BIOMETRIC BASED SMART CARD FOR SECURITY

Chunlei Yang
Advanced Technology Department, Ingenico Group, 9 Quai De Dion Bouton -92816 Puteaux, France

Guiyun Tian, Steve Ward
School of Computing & Engineering, University of Huddersfield, UK

Keywords: Biometrics, Security, Smart card, Integration.

Abstract: Fingerprint has been increasingly used in authentication applications. Smart card is becoming more and more common and is moving toward a multi-function era. The integration of biometric and smart card is a trend for the future of smart card. As a part of our research project which concerns a novel security card, we propose to integrate the fingerprint sensor with the smart card instead of the normal solution where the sensor is installed with a terminal machine. This solution has some advantages regarding security, user privacy as well as flexibility. In this paper, we study the biometric security and outline our solution. In addition, in the system authentication decision part, a novel adaptive decision algorithm which combined with biometrics, PIN (personal identify number) is introduced. This algorithm can be a better trade-off between user convenience and security.

1 INTRODUCTION

Biometrics refers to the automatic identification or verification of living persons using their enduring physical or behavioural characteristics. Biometric personal authentication uses data taken from measurements of a person's body, such as fingerprints, faces, irises, retinal patterns, palm prints, voice, signature, DNA, and so on. Since biometrics has features of "not be lost or forgotten, unique", it is increasingly used in security or privacy needed devices.

As shown in Table 1, different biometric technology has its merits and weaknesses (Rodrigo et al., 2003). For instance, retina scanning requires that a laser is shone onto the back of the eyes and the unique characteristics of the retina are measured. The retina is an extremely stable biometrics because it is 'hidden' and not subject to wear, the system is hard to fool because the retina is not visible and cannot be faked easily. However, it is a potential risk to health and the invasive nature is unattractive to customers. Face recognition is a quite natural method, but in practice, it is affected by lighting, pose and expression strongly. It also needs high computation power and the embedded system cannot meet this requirement. Therefore, thinking comprehensively based on the factors of accuracy, cost, convenience and marketing, fingerprint has the feature of convenient, proven, miniaturization and inexpensiveness, and it has the best potential for mass market authentication schema.

As in a typical biometrics-based personal authentication, fingerprint authentication uses a four-step process including capture, extraction,

Table 1: Comparison of common biometric.

Type	Merits	Weakness
Iris	High accuracy, hard to fool	Large and expensive equipment
Face	Non-invasive, no physical interaction with sensor needed	Low accurateness, affected by lighting & face position
Finger-print	Convenient, well-developed, inexpensive, high potential for miniaturization	Accuracy depends on fingerprint quality, Finger subject to wear
Voice	Non-invasive and natural	Subject to wide variation, hard to detect recorded voice
Retina	Stable, hard to fool	Invasive, not well tested, expensive

Yang C., Tian G. and Ward S. (2005).
BIOMETRIC BASED SMART CARD FOR SECURITY.
In *Proceedings of the Second International Conference on e-Business and Telecommunication Networks*, pages 240-246
DOI: 10.5220/0001407302400246

comparison and matching. The pre-stored minutiae for matching during an enrolment is also called template. Two techniques are used to decide if the verification data really corresponds with the reference data. One is based on minutia matching (local details) and the other is based on pattern matching (global structure). Generally speaking, minutia matching is more commonly used. Figure 1 illustrates how to extract fingerprint minutiae.

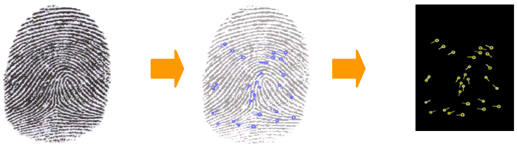

Figure 1: Fingerprint minutiae extraction.

