# CHAPTER 1

**INTRODUCTION**

A payment system is a system for the transfer of money, which employs cash-substitutes. Traditional payment systems are negotiable instruments such as drafts (e.g., checks), credit cards and other charge cards, documentary credit and electronic funds transfers. But these payment systems suffer the shortcomings that the tokens or passwords to ensure the security of the systems are easily lost, forgotten, copied, shared or distributed. Biometrics payment is a kind of technology that allows people to pay at shops or markets with just touch of their fingers, moving their face or laying up their hands. Different with the normal payment methods, they won’t need tokens or passwords except their own biometrics. When people use a biometrics payment system, their account information in the bank is automatically recognized to finish the payment procedure. Biometrics payment has the following advantages

The authentication of the enrolled data is the key part of the payment system. Biometrics has the characteristics such as difficulty to be lost or forgotten, extremely difficult to copy, share, and distribution. Fingerprint is one of the biometrics, which has high university, distinctiveness, easy collectability, and high performance. So it is able to be used for the payment system which needs high security to identify the person are genuine owner. For the data translation securely in public network, digital signature is a popular way to ensure the integrity of the data. One of the biometrics payment approach is the fingerprint payment system as below Figure 1, people just place their finger on the fingerprint reader, then enter their own personal identify number (PIN) and choose the payment method. Then people had done the payment with their fingers. The processes are without signing and swiping.

However, due to the complex input conditions such as input with broken fingers, smeared fingers and fuzzy fingers, it is difficult for extracting all the correct minutiae. So the traditional minutiae-based fingerprint identification system may cause identification failure. In addition, based on single biometric verification technology (fingerprint, face or hand recognition), there are demerits: some biological features missing (such as broken finger), injuries (such as damaged fingers), disease (such as cataract), or feature collection of poor quality (such as light changes in face recognition), these factors will result in non-robust, poor reliability, weak identification.

Comparing with single biometric verification technologies, multimodal ones have clearly advantages. The multimodal biometric is able to integrate various single biometric verification, and uses of the merits of all kinds of single biometrics to improve the performance of the system and achieve a more robust system with noise immunity, universality, reliability, security. Multimodal biometric is widespread in recent years and becomes a research focus. However, the choice of biometrics is crucial, both fingerprint and face verification methods are widely used and have their own merits. Face verification is the best supplement to the fingerprint verification system. On the other hand, the complex system is proportional to the number of input biometrics. For a payment system, less time consuming is need. The fingerprint and face biometrics are proved to ensure the security of identification with high speed . So, in this paper, we explore a multimodal biometrics authentication technique including fingerprint and face biometrics.

**CHAPTER 2**

**Types of Biometrics**

There are several human distinguishable traits that fit the definition of biometrics given above. In order to be used for recognizing a person, the human trait needs to be unique and not subject to change. Fingerprints, for example, have been used for over one hundred years and, therefore, are generally well accepted as a recognition technology. Other technologies such as face, hand geometry, speaker and iris recognition are also generally accepted. A biometric that would require giving a blood sample for frequent personal verification would probably not be very well accepted. Performance considerations are important. No biometrics can guarantee one hundred percent accuracy. A brief introduction of the commonly used biometrics is given below:

**2.1 DNA:**

Deoxyribo Nucleic Acid (DNA) is the one- dimensional ultimate unique code for one’s individuality - except for the fact that identical twins have identical DNA patterns. It is, however, currently used mostly in the context of forensic applications for person recognition. Three issues limit the utility of this biometrics for other applications:

(i) Contamination and sensitivity

(ii) Automatic real-time recognition issues

(iii)Privacy issues

**2.2 Ear:**

It has been suggested that the shape of the ear and the structure of the cartilegenous tissue of the pinna are distinctive. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual.

**2.3 Face Recognition:**

Different technologies can be used for face recognition. One approach consists on capturing an image of the face using an inexpensive camera (visible spectrum). This method typically models key features from the central portion of a facial image extracting these features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. Major benefits of facial recognition are that it is non-intrusive, hands-free, provides for continuous authentication and is accepted by most users. Enrollment sample sizes (e.g.,5 face samples) may range from 1 KB-2KB/sample). Smaller template sizes are also used (e.g., less than 100 bytes).

