Incorporating Biometrics and Smart Cards

Sandeep Anand
Department of Computer Science
University of Auckland
sana016@ec.auckland.ac.nz

Abstract

Smart cards have become a common application that can perform a variety of secure Transactions and have a significant number of advantages. They are however not secure enough in identifying the person using the smart card. Biometrics in smart cards retains the functionality of the smart card while providing an extra layer of security to it. This paper discusses two schemes of embedding Biometrics in Smart Cards and talks about their limitations and advantages.

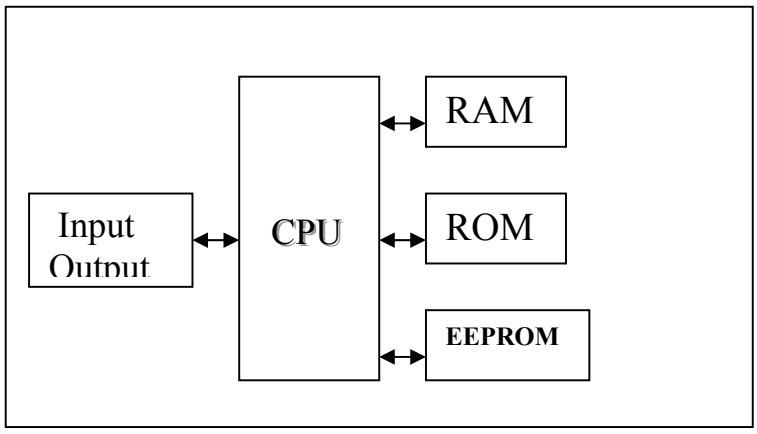
Introduction

There is a need of having an identification scheme that can be reliable and secure, when identifying individuals for purely identification reasons, or to identify them before they have access to sensitive and confidential information. Biometric Authentication in systems has been considered to provide one of the most reliable forms of security. They are being used for identification checks in many secure systems. Smart cards have become popular because of their compactness, ability to process and store large amounts of data, and perform a variety of functions. They are also used in various identification systems. But they can also be vulnerable to attacks because they cannot identify the individual using the smart card. They only check the identity of the validity of the card. By incorporating Biometric authentication in Smart cards it is possible to have the security features of biometrics and the Information processing and benefits of a smart card. A smart card is the most optimal solution for a secure identification system because it is already popular, requires no end user training and the existing technology can be exploited. There isn't a need of additional high costs as, if a new system was to be implemented. Smart cards along with Biometrics provide an additional level of security.

This paper discusses about the about the advantages of having Biometrics in Smart Cards and the type of security they can offer.

Smart Cards

A smart card is a card with a chip embedded in it that is able to store and process a large amount of information. They are multi-Application capable, are portable and are able to perform secure transactions. They are able to perform a wide variety of logical and mathematical computations. The chip may contain a microprocessor (usually 8 bit) and memory (RAM, ROM and EEPROM) that makes it a small on board computer itself or it may contain only memory depending on the task it has to perform. The RAM is usually used for temporary storage while the processor performs functions and the EEPROM is used for the storage of more permanent critical data like the key and application programs when used in Banking, E Commerce and Electronic Cash. The architecture of a common smart card is given in Fig.1 [2].



RAM – Buffer Storage

ROM – Operating System

EEPROM – Application Software

Fig 1. Basic Smart Card Architecture [2].

Security and Benefits of Smart Cards

Since Smart Cards are used mainly for security related applications the data stored inside the smart card is sensitive and should be secure. It should not be accessible to the unauthorized individuals. They are designed in such a way that the access to the information stored inside the card is possible only after some valid security checks are performed. Smart cards are placed in Smart card readers when used that verify if the card is genuine. The user having the smart card has to go through an additional security check by entering a PIN. In general, access to a protected system or sensitive data is possible only when the correct Smart Card is placed in the reader and the correct PIN is entered. The Authentication can be performed by the smart card or by he smart card reader.