There are two common ways to implement a biometric system according to the different places of storing templates and matching: online and offline. Online means the fingerprint templates are stored and matched in a centralized server computer. This solution has advantages in terms of management and rapid system update, however a stable communication is always needed and it will increase the cost and slowdown the transaction. Offline means the authentication can be done locally because the template is stored and matching is finished locally. This solution can verify identity without complex communication infrastructures and cut cost. It is especially important in mobile application and at sites away from the communication line. The vital question for offline solution is how to store the template securely. A smart card can be an ideal solution to address these questions. It can operate both online and offline.

A smart card has an embedded processor and memory. From a functional standpoint a smart card is a miniature computer. The smart card has the capability to record and modify information in its own non-volatile memory and the security data can be well protected or 'hidden' by the operating system and hardware. These features make the smart card a powerful and practical tool against unauthorized data access and copy (Peyret P. et al., 1990; David M. and Moti Y., 2001.). More and more technologies are integrated with the smart card. The PKI (public key infrastructure) has reinforced the smart card security and makes the smart card be an ideal place to carry varying degrees of sensitive information. In the past years, the biometric and smart card technology have been combining together in some applications (BioT1, 2003; Chunhsing L. and Yiyi L, 2004). As illustrated in Fig.2, a terminal with a fingerprint sensor captures the fingerprint and extracts the minutiae, then the extracted minutiae are sent to the smart card to match with the stored fingerprint templates in the smart card. The process is called match-on-card (MOC) and the card is called biometric card (BioT3, 2003).

The rest of the paper is organized as follows: Section 2 analyses the general security of the fingerprint authentication system, namely attacks and countermeasures. Section 3 describes the proposed system, including architecture, procedure and an adaptive decision algorithm. Section 4 is a conclusion and future work description.

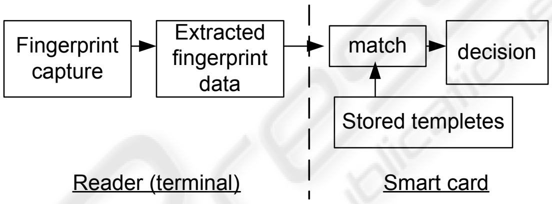

Figure 2: Diagram of Match-on-Card process.

2 BIOMETRIC SYSTEM SECURITY

2.1 Fingerprint System Security

In this section, the general security of biometric system will be analysed.

A generic biometric data processing model is shown in Figure 3. Within this model, following the data process from sensor until application, we identify nine basic biometric attacks (Attack 1; . . . ; 9) that plague biometric based authentication systems. For simplicity, the enrolment of the fingerprint template is not included, although that is a quite important link of the whole biometrics security system.

Typically, Attack 1 could be an *impersonation attack* where the attacker uses a fake fingerprint to fool the sensor. Attack 2, 4, 7, 8 belong to *channel attacks* where the attacker can use line taping, intercept the biometric data or use previous recorded signal to replay attacks. Besides such direct channel attacks, some advanced crypt-analytical techniques, so called *side channel* attacks, also pose serious threats to biometric system even to the channels that are encrypted. For instance, by analyzing the power dissipation or timing of encryptions in device, encrypted information inside can be deduced (An Y. and David S., 2004.; Ross A. and Markus K., 1997.).

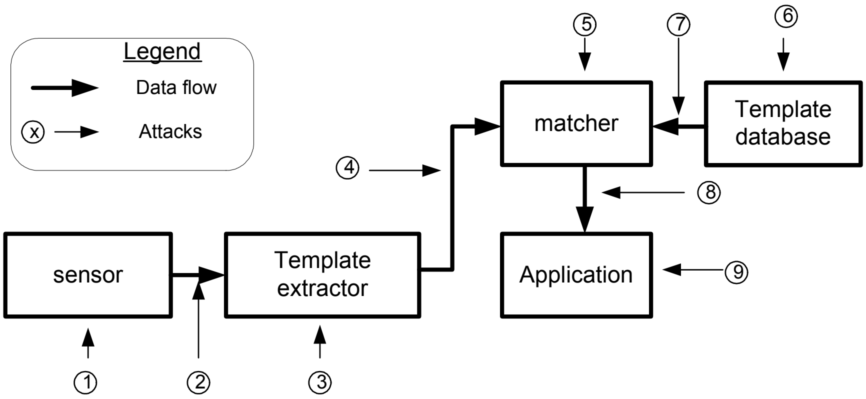

Figure 3: Biometric system security model.

