GESTS International Transactions on Computer Science and Engineering

Volume 64, Number 1, May 2011

Global Engineering, Science, and Technology Society
http://www.gests.org

Volume Editors

Dr. Bruce M. Bae
Acoustic Sci. and Engr.
A General Chair, GESTS
Seoul 156-743, Korea

Dr. Ki Young Lee
Signal Processing Engr.,
A Vice Chair, GESTS
Kangwon-Do Korea

Dr. Henry S. Hong
Acoustic Sci, and Engr.,
A Vice Chair, GESTS
San Diego, CA, USA

Publication Team

Kelvin E. Bae
BR. Director, GESTS
Renton, WA98058, USA
gests@gests.org

Sang Bae Kim
Designer, E-Sound Lab.
Seoul 156-833, Korea
Sangbai@sangbai.com

Myung Yul Park
President
SunJin Publishing Co.
Euljiro Seoul, Korea

ISSN 1738-6438
ISBN 89-953729-5-8

GESTS Publishing team, May 30, 2011 Printed in America, Canada, China, and Korea.

Type setting : Camera-ready by author

Table of Contents

Fingerprint Authentication System in Ban king Transaction 1
Nguyen Tran Lan Anh, Phan Thi My Dung, and Pham The Bao

A study on the Analysis of Sound Field of Domestic Recreation Vehicle according to the Characteristics of Hearing and Speech Signal 11
Jong-Jin Yun, Hyung-Woo Park, Kyu-Tae Baek,
Young-Hun Yu, and Myung-Jin Bae

Presenting a new Methodology for Implementation of E-Bu siness Systems with Multi-Layer Security (MLS) Agents 19
Amin Daneshmand Malayeri

Field Data Collection of a D istributed Spoken Dialog System for Music Retrieval and Its Evaluation 33
Sunao Hara, Norihide Kitaoka, and Kazuya Takeda

A Study on Improvement of the Variable Rate Speech Codec by Preprocessing Techni que 59
Jiho Seo and Myungjin Bae

Design Parallel Genetic Algorithms for Multi-Agent Systems 67
Andriy Sadovnychyy, Pedro Pablo Gonzales Perez, and Jorge Cervantes

YAML based Long-Term Log Management 73
Akihiro Tomono, Minoru Uehara, and Yuji Shimada

Modified Weighting Model Rank Method for Real-Time Korean Speaker Identification System 91
Kwang-Soo Kim

Design of Educational Content for the Teaching of Physics by means of Learning Objects 97
Roberto Montiel, Carmen Ceron G, Etelvina Archundia S ,
Beatriz Beltran M, and Eugenia E. Vera C

A Study on Dogs That Spea k Human Language 109
Jin-Hwa Jeong and Myung-Jin Bae

Statistical Change-Point Analysis of Tr affic Flow Non-Stationary Time Series 117
Jinglei Zhang and Xiaoyuan Wang

DIAMOND Data Incursion And Mining by Optimistic Nobelium Distribution 128
SarathChand P.V., Srilatha K., Kiranmai A.,
Benarji T. , and Raghvendar Rao A.G.

A study on SNR Estimation of Continuous Speech Signal with Additive Colored Noise 137
Hyung-woo Park and Myung-jin Bae

Performance of Encryption/Decryption in CryptoSys API 148
Uzair Aslam and Seema Ansari

Author Index 157

Fingerprint Authentication System in Banking Transaction

Nguyen Tran Lan Anh, Phan Thi My Dung, and Pham The Bao

Faculty of Mathematics and Computer Science
University of Science, Ho Chi Minh City
{nguyen.tran.lan.anh, dungptmy}@gmail.com, ptbao@hcmus.edu.vn

Abstract. *In this paper, we introduce a combination of fingerprint authentication and data encryption to build a real time system in online banking transaction. To serve this purpose, our system has four modules: image enhancement, minutiae extraction, data encryption and fingerprint authentication. At the beginning, we enhanced the fingerprint image based on the Gabor filter. Next, minutiae of fingerprint, or feature vector, was extracted and postprocessed to remove the false. Finally, it was authenticated with template vectors stored in the database. Furthermore, to secure the data transmission, we applied symmetric-key cryptography to encrypt and decrypt these vectors. In the experiments, we have tested our system in two different databases and had an effectiveness of accuracy and processing time.*

Keywords – fingerprint, authentication, minutiae extraction, banking transaction, advanced encryption standard.

