ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Biometrics and Fingerprint Payment Technology

S.Padma Priya
Assistant Professor & Head, Department of Information Technology,
Sri Adi Chunchanagiri Women's College, Cumbum.

Abstract
This article discusses biometric authentication in relation to payment systems. Biometrics uses biological traits or behavioural characteristics to identify an individual. A Biometrics system is effective pattern recognition system that utilizes different patterns similar to retina patterns, iris patterns and biological qualities like fingerprints, voice recognition, facial geometry and hand recognition etc. Biometric payment system is protected and sheltered and incredibly trouble-free to use and even without using password or top secret codes to keep in mind as compare with previous system like credit card payment system, and mobile banking etc. In daily life the usage of credit cards and debit card for shopping, bill payment, travelling and so on. So problem is that a person has to remember their passwords or secret code and to keep secure to take with him all time. So biometric system will solve this problem. Greater implementation of biometric payment system is more reasonably priced to small business owners. We actually require alternate payment systems.

Keywords
Biometrics, Biometrics Payment System, Biometrics technology.

I. Introduction

Biometrics is automated methods of recognizing a person based on a physiological or behavioral attribute. Along with the quality considered are; face, fingerprint, hand geometry, iris, retinal, signature, and voice. Biometric technologies are fetching the establishment of an extensive array of extremely safe recognition and personal authentication solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

Biometric-based solutions are proficient to offer for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies.

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and inexpensive.

The security field uses three different types of authentication:

●	Something you know — a password, PIN, or piece of personal information (such as your mother's maiden name)
●	Something you have — a card key, smart card, or token (like a Secure ID card)
●	Something you are — a biometric.

Of these, a biometric is the most secure and convenient authentication tool. It can't be borrowed, stolen, or forgotten, and forging one is practically impossible.

II. Types Of Biometric

1. Face Recognition

Face recognition analyzes facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. This technique has attracted considerable interest, although many people don't completely understand its capabilities. Some vendors have made extravagant claims — which are very difficult, if not impossible, to substantiate in practice — for facial recognition devices. Because facial scanning needs an extra peripheral not customarily included with basic PCs, it is more of a niche market for network authentication. However, the casino industry has capitalized on this technology to create a facial database of scam artists for quick detection by security personnel.

2. Fingerprint

Fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional police method of matching minutiae; others use straight pattern-matching devices; and still others are a bit more unique, including things like patterns and ultrasonic. Some verification approaches can detect when a live finger is presented; some cannot.

A greater variety of fingerprint devices is available than for any other biometric. As the prices of these devices and processing costs fall, using fingerprints for user verification is gaining acceptance — despite the common — criminal stigma.

Fingerprint verification may be a good choice for in-house systems, where you can give users adequate explanation and training, and where the system operates in a controlled environment. It is not surprising that the workstation access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size, and ease of integration of fingerprint authentication devices.

3. Hand Geometry

Hand Geometry involves analyzing and measuring the shape of

the hand. This biometric offer a good balances of performance characteristics and is relatively easy to use. It might be suitable where there are more users or where users access the system infrequently and are perhaps less disciplined in their approach to the system.

Accuracy can be very high if desired and flexible performance tuning and configuration can accommodate a wide range of applications. Organizations are using hand geometry readers in various scenarios, including time and attendance recording, where they have proved extremely popular. Ease of integration into other systems and processes, coupled with ease of use, and makes hand geometry an obvious first step for many biometric projects.

4. Iris

Iris based biometric, on the other hand, involves analyzing features found in the colored ring of tissue that surrounds the pupil. Iris scanning, undoubtedly the less intrusive of the eye-related biometrics, uses a fairly conventional camera element and requires no close contact between the user and the reader. In addition, it has the potential for higher than average template-matching performance. Iris biometrics work with glasses in place and is one of the few devices that can work well in identification mode. Ease of use and system integration have not traditionally been strong points with iris scanning devices, but you can expect improvements in these areas as new products emerge.

