

Biometrics in Smart Cards

Monika Gupta

Abstract

Smart cards functions include electronic payment, identification, network computing, health care management, transit, and access control. When performing these functions, the user of the smart card has to validate his or her identification by providing a PIN code. The problem with a PIN code is that a valid user can forget it or an invalid user may guess it. One of the secure ways to overcome the problem is the use of biometrics with smart cards. Biometric features have the advantage that they cannot be lost, forgotten or unintentionally given to someone else. This paper explains how a smart card verifies its user using biometrics. With respect to the processing of the biometric data, the smart card may fulfill one of two functions: it may simply be a device for storing the data or it may process the data, i.e. perform the biometric verification. Three biometric techniques: fingerprint, hand geometry and iris recognition are compared to evaluate which technique is most viable to be used with smart cards. The comparison and analysis is done on the basis of template size, verification time, false acceptance rate and false rejection rate.

1. Introduction

A very basic definition of a processor smart card is: a credit card sized plastic card that contains a microprocessor and provides some quantity of computing power and storage capacity [4]. Turban and McElroy [11], describe applications and benefits of smart cards such as access control, community services, education, electronic payment, transit etc. The convenience and security of any transaction using smart card has led to its widespread use. To ensure a higher level of security, it has become imperative to make the use of smart cards more secure as it contains very important information related to its user. Theft of smart cards could lead to putting all the confidential data in the hands of unauthorized users and could potentially be used to steal identity, money etc. A simple PIN code verification also by itself is not sufficient. A smart card has to be “smart” enough so as to verify that it is being used by the authorized user. Biometric methods, by which an individual is identified from his or her personal features, are becoming increasingly important. Biometric identification refers to identifying an individual based on his or her distinguishing physiological and/or behavioral characteristics [2]. Since these characteristics are different for each person, biometric identifiers are more reliable and more capable in differentiating between an authorized person and an imposter. There are a multitude of biometric techniques either widely used or under investigation. This paper discusses fingerprint, hand geometry and iris recognition techniques and compares four of their attributes. The biometric technique that scores the highest across all the

attributes will be considered most viable to integrate in smart cards.

2. Smart cards

A smart card has an integrated circuit chip embedded within the plastic card and this makes it “smart”. The marriage between a convenient plastic card and a microprocessor allows an enormous amount of information to be stored, accessed and processed either online or offline. Smart cards can store several hundred times more data than a conventional card with a magnetic stripe. The information or application stored in the IC chip is transferred through an electronic module that interconnects with a terminal or a card reader. A contactless smart card has an antenna coil which communicates with a receiving antenna to transfer information. Depending on the type of the embedded chip, smart cards can be either storage cards or processor cards.

Storage cards are the most basic form of smart cards. They can only be used to store data, which can be read out at any time. They contain no processor to execute functions. The advantage of these cards is that they are smaller and easier to handle than paper documents and the data on them can be directly read and processed electronically by a PC [10]. Once manufactured, it is not possible to write on the card, which is a good security feature.

Processor cards are intelligent smart cards that not only provide electronic storage of data but also offer multiple functions such as encryption, advanced security mechanism, local data processing, complex calculation and other interactive processes. Processor cards contain a microprocessor to process the data and execute functions. They can be personalized and bound to a certain person. A processor smart card has the fundamental components, as does an ordinary PC. Figure 1 shows the basic architecture of a processor smart card.

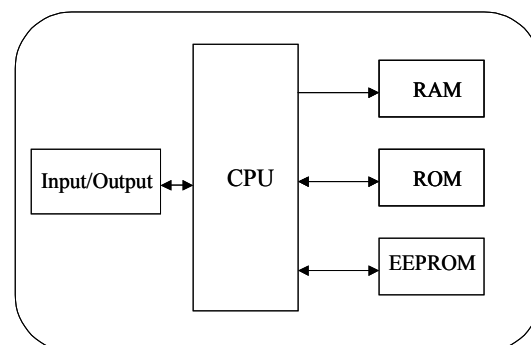


Figure 1: Basic architecture of a processor smart card [1]

One particular type of processor smart card has an important feature for users who want more flexibility to design their own applications: they can use downloadable program code [10]. An important variety of these cards are the Java cards, which allows Java byte code to be implemented in EEPROM.