A process of secure Encryption and Decryption Algorithms is used along with the Private key and Public key Cryptography to deal with the sensitive information that is sent outside the card. The Public key is used to encrypt the data being sent and the Private key is used to decrypt the encrypted data. Private keys are stored in the card itself and are never sent outside the card. They also have the ability to store a large number of personal Keys and digital signatures of the user. Thus it is possible to have separate keys for different applications. They can also perform the encryption process within the card itself thus preventing the chances of the data being replicated when it is sent outside the card for processing.

But the smart card even though being highly secure cannot verify if the person using the smart card is the true and rightful person.

Biometrics

Dr Jim Wayman gave a working definition of Biometrics as "The auto-matic identification or identity verification of living, human individuals based on behavioral and physiological characteristics [12]. Biometrics for a long time till now has been confined only to government and military agencies as a means of identity check for security purposes. But now with a demand for reliable security in almost all fields, and biometric systems becoming much cheaper and easier to use they have found use in many systems that require reliable security. Biometric authentication verifies if the biometric is of the person at real time verification, and if it matches with an already stored biometric.

It operates on the fact that every person has a unique set f features and these features are used for authentication to that person.

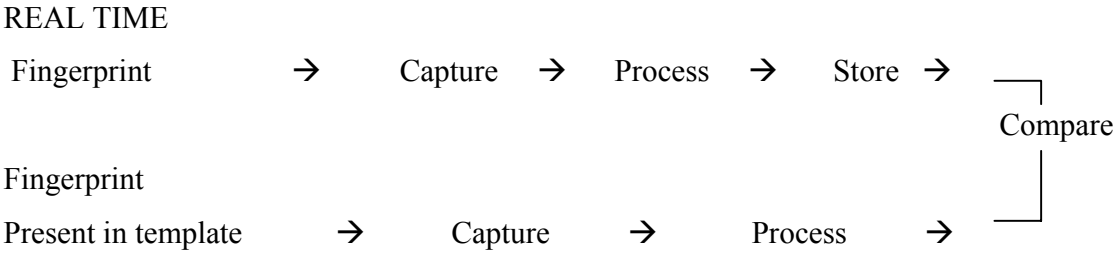
Biometrics can be classified into two categories – Physiological and Behavioral [12]. While Behavioral Biometrics work by verifying behavioral attributes of a person like voice, gait and signature, the physiological Biometrics work by verifying the physical attributes like fingerprint, Iris and Retina Patterns.

The fingerprint verification is the most widely and commonly used form of biometric Authentication. It is most flexible and useful Biometric technology. It matches the fingerprint of a person captured at real time to an already stored fingerprint to verify the identity of the person.

They can protect vital information and can provide increased security to sensitive applications. Biometric technologies are not harmful; they do not pose health hazards, nor are they "The mark of the Beast" [12].

Integrating Biometrics in Smart Cards.

The most appropriate Biometric to be used in Smart Card will be the fingerprint recognition, as it requires less processing and lesser space when compared to the other forms of biometric authentication and taking into account the configuration of a Smart card. The process of how the verification is done using a Biometric technology is shown below



Smart Card with Fingerprint Biometric

The Fingerprint form of Biometric recognition is the most suitable form of Biometric Authentication that can be used to verify the authenticity of the person using the smart card. When taking into account the limited space capabilities of a Smart card, the fingerprint recognition takes less space (Space complexity) as compared to the other forms of Biometric Authentication [1]. The space available on the common smart cards range from 8k to 16k of Volatile memory and the up-to-date fingerprint recognition technology takes a only few hundreds of bytes [7-9],.

The process of matching two fingerprints can be done using different techniques. The procedures till now that involves the fingerprint recognition in a smart card, do the matching process outside the card. The critical fingerprint template is sent outside to an externally present fingerprint reader that performs the authentication function. This is not secure and not suitable as the template information can be changed or can be modified.