1 Introduction

Together with the development of Internet and world economy, online transaction becomes more popular every day. Banking is one of fields which use this method a lot to develop their business in the widespread way around the world. Although it is fast and user-friendly, it is not really too safe to withdraw or forward a sum of money. Many works have been done in the field of biometric authentication based on fingerprint, iris, voice and face. To be used in a real context for banking authentication, there are researches on fingerprint based biometric system. Because fingerprint is unique, immutable and not easy to fake, it solved a lot of security problems or material aspects in a simple and quick way [1]. It helps customers not to remember the PIN or be worry about ATM credit card steal if they have many credit cards at many different banks. Moreover, its security is increased significantly since only the owner has an ability to access his/her own account.

Many approaches and techniques to solve separate stages of fingerprint have been developed [1], [2]. Most image enhancement methods are morphological transform [3], [4], dyadic scale-space [5], or Gabor filter [6], [7]. When extracting feature vectors, the minutiae are always found on thinning [8], [9] or gray-scale images [10], [11]. In authentication stage, all of techniques are based on the properties of ridges [14], or local features [13]. However, their combination to construct a complete system is still a challenge to researchers for acceptable processing time and high security.

Motivated by the desire to provide users a capable fingerprint authentication system, recently there are some banks applying this system in their business while they saved the owners' fingerprint directly in their cards. Different from them, we proposed a combination and some improvements to create an online authentication between transaction points and the host computer placed at the headquarters of the bank. It makes our system achieve higher security, better accuracy and acceptable processing time than others now.

2 System Overview

We built a real-time fingerprint authentication system which was divided into two parts at two places: transaction points and headquarters. In general, given an input fingerprint image from the scanner, this idea is as follows:

- At the transaction point: enhance the quality of the input image, extract all minutiae, encrypt as an output data, and transfer to the server.
- At the headquarters: decrypt the input data, match with owner's account's feature vectors stored in the database, and return the final result.

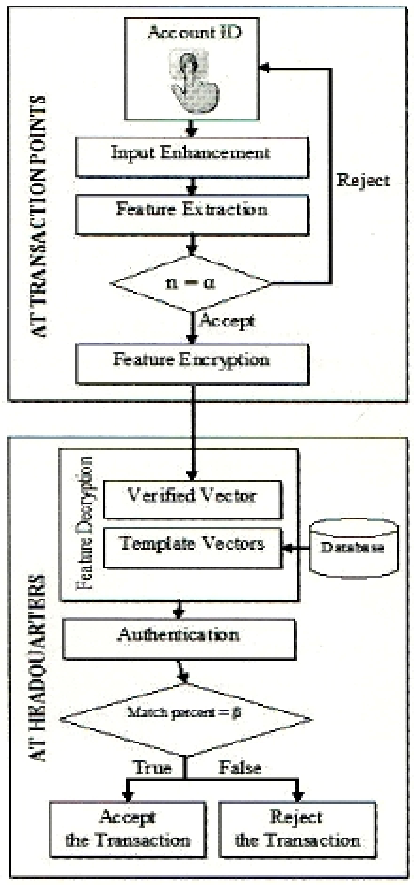

Diagram 1. Operation model of fingerprint authentication system in banking transaction

3 Fingerprint Authentication System

In this paper, we separated our system into four modules to make it more convenient for users to be able to change their approach easily if they want.