**2.4 Fingerprints:**

Fingerprints are important. By 1998, fingerprint recognition products accounted for 78% of the total sales of biometric technology. These products look at the friction ridges that cover the fingertips and classify patterns of minutiae, such as branches and end points of the ridges. Some also look at the pores in the skin of the ridges. Fingerprint recognition devices for desktop and laptop access are widely available from many different vendors at a low cost. [15] The relatively small size allows the sensor to be integrated in other devices (e.g., mice, keyboards). This biometric technology uses the pattern of friction ridges and valleys on an individual's fingertips. These patterns are considered unique to a specific individual. The same

fingers of identical twins will also differ. A user does not need to type passwords - instead, only a touch to a fingerprint device provides almost instant access (typically less than 1 sec.). A typical enrollment identifier may include 2 finger samples (e.g., 1 KB) although smaller finger samples are also used. One of the challenges of fingerprint technology is individuals that have poorly defined (or tenuous) ridges in their fingerprints.

**2.5 Hand and Finger Geometry:**

Hand recognition has been available for over twenty years. To achieve personal authentication, a system may measure physical characteristics of the fingers or the hand such as length, width, thickness and surface area of the hand. These methods of personal authentication are well established. Some systems require a very small biometric sample (e.g., 9 bytes). Hand geometry can frequently be found in physical access control for commercial and residential applications, for time and attendance systems, and for general personal authentication applications. In addition, an individual's jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry information.

**2.6 Retinal Scanning:**

This method of personal authentication uses the vascular patterns of the retina of the eye. In healthy individuals, the vascular pattern in the retina does not change over the course of an individual’s life. The patterns are scanned using a low-intensity (e.g., near-infrared) light source. It requires the user to look into a device and focus on a given point. The image acquisition involves cooperation of the subject, entails contact with the eyepiece.

**2.7 Signature Verification:**

The way a person signs her name is known to be a characteristic of that individual. Signatures of some people vary substantially: even successive impressions of their signature are significantly different. It is based on measuring dynamic signature features such as speed, pressure and angle used when a person signs a standard, recorded pattern (e.g., autograph). One focus for this technology has been e-business applications.

**2.8 Voice Recognition:**

Voice recognition or speaker recognition is the problem of identifying a speaker from a short utterance. This biometric technology uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style). A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel.

**CHAPTER 3**

**Fingerprint Payment System**

Biometric payment technology allows the consumer to pay with the touch of a finger on a fingerprint scanner linked to a payment file. The fingerprint template is typically linked to a router and transmission media necessary to clear the transaction through an automated clearinghouse. While many biometric payment transaction providers focus on grocery, home improvement and convenience stores, others have indicated interest in quick-serve eateries, car wash locations and select vending operations. Biometric payment providers (e.g., Pay-by-Touch and BioPay) require completion of a pre-enrollment process in which index fingers are scanned and driver’s license and banking information is recorded in an account database. This process reportedly takes less than two minutes. In addition to transaction settlement, biometric payment providers may also link captured transactions to loyalty reward programs, gift cards, discount coupons and Web access services.

**3.1 Rapid Transactions and Reduced Fees:**

Just how fast can biometric payment systems process transactions? Pay-by-Touch and BioPay state transaction times range from 5 to 15 seconds, which they claim is favorable compared to cash, credit card or debit card settlement. While the speed of the transaction may be attractive, decreased transaction fees may be more persuasive as a selling point. Since a biometric payment transaction is treated as an automated clearinghouse debit, fees tend to be significantly lo-wer (estimated at 75 percent) than comparable credit card or signature-debit card transactions.

