Enhancement of security via real time authentication with biometric methods in e-commerce transactions

S. Mohammadi[1], S. Zareh Hosseini[2]

Department of Industrial Engineering, University of KNTU, Tehran,Iran

---

Abstract

As e-commerce industry is growing rapidly, security issues become more crucial. One of the most important factors in e-commerce transactions and payments is security. While information about customers and their transactions is extremely sensitive, privacy protection is very vital. So, privacy policies to address customer data security are required. At the same time, authentication is one of the most important security requirements and prevents fraud and theft in e-payment transaction. Online biometric authentication is the best solution for preventing false authentication and identity theft. This research reviews authentication ways, and proposes two online biometric authentication methods with credit cards. Finally, the proposed solutions are analyzed using available methods and solutions.

Keywords: e-commerce, authentication, biometric, privacy, online payment, credit card

1- Introduction

Authorization, privacy, integrity, audit ability availability, confidentiality, Identification, authentication and non reputation are defined as security requirements in any e-commerce session. These eight security requirements have been proposed as the basis for e-commerce security framework [1]. As e-payment become more accepted, authentication mechanisms are developing.
Authentication factors include one or more of the following:

Something a person knows: commonly a password or PIN. If the user types in the correct password or PIN, access is granted.

1- *Something a person has*: most commonly a physical device referred to as a token. Tokens include self-contained devices that must be physically connected to a computer or devices that have a small screen where a one-time password (OTP) is displayed, which the user must enter to be authenticated.
2- *Something a person is*: most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of

[1] Smohammadi40@yahoo.com
[2] Saeede626@yahoo.com

veins in the user's eye. This type of authentication is referred to as "biometrics" and often requires the installation of specific hardware on the system to be accessed [2].

Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (*something a person is*). Personal identification numbers, password, smart card and credit card are some of the means employed for user authentication in various electronic commerce applications. However these means do not really identify a person, but only knowledge of some determined object. The main risk of these authorization methods is that they are sensitive to be stolen, guessed or retrieved by a person. The purpose of this paper is to reach high security authentication with real time biometric methods in e-payment of e-commerce transactions.

2. Literature review

In 1981, Lamport [3] proposed a password-based authentication scheme using password tables to authenticate remote users over insecure network. Because of Lamport method' risk, in 2000, Hwang and Li [4] proposed a remote user authentication scheme without using password tables based on El-Gamal public key cryptosystem [5]. Later on, Sun [6] proposed more efficient smart card based remote user authentication scheme to improve the performance of [4]. Sun's scheme significantly reduced the communication and computation costs of the whole system. Recently, many remote authentication schemes using smart cards have been proposed to improve the previously published methods [7–22]. More recently, some biometric-based remote user identity authentication schemes are also proposed in [10], [16], and [17]. Lee et al. [10] proposed a fingerprint based remote user authentication scheme using smart cards. Due to the uniqueness and non-reputation of biometric characteristic, we can except that biometric–based authentication is a more powerful alternative than password-based authentication [23][24].

In this paper, first, review details of biometric methods, biometric certificate, biometric-cryptosystem and requirements of e-payment transaction. Then, explain two schemes with real time authentication via biometric methods, authentication system of schemes and the scenarios of them. Finally the conclusion of this research presented.

3. Details of biometric methods

Biometric is the automated use of physical or behavioral characteristics to determine or verify the identity of an individual [25]. Physiological characteristics include: fingerprint recognition, face recognition, voice recognition, finger and hand geometry, retinal scan and iris scan. Biometric identifiers are most commonly used as part of a multifactor authentication system, combined with a password (*something a person know*s) or a token (*something a person has*). Two biometric techniques that are increasingly gaining acceptance are fingerprint recognition and face recognition [2]. Biometric-enhanced authentication tops the pyramidal security infrastructures as shown in Fig. 1 [2].