3. Biometrics

There can be three different types of authentication:

- i. Something you know—a password, PIN, or piece of personal information (such as your mother's maiden name);
- ii. Something you have—a card key, smart card, or token (like a SecurID card); and/or;
- iii. Something you are—a biometric.

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

Biometrics refers to automatic identification of a person based on his or her physiological or behavioral characteristics [2]. Biometrics relies on “something that you are or do” to make identification, therefore it has a very good capability to differentiate between an authorized user and a fraudulent imposter. Common physical biometrics include fingerprint, hand geometry; retina, iris, or facial characteristics. Behavioral characters include signature, voice (which also has a physical component), keystroke pattern. Despite the various biometric identifiers, the process of biometric authentication is similar for all biometrics. A biometric system is essentially a pattern recognition system. Logically, it can be divided into the enrollment module and the identification module [2]. In the enrollment phase, a biometric sensor scans the biometric characteristic of an individual to acquire its digital representation. A feature

extractor to generate a template further processes this digital representation. The template may be stored in the central database of the biometric system or be recorded on a magnetic card or smart card issued to the individual. In the identification phase, the characteristic of the individual to be identified is captured by the biometric reader and converted to a digital format. The feature extractor to generate the same representation as the template further processes this format. The resulting representation is input to the feature matcher that compares it against the template to establish the identity of the individual.

Depending on the application context, a biometric system may operate in a verification mode or in a recognition mode [2]. A verification system authenticates a person's identity by comparing the captured biometric characteristic with the person's own biometric template pre-stored in the database. In this system, the individual submits a claim to an identity usually via a magnetic-stripe card, login name or a smart card, and the system rejects or accepts the submitted claim of identity. In a recognition system, the system establishes an individual's identity or fails to if the individual is not enrolled in the system database by searching the entire template database for a match – without the individual having to claim an identity.

Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification 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 able to provide for confidential financial transactions and personal data privacy. Existing biometric applications include e-commerce, electronic banking, forensics, government Ids, health and social services, and law enforcement. Utilized alone or integrated with other technologies such as smart cards, biometrics are set to pervade nearly all aspects of

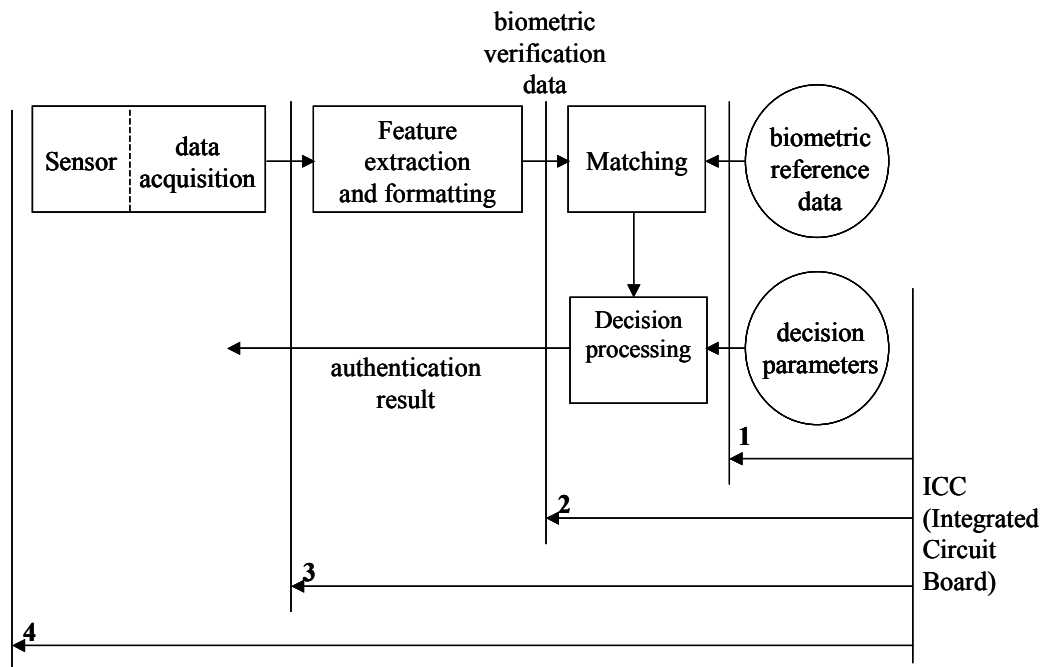


Figure 2: Possible roles of smart cards in biometric verification systems [10]