3.1 Image Enhancement

The performance of automatic fingerprint authentication depends heavily on the quality of the input [1]. However, most of fingerprint images aren't good enough to extract minutiae exactly and directly because of skin conditions, sensor noise, incorrect finger pressure, and inherently low-quality fingers. So, the enhancement step is needed to improve its quality. In our fingerprint authentication system (FAS), we chose a method using Gabor filter employed by Hong et al. [6]. It is an even-symmetric filter which can performs a low-pass filtering along the ridge orientation and a band-pass filtering orthogonal to the ridge orientation. Since it has optimal joint resolution in both spatial and frequency domain, it can efficiently remove the undesired noise, preserve the true ridge and valley structures. After enhancement, to extract features of fingerprint more easily, we decided to binaries and thin the input image.

Before that, we applied a segmentation step to enclose the region of fingerprint and get its boundary exactly in the image by combining some morphological methods such as erosion, area opening and holes filling. Relying on that, we can edit out the maximum background which doesn't contain the fingerprint region. As a result, we decreased the size of the image to help our system reduce the processing time in next steps.

3.2 Feature Extraction

Many authentication techniques are based on minutiae matching [1]. The minutiae, which are the local discontinuities in the ridge flow, provide the features that are used for identification. There are two main types of minutiae, ridge endings and bifurcations.

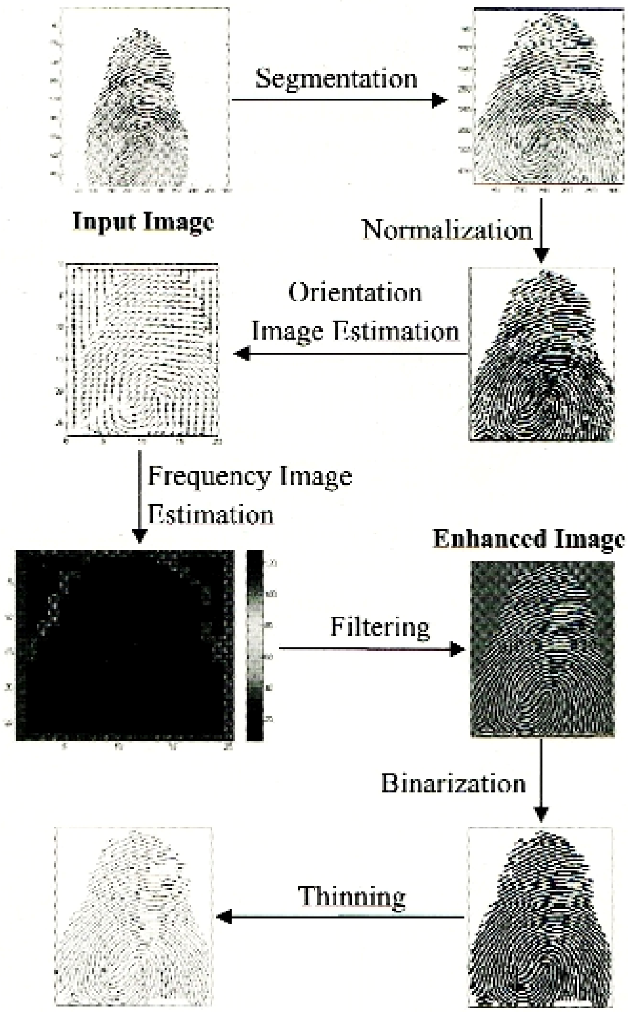

Diagram 2. A diagram to summarize main steps of this module

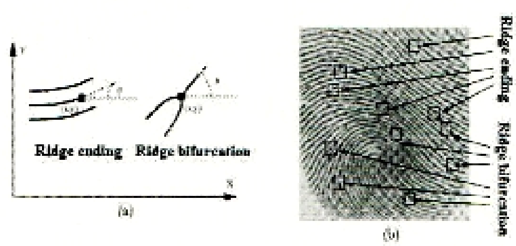

Figure 1. The minutiae of a fingerprint: (a) Defined by its orientation and location; (b)In the fingerprint

The extraction step is as important as other steps. If our system doesn't do extract all minutiae precisely and sufficiently, its accuracy will not be high. So, we split this step into two parts: extract coarse minutiae and remove the false. In the first part, we applied the most commonly employed method, which is Crossing Number (CN) concept [18]. The minutiae are extracted by scanning the eight-connected neighborhood of each foreground pixel in the image using a 3×3 window. The CN value is then computed. At first, if this value is 1, this pixel will be a ridge ending. Otherwise, if this value is 3, it will be a ridge bifurcation. After that, the system saves all its details such as the type, orientation, and location to create a feature vector (its size is $n \times 4$).