5. Retina

Retina based biometric involves analyzing the layer of blood vessels situated at the back of the eye. An established technology, this technique involves using a low-intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient if you wear glasses or are concerned about having close contact with the reading device. For these reasons, retinal scanning is not warmly accepted by all users, even though the technology itself can work well.

6. Signature

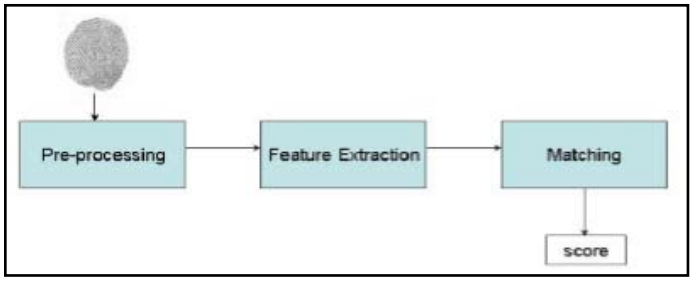
Signature verification analyzes the way a user signs her name. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape. Signature verification enjoys a synergy with existing processes that other biometrics do not. People are used to signatures as a means of transaction-related identity verification, and most would see nothing unusual in extending this to encompass biometrics. Signature verification devices are reasonably accurate in operation and obviously lend themselves to applications where a signature is an accepted identifier. Surprisingly, relatively few significant signature applications have emerged compared with other biometric methodologies. But if your application fits, it is a technology worth considering.

7. Voice Authentication

Voice authentication is not based on voice recognition but on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics has the most potential for growth, because it requires no new hardware — most PCs already contain a microphone. However, poor quality and ambient noise can affect verification. In addition, the enrollment procedure has often been more complicated than with other biometrics, leading to the perception that voice verification is not user friendly. Therefore, voice authentication software needs improvement. One day, voice may become an additive technology to finger-scan technology. Because many people see finger scanning as a higher authentication form, voice biometrics will most likely be relegated to replacing or enhancing PINs, passwords, or account names.

IV. Fingerprint Recognition

The main modules of a fingerprint verification system (cf. Fig.4.1) are: a) fingerprint sensing, in which the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation; b) pre processing, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction; c) feature extraction, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors; and d) matching, in which the feature vector of the input fingerprint is compared against one or more existing templates. The templates of approved users of the biometric system, also called clients, are usually stored in a database. Clients can claim an identity and their fingerprints can be checked against stored fingerprints



1. Fingerprint Sensing

The acquisition of fingerprint images has been historically carried out by spreading the finger with ink and pressing it against a paper card. The paper card is then scanned, resulting in a digital representation. This process is known as off-line acquisition and is still used in law enforcement applications. Currently, it is possible to acquire fingerprint images by pressing the finger against the flat surface of an electronic fingerprint sensor. This process is known as online acquisition.

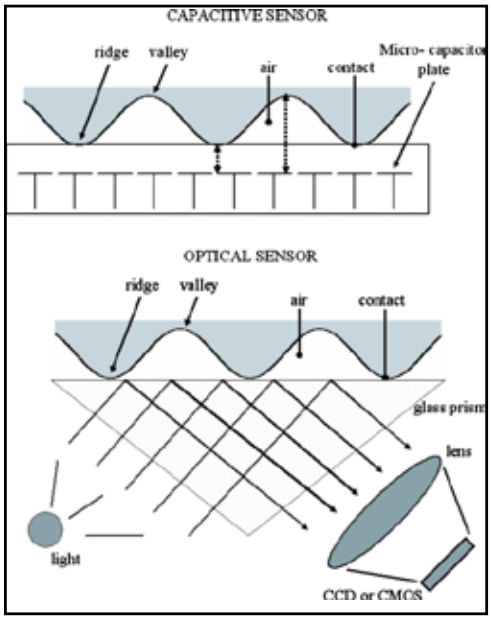


Fig. 4.2 Acquisition principles of silicon and optical sensors

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

There are three families of electronic fingerprint sensors based on the sensing technology

• **Solid-state or silicon sensors** (left part of Fig.4.2): These consist of an array of pixels, each pixel being a sensor itself. Users place the finger on the surface of the silicon, and four techniques are typically used to convert the ridge/valley information into an electrical signal: capacitive, thermal, electric field and piezoelectric. Since solid-state sensors do not use optical components, their size is considerably smaller and can be easily embedded. On the other hand, silicon sensors are expensive, so the sensing area of solid-state sensors is typically small.