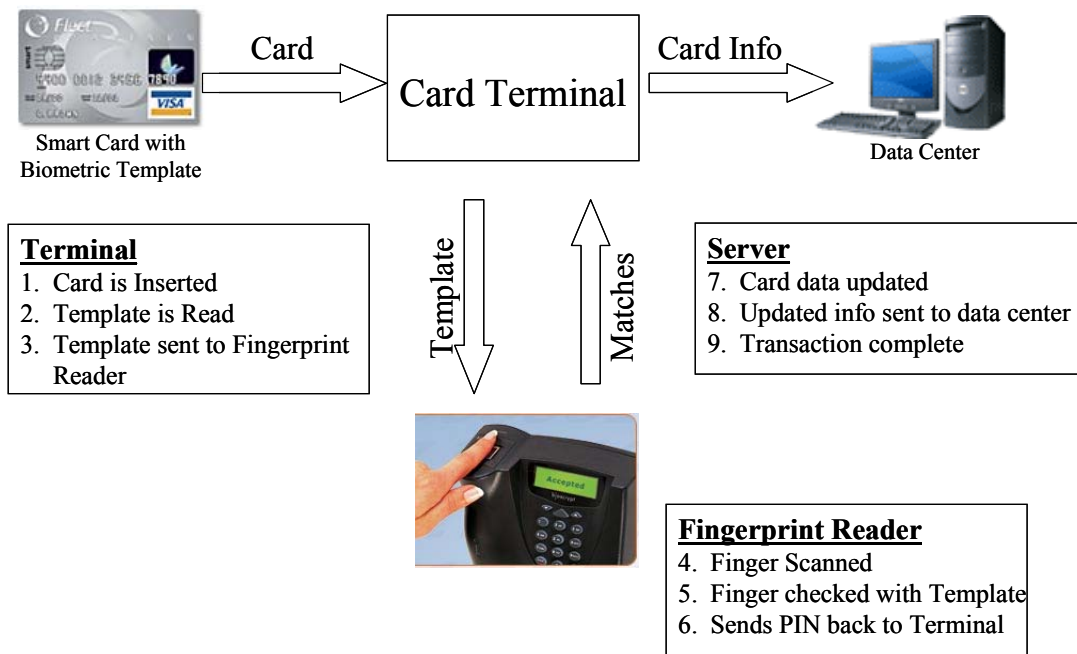


Figure 3: Smart Card with Biometric template verifies the cardholder

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. The reason is that biometrics links the event to a particular individual. Someone other than the authorized user may use a password or PIN. Biometric 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 [3].

4. Smart cards and Biometrics

In this era of heightened security, the identity of an individual is doubted many times. Questions like "Is this the person who he or she claims to be?" come to our minds every now and then. Identity fraud cases are often heard in applications like credit card transactions, ATM withdrawals, and cellular phone calls etc. All this has motivated organizations to search for more secure automated identification and/or verification systems. Traditionally, there are two approaches to user identification [2]: (1) Token -based, (2) Knowledge -based. Token-based approaches use something the user has to make a personal identification, such as a passport, driver's-license, and credit card. Knowledge-based approaches use something the user knows to make a personal identification, such as a password or a personal identification number (PIN). These traditional approaches have the obvious disadvantages: tokens can be lost, stolen, forgotten, or misplaced, and a PIN may be forgotten by a valid user or guessed by an impostor. Thus, these are unsatisfactory means of acquiring the security requirements of our electronically interconnected information society. Here biometrics can play an important role. Biometric features belong to the user and they cannot be stolen or forgotten. The widespread use of smart cards in various sensitive applications has led to profound concern for security and

reliability. Smart cards, today, use the traditional approaches. Significant research has been done and is continuing to be done to design and implement an authentication system in which we can use smart cards with biometrics. Biometric verification and identification methods are becoming more important in connection with smart cards; they provide a means not only to relate but also to bind mobile security devices to an individual [10]. The four possible roles of the smart card in biometric verification systems, as shown in Figure 2, are [10]:

- (1) Data storage only
- (2) Biometric verification on the card, the sensor and feature extraction outside it
- (3) Feature extraction and feature matching with decision processing on the card, the sensor outside, and
- (4) Complete system on the card.