Attack 3, 5, 6, 9 fall into the categories which attack the inside software or secure keys (if the cryptographic technology is employed for secure data transmission). Below more details about attacks and countermeasures will be examined.

A fake finger attack is a serious threat to biometric authentication systems, since this type of attack directly exploits the intrinsic weakness of biometrics: easy to be captured and hard to revoke. When fingers touch an object, the chemicals in finger sweat may be absorbed into that object (paper Matsumoto T. 2002 is a good example), and there are new chemicals which can develop these quite nicely. Afterwards, a fake finger can be made to fool the biometric system. With the ongoing development of technology, a latent fingerprint can be detected and captured easily and a very sophisticated fake finger can be made. E.g. the fake print made from gelatine, which is low-cost, electrically quite like real flesh, can already fool many optical, capacitive, pressure based sensors (Matsumoto et al., 2002).

Theoretically each data transfer channel is susceptible to channel and side channel attacks if it is not well protected. The typical attacks can be a replay attack, resubmission of an old digitally stored biometric signal, or an electronic impersonation. More specifically, like in Attack 2, after the features have been captured by the sensor, if the sensor and the extractor hardware has a long and exposed channel (e.g. connected with cables), this captured data can be replaced with a different synthesized feature set. In Attack 4 the minutiae can be replaced. In Attack 7 the templates from the stored database which are sent to the matcher can be altered before they reach the matcher. In Attack 8, the final decision of the matching module can be overridden.

From a software perspective, the compiled source code stored in the system is susceptible to de-compilation and reverse engineering (Gleb N. and Nasir M., 2003.), which means the program could be read and analyzed. Therefore, if the security mechanism is merely based on some tricks in the program, it will be easily subverted by analyzing the program and designing some actions to avoid triggering the security mechanism. If the adversary can install a Trojan horse into the biometric system, some information will be disclosed to the attacker, etc.

2.2 Countermeasures for Biometrics Attacks

Based on above threat analysis, some countermeasures can be taken to improve the security.

To prevent a fake finger attack, a multi-modal sensor could be an effective way. In a multi-modal sensor, for example, in addition to capturing a fingerprint, the warmth and pulse can also be detected. Or like some advanced sensor, instead of taking a static picture of the surface of the finger, it reads the fingerprint from the live layer below the surface of the skin. This method ensures that the device will acquire the fingerprint despite varying skin moisture levels; abrasion of the fingerprint from harsh chemicals or friction like rubbing; and common contaminants such as lotion, grease, or smoke. This subsurface-imaging approach thereby eliminates the surface-based recognition failures common with surface-imaging fingerprint sensors based on capacitive, thermal, optical, or pressure-sensing techniques (AuthenTec, 2004).

There are several solutions that can improve the system security. As proposed in the paper by Nalini K. et al. (Nalini et al., 2003), 1) "*Image based challenge/response method*". The matcher unit generates a pseudorandom challenge for the transaction and the sensor unit acquires a signal at this point of time and computes a response to the challenge based on the new biometric signal. 2). *WSQ* (Wavelet Scalar Quantization) *-based data* *hiding*. It uses data hiding techniques to embed additional information directly in compressed fingerprint images to guard against replay attacks. However, such measures can hardly meet high security requirements. If the hardware is not secured and the program can be reverse engineering and analyzed, such a system can be subverted without difficulty.

Therefore, finally, the essential protection is to seal as many of the system components as possible into a tamper-proof device, including the data transmission channels. If some channels cannot really be sealed, then cryptographic technology should be employed to ensure data integrity and confidentiality. The security key must be very well protected. Following these thoughts, we consider the combination of biometrics and smart card could be an attractive solution. As the match-on-card solution which is introduced before, the smart card is used to store the biometric template to match the signals from outside of the card.

