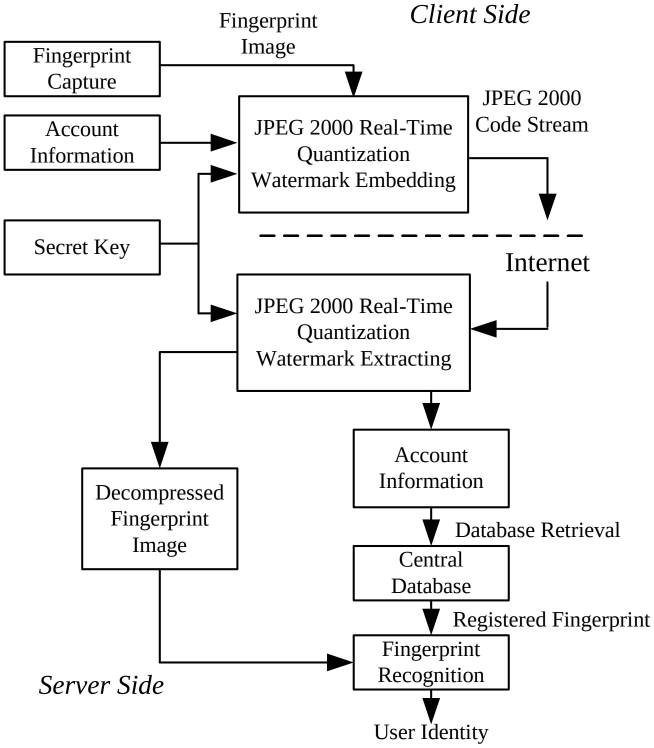

Fig.3 Proposed JPEG 2000 Based System

Identity Registration Clients must register their fingerprint images and account information to the central database before verification. The fingerprint capture device captures the user's same fingerprint 3 times, from which features are selected. Finally, fingerprint features and account information is stored in the central database.

Identity Verification At home, clients can use the client fingerprint device shown in Fig.4 to obtain client's fingerprint. This device is an embedded system running uClinux, right below of which is Veridicom fingerprint capture IC. Then, client can input his/her account information, which will be encrypted and embedded into the fingerprint image using JPEG 2000 real-time quantization watermarking algorithm. The fingerprint image with hidden data is transferred to the bank server via Internet. At the server side, account information is extracted to retrieve the user's registered fingerprint from the central database. If the decompressed and registered fingerprints match, the user is authorized for further operation.

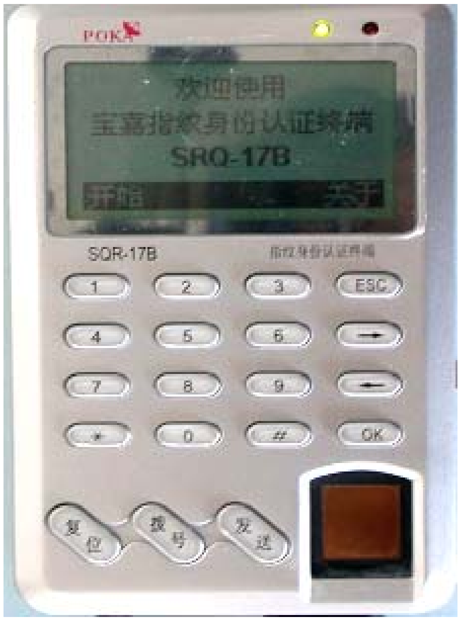

Fig.4 Photo of the identity verification system's client device

IV. EXPERIMENTS

Since lossy image compression is adopted, the features of the original fingerprint image will endure some kind of loss during compression. The impact of lossy compression on the fingerprint recognition needs to be evaluated.

In this part, we will test our watermarking algorithm on some typical fingerprint databases. Two experiment databases can be accessed freely, which is represented by symbol A and B in this paper. Library A is FVC 2000 benchmark database 1 [7], where each image is 300×300 256-gray levels BMP. Library B is captured by Veridicom [8] fingerprint capturing device, where each image is 256×300 256-gray levels BMP. Each database has 10 categories and each category has 8 fingerprints.