Smart card as a data storage device

The smart card is used as a data storage device if the application that is protected by the biometric verification is located outside the smart card. Examples of such applications include access control systems and banking systems. The biometric data is stored in the smart card avoiding the necessity to store it in a central database. Figure 3 illustrates how a smart card that has the biometric template stored in it verifies the cardholder.

Smart card as a Verification device

If a security application or critical data are contained in a smart card then the smart card itself should be able to recognize its authorized user. In this case, the biometric verification process must be incorporated into the smart card. Significant research is being done to make the processor inside the smart card to execute the entire authentication and verification steps so that the card can

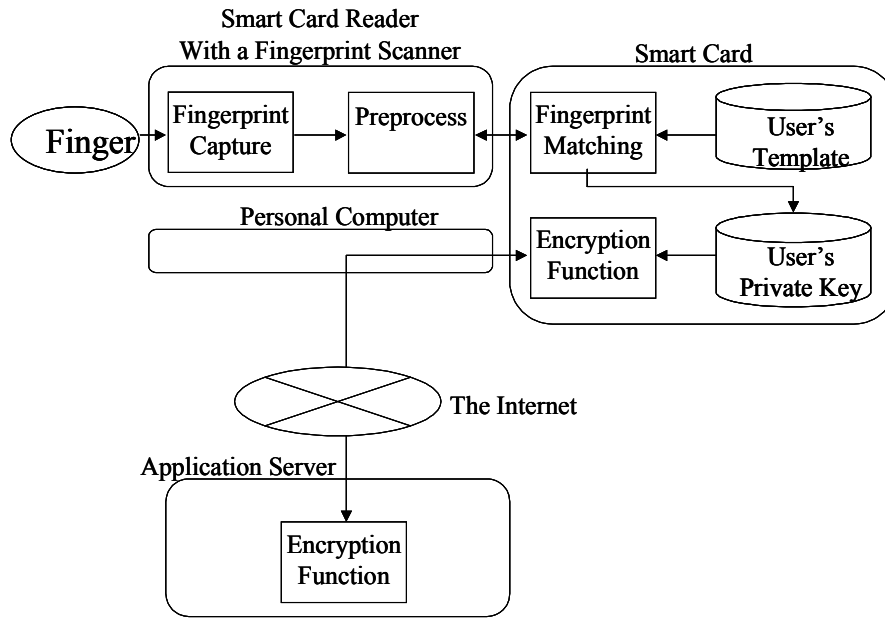


Figure 4: Proposed authentication system [13]

encapsulate all the critical information, including the biometric data, and perform all the comparison securely inside the card without any data leaking out. Or, at least, the in-card processor should be partially involved in the matching and verification process.

Fingerprint verification system on smart card

Seto, Ishida and Mimura [13], propose a fingerprint verification system operating on smart card. The card matches the cardholder's fingerprint and the template in it, then executes the electronic authentication process based

on the PKI if they are identified. The proposed system accomplishes the authentication over the Internet because the template and the result of the matching are protected by the tamper-resistance of the card, and not revealed out of the card. Figure 4 shows the proposed cardholder authentication system [13].

Figure 5 describes the flowchart of the fingerprint matching process [13].

Hand Geometry verification system on smart card

Sanchez-Reillo and Gonzalez-Marcos [8], propose an access control system with hand geometry verification on smart card. The innovation in the system proposed is that the smart card not only stores the user's template, but also performs the whole verification process with the features sent by the terminal to the card. For the verification process, three methods: Euclidean Distance, Hamming Distance and Gaussian Mixture Modeling (GMM), have been studied.

Iris Verification system on smart card

Sanchez-Riello [7], describes how an iris recognition system can be integrated into a smart card. To perform the integration Sanchez-Riello developed a prototype using an Open Operating System smart card.

