IMPLEMENTATION OF FINGER TOKEN AUTHENTICATION TECHNIQUE USING ARTIFICIAL INTELLIGENCE APPROACH IN NTT MICROSYSTEMS

Neha Singh
Asst. Professor
IIMT Eng. College
Meerut

Sumit Chaudhary
Asst. Professor
Shri Ram Group of Colleges
Muzaffarnagar

Monika Garg
Asst. Professor
Shri Ram Group of Colleges
Muzaffarnagar

ABSTRACT

Personal authentication that correctly identifies valid users in an indispensable security technology for enabling people to enjoy the access to data services with a sense of confidence and assurance. Passwords have been extensively used to identify authorized users in the past, but passwords alone are vulnerable because people tend to choose weak password relating to some aspect of them (e.g. birthday, phone number, family name) that can be guessed. This has led to growing interest in biometric authentication using fingerprints that make it possible to identify personal authentication correctly. It eliminates problems of forgotten passwords or lost cards and is currently becoming more popular for convenient and secure authentication. **NTT Microsystems**' is a new and exclusive technology that overcomes the limitations of previous systems and sets a new standard for compact, reliable and low-cost fingerprint authentication. NTT laboratories have developed Finger Token, a portable fingerprint identification device that substitutes a fingerprint instead of password for authentication.

Keywords

Finger Token, USB, CMOS, NTT Microsystems.

1. INTRODUCTION

1.1 Fingerprint Classification

Fingerprint classification [1] is a technique to assign a fingerprint into one of the several pre-specified types already established in the literature which can provide an indexing mechanism. Fingerprint classification can be viewed as a coarse level matching of the fingerprints. An input fingerprint is first matched at a coarse level to one of the pre-specified types and then, at a finer level, it is compared to the subset of the database containing that type of fingerprints only.

1.1.1 Fingerprint Scanning

Fingerprint scanning is the acquisition and recognition of a person's fingerprint characteristics for identification purposes. This allows the recognition of a person through quantifiable physiological characteristics that verify the identity of an individual. There are basically two different types of finger-scanning technology that make this possible. One is an optical method, which starts with a visual image of a finger. The other uses a semiconductor-generated electric field to image a finger. Fingerprint scanning has a high accuracy rate when users are sufficiently educated. Fingerprint authentication is a good choice for in-house systems where enough training can be provided to users and where the device is operated in a controlled environment. The small size of the fingerprint scanner, ease of integration - can be easily adapted to keyboards, and most significantly the relatively low costs make it an affordable, simple choice for workplace access security.

1.1.2 Fingerprint Identification

Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

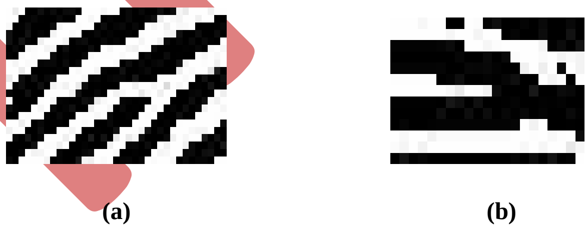
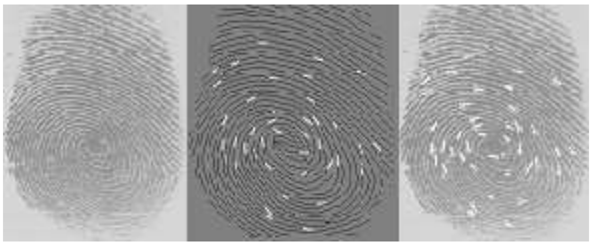

(a)
(b)

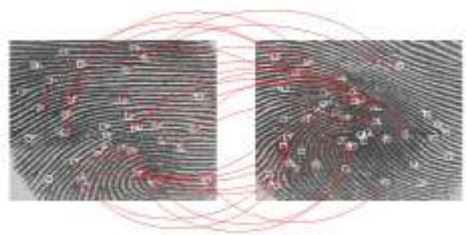
Fig 1: Different Types of minutiae (a) a ridge ending minutiae (b) a ridge bifurcation

1.1.3 Fingerprint Matching

Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows. However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.



(a)



(b)

Fig 2: (a) Finding minutiae points & (b) Matching

1.2 Fingerprint Image Enhancement

A critical step in automatic fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. In order to ensure that the performance of an automatic fingerprint identification/verification system will be robust with respect to the quality of the fingerprint images, it is essential to incorporate a fingerprint enhancement algorithm in the minutiae extraction module.