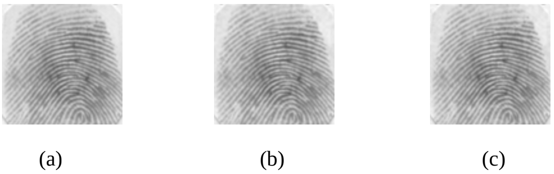

Fig.5 Original image and decompressed images (a)Original image (b) Decompressed image with compression rate = 0.4bpp (PSNR=33.84) (c) Decompressed image with compression rate = 4bpp (PSNR=38.57)

We apply 3-level wavelet decomposition to the original fingerprint image. We embed 160 bytes of random data into fingerprints from Library A; 130 bytes of random data into fingerprints from Library B. This process is repeated 10 times, and 10 compressed fingerprint databases are obtained. Examples of the original image and decompressed image using this algorithm are shown in Fig.5.

For each compressed image, we extract the watermark and compare the extracted watermark with the original watermark to test the robustness. Veridicom fingerprint recognition software is used to do fingerprint recognition. Each fingerprint image of the original library is used to train the recognition system. 80 decompressed fingerprint images from each compressed database are used to match with the trained fingerprint image one by one. Finally we average the *Correct Recognition Rate*, *False Reject Rate* and *False Recognition Rate* over 10 compressed databases. If the matched features of two fingerprints exceed a certain Threshold, we consider them belonging to the same person. *Correct Recognition* stands for verifying a user's identity successfully (when two fingerprints belong to the same person and matched features above Threshold, OR two fingerprints belong to different persons and matched features below Threshold). *False Reject* happens when two fingerprints belong to the same person and matched features below Threshold. *False Recognition* happens when two fingerprints belong to different persons and matched features above Threshold.

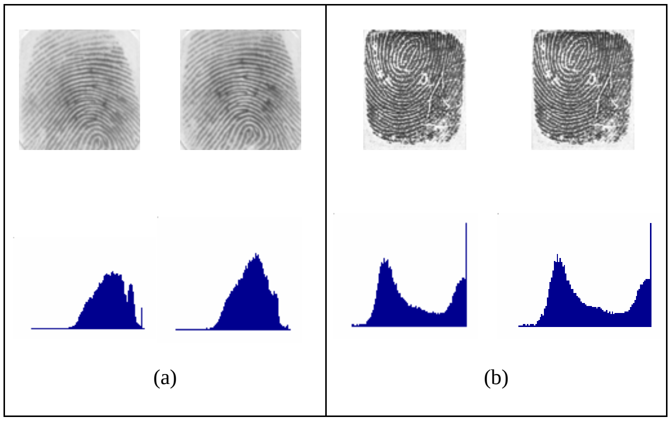

Fig.6 Two different fingerprint images and their histograms from Library A (a) and Library B (b)

In our experiments, we find that Library A and Library B have different nature. Fig.6 shows the histogram of two different fingerprint images from the two libraries. Fingerprints in Library A have a dense histogram, while histograms of fingerprints in Library B are more equalized. The differences will affect the watermarking embedding capacity and compression rate. Experiments show that we can get better compression rate on Library A than Library B. Fingerprint in Library A can compressed to 1/20 of its original size, while only 1/4 for images in Library B. Even though fingerprint images can be compressed only to 1/4, the respond time will be reduced to below 10 seconds. It is acceptable to most clients.

Table Ⅰ and Table Ⅱ list experiments results on Library A and Library B separately. Fig.7 shows the Average Correct Recognition Rate on Library A and Library B.

TABLE I. EXPERIMENTS RESULTS ON LIBRARY A

Compression Rate (bpp)	Avg. Correct Recognition Rate	Avg. False Reject Rate	Avg. False Recognition Rate
0.4	95.98%	4.02%	0
0.8	96.39%	3.60%	0.004688%
1.2	96.38%	3.61%	0.003125%
4	96.49%	3.53%	0.00625%
8	96.75%	3.25%	0

TABLE II. EXPERIMENTS RESULTS ON LIBRARY B

Compression Rate (bpp)	Avg. Correct Recognition Rate	Avg. False Reject Rate	Avg. False Recognition Rate
2	98.86%	1.13%	0.001563%
2.4	98.85%	1.15%	0
2.8	98.85%	1.15%	0
4	98.89%	1.11%	0
8	98.86%	98.86%	0