3 PROPOSED 'CAPTURE & MATCH-ON-CARD' SOLUTION

However, we propose another solution which is other than the above outlined match-on-card solution. The fingerprint sensor is integrated with the smart card body in our new proposed system. The considerations are listed as follows:

- Increase the difficulty for attackers. In practice, most of the attackers need to install an electric bug or apparatus to the attacked object. A terminal machine (card reader) normally has a spacious plastic housing which contains many PCBs, electric components, etc. The wires linking the system components to each other could become potentially passive or active penetration routes. It is not difficult to find a small space in the terminal for installing an electric bug inside. However, if the fingerprint sensor is integrated with the smart card, all these electric elements can be packed into one very thin plastic package, or even be integrated into one single chip and interlinks can be hidden.
- Distribute the security risk. The adversary can get far more potential benefits from compromising a terminal security system than compromising a single card. If the biometric sensor in a terminal is compromised, it will jeopardize all its users. Thus by distributing the sensor to the cards can distribute the risk.
- Protect the privacy and increase the flexibility. Nowadays, the sensor is installed with the terminal machine. Although the terminal providers as well as the merchants declare that "we don't take your fingerprint images but only features", it is hard to believe when the customers see their fingerprints scanned by the terminal. Meanwhile, if the card has a biometric sensor itself, it can improve the flexibility and customers can use and benefit from the potential advanced biometric technology everywhere.

Obviously the feasibility of this solution relies on two issues: the cost of a sensor and whether the physical shape of the sensor allows it to be integrated into a card. Thanks to the ever evolving research and improvements in biometric sensors, especially the new silicon swipe fingerprint sensor, this proposed work becomes more realistic than ever. For example, recently the cost of a swipe sensor can already be less than four US dollars, and the dimension and the thickness makes it nearly possible for it to be integrated into the smart card body, the thickness of which is 0,8mm. The fragile sensor can be protected by a thin metal sheet around it.

The novel security card is illustrated in Fig. 4. In this paper, we only describe the part of our project which concerns biometric security. The envisioned architecture and procedures are presented. In addition, an adaptive decision algorithm of authentication, which is combined with biometrics and PIN (Personal identify number), is introduced. This algorithm can be a better trade-off between user convenience and security.

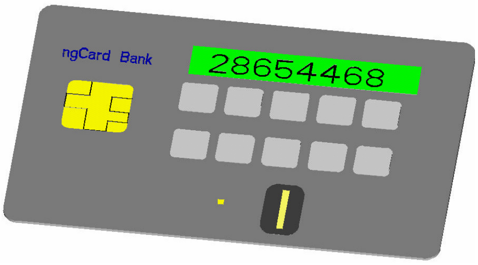

Figure 4: A 3D simulation picture of our project.

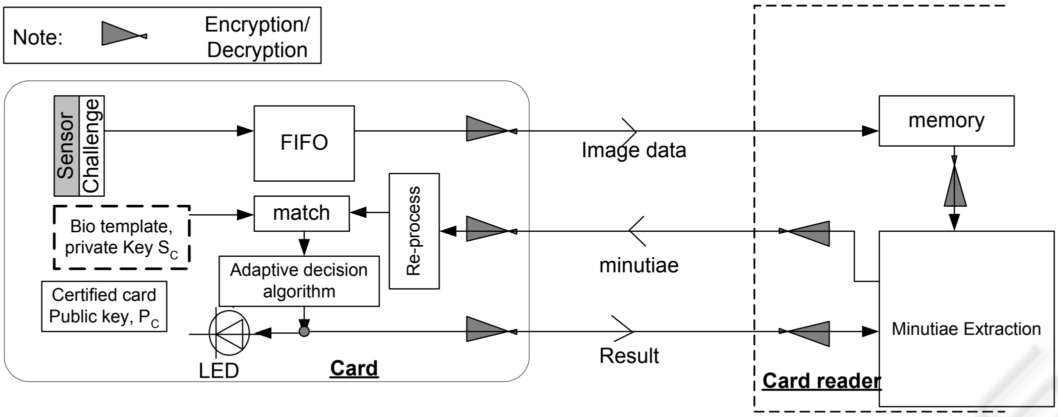

Figure 5: Architecture of the proposed system.