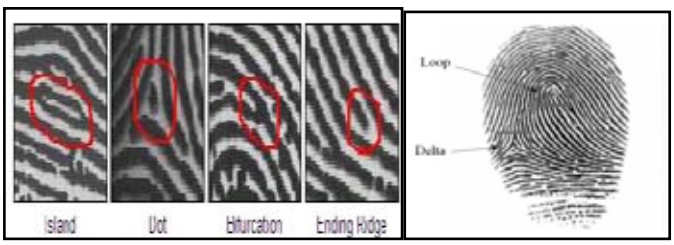
• **Optical** (right part of Fig.4.2): The finger touches a glass prism and the prism is illuminated with diffused light. The light is reflected at the valleys and absorbed at the ridges. The reflected light is focused onto a CCD or CMOS sensor. Optical fingerprint sensors provide good image quality and large sensing area but they cannot be miniaturized because as the distance between the prism and the image sensor is reduced, more optical distortion is introduced in the acquired image.

• **Ultrasound:** Acoustic signals are sent, capturing the echo signals that are reflected at the fingerprint surface. Acoustic signals are able to cross dirt and oil that may be present in the finger, thus giving good quality images. On the other hand, ultrasound scanners are large and expensive, and take some seconds to acquire an image.

A new generation of touch less live scan devices that generate a 3D representation of fingerprints is appearing [22]. Several images of the finger are acquired from different views using a multi camera system, and a contact-free 3D representation of the fingerprint is constructed. This new sensing technology overcomes some of the problems that intrinsically appear in contact-based sensors such as improper finger placement, skin deformation, sensor noise or dirt.

2. Preprocessing and Feature Extraction

A fingerprint is composed of a pattern of interleaved ridges and valleys. They smoothly flow in parallel and sometimes terminate or bifurcate. At a global level, this pattern sometimes exhibits a number of particular shapes called singularities, which can be classified into three types: loop, delta and whorl. In Fig.4.3a, we can see an example of loop and delta singularities (the whorl singularity can be defined as two opposing loops). At the local level, the ridges and valleys pattern can exhibit a particular shape called minutia. There are several types of minutiae, but for practical reasons, only two types of minutiae are considered: ridge ending (Fig.4.3b) and ridge bifurcation (Fig.4.3c). Singularities at the global level are commonly used for fingerprint classification, which simplifies search and retrieval across a large database of fingerprint images. Based on the number and structure of loops and deltas, several classes are defined, as shown inFig.4.4.



The gray scale representation of a fingerprint image is known to be unstable for fingerprint recognition [59]. Although there are fingerprint matching techniques that directly compare gray images using correlation-based methods, most of the fingerprint matching algorithms use features which are extracted from the gray scale image. To make this extraction easy and reliable, a set of pre-processing steps is commonly performed: computation of local ridge frequency and local ridge orientation, enhancement of the fingerprint image, segmentation of the fingerprint area from the background, and detection of singularities. The local ridge orientation at a pixel level is defined as the angle that the fingerprint ridges form with the horizontal axis [59]. Most of the algorithms do not compute the local ridge orientation at each pixel, but over a square-meshed grid (Fig.4.5). The simplest approach for local ridge orientation estimation is based on the gray scale gradient. Since the gradient phase angle denotes the direction of the maximum pixel-intensity change, the ridge orientation is orthogonal to this phase angle. There are essentially two orientation estimation techniques: direction tensor sampling and spectral tensor discretization using Gabor filters. For its computational efficiency the method independently suggested by is the most commonly used in fingerprint applications because the spectral approach needs more filtering. We refer to[12] for a detailed treatment of both approaches.