Biometric systems convert data derived from behavioral or physical characteristics into templates, which are used for subsequent matching. Their components and processes are:

Enrollment: The process through which a user's initial biometric sample or samples are collected, assessed, processed, and stored for ongoing use in a biometric system.

Submission: The process through which a user provides behavioral or physiological data in the form of biometric samples to a biometric system. A submission may require

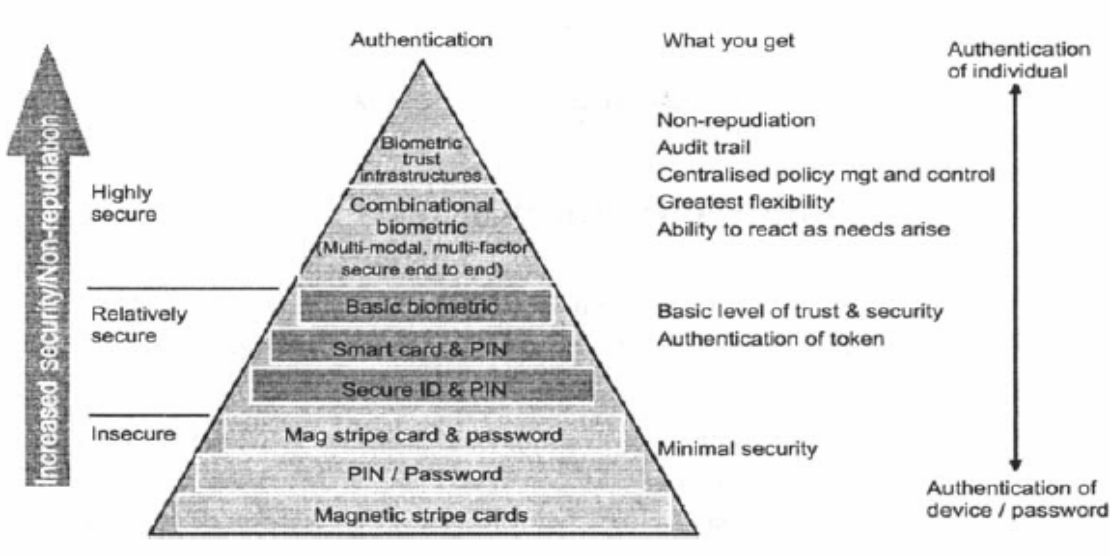

Figure 1. Biometric and security infrastructure

looking in the direction of a camera or placing a finger on a platen.

Acquisition device: The hardware used to acquire biometric samples.

Biometric sample: The identifiable, unprocessed image or recording of a physiological or behavioral characteristic, acquired during submission, used to generate biometric templates.

Feature extraction: The automated process of locating and encoding distinctive characteristics from a biometric sample in order to generate a template. The manner in which biometric systems extract features is a closely guarded secret, and varies from vendor to vendor.

Template: A comparatively small but highly distinctive file derived from the features of a user's biometric sample or samples, used to perform biometric matches.

Matching: The comparison of biometric templates used to calculate their degree of similarity or correlation.

Score: A number indicating the degree of similarity or correlation of a biometric match.

Threshold: A predefined number establishing the degree of correlation necessary for a comparison to be deemed a match.

Decision: The result of the comparison between the score and the threshold.

Applications of biometric techniques are: Identification systems, IT Network security, e-Commerce and Internet, Access control [25].

3.1 Biometric certificate

The primary problem with using biometric information within a PKI context is the inherent unwillingness of people to provide this information. This is related to a psychological feeling of unease regarding giving such information and with the fear that this information is being used for wider surveillance purposes. A second problem with biometric information is that once it is compromised it cannot be replaced [29].