Next part is to remove the false minutiae. We chose the algorithm employed by Tico and Kuosmanen [15] as the first step. However, it cannot absolutely reject the false which are at the beginning and the ending of a ridge. Thus, we add an improvement to do that. When segmenting the input, the system can get the accurate boundary of the fingerprint region by morphology. So, after checking by Tico and Kuosmanen algorithm, we will find the pixel which is in the boundary and the nearest to this minutia. If the distance between two pixels is smaller than a threshold, it will be considered as a false minutia at the beginning or the ending of the ridge.

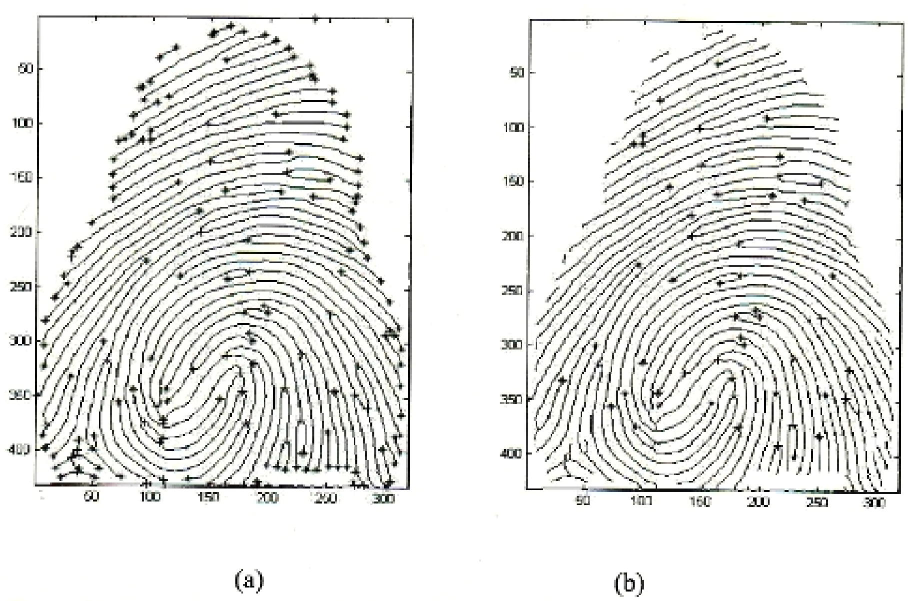

Figure 2. The minutiae are marked in a fingerprint image: (a) Coarse minutiae are extracted;
(b)The false minutiae are removed

3.3 Fingerprint Authentication

In banking transaction, when a customer registers a new account, he/she will have its id and give the bank his/her fingerprint images of the same finger, which is considered as its password. Therefore, fingerprint authentication refers to the method of matching the verified one with the known one of owner's account. FAS will perform a comparison between the verified feature vector with template vectors, which is encrypted and stored in database. It means that we have pairs of feature vectors. In this module, there are two stages: alignment and match.