Fig. 4.4 The six major fingerprint classes: (a) arch, (b) tented arch, (c) left loop, (d) right loop, (e) whorl, and (f) twin-loop

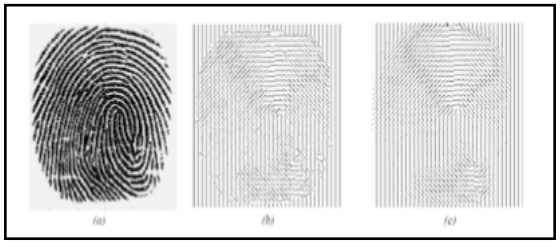


Fig. 4.5 Local ridge orientation of a fingerprint image computed over a square-meshed grid: (a) original image, (b) orientation image, and (c) smoothed orientation image. Each element of (b) and (c) denotes the local orientation of the ridges

The local ridge frequency at a pixel level is defined as the number of ridges per unit length along a hypothetical segment centred at this pixel and orthogonal to the local ridge orientation[59]. As in the case of the local ridge orientation, the local ridge frequency is computed over a square-meshed grid. Existing methods [39, 56, 52] usually model the ridge-valley structure as a sinusoidal-shaped wave (Fig.4.6), where the ridge frequencies set as the frequency of this sinusoid, and the orientation is used to angle the wave.

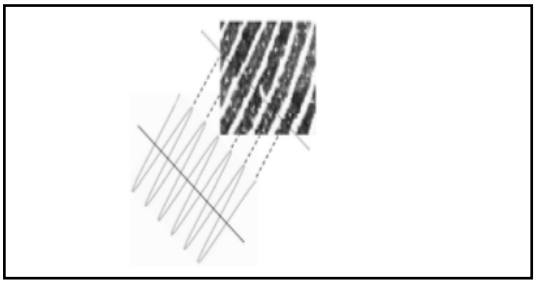


Fig. 4.6 : Modelling of ridges and valleys as a sinusoidal-shaped wave

Ideally, in a fingerprint image, ridges and valleys flow smoothly in a locally constant direction. In practice, however, there are factors that affect the quality of a fingerprint image (cf.,Fig4.7): wetness or dryness of the skin, noise of the sensor, temporary or permanent cuts and bruises in the skin, variability in the pressure against the sensor, etc. Several enhancement algorithms have been proposed in the literature with the aim of improving the clarity of ridges and valleys. The most widely used fingerprint enhancement techniques use contextual filters, which mean changing the filter parameters according to the local characteristics (context) of the image. Filters are tuned to the local ridge orientation and/or frequency, thus removing the imperfections and preserving ridges and valleys (cf.Fig.4.8).

Fig. 4.7 : Fingerprint images with different quality. From left to right: high, medium and low quality, respectively

Fingerprint segmentation consists of the separation of the fingerprint area (foreground) from the background. This is useful to avoid subsequent extraction of fingerprint features in the background, which is the noisy area. Global and local thersholding segmentation methods are not very effective and more robust segment

58 F. Alonso-Fernandez, J. Bigun, J. Fierrez et al.

Fig. 4.8 Examples of original and enhanced fingerprint images techniques are commonly used [65, 44, 55, 9, 79, 67].

These techniques exploit the existence of an oriented periodical pattern in the foreground and a no oriented isotropic pattern in the background (Fig.4.9).