The principle and architecture of proposed system is illustrated in Fig.5. The smart card has a fingerprint sensor and a small LED. They are packaged together and offer the possibility of integrating the security sensitive components into one small chip and apply some ripe tamperproof technologies from the smart card industry (Wolfgang, 2003). Meanwhile part of the system security risk can be distributed to many cards.

For our system experiments, a swipe type fingerprint sensor AES2510 from AuthenTec Inc has been selected, not only for its small size and low cost, but also for security. It uses a radio frequency (RF) imaging technique that allows the sensor to generate an image of the shape of the live layer of the skin that is buried beneath the surface of the finger. Thus it can better prevent attacks like gelatine fake finger. AuthenTec promised to offer a smaller and cheaper version of swipe fingerprint later.

3.1 Architectural Description

As illustrated in Figure 5, theoretically after the sensor has been integrated with the smart card, all the capture, feature extraction and matching can be done inside the card. However, due to the fact that the normal embedded processor of the smart card as well as the memory can hardly fulfil the requirements of complex image processing, the image data store and fingerprint minutiae extraction parts are moved to the card reader side. The swipe fingerprint sensor reads the finger line by line, generates a challenge and sends the data to FIFO (first in, first out) via parallel or DMA (direct memory access) communication. The data in FIFO will be encrypted and directly sent out to the memory of the card reader machine. After the image capture is complete, the image data will be decrypted and the minutiae extracted before it is sent back to the smart card for verification. In addition, one LED light is added and integrated with the smart card. This LED can change the role of the smart card from a passive and 'dumb' card to an active one, e.g., it can indicate some serious edicts to improve the security as well as user convenience.

3.2 Procedure and Security

The authentication procedures are outlined as below in five steps:

1. Mutual authentication using PKI technology between the card and the card reader (EMV4.1, 2004)

As shown in Figure 6. The card issuer uses its Issuer private key S_I to certify the card public key $P_{C,}$ and saves the certified P_C in a readable area of the smart card. However, the card private key S_C and the fingerprint template are saved in the 'hidden' area in the smart card. These data are hidden, and cannot be copied or read out by an external card reader.

The issuer public key P_I is distributed to the card reader. So the card reader can use P_I to verify that the card's P_C was certified by the issuer, and use P_C to verify the digital signature of the card data. Therefore, in this way the terminal can confirm that the card is original and has not been modified. On the other side, to determine whether the card reader is genuine, the card can check the certification of the card reader. In case the above mutual authentication fails, the application will be cancelled and both the card reader display and the card will indicate the error message, i.e. the LED on the card will flash. This is an important feature because it can detect a dummy terminal which is made by an adversary to cheat the user.

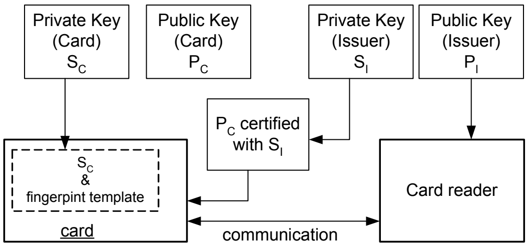
Private Key (Card) S_C
Public Key (Card) P_C
Private Key (Issuer) S_I
Public Key (Issuer) P_I
P_C certified with S_I
S_C & fingerpint template
card
Card reader
communication

Figure 6: Diagram of Dynamic Data Authentication.