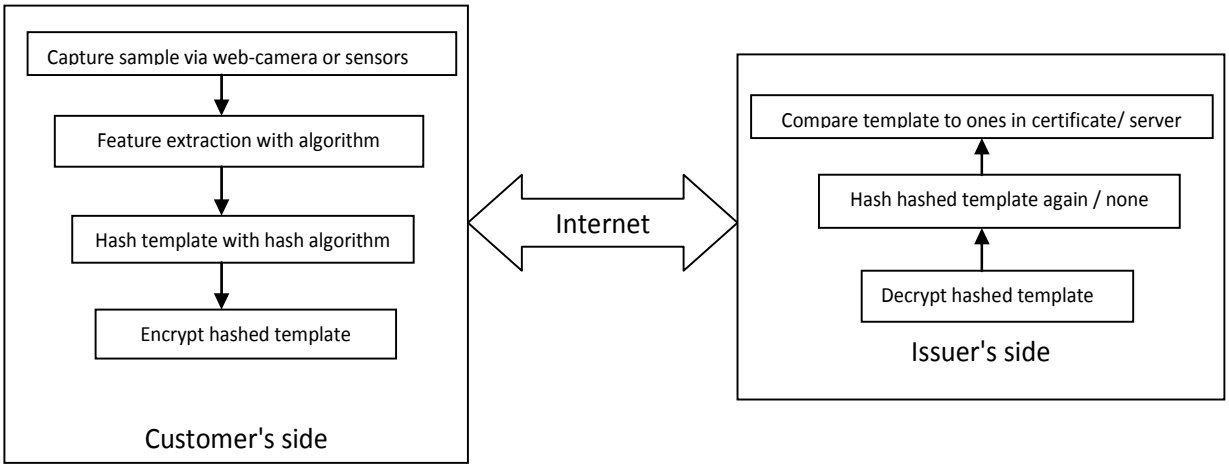

Figure 2. Biometric authentication system

The biometric certificate defined is to use by applications on requirements for identify authentication. The binding of the user's identity and biometric feature data to an entity is provided by an authority through a digitally signed data structure called a biometric certificate [28]. Based on the existing biometric-based digital signature scheme such as [26], [27] and analysis them on the fly, firstly those schemes can be classified into key generation, signature generation and verification framework. The key derivation scheme implies that the signature key is derived directly from biometrics while the key authentication schemes mean that the signature key is accessed by biometric authentication. Biometric data are directly mapped into a unique and repeatable binary string and then are transformed into a cryptographic key. The hardest problem of this model is that the biometric data of a person vary dramatically depending on the acquisition method, acquisition environment and user's interaction with the acquisition devise [28]. Toronto based Mytec Technologies Inc. has developed a process known as biometric encryption in which the biometric image is combined with a digital key (to be used as a cryptographic key) during enrollment to create a secure block of data known as bioscrypt in such a way that neither the key nor the biometric can be independently obtained from it. The main advantages of this method for digital signing are [27]:

- This method will correctly identify an individual and not a person's belonging or what he/she remembers.
- No storage of the biometric template required to retrieve the private key, since it can be regenerated on demand using a live biometric. Therefore, it eliminates the problem of vulnerability of stored private keys for PKI and resolves the key management issue.
- Even the owner does not know what his /her private key is.
- Have all advantages of PKI and digital certificate.

Biometric signature using RSA algorithm and digital signature algorithm (DSA) explained in [27].