5. Comparisons and Evaluation

In this section, fingerprint, hand geometry and iris verification systems on smart cards will be compared and evaluated based on the following metrics: template size, verification time, false acceptance rate, false rejection rate.

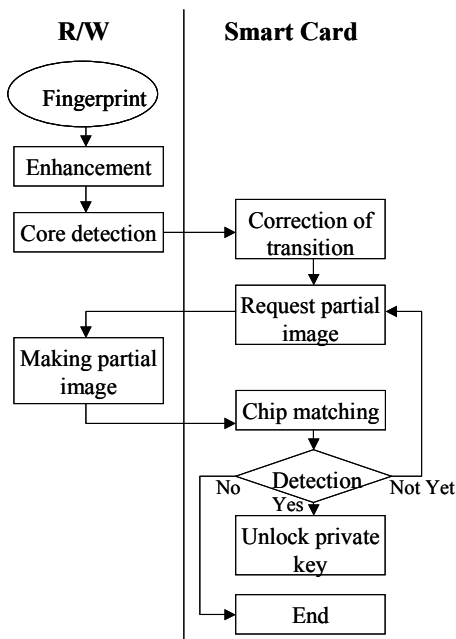


Figure 5: Flow chart of fingerprint matching process [13]

Template Size

A template is a mathematical representation of biometric data. It is measured in bytes. A template can vary in size depending upon the particular biometric pattern/measurement that is being stored. A typical smart card may hold a few kilobytes of information, for instance 8K; therefore, template size becomes an important design issue. Since smart cards have small data storage capability, the smallest sized template would be the most preferred.

Verification Time

Verification is an authentication process by which the biometric system matches a captured biometric against the individual's stored template (1:1) in the smart card. The total time taken in this authentication process will be termed as verification time and is measured in seconds. Since smart cards are used in various applications where speed is of the essence, it is imperative that the biometric technique incorporated in the smart card does not take undue amount of time in verifying the user. The acceptance of biometrics in smart cards will hinge significantly on the speed of completing the transaction.

False Acceptance Rate (FAR)

Biometric systems are not perfect, and will sometimes mistakenly accept an unauthorized individual as a valid individual. The probability that the unauthorized individual is accepted with a measurement that does not belong to the enrolled user is termed as False Acceptance Rate. It is measured in percentage. Good biometrics should have low FAR.

False Rejection Rate (FRR)

The probability that the valid individual is not recognized by the biometric system is termed as False Rejection Rate. It is also measured in percentage. Good biometrics should have low FRR.

The single most important criteria for incorporating biometrics in smart cards is to ensure that the authorized individual is using the card to make various types of transactions. Thus, the biometric technique with the lowest FAR will be most viable. Because there are millions of users and transactions occurring daily, the next most important criteria would be the speed of verifying the individual with the card so that productivity is not compensated. To gain widespread acceptance of smart cards with biometrics, it is very critical that the False Rejection Rate (FRR) is very low so that users are not frustrated by being mistakenly rejected from executing a transaction. However, I believe FAR and verification speed is more important than FRR. Finally, since a smart card has limited storage capacity, the biometric technique that requires least amount of storage will be most suitable, although FAR, verification speed and FRR should not be compromised for storage capacity. Thus, template size would be relatively the least important of the four criteria listed above. Each of the comparison criteria can be ranked in the following way:

1. False Acceptance Rate (FAR)
2. Verification Time
3. False Rejection Rate (FRR)

4. Template Size

In order to get aggregate scores for each of the biometric verification systems on smart cards, weights have been assigned to each of the comparison criteria in Table 1.

Table 1: Weights assigned to comparison metrics

Comparison Metrics	Weight Assigned
False Acceptance Rate (FAR)	35.0%
Verification Time	30.0%
False Rejection Rate (FRR)	25.0%
Template Size	10.0%

Using the data from Table 1, one can arrive at a weighted average rank for each biometric technique across all the four criteria. The biometric verification system that scores the highest weighted average rank will be considered to be the most viable. Table 2 summarizes the ranking of each biometric technique.