**3.2 Fingerprint template:**

The first step in fingerprint identification is collecting the fingerprint using a special sensing device. This process is referred to as enrollment. In this step, the fingerprint is acquired for authentication. The captured image (called the fingerprint template) can be stored directly as an image or can be stored as a biometric algorithm. In the case of a biometric algorithm, several data points on the fingerprint template are scientifically measured and stored, thereby leading to discarding of the actual fingerprint. Algorithm software measures 40 or more data points for each fingerprint and may store these measurements as data coordinates or encrypt them into a digital certificate for future authentication. When the mathematical representation of the fingerprint, not the actual fingerprint, is used to prove identity, a higher level of reliability is realized. In addition, some biometric payment systems may require the consumer to also swipe or wave a smart card in addition to scanning a finger to authenticate a transaction. This approach provides another layer of security than exclusively relying on fingerprint matching.

**3.3. Fingerprint Recognition through Circular Sampling**

The use of one’s fingerprints as a means of identification has existed long before its common usage today in the field of criminal investigation. Before nineteenth century, fingerprints were primarily used only as a signature for indicating authorship or ownership. Other applications were not acknowledged until about 1860 when William Hershel was regularly imprinting the handprints of those engaged in his contracts. It was not until 1881 when Henry Faulds recognized that fingerprints found at crime scenes may be used to identify the perpetrator. Since 1924, the FBI has accumulated about 30 million sets of fingerprints acing the matching of a single fingerprint with such a collection very difficult. With the advent of advanced computer technology in the past few decades, automated fingerprint identification systems (AFIS) can

effectively perform what would otherwise be a laborious and time consuming task.

**3.4 Fingerprint Uniqueness**

What actually makes a fingerprint unique depends on one main factor. Fingerprints basically consist of ridges (raised skin) and furrows (lowered skin) that twist to form a distinct pattern. When an inked imprint of a finger is made, the impression created is of the ridges while the furrows are the uninked areas between the ridges. Although the manner in which the ridges flow is distinctive, other characteristics of the fingerprint called ‘minutiae’ are what is most unique to the individual (See figure 1 for several minutiae representations). These features are particular patterns consisting of terminations or bifurcations of the ridges. Moreover, all fingerprints can be classified into three categories based on their major central pattern. These patterns are the arch, loop, and whorl, which are shown in figure 1.



Figure 3.1 Minutiae examples



Figure 3.2 Three major fingerprint classifiers

An image, such as that of a fingerprint, may be considered as a two-dimensional continuous signal. By this, it can have an infinite number of brightness intensities in an infinitesimal area. In order for an image to be handled by a computer, it must first be digitized. For this study, the image had to be sampled in a different manner. Instead of sampling in the general Cartesian space, the image is sampled through a pattern consisting of concentric circles. It may be considered that this technique is sampling in a polar coordinate space. Under this approach, the sampling resolutions are the distance between the concentric circles and the sampling interval within the circumference of the circles

**CHAPTER 4**

**Fingerprint Identification**

**4.1 Fingerprint Matching**

Fingerprint matching techniques can be placed into two categories: minutae-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. The correlation-based method is able to overcome some of the difficulties of the minutiae-based approach. 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 as shown in figure 2.





Figure 4.1 Fingerprint matching

**4.2 Fingerprint Classification**

Fingerprint classification 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 prespecified types and then, at a finer level, it is compared to the subset of the database containing that type of fingerprints only. Fingerprints are classified into five classes, namely, whorl, right loop, left loop, arch, and tented arch as shown in Figure.5. This information is quantized to generate a Finger Code which is used for classification.

**4.3 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.





Figure 4.2 Five classes of fingerprints

**4.4 Fingerprint readers**

Before we can proceed any further we need to obtain the digitalized fingerprint. The traditional method uses the ink to get the fingerprint onto a piece of paper. This piece of paper is then scanned using a traditional scanner. This method is used only rarely today when an old paper-based database is being dig- *scanning* italised, a fingerprint found on a scene of a crime is being processed or in law enforcement AFIS systems. Otherwise modern live fingerprint readers are used. They do not require the ink anymore. These live fingerprint readers are most commonly based on optical, thermal, silicon or ultrasonic principles. Optical fingerprint readers are the most common at present. Theyare based on reflection changes at the spots where the finger papilar lines touch the readers surface. The size of the optical fingerprint readers typically is around 10 \_ 10 \_ 5 centimeters. It is difficult to minimize them much more as the reader has to comprise the source of light, reflection surface and the light sensor.