The smart card with the biometric template is made secure by not letting any data outside the card. A suitable technique processes the data inside the smart card itself without letting any data to go outside. This significantly reduces the risk of the template information being altered. It would require all the software and processing capabilities of the processor inside the smart card. It involves extraction of the important and unique points of the fingerprint from the images initially and then comparing these points. This significantly reduces the processing time. This kind of matching is more efficient when compared to the pixel-by-pixel comparison of the two fingerprint images. The processing speed and the time taken also depend on the processor inside the smart card. Since the entire comparison process is done inside the card itself the processor should be able to solely perform the entire fingerprint recognition and matching procedure.

Fingerprint Comparison and matching

The procedure that converts the fingerprint template into a set of important unique points has a number of steps involved from the initial image got from the fingerprint reader to the final set of points (Minutia) that are used for comparison and verification [1],[7-11].

The initial step is to enhance the image got from the fingerprint reader of any distortions. The unique features are then extracted from the image after researching procedures defined in various papers [7-11]. A set of Minutia are extracted (Scaling, Translation and Rotation steps [1]) and stored in the template file. During the matching (verification) process the same steps are applied to the fingerprint read at real time and the Minutia are compared.

Arithmetic Modification

The processor inside the smart card is a processor that adheres to the Java Card specifications but for simplicity reasons certain features of the processor are not included. The processor is thus capable of doing only integer arithmetic and cannot perform floating-point arithmetic. As this card is based on the Java Card specifications the integer used in Java is of 32-bit integer data type. Suitable mechanisms and modifications have to be used to overcome the limitations of the simple processor, when performing 32-bit arithmetic [1].

Limitations.

This system even though can significantly improve security, it has certain limitations. The system can function efficiently only if the biometric image captured is clear and not clogged. It can however remove a small amount of distortions and can correct the image but it would not be accurate enough.

It requires the fingerprint reader has to be modified to reduce the angular and positional deviations of the captured image by the reader. This would help during the matching process. The fingerprint reader has to be padded so that the finger can only be placed in one position. This would help in reducing the deviation.

Another Smart card with Biometric Architecture that can overcome the above said limitations and that can provide a better reliable security is the Smart card with dual Biometric sensors on either side of the card.

Smart card with Dual Biometric Sensors

This architecture has two Biometric Sensors placed on either sides of the card. Combinations of the sensors do the capturing and verification of the fingerprints. A Biometric Sensor uses the Physiological or Behavioral characteristic to verify the identity of an individual [2]. The Biometric sensors are small, reliable and not expensive. They store a number of sensors that capture the fingerprints by measuring the ridges and valleys of a fingerprint. They perform the verification of the user and the card. The Biometric Sensors capture and store information of two different fingerprints. This technique provides dual security. In addition it can still do the verification process incase one sensor fails or if the image captured by one sensor is corrupt.

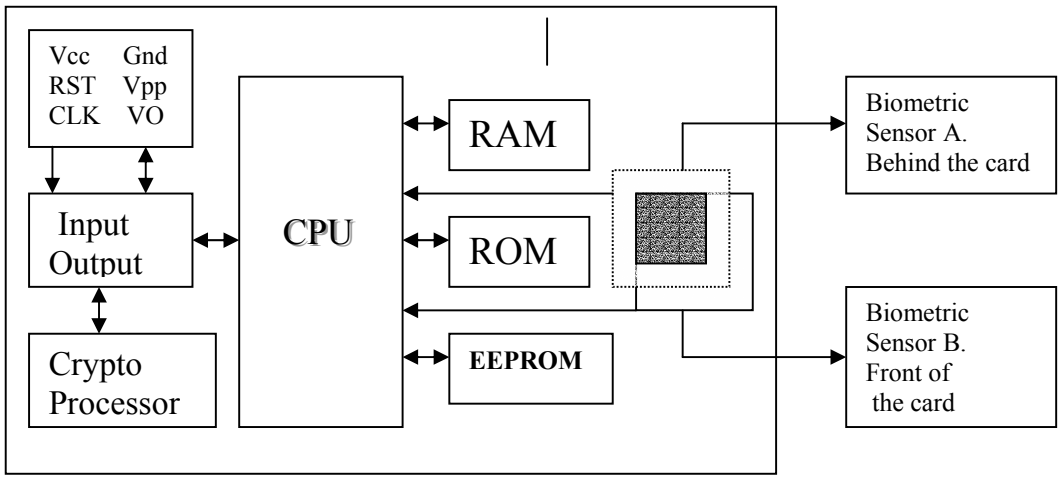


Fig 2. Architecture of Smart Card embedded with dual Biometric Sensors.[2]