2. Session key generation

A session key can be used as a secure key for the encrypted communication between the card and the reader (e.g. DES encryption). The session key derivation function in both the card and the reader, generate a unique session key Ks for each ICC application transaction as per the following method. The system first generates unique Master Keys K_M from the user primary account number and Issuer Master key, then Ks can be derived from K_M, ATC (Application Transaction Counter) using diversification data R. The detailed generation method can refer to EMV definition (EMV 2004).

K_M := F (Primary Account Number, Issuer Master key)

Ks : = F ($K_{M,}$ ATC) [R]

3. Fingerprint capture and extraction

The fingerprint sensor reads the finger image and adds random data to the fingerprint data. The random data can prevent replay attack. The mixed data are sent to FIFO, after DES-encryption using the session Ks, they are sent out to the memory of the card reader. After fingerprint reading is complete, the stored image can be decrypted and the minutiae extracted. The minutiae are encrypted again and sent back to the card for authentication.

4. The card decrypts the received minutiae.

5. Match the acquired minutiae with the hidden fingerprint template in the smart card and generate a similarity score. The final decision comes from an adaptive algorithm (refer to section 3.3). The decision is encrypted and sent both to the card reader and the smart card LED. This is a special measure because the conventional way is just to send it either to the card or the card reader. In this way, even the attacker faked a result in card reader and the card reader display shows the operation is right, but the LED on the smart card will start to flash and give a warning.

3.3 An Adaptive Decision Algorithm

Two authentication methods, PIN and biometric, have their own features. The PIN authentication is stable but prone to be disclosed and forgotten; the biometric authentication is convenient but cannot reach a perfect recognition rate and be updated. Thus they cannot really replace each other completely. Actually, a high security system can be based on a combination of three factors: 'something-you-have' which is the smart card factor, 'something-you-know' which is the PIN factor and 'something-you-are" which is the biometrics factor (Stephen et al., 2000). Nowadays the smart card becomes a platform for multi-applications. More and more payment and non-payment applications (lottery, access control) have been integrated into a single card. Actually different applications need different level authentications. Even the same application, e.g. payment application, the risk for low amount and high amount transaction are different.

In order to better balance the security requirements and user convenience, we propose an adaptive algorithm and apply it in the authentication decision. Principally, we first classify different applications into several predefined levels according to various security requirements and transaction value. Then the algorithm selects different methods, varies the threshold value of biometric similarity degree, even vary the similarity degree of PIN. Adaptive decision algorithms are illustrated in Figure 7.

A new concept of PIN match with a tolerance (fuzzy PIN) is proposed. For example, for some applications, when the user can offer a standard fingerprint, then even he/she makes some small mistakes in PIN, (e.g. should be 63456 but entered 63455), which the system will also accept (but issue a warning, so the legitimate user can check it later at home). To protect the card against exhaustive search, the card will be locked after 10 successive unsuccessful fingerprint verifications.

These measures have practical significances and can cut the management cost. Many calls to the help desk concern the PIN because it is forgettable. A lot of legitimate users' cards are mis-locked or applications have to be cancelled on site. A recent IDC study put annual password management costs at between US$230-460 per user (BioT2, 2004), which would add up to a significant amount when a bank has a large number of customers. The fuzzy PIN matching combined with biometric measures can help to avoid such nuisances without lowering the security.