Figure 4.3 Different Biometric fingerprint reader

**CHAPTER 5**

# How Biometrics Works

Today’s world in Airports, hospitals, hotels, grocery stores and even theme parks increasingly use **biometrics** -- technology that identifies you based on your physical or behavioral traits -- for added security. In this topic, you'll learn about biometric systems that use handwriting, hand geometry, voiceprints, iris structure and vein structure. You'll also learn why more businesses and governments use the technology, recorded voice and silicone hand could really get James Bond into the lab (and let him save the world). You take basic security precautions every day -- you use a key to get into your house and log on to your computer with a username and password. You've probably also experienced the panic that comes with misplaced keys and forgotten passwords. It isn't just that you can't get what you need -- if you lose your keys or jot your password on a piece of paper, someone else can find them and use them as though they were you.Instead of using something you have (like a key) or something you know (like a password), biometrics uses **who you are** to identify you. Biometrics can use **physical characteristics,** like your face, fingerprints, irises or veins, or **behavioral characteristics** like your voice, handwriting or typing rhythm. Unlike keys and passwords, your personal traits are extremely difficult to lose or forget. They can also be very difficult to copy. For this reason, many people consider them to be safer and more secure than keys or passwords.

**Biometric systems can seem complicated, but they all use the same three steps:**

1.**Enrollment**: The first time you use a biometric system, it records basic information about you, like your name or an identification number. It then captures an image or recording of your specific trait.

**2.Storage**: Contrary to what you may see in movies, most systems don't store the complete image or recording. They instead analyze your trait and translate it into a code or graph. Some systems also record this data onto a smart card that you carry with you.

3.**Comparison**: The next time you use the system, it compares the trait you present to the information on file. Then, it either accepts or rejects that you are who you claim to be.

**Systems also use the same three components:**



**1.Sensor** that detects the characteristic being used for identification

**2.Computer** that reads and stores the information

**3.Software** that analyzes the characteristic, translates it into a graph or code and performs the actual comparisons

This laptop features a fingerprint scanner,

bringing biometric security to the home.

# How Fingerprint Scanners Work

Consists of automated methods of recognizing a person based on unique physical characteristic. Each type of biometric system, while different in application, contains at least one similarity: the biometric must be based upon a distinguishable human attribute such as a person's fingerprint, iris, voice pattern or even facial pattern.Today fingerprint devices are by far the most popular form of biometric security used, with a variety of systems on the market intended for general and mass market usage. Long gone are the huge bulky fingerprint scanners; now a fingerprint scanning device can be small enough to be incorporated into a laptop for security.A fingerprint is made up of a pattern of ridges and furrows as well as characteristics that occur at Minutiae points (ridge bifurcation or a ridge ending). Fingerprint scanning essentially provides an identification of a person based on the acquisition and recognition of those unique patterns and ridges in a fingerprint. The actual fingerprint identification process will change slightly between products and systems. The basis of identification, however, is nearly the same. Standard systems are comprised of a sensor for scanning a fingerprint and a processor which stores the fingerprint database and software which compares and matches the fingerprint to the predefined database. Within the database, a fingerprint is usually matched to a reference number, or PIN number which is then matched to a person's name or account. In instances of security the match is generally used to allow or disallow access, but today this can also be used for something as simple as a time clock or payroll access.

**Here's an example of how one fingerprint payment system works:**

* The shopper registers for a biometric program at a store kiosk by presenting valid identification and bank account information.
* The shopper scans his index finger using the kiosk's fingerscan reader.
* The store's fingerscan reader encrypts multiple point-to-point measurements of the fingerprint and stores the customer's biometric data and banking information in a centralized database.
* The shopper now has the option of selecting biometric payment at the point of sale register. If he chooses biometric payment, he scans his finger at the checkout register with the store's electronic reader and enters his personal identification number.
* The electronic reader compares the data from the new scan to the encrypted data in the database and either approves or declines the transaction. If approved, the funds are electronically transferred from the shopper's account to the merchant.