To find maximum percent of matching one pair, it is necessary to align two vectors first. Alignment builds a new axis from two reference points by determining transformation parameters $(\Delta x, \Delta y, \Delta\theta)$, where Δx, Δy are the adjustable distances in x-axis and y-axis, and $\Delta\theta$ is the rotate angle. These reference points are the two-minutia pair having the same value type and near distance. Because all minutiae play the same role in the feature vector, each pair can be chosen as reference points. It is really time consuming. Therefore, we suggested using the k-d tree method [17] to find three minutiae from template vector which have the nearest distance with the minutia being selected in verified vector. Although this improvement isn't considerable, it helped reduce the large computation complexity. After all parameters are determined, these remaining minutiae are translated and rotated as the following formula 1.

$$\begin{pmatrix} x_i\_new \\ y_i\_new \\ \theta_i\_new \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} * \begin{pmatrix} x_i - \Delta x \\ y_i - \Delta y \\ \theta_i - \Delta\theta \end{pmatrix} \quad (1)$$

Where (x_i, y_i, θ_i) :the original coordinate, $(x_i\_new, y_i\_new, \theta_i\_new)$: the new coordinate, $(\Delta x, \Delta y, \Delta\theta)$: transformation parameters.

After aligning all of them, two feature vectors are matched by using elastic match algorithm to count the matched minutiae pairs by assuming two minutiae having the same type, nearly same position and direction are identical [1]. The match result is maximum matched percent. The final result for two fingerprints will be the average of these matched percent of these pairs of feature vectors. If the percent is larger than a pre-specified threshold, the two fingerprints are from the same finger.

6.4 Data Encryption and Decryption with AES

Security is a great necessity to transfer data through the internet. There are several ways to guarantee the operation of these authentication systems. Cryptography is one option and used very popularly. According to Tran Minh Triet's PhD thesis "Research and develop information security methods based on AES" [16] in Computer Science, Vietnamese language, we used the Advanced Encryption Standard algorithm (AES) to implement the data encryption module to help secure data transactions in this system.

AES algorithm is a symmetric block cipher. It is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data safely in blocks of 128 bits. It is designed to be fast, unbreakable, and able to support even the smallest computing device. Thus, it is suitable for banking transaction. Since AES is a public key cryptography, the security of keys is very important. Therefore, the key cannot be stored or transferred. This system generated two same keys from transaction time to be used in data encryption module at the transaction point both the server of the headquarters.

4 Experimental Results

We made the test in our PC Core 2 Duo CPU T5500, RAM 512M, and Windows XP SP3 on the Matlab R2008a programming environment. We collected the fingerprint database from DB_FP* including 46 people's fingerprints and from UareU (http://ai.pku.edu.cn/biometrics2007/fingerprintlib/) including 64 people's fingerprints with 4 images of the same finger per person. From the experimental results, we chose T, the threshold to decide whether two fingerprints are the same, to be equal 3.5 for the best result with high accuracy, small false rates (FAR: False Acceptance Rate; FRR: False Rejection Rate), and the average time is approximate 3 seconds.

Table 1. The result comparison of 2 databases with different thresholds.

Database	Accuracy Rate (%)	FAR (%)	FRR (%)	Average Time (s)
T = 0.3				
DB_FP	100	0.00	8.69	2.8546
UareU	95.31	4.69	26.56	1.6759
T = 0.35				

DB_FP	93.48	6.52	2.17	2.8565
UareU	89.06	10.94	7.81	1.6701
T = 0.4				
DB_FP	86.96	13.04	0.00	2.8552
UareU	73.44	26.56	6.52	1.6690
T = 0.45				
DB_FP	86.96	13.04	0.00	2.8533
UareU	68.75	31.25	1.56	1.6685
T = 0.5				
DB_FP	86.96	13.04	0.00	2.8533
UareU	65.63	34.38	0.00	1.6702
T = 0.55				
DB_FP	69.57	30.43	0.00	2.8114
UareU	65.63	34.38	0.00	1.6687

5 Conclusion

We have developed a good system combining the fingerprint authentication and cryptographic algorithm to online banking transactions which consists of four parts: image enhancement, feature extraction, data encryption and fingerprint authentication. With some improvements which maybe inconsiderable but really effective, our FAS satisfied the high accuracy, the reliable security and the processing time. Furthermore, our system can be suitable for all kinds of online transaction, not only banking transaction since its four modules made it be flexible in various environments. However, it is still needed to limit the dependence of our FAS on experimental thresholds.