6. Conclusion

Biometric technology is evolving at a rapid speed and is now being considered as a better option against traditional identification and verification systems. Smart cards when used with biometrics make any transaction more secure. Integrating biometrics in smart cards provides a solid foundation for developing secure applications and communications. Three biometric techniques; fingerprint, hand geometry, and iris recognition, when used with smart cards were evaluated on the basis of template size, verification time, false acceptance rate and false rejection rate. Iris recognition seems to be the most viable technique to be integrated with smart cards. However, this technique is well suited to be applied to applications that require a high level of security. The computational and economical cost involved in such a system is high which prevents its popularity as a commercial product. The hand geometry technique when used with smart cards seems to be more promising. The computational and economical cost is also low. But, because hand geometry based systems are bulky, it may not be well suited for some applications. User acceptance is also an important factor when deciding on a technique. People might consider Iris recognition to be user-friendly, as it does not involve touching an individual or anything else.

Table 2: Ranking of Biometric Techniques

Biometric Technique	FAR		Verification Speed		FRR		Template Size	
	%	Rank	Seconds	Rank	%	Rank	Bytes	Rank
Hand Geometry [8]	6.60%	1	2.1	2	9.00%	2	153	1
Fingerprint [13]	0.01%	3	3.75	3	5.00%	3	250	3
Iris Recognition [7], [9]	0.00%	2	9 ms	1	3.51%	1	233	2
Weighting	35.00%		30.00%		25.00%		10.00%	

Overall Ranking (Rank * Weighting):	
Iris Recognition	1.45
Hand Geometry	1.55
Fingerprint	3.00

7. References

[1] Afzel Noore, "Highly Robust Biometric Smart Card Design", IEEE Transactions on Consumer Electronics, November 2000, Vol.46, pp. 1059-1063

[2] Anil Jain; Lin Hong; Sharath Pankati, "Biometric Identification", Communications of the ACM, February 2000, Volume 43, No.2, pp.91-98

[3] Biometrics Consortium homepage; www.biometrics.org

[4] Husemann D., "The Smart Card: Don't Leave Home Without It", Concurrency, IEEE, April-June 1999, Volume: 7, Issue: 2, pp. 24-27

[5] Lee, J.K.; Ryu, S.R.; Yoo, K.Y., "Fingerprint based Remote User Authentication Scheme Using Smart Cards", Electronic Letters, June 2002, Volume 38, No. 12, pp. 554-555

[6] Sanchez-Reillo, R., "Fingerprint Verification using Smart Card for Access Control Systems", IEEE AESS Systems Magazine, September 2002, pp. 12-15

[7] Sanchez-Riello, R., "Securing Information & Operations in a Smart Card Through Biometrics", Security Technology 2000: Proceedings. IEEE 34th Annual 2000 International Carnahan Conference on Security Technology, Ottawa, October 2000, pp. 52-55

[8] Sanchez-Reillo, R.; Gonzalez-Marcos, A., "Access Control System with Hand Geometry Verification and Smart Cards", IEEE Aerospace & Electronic Systems Magazine, October 1999, pp. 485-487

[9] Sanchez-Riello, R.; Sanchez-Avila, C.; Gonzalez-Marcos, A., "Improving Access Control Security Using Iris Identification", Proceedings. IEEE 34th Annual 2000 International Carnahan Conference on Security Technology, Ottawa, October 2000, pp. 56-59

[10] Scheuermann, D., "The Smartcard as a Mobile Security Device", Electronics & Communication Engineering Journal, October 2002, Vol. 14, Issue 5, pp. 205-210

[11] Turban E.; McElroy D, "Using Smart Cards in Electronic Commerce", Proceedings of the 31st Annual Hawaii International Conference on System Sciences, Hawaii, January 1998, Volume 4, pp. 62-69

[12] Wahab, A; Tan, E.C.; Heng, S.M., "Biometrics Electronic Purse", Tencon 1999, Proceedings of the IEEE Region 10 Conference, Volume 2, pp. 958-961

[13] Yoichi Seto; Masahiro Mimura; Shuichi Ishida, "Fingerprint Verification system on Smart card", Consumer Electronics, 2002, ICCE. 2002 Digest of Technical Papers, International Conference, June 2002, pp. 182-183