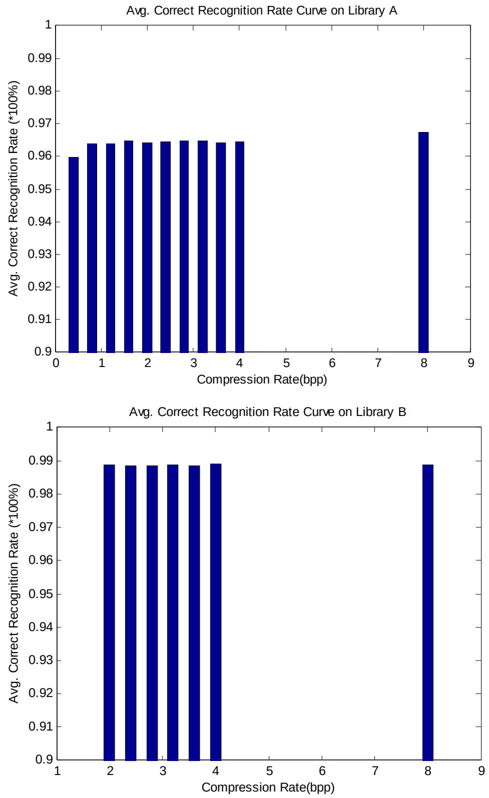

Fig.7 Avg. Correct Recognition Rate on Library A and Library B

Experiments on typical testing databases show that JPEG 2000 real-time quantization watermarking algorithm can extract watermark data correctly under certain compression rate, and has little effect on fingerprint recognition performance. The false recognition may occur (at most 4 out of 6400 matches). But it can be overcome by raising the Threshold and with multiple-time verification methods.

V. CONCLUSIONS

This paper proposes a new identity verification system using data hiding and fingerprint recognition. Both the proposed system and the previously proposed system [1] have been used in bank pension distribution system successfully.

Previous system uses lossless watermarking algorithm. SHA-256 is used to ensure the integrity of fingerprint image. It has excellent performance in terms of security.

The new system uses JPEG 2000 real-time quantization watermarking algorithm. Experiments show that FVC 2000 testing fingerprints can be compressed to 1/20, while Veridicom captured fingerprints can be compressed to 1/4. The traffic data between client and server is hence reduced. The interaction time will be shorter for narrow band users. At the same time, the embedded watermark can be extracted. Although fingerprint images endure some kind of loss because of JPEG 2000 compression, the recognition rate is not affected. The new system is less secure than previous system, but has a better performance in the band limited network situation.

The advantages of these systems are as follows. Firstly, biometric recognition is used to enhance the reliability of the system. Secondly, watermark data is embedded into the fingerprint image secretly. It is more difficult for hostile party to realize the very existence of the secret message. As a result, the system secrecy is enhanced. Besides, previous system uses SHA-256 to ensure the integrity of the original fingerprint image. New system uses JPEG 2000 to compress the fingerprint image. The transferred data is greatly reduced.

ACKNOWLEDGMENT

This project is supported by China NSF: The Research of Theory and Key Technology of Lossless Data Hiding (90304017).

REFERENCES

[1] G. Xuan, J. Zheng, C. Yang, Y. Shi, D. Zou, L. Liu, W. Bai, “A Secure Internet-Based Personal Identity Verification System Using Loseless Watermarking and Fingerprint Recognition”. The 3rd International Workshop on Digital Watermarking, Korea Seoul, Oct. 2004.

[2] G. Xuan，J. Chen，J. Zhu, Y. Shi, Z. Ni, W. Su, “Distortionless data hiding based on integer wavelet transform”. IEE Electronics Letters, vol. 38, no. 25, pp. 1646-1648, Dec.2002.

[3] P. Meerwald, “Quantization Watermarking in the JPEG2000 Coding Pipeline”. Communications and Multimedia Security Issues of The New Century, IFIP TC6/TC11 Fifth Joint Working Conference on Communications and Multimedia Security, May 2001.

[4] ISO/IEC 15444-1: Information Technology---JPEG 2000 image coding system---Part 1: Core coding system, 2000.

[5] M. Adams. “The JPEG-2000 Still Image Compression Standard”. ISO/IEC JTC 1/SC 29/WG 1 N 2412, Dec. 2002.

[6] Charilaos Christopoulos, Athanassios Skodras, Touradj Ebrahimi, “The JPEG2000 Still Image Coding System: An Overview”. IEEE Trans. on Consumer Electronics, vol. 46, No. 4, pp. 1103-1127, Nov.2000.

[7] http://bias.csr.unibo.it/fvc2000/.

[8] http://www.veridicom.com.