2. APPROACH

2.1 Fingerprint identification using artificial neural network with optical wavelet preprocessing

The advantages of optical wavelet transform used as a preprocessor for an artificial neural network are investigated. It is shown by digital simulation that this set-up can successfully identify and discriminate complex biometric images, such as fingerprints. The achieved capabilities include limited shift-, rotation-, scale- and intensity-invariance. It is also shown that the edges-enhancement filter, applied before the wavelet transform, significantly improves abilities of the system. The recognition is performed by the artificial neural network with built-in position invariance. Proper choice of the learning method additionally provides rotation-, scale-, and intensity-invariance. To some extent also occluded images can be properly identified.

2.2 Single-Chip Fingerprint Identification LSI using NTT Microsystems

The single-chip fingerprint LSI is a semi-conductor chip that implements all of the processing required for fingerprint identification, from fingerprint sensing to registration and authentication. It is the world's smallest and most energy-efficient fingerprint identification device and can be used to implement compact and highly secure fingerprint identification equipment. The expanding use of digital information and the Internet in recent years has led to steadily increasing attention on personal authentication technology for prevention of unauthorized access impersonation. The methods of personal authentication include cards or keys (possessed items), passwords (remembered), and fingerprints or iris patterns (physical characteristics). Identification by physical characteristics is an appealing method because it is both convenient and reliable. Of the physical methods, fingerprint identification offers the advantages of a superior balance of accuracy and cost, and easily miniaturized sensors.

This chip comprises a 128_128 pixel array, a controller and memory. The small 50 micron pixels contain sensor plates for detecting the ridges and valleys of the fingerprint as differences in capacitance, as well as sensing circuits and parallel processing circuits for comparison in a layered configuration. We developed image processing and matching algorithms for that parallel processing circuits. In addition, the sensor structure is robust against static electricity and soiling and is fabricated by a low-cost process. The fingerprint data does not leave the chip, so user privacy is fully protected. Furthermore, it allows fingerprint identification to be introduced even to devices that do not have processors and can operate on less than 1/30 the power required by conventional technology. The single-chip fingerprint identification LSI is planned to be released as a product by NTT Group companies in 2005. In future work we will proceed with development of applications such as mobile identification equipment that take advantage of the features of the single-chip design.

2.3 How the Finger Token used

The Finger Token is recognized as a standard keyboard when it is connected to a USB port on a PC, and when fingerprint identification succeeds, a password is sent to the PC as if it was entered from the keyboard because there is no need to install any special software or driver software on the PC side, fingerprint authentication can be easily added to applications that are only password protected. Finger Token is a compact and lightweight portable device consisting of a capacitive CMOS fingerprint sensor LSI, a flash memory to store fingerprint reference data, and a CPU to perform the verification processing, and thus provides a convenient and fool- proof method of personal authentication in all kinds of environments. Furthermore, Finger Token also supports multiple fingerprint reference data, and different passwords can be set for each fingerprint, so different fingers can be used for authentication on different applications. In addition to permanent passwords, the system also supports one-time passwords that can be used for enhanced security in some situations. The fingerprint reference data is stored inside the Finger Token device where it can be accessed and managed only by the user, thus giving added assurance to users who are concerned about privacy. We plan to follow up with a practical device for implementing safe and secure personal authentication that can be used anytime and any- where but only by the valid user for accessing ubiquitous services.