**PROCESS OF ENROLLING AND IDENTIFYING THE USER**

The biometric companies must research why some merchants are hesitated from implementing this cost-saving and convenient system in their business. A similar problem to this hesitation is the introduction of the credit cards back in the 1960s. They were not actually fully accepted by the public until a decade later (Cuneo, 2004). The biggest problem that biometric companies have to face is the privacy issues. Some feel uncomfortable letting a system take their fingerprint because they fear that it will be tracked by the government or law enforcement (Embrey, 2003). Others feel that even though the fingerprint is encrypted, computer hackers will find a way to decrypt the fingerprint into the actual print (Ananthaswmy, 2007). Another problem with the biometric payment technology is valid customers could be denied access to their financial information if their fingerprint is affected by a bad cut, chemical solutions, or even dirt on their finger like construction workers (Down, 2005 and Halperin, 2005). Shown below is an example of a damaged finger. One of the ways to ease customer’s concerns about biometric technology is to conduct a focus group to discuss the benefits and pitfalls of this system. The benefit of a focus group is to obtain information from real people and gather ideas on what could be done to get the public to be comfortable with this new technology. They also might be able to provide some valuable suggestions that biometric companies have not thought of. In order for biometric payment companies to be more accepted in the community, according to the article “Everything’s Changing,” “education will help customers adapt to new tools and make the transition as easy as possible” An example of a technology that was successful at this was the introduction of the barcode, now business life is unimaginable without it.

**Process of Verifying User.**

The verification process involves the customer verifying their identity through a live fingerprint to authenticate a payment. This process is carried out every time the customer is carrying out a payment. The factors to be considered in designing an online verification system are:

a) Is the system supposed to recognize any of the enrolled fingers or will the customer be prompted to present a specific finger or sequence of fingers.

b) Are all enrolled fingers to be verified for completing verification or any one finger will be sufficient.

c) Is 360 degrees rotation to be allowed for verification?

d) What is the extent of verification required (strict, moderate, weak)?

In verification process the customer enters their customer identity number into the verification system. The system then prompts the customer to present their live fingerprint on the scanner. The live fingerprint is then compared with the biometric template stored against the customer identity number in the biometric server. In case the verification is successful the payment transaction is considered authenticated and the transaction sent to the bank for processing. In case of a failure the customer may be asked to present the finger again up to a certain maximum number of tries.

verification process involves a customer entering their customer ID into the system through a numeric keypad. The device then connects to the biometric server over GPRS or dial-up (both options available) to retrieve the templates stored against that ID. Verification is then carried out and if verified, the system allows the payment to proceed to the acquirer. There are two methods possible to connect the biometric verification process to the payment process as follows;

1. First verification is carried out. The verification status is then sent from the PoS as a part of the payment packet (as a flag) to the acquirer for payment processing. The flag status is considered as verification status by the acquirer.
2. A payment packet is sent with the customer ID to the bank host, which in turn connects to the biometric server with the customer ID and PoS number and requests it to complete the verification. The biometric server connects to the PoS to complete the verification process between the live fingerprint and the template extracted using the customer ID. The verification status is then sent back by the server to the bank host for further processing. The primary difference between the approaches is in the network configuration. Option

**CHAPTER 6**

# Advantages and Disadvantages of Biometrics

**Advantages of Biometrics:**

* Increase security - Provide a convenient and low-cost additional tier of security.
* Reduce fraud by employing hard-to-forge technologies and materials. For e.g.Minimise the opportunity for ID fraud, buddy punching.
* Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For e.g. Prevent unauthorized use of lost, stolen or "borrowed" ID cards.
* Reduce password administration costs.
* Replace hard-to-remember passwords which may be shared or observed.
* Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access
* Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN!
* Offer significant cost savings or increasing ROI in areas such as Loss Prevention or Time & Attendance.
* Unequivocally link an individual to a transaction or event.