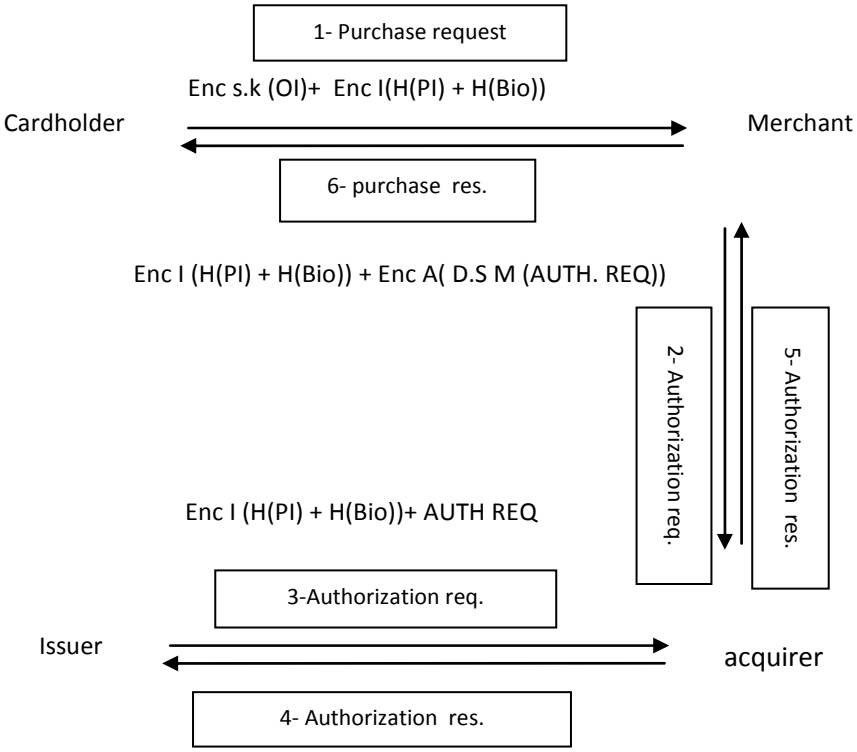

Figure3. using credit card for less sensitive transaction

4. Proposed schemes

4.1 Authentication system of schemes:

Both schemes have a biometric authentication system as depicted in figure 2. The biometric authentication system consist four steps. First, image of iris or fingerprint are captured via web camera or sensor then give the image to software for feature extraction by applying the principle components analysis technique. The principle components analysis is a statistical technique which is applied in such fields as face recognition and image compression [30]. By using hash function, the feature extraction is hashed and then, hashed template will be encrypted with public key's issuer. Finally, the acquired mixture is transmitted to merchant's site or issuer's site. On the other side, first received data will decrypt, and then according to scheme will complete process.

4.2. Requirement

Two major factors are necessary for successful e-payment transactions:

1- Create privacy protection or information privacy in e-payment transactions, to achieve cardholder's trust and prevent misuse of sensitive information.

2- Implement robust authentication that ideally should be a real time authentication, to prevent fraud and theft in credit card and smart card transactions.

The SET can be a proper solution to achieve the first factor. It meets all aspect of privacy protection. But however, SET needs more computation and its transaction time is more

than other protocols such as SSL. Also the cardholder should trust the Payment Gateway. But SSL is simple, cheap and quick to implement and moreover is the most widely used payment protocol in the internet. SSL also provides confidentiality and integrity of data exchanged between two entities. A confident authentication can be achieved with the real time biometric means. Therefore, such an authentication can meet the second factor discussed earlier. In the next section, two schemes for e-payment transactions which meet the mentioned two factors are discussed.

4.3 Scheme 1. Using credit card for less sensitive transactions

Scheme one as shown in figure 3 is suitable for transactions with medium cost. For this scheme, a modified SSL protocol is used because of its simple implementation. Here the customer does not need additional software; however needs to provide her/ his sample of fingerprint to achieve the second factor. Assume the cardholder has the certificate presented in figure 4.