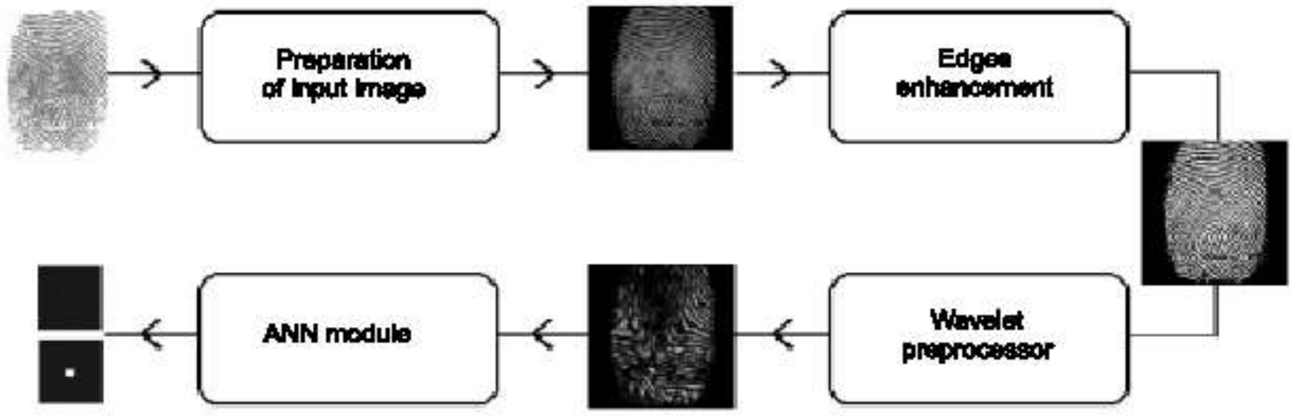


Fig 3: Flowchart of the recognition system

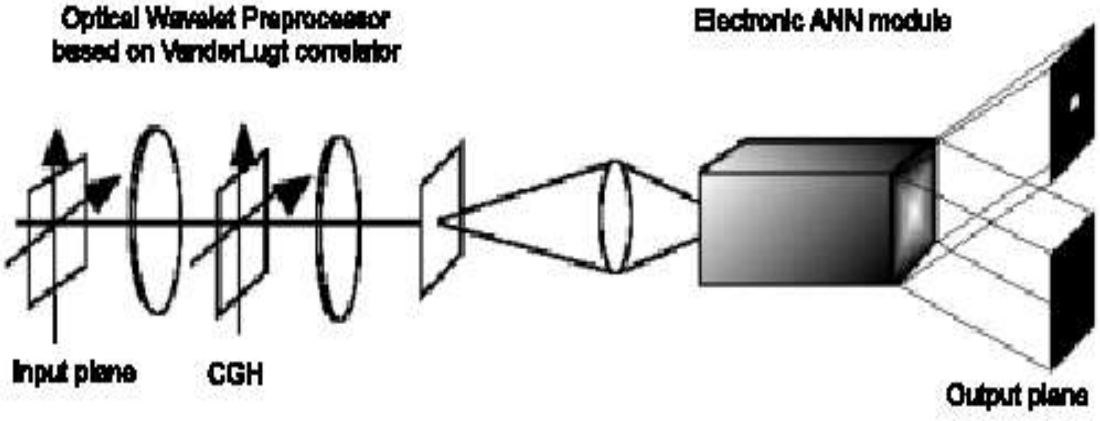


Fig 4: Electronic ANN module with Optical Wavelet Preprocessor based on VanderLugt correlator

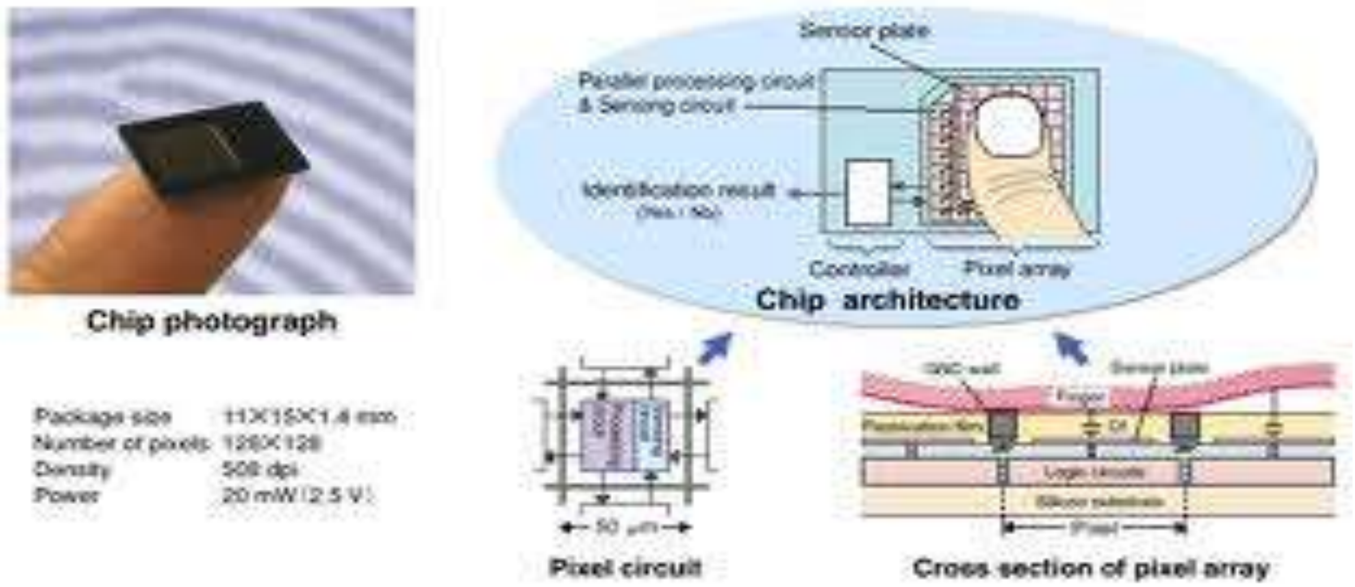


Fig 5: Single-Chip Fingerprint Identification LSI

2.3.1 *Examples of Finger token*

(i) BioPass3000 is a smart card based portable biometric token.