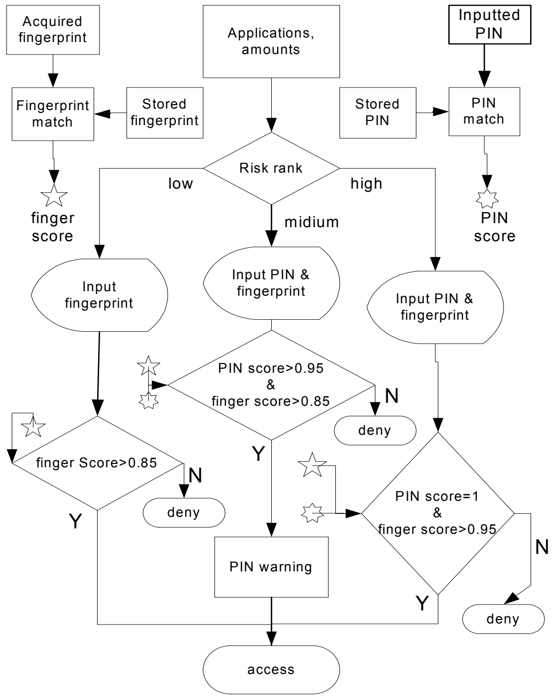

Figure 7: Diagram of adaptive decision algorithm.

4 CONCLUSION AND FUTURE WORK

This paper has reviewed the security of biometric system. It argues the advantages of integrating a fingerprint sensor with smart card, in terms of security, privacy protection as well as system flexibility. Based on the review, proposed types of architecture, procedures and security issues are presented and analyzed. The merits of the proposed approach are heightened.

The project is still in progress. Further work on the system fabrication, implementation and system evaluation such as system design, minutiae extraction and testing the system's real performance, etc, will be undertaken.

REFERENCES

Anil K. J., Umut U., 2003. *Hiding Biometric Data,* IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 25, No. 11, pp. 1494-1498.

An Y. and David S., 2004. *Clock-less Implementation of the AES Resists to Power and Timing Attacks*, International Conference on Information Technology: Coding and Computing (ITCC'04) Volume 2, Las Vegas, Nevada, p. 525 A.

AuthTec, 2004. Website of AuthenTec, www.authTec.com.

BioT1, 2003. *Match on card system for IT security,* Biometric Technology Today, Volume 11, Issue 7, Pages 3-4.

BioT2, 2004. *Biometrics secure loan application*, Biometric Technology Today, Volume 12, Issue 7, Page 3.

BioT3, 2003. Match on card system for IT security, Biometric Technology Today, Volume 11, Issue 7, pp. 3-4.

Chunhsing L. and Yiyi L., 2004. *A flexible biometrics remote user authentication scheme*, Computer Standards & Interfaces, Volume 27, Issue 1, Page 19-23.

David M. and Moti Y., 2001. E-commerce applications of smart cards, Computer Networks, Volume 36, Issue 4, pp. 453-472.

EMV 4.1, 2004. *Integrated Circuit Card Specification for Payment Systems.* Book 2. They can be downloaded from http://www.emvco.com

Gleb N. and Nasir M., 2003. *Preventing Piracy, Reverse Engineering, and Tampering*, COMPUTER, IEEE Computer Society, Vol. 36No. 7, pp. 64-71.

Matsumoto T. and Matsumoto H. and Yamada K. and Hoshino S., 2002. *Impact of Artificial Gummy Fingers on Fingerprint Systems,* Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV.

Nalini K. R. and Jonathan H. C. and Ruud M. B., 2003. *Biometrics break-ins and band-aids,* Pattern Recognition Letters 24 (2003) 2105–2113.

Peyret P. and Lisimaque G. and Chua T.Y., 1990. Smart cards provide very high security and flexibility in subscribers management, IEEE Transactions on Consumer Electronics 36 3, pp. 744–752.

Rodrigo de Luis-García, Carlos Alberola-López, Otman Aghzout and Juan Ruiz-Alzola. 2003. *Biometric identification systems,* Signal Processing, Volume 83, Issue 12, Pages 2539-2557.

Ross Anderson and Markus Kuhn, 1997. *Low Cost Attacks on Tamper Resistant Devices,* Proceedings of the 5th International Workshop on Security Protocols, Springer-Verlag LNCS No.1361, April 1997, p.125.

Stephen M. and Matyas Jr. and Jeff S., 2000. *A Biometric Standard for Information Management and Security*, Computers & Security, 19 (2000) 428-441.

Wolfgang R., 2003. Overview about attacks on smart cards, Information Security Technical Report, Volume 8, Issue 1, Pages 67-84 .