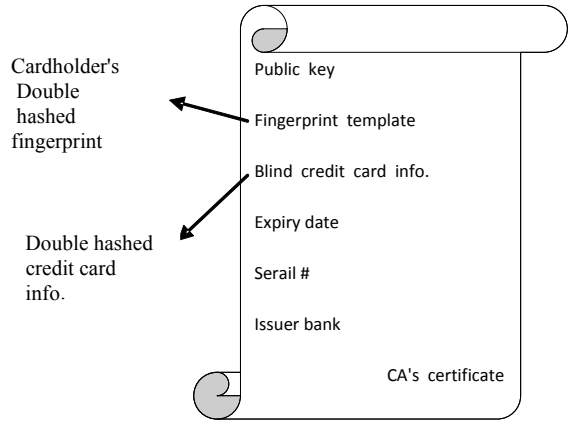

Figure 4. The certificate format

Notations of two schemes:
OI: represents order information
PI: represents payment or credit card information
Enc x (m): represents encryption of massage m by x's public key
D. S. x: represents digital signature with x
H(m): represents Hash function of massage m
Enc s.k: represents encryption by session key of SSL session.
OI is encrypted with session key in secure channel created between the merchant and the cardholder, but PI should be encrypted with the public key of the issuer. Hash of fingerprint's sample and hash of credit card information are presented to the merchant, followed by their encryption with the issuer's public key then they are sent to the issuer through the merchant and the acquirer. Consequently neither the merchant nor the acquirer can understand the payment information and sample of fingerprint. This means the mentioned first factor has been met. After receiving the purchase request from the cardholder, the merchant generates an authorization request (AUTH REQ), which includes the amount to be authorized. The request is signed with merchant's private key, protected by encryption with acquirer's public key
Benefits of this scheme:

- Issuer doesn't need to have biometric server, having a biometric server bring a high security requirement.
- Ease of implementation and higher speed than SET protocol.
- Because of using hash function, merchant or acquirer are able to compare sample of biometric with template of certificate of cardholder and recognize the genius cardholder.