**Disadvantages of a Biometric System.**

* The finger print of those people working in Chemical industries are often affected. Therefore these companies should not use the finger print mode of authentication.
* It is found that with age, the voice of a person differs. Also when the person has flu or throat infection the voice changes or if there there are too much noise in the environment this method maynot authenticate correctly. Therefore this method of verification is not workable all the time
* For people affected with diabetes, the eyes get affected resulting in differences.
* Biometrics is an expensive security solution

**CHAPTER 7**

**Application of Biometric payment**

**Biometric ATM Uses Fingerprints Instead of a PIN**

Biometric ATM's are the latest inventions to help us avoid fraud and duplication. If somebody steals our card and also knows our PIN they can easily withdraw cash from our account. In case of biometric ATM's they cannot. Usually the PIN for bio ATM's is the finger print of the card holder or his eye retina scan etc. These cannot be duplicated and hence they are very safe and secure.

**Biometric In Retail Industry**

Buying groceries with the touch of a finger could be closer than you think, if new research touting the benefits of biometric payment for retail giants like Wal-Mart, Target, and Costco is anything to go by using biometric.

# Pay By Touch

Pay By Touch was a company founded by John P Rogers. It was a privately held company which enabled consumers to pay for goods and services with a swipe of their finger on a biometric sensor. It allowed secure access to checking, credit card, loyalty, healthcare, and other personal information, through the unique characteristics of an individual's biometric features, thereby creating a highly security-identity theft platform.

**CHAPTER 8**

**CONCLUSION**

Biometric payment technology has become a mature technology and can actually support applications in the real world. However, few organizations have embraced this technology. In this Report, a pivotal survey was conducted to investigate into the reasons why organizations resist the adoption of this technology. Preliminary results provide some useful information to help organizations assess the feasibility of incorporating this technology into the framework of their enterprise-wide information systems. The example of biometric aided ATMs in Japan is the start of a proliferation of biometric technologies in the banking sector. There is a high potential for biometrics in combination with smart cards. In the near future there will be more and more impact on the finance and banking sector in relation to biometric technologies. Anyway there are challenges, in particular the huge investment in the IT infrastructure at ATMs and POS terminals and the lack of interoperability of biometric technologies. Concerning legal aspects the data privacy protection laws in Europe have to be taken into account.

.

**CHAPTER 9**

**REFERENCES**

[1] http://www.paybytouch.com/portal/site/main.

[2] Y. Isobe, Y. Seto, M. Kataoka, “Development of Personal Authentication System using Fingerprint with Digital Signature Technologies”, 34th Annual Hawaii International Conference on System Sciences (HICSS-34)-Vol. 9, 2001.

[3] A. A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[4] A.K. Jain, K. Nandakumar, A. Ross, “Score Normalization in Multimodal Biometric Systems”, Pattern Recognition, 2005.

[5] N. Ratha, K. Karu, C. shaoyun, and A. Jain, “A real-time matching system for large fingerprint databases”. IEEE Trans. On Pattern Anal.And Machine Intell. 18(8), pp 799-813, Aug. 1996.

[6] A.K. Jain, R.Bolle, and S. Pankanti, “On-line fingerprint verification”. IEEE Trans. On Pattern Anal. And Machine Intell. 19(4), pp 302-314, Apr. 1997.

[7] C. Powell “UK Co-op offers biometric payment” in Biometric Technology Today M. Lockie, Ed. March 2006.

[8] G. von Graevenitz „Erfolgskriterien und Absatzchancen biometrischer Identifikations verfahren“, 1st ed. ser. Management Wissen aktuell G.-M. Hellstern, Ed. Berlin:

Lit Verlag, 2006.

[9] Heise Online “Citibank Singapur führt biometrisches Bezahlsystem ein” November 2006. Online: http://www.heise.de/newsticker/melding /81378