Fig. 4.9 : Segmentation of fingerprint images: (left) original image and (right) segmentation mask

As mentioned above, the pattern of ridges and valleys exhibits a number of particular shapes called singularities (Fig.4.3a). For the detection of singularities, most of the existing algorithms rely on the ridge orientation information (Fig.4.5). The best-known algorithm for singularity detection is based on the Poincar´ e index[48, 47, 10]. Alternatively, detection of core and delta type singularities was shown to be efficient and precise using different filtering techniques. Once the fingerprint image has been pre-processed, a feature extraction step is performed. Most of the existing fingerprint recognition systems are based on minutiae matching, so that reliable minutiae extraction is needed. Usually, the pre-processed fingerprint image is converted into a binary image, which is then thinned using morphology (Fig.4.10). The thinning step reduces the ridge thickness to one pixel, allowing straightforward minutiae detection. During the thinning step, a number of spurious imperfections may appear (Fig.4.11a) and thus, a post processing step is sometimes performed (Fig.4.11b) in order to remove the imperfections from the thinned image. Several approaches for binarization, thinning and minutiae detection have been proposed in literature[59]. However, binarization and thinning suffer from several problems: a) spurious imperfections; b) loss of structural information; c) computational cost; and d) lack of robustness in low quality fingerprint images. Because of that, other approaches that extract minutiae directly from the gray scale image have been also proposed[53, 55, 54, 46, 20, 17, 31].

Fig. 4.10 : Binarization and thinning of fingerprint images using contextual filters

Fig. 4.11 : Thinning step: (a) typical imperfections appeared during the thinning step, and (b) a thinned fingerprint structure before and after removing imperfections

V. Conclusions

Biometrics is a means of verifying personal identity by measuring and analyzing unique physical or behavioural characteristics like fingerprints or voice patterns. The conclusion of this whole paper is that the card-less payment system should be replaced and there must be more easier, reliable, secure, cash free and tension free payment system, i-e biometric payment system in which no body have to take with dozens of cards for shopping, travelling, pass in office, university or bank as door lock. And the International Journal of Advanced Science and Technology Vol. 4, March, 2009 36 must have some secure codes to access as authorization and there is also one another disadvantage is that there may be stolen of cards or it can be losses at any time without any care. So to consider all these kinds of problems and disadvantages of card payment system the fingerprints payment system is suggested to be implemented because it is easier, reliable, feasible, secure and easily authorized to everyone. And there is no any worry that anyone can stolen my finger are can be loosed anywhere so other body can use it. In fingerprint payment system customer has to place his fingers on the finger scanner and then scanner will recognize the account which belongs to that person and charge the bill. So it is easy for both customer and seller because there is no

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

need to scratch the credit card and then enter code if code is forgot or if some time card cannot read and many more problems can occur in card payment system. And in biometric payment system no need to carry cash with them. Biometric payment system may be like fingerprints, IRIS, face recognition and blood reading or skin reading and it may be installed at any store, university, library, hostel, bank, office, home door lock, internet online shopping and many kinds where card system is installed. So in this paper we explain the biometrics with detailed term, how fingerprint system works, fingerprints' types and fingerprint recognition through circular sampling.

References

[1] *T. F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. G. Neumann, H. S. Javitz, A. Valdes, and T. D. Garvey. AReal-Time Intrusion Detection Expert System (IDES) - Final Technical Report. Technical report, SRI Computer Science Laboratory, SRI International, Menlo Park, CA, Feb. 1992.*

[2] *Dr. Yashpal Singh and Singh Chauhan, Neural networks in data mining. Journal of Theoretical and Applied Information Technology (2005-2009), vol, 5, no. 6. pp. 37-42.*

[3] *Khyati Chaudhary, Jyoti Yadav and Bhawna Mallick, A review of fraud detection techniques: credit-card, International Journal of Computer Applications (2012), vol. 45, no. I, pp.39-44*

[4] *Cybercrime: protecting against the growing threat Global Economic Crime Survey – PWC Global Economic. [ONLINE]. Available at: http://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf. [Accessed 12 December 2012].*

[5] *S. Rosset, U. Murad., E. Neumann, Y. Idan, and G. Pinkas. Discovery of fraud rules for telecommunicationslchallenges and solutions. In Proceedings of the fifth ACM SlGKDDinternational conference on Knowledge discovery and data mining, pages 409-413. ACM Press,1999.*