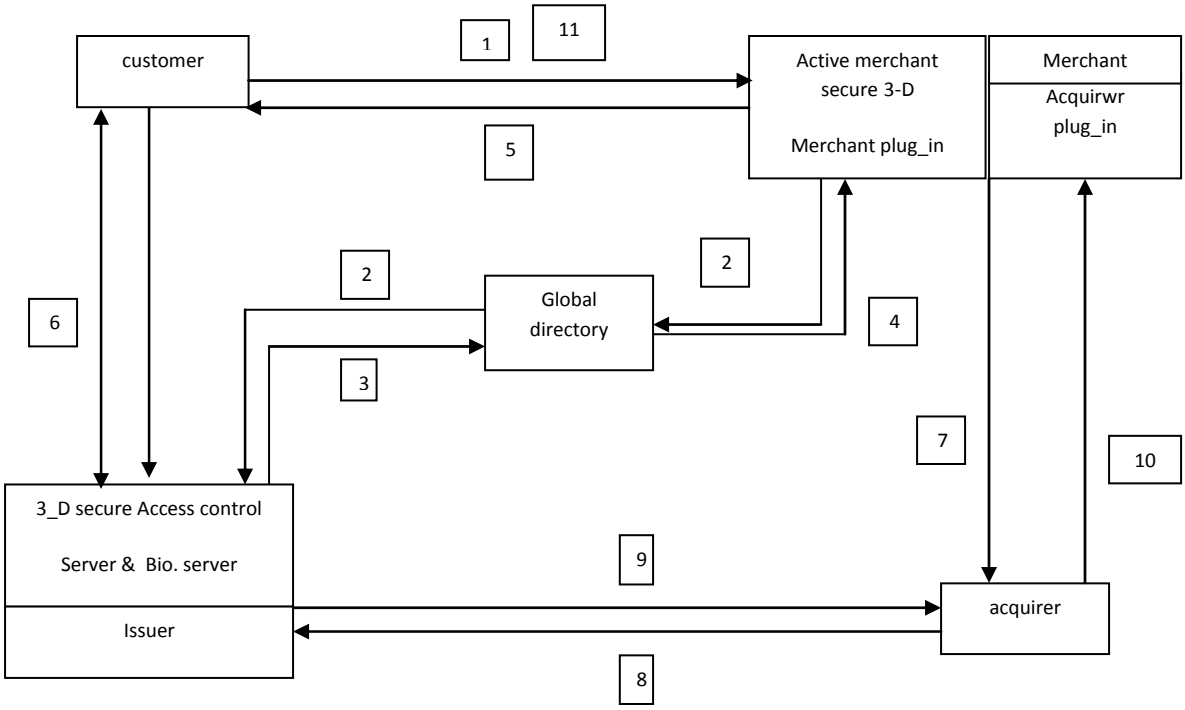

Figure 5. Using credit card for more sensitive transactions

4.3 Scheme 2. Using credit card for more sensitive transactions

Merchant should support this scheme when customer needs a high amount of deal. Sensitive dealing needs real time authentication with more precise biometric way than fingerprint, so iris scan selected. Iris scan is one of ways that cost and complexity is far exceed than other ways, but it however, provides the best security [31]. In this way, authentication can fulfill with direct relation between cardholder and card issuer to reach confidential identification and proper speed. Also, merchant is assured of accuracy of customer who's dealing with. So it uses 3_D secure protocol that merchant and cardholder must support it. It requires the user to answer a challenge in real-time that comes from the issuing bank. Here, request for cardholder's iris scan is challenge. Also normal transactions in credit card are remained. Figure 5 shows the transactions. This scheme has more cost than before schemes but it provides higher level of security.

Steps of transaction are:

1- Purchase request (Enc I(PI), Enc M(OI)).

2- Check card issuer participation.

3- Issuer confirms card participation.

4- Location of issuer's access control server sent to merchant.

5- Merchant redirects customer browser to issuer.

6- Issuer's access control server requests customer's iris sample (real

time)+ customer presents hers iris specification+ issuer's biometric server check sample with temples for verification and signs response and redirects customer to merchant.

7- Merchant submits normal transaction such as authorization request + Enc I(PI) to acquirer

8- Acquirer sends authorization request + Enc I(PI)

9- Issuer sends authorization response

10- Acquire sends response.

11- Merchant confirmes transaction.

4.4 The scenarios

Credit card is popular mean for customer to pay online. However, privacy protection and robust authentication are two major concerns for a trustful deal. Privacy protection should be improved to build up cardholder's confidence. Robust authentication causes to decrees fraud and forgery in transactions of e-commerce. The mentioned schemes use credit card with real time authentication via biometric ways based on sensibility of transactions to build high level of security. They use SSL and 3 D-secure protocol instead of SET. The first scenario uses the sample of fingerprint of cardholder. Hash of sample and hash of payment information encrypted with public key of issuer then transmitted in networks. Also issuer must hash sample and payment information again then compare it with the fingerprint template and blind credit card information in certificate of cardholder. The second scheme uses iris scan. Cardholder must present her/his iris scan via web camera to issuer site directly. Payment of information is encrypted with issuer' public key and order information with merchant's public key.

5- Conclusion

Due to the uniqueness and non-reputation of biometric characteristic, biometric-based authentication is more reliable than other methods of authentications. In this research, methods with biometric authentication based on sensibility of e-commerce transactions is presented that used fingerprint and iris biometric to reach robust identification and authentication. In addition, use modified SSL and 3-D secure protocols instead of SET to achieve privacy protection with better speed. Hash function and encryption methods used for security of biometric template. The importance of this web-based architecture is using SSL protocol that causes better speed than SET protocol and 3D-secure protocol that is suitable for online authentication.

References

[1] Labuschagne, L (2000) A new approach to dynamic Internet risk analysis, Thesis (D.Com) – Rand Afrikaans University, South Africa, 2000. http://csweb.rau.ac.za/deth/acad/thesis/ (accessed 16 August 2000).

[2] Federal Financial Institutions Examination Council, authentication in an internet banking environment

[3] L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 (11) (Nov. 1981) 770–772.

[4] M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (1) (2000) 28–30.