References

[1] Davide Maltoni, Dario Maio, Anil K. Jain and Salil Prabhakar, "Handbook of Fingerprint Recognition", SpringerLink, 2009.

[2] A. K. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," *IEEE Trans. on Pattern Anal. Mach. Intell.*, Vol. 19, pp. 302-314, 1997.

[3] V. Conti, G. Milici, S. Vitabile and F. Sorbello, "Morphological Enhancement and Triangular Matching for Fingerprint Recognition", proc. of International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering, (CIS2E 07), e-conference on December 3 - 12, 2007.

[4] Marcelo de Almeida Oliveira and Neucimar Jeronimo Leite, "Reconnection of Fingerprint Ridges Based on Morphological Operators and Multiscale Directional Information", Proceedings of the Computer Graphics and Image Processing, XVII Brazilian Symposium, p.122-129, 2004.

[5] Jiangang Cheng and Jie Tian, "Fingerprint enhancement with dyadic scale-space", *Pattern Recognition Letters*, Vol. 25, pp. 1273-1284, 2004.

[6] Lin Hong, Yifei Wan and Anil K. Jain, "Fingerprint Image Enhancement: Algorithm and performance algorithm", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 8, pp. 777–789, 1998.

[7] Jianwei Yang, Lifeng Liu, Tianzi Jiang and Yong Fan, "A Modified Gabor Filter Design Method For Fingerprint Image Enhancement", Pattern Recognition Letters, vol. 24, issue 12, pp. 1805-1817, 2003.

[8] A. Farina, Z.M. Kovács-Vajna, and A. Leone, "Fingerprint minutiae extraction from skeletonized binary images", Pattern Recognition, pp. 877-889, 1999.

[9] J. C. Amengual, A. Juan, J. C. Prez, F. Prat, S. Sez, and J. M. Vilar, "Real-time minutiae extraction in fingerprint images", Proc. of the 6th Int. Conf. on Image Processing and its Applications, pp. 871–875, 1997.

[10] DarioMaio and David Maltoni, "Direct gray scale minutae detection in fingerprints", IEEE Transaction on Pattern Recognition and Maching Intell., Vol. 19, No. 1, 1997.

[11] Wahab, A., Tan, E. C. and Jonatan, A. "Direct Gray-Scale Minutiae Extraction", Biometric Authentication: First International Conference, ICBA 2004, Hong Kong, China, 2004.

[12] D.P. Mital, Eam Khwang Teoh, "An automated matching technique for fingerprint identification", Proceedings of 22nd International Conference on Industrial Electronics, Control, and Instrumentation, vol.2, pp. 806 - 811 , 1996.

[13] He, Y., J. Tian, X. Luo, and T. Zhang, "Image enhancement and minutiae matching in fingerprint verification", Pattern Recognition Letters, vol.24, pp.1349-1360, 2003.

[14] Yuliang He, Jie Tian, Liang Li, Hong Chen, Xin Yang, "Fingerprint matching based on global comprehensive similarity", Pattern Analysis and Machine Intelligence, IEEE Transactions on vol. 28, pp. 850-862, 2006.

[15] M. Tico, and P. Kuosmanen, "An algorithm for fingerprint image postprocessing", In *Proceedings of the Thirty-Fourth Asilomar Conference on Signals, Systems and Computers,* vol. 2, pp. 1735–1739, 2000.

[16] Tran Minh Triet, "Research and develop information security methods based on AES", PhD thesis, Vietnamese language, 2009.

[17] Jeremy Kubica, Joseph Masiero, Andrew W. Moore, Robert Jedicke, and Andrew Connolly, "Variable KD-Tree Algorithms for Spatial Pattern Search and Discovery", Neural Information Processing Systems, NIPS 2005, Vancouver, British Columbia, Canada, 2005.

[18] C. Arcelli, G. Baja, "A width-independent fast thinning algorithm", IEEE Trans., Pattern Analysis and Machine Intelligence, pp. 463-474, 1985.