(ii) It combines fingerprint sensor module and the fingerprint verification module with an USB token in one device.
With the on-chip stored fingerprints, BioPass3000 uses the unique fingerprint verification rather than the traditional Password/PIN verification. The BioPass3000 token has all the advantages of a smart card.

Typical applications of finger token are:

(i) E-mail and data encryption
(ii) Web logon
(iii) Digital Signature
(iv) Smart Card logon
(v) Remote Desktop

2.3.2 *Features of finger token*

(i) 32-bit smartcard and high speed fingerprint processor
(ii) 128k On-chip memory, 64K user accessible
(iii) 2048-bit RSA key-pair generation supported
(iv) Long life thermal fingerprint sweep sensor
(v) Resistant to abrasion more than 1 million finger sweeps
(vi) Sensitive data non-exportable outside token
(vii) PKI Ready, CSP and PKCS#11 interface provided

3. CONCLUSION

Current electronic security systems, which rely primarily on passwords, personal identification numbers, and authentication tokens (smart cards) to ensure that a client is an authorized user of a system, all have a common vulnerability,: the verification can be lost, stolen, duplicated, or guessed. With the use of biometric technology, this vulnerability can be nearly eliminated. Different organizations place different value on information protection. While too possibilities for biometrics are great, biometric technology may not be the answer for everyone. The costs per user for some solutions may still be too high. Also to be considered, are the legal considerations of using biometrics, specifically privacy issues? However, for some, biometrics may be the answer.

4. REFRENCES

[1] Le Hoang Thai and Ha Nhat Tam, “Fingerprint recognition using standardized fingerprint model”, IJCSI, volume 7, Issue 3, pp 11-17, May 2010.

[2] Kuntal Barua, Samayita Bhattacharya and Dr. Kalyani Mali, “Fingerprint Identification”, Global Journal of Computer Science & Technology, volume 11, Issue 6, pp 60-64, April 2011.

[3] Nizar Rokbani and Adel Alimi, “Fingerprint identification using minutiae constellation matching”, IADIS Virtual Multi Conference on Computer Science and Information Systems, pp 157-162, 2010.

[4] Raffaele Cappelli, Dario Maio, James L. Wayman, and Anil K. Jain, “Performance Evaluation of Fingerprint Verification Systems”, IEEE Transactions on pattern analysis and machine intelligence, volume 28, Issue 1, pp 3-18, January 2006.

[5] Mary Lourde R and Dushyant Khosla, “Fingerprint Identification in Biometric Security Systems”, International Journal of Computer and Electrical

Engineering, volume 2, Issue 5, pp 852-855, October 2010.

[6] Dr. Neeraj Bhargava, Dr. Ritu Bhargava, Prafull Narooka and Minaxi Cotia, "Fingerprint Recognition Using Minutia Matching" , International Journal of Computer Trends and Technology, volume 3, Issue 4, pp 641-643, 2012.

[7] S.Uma Maheswari and Dr. E. Chandra, "A Review Study on Fingerprint Classification Algorithm used for Fingerprint Identification and Recognition", IJCST, volume 3, Issue 1, pp 739-745, March 2012.

[8] Dayashankar Singh, Dr. P.K.Singh and Dr. R.K.Shukla, "Fingerprint Recognition System Based on Mapping Approach", International Journal of Computer Applications, volume 5, Issue 2, pp 1-4, August 2010.

[9] Madhuri and Richa Mishra, "Fingerprint Recognition using Robust Local Features", IJARCSSE, volume 2, Issue 6, pp 1-5, June 2012.

[10] Minwei He and Huimin Zhao, "A Identity Authentication Based on Fingerprint Identification", International Symposium on Web Information Systems and Applications, pp 261-263, May 2009.

[11] Prathima Devi Sirivella and Mrs D.Raaga Vamsi, "Fingerprint Validation and Outlier Detection Using Minutiae Approach in Network Security", International Journal of Computer& Organization Trends, volume 2, Issue 5, pp 123-127, 2012.

[12] Anil K. Jain and Jianjiang Feng, "Latent Fingerprint Matching", IEEE Transactions on pattern analysis and machine intelligence, volume 33, Issue 1, pp 88-100, January 2011.

[13] Sangram Bana and Dr. Davinder Kaur, "Fingerprint Recognition using Image Segmentation", IJAEST, volume 5, Issue 1, pp 12-23, 2011.

[14] Le Hoang Thai and Ha Nhat Tam, "Fingerprint recognition using standardized fingerprint model", IJCSI, volume 7, Issue 3, pp 11-17, May 2010.

[15] Dr. H.B. Kekre, Dr. Tanuja Sarode and Rekha Vig, "Fingerprint Identification using Sectorized Cepstrum Complex Plane", International Journal of Computer Applications, volume 8, Issue 1, pp 12-15, October 2010.