The sensors can capture the fingerprints and matching this information with the available sample fingerprints performs the verification. In addition to the embedded Biometric Sensors there is also a Crypto Processor embedded in the card. This processor helps in

speeding up the matching and verification process. The architecture of the smart card with the dual Biometric Sensors is given in Fig.2.[2].

The Biometric Sensors A & B, capture the two different fingerprints using the 'DC Capacitive fingerprint sensing technology' and the 'AC Capacitive fingerprint technology' [2]. The dual sensors improve the security because they are able to verify two fingerprints to check the authenticity of the person. They are also reliable as they do the capturing and verifying process even if any one of the sensors fail and also take care of the problem of distorted captured images.

In general the sensors can operate in six different modes, which is specified in table 1 [2].

Modes	Action Performed
Mode 1	Sensor A verifies fingerprint f1.
Mode 2	Sensor B verifies fingerprint f2
Mode 3	Sensor A verifies fingerprint f2
Mode 4	Sensor B verifies fingerprint f1
Mode 5	Sensor A verifies fingerprint f1 & Sensor B verifies fingerprint f2
Mode 6	Sensor A verifies fingerprint f2 & Sensor B verifies fingerprint f1

Table 1. [2]

The captured image can be stored as Minutia as discussed earlier in the paper and any of the matching algorithms can be used for the verification process. Since the Biometric Sensors can operate in the six modes as specified in the Table 1. , this type of Biometric verification proves to be reliable and can provide dual additional security. Also as no information is sent outside the card the data is securely encapsulated inside the card.

Conclusion

Smart card with Biometrics can help give the ultimate solution to security, having all the utilities and functions of the smart card. Biometrics adds a layer of security to the already existing smart cards. They prove to be accurate and can provide positive authentication. They can prevent impersonation and can protect privacy. This paper discussed two methods of embedding Biometrics in Smart cards and gave an insight into their benefits and the additional layer of security they can offer.

References

[1] A secure card system with biometrics capability, Moon, Y.S.; Ho, H.C.; Ng, K.L.; Electrical and Computer Engineering, 1999 IEEE Canadian Conference on , Volume: 1 , 1999, pp 261 –266, vol.1.

[2] Highly robust biometric smart card design, Noore, A.; Consumer Electronics, IEEE Transactions on, Volume: 46 Issue: 4 , Nov 2000, pp 1059 -1063

[3] Veridicom, http://www.veridicom.com

[4] STMicroelectronics, http://us.st.com

[5] Infineon, http://www.infineon.com

[6] Authentec, http://www.authentec.com

[7] D.Maio,D.Maltoni,S.Rizzi, "An efficient approach to on-line fingerprint verification", proceedings VIII Int. Symp. on Artificial Intelligence, Mexico, Oct 1995.

[8] D.Maio,D.Maltoni, " Direct Gray-Scale Minutiae detection in Fingerprints", IEEE Transactions on Pattern Analaysis Machine Intelligence, v.19, no.1, pp 25-29, 1997.

[9] O.Bergengruen, Matching Minutiae of Fingerprint Images, pp 5-7, 1994.

[10] A.Jain, L.Hong, R.Bolle, On-line Fingerprint Verification, pp 1-33, 1996.

[11]Jonathan D, Stosz, Lisa A, Alyea, Automated system for fingerprint authentication using pores and ridge structure.

[12] John Armington, Purdy Ho, Paul Koznek, Richard Martinez: Biometric Authentication in Infrastructure Security. pp 1-18