[5] T. El Gamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory 31 (4) (July 1985) 469–472.
[6] H.M. Sun, An efficient remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (4) (2000) 958–961.
[7] S.J. Wang, J.F. Chang, Smart card based secure password authentication scheme, Computers & Security 15 (3) (1996) 231–237.
[8] W.H. Yang, S.P. Shieh, Password authentication schemes with smart cards, Computers & Security 18 (8) (1999) 727–733.
[9] C.C. Lee, M.S. Hwang, W.P. Yang, A flexible remote user authentication scheme using smart cards, ACM Operating Systems Review 36 (3) (2002) 46–52.
[10] J.K. Lee, S.R. Ryu, K.Y. Yoo, Fingerprint-based remote user authentication scheme using smart cards, IEE Electronics Letters 38 (12) (2002) 554–555.
[11] J.J. Shen, C.W. Lin, M.S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 49 (2) (May 2003) 414–416.
[12] C.C. Chang, K.F. Hwang, Some forgery attacks on a remote user authentication scheme using smart cards, Informatics 14 (3) (2003) 289–294.
[13] K.C. Leung, L.M. Cheng, A.S. Fong, C.K. Chan, Cryptanalysis of a modified remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 49 (4) (Nov. 2003) 1243–1245.
[14] C.L. Hsu, Security of Chien et al.'s remote user authentication scheme using smart cards, Computer Standards and Interfaces 26 (3) (2004) 167–169.
[15] M. Kumar, New remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (2) (May 2004) 597–600.
[16] C.H. Lin, Y.Y. Lai, A flexible biometrics remote user authentication scheme, Computer Standard and Interfaces 27 (1) (2004) 19–23.
[17] W.C. Ku, S.T. Chang, M.H. Chiang, Further cryptanalysis of fingerprint based remote user authentication scheme using smartcards, IEE Electronics Letters 41 (5) (2005).
[18] E.J. Yoon, E.K. Ryu, K.Y. Yoo, An improvement of Hwang-Lee-Tang's simple remote user authentication scheme, Computers & Security 24 (2005) 50–56.
[19] M.L. Das, A. Saxena, V.P. Gulati, A dynamic ID-based remote user authentication scheme, IEEE Transactions on Consumer Electronics 50 (2) (May 2004) 629–631.
[20] A.K. Awashti, Comment on a dynamic ID-based remote user authentication scheme, Transactions on Cryptology l (2) (Aug. 2004) 15–16.
[21] H.Y. Chien, C.H. Chen, A remote authentication scheme preserving user anonymity, Intl. Conf. on AINA'05, vol. 2, March 2005, pp. 245–248.
[22] W.C. Ku, S.T. Chang, Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards, IEICE Transactions on Communication E88-B (5) (May 2005) 2165–2167.
[23] A. Jain, L. Hong, S. Pankanti, Biometric identification ,communications of the ACM, February 2000.
[24] P. Orvos, Towards biometric digital signatures, Net workshop, Eszterhazycollege,Eger,pp.26-28. March 2002
[25] L. Yong-Ping, Biometric technology overview, Nuclear Science and Techniques, Vo1.17, No.2 *(2006)* 97-105
[26] R. nagpal , S. nagpal, biometric based digital signature scheme, internet-Draft, draft-nagpal-biometric-digital-signature-00.txt, May 2002
[27] P. Janbandhu, M. Siyal, Novel biometric digital signature for internet-based applications, Information Management & Computer security, vol.9, no.5, pp.205-212, 2001
[28] Y. Chung, K. Moon, H. Woo, biometric certificate based biometric digital key generation with protection mechanism, computer society
[29] B. Gelbord, G. Roelofsen, A Solution to Privacy Issues in the Use of Biometrics in PKI
[30] L. I Smith , A tutorial on principle components analysis, February 2002
[31] R. R. Vangala, S.Sasi, biometric authentication for ecommerce transaction, IEEE IST 2004-International Workshop on imaging systems and techniques