A Survey of Security and Privacy Issues for Biometrics Based Remote Authentication in Cloud

Tapalina Bhattasali, Khalid Saeed, Nabendu Chaki, Rituparna Chaki

A Survey of Security and Privacy Issues for Biometrics based Remote Authentication in Cloud

[1]Tapalina Bhattasali, [2]Khalid Saeed, [3]Nabendu Chaki, [4]Rituparna Chaki

[1,3]Department of Computer Science & Engineering, University of Calcutta, India
[2]Faculty of Computer Science, Bialystok University of Technology, Poland
[4]A. K. Choudhury School of IT, University of Calcutta, India

[1]tapolinab@gmail.com,[2]saeed@agh.edu.pl,
[3]nabendu@ieee.org,[4]rchaki@ieee.org

Abstract. Rapid development of smart technologies enables use of cloud service for large-scale data storage. Remote access of original data as well as biometric data from cloud storage enhances several challenges. It is inevitable to prevent unauthorized access of data stored in cloud. Biometrics authentication is more efficient than the known traditional authentication mechanisms. Authentication is a major security feature used to protect data privacy, whereas additional security features used to protect data may adversely affect it. There must be a balance between security and privacy during secure authentication design. Here a survey of security and privacy issues for biometrics based remote authentication in cloud is briefly presented and the research gaps are identified to attract more research on this domain in near future.

Keywords: Cloud Storage; Remote Authentication; Security; Privacy; Biometrics

1 Introduction

Amount of digital content has been growing day by day with the exponential increase in number of devices connected to Internet. High volume data not only demand for huge storage space, but also looking for intelligent processing in a cost-effective manner. The popular choice in such cases is the cloud environment, which provides unlimited storage space, on demand service, parallel processing and rapid distribution of data. Cloud service provider provides a flexible way for users to access their data from anywhere and at any time. The flexibility of data usage however takes away control from the data owner. Thus the manner in which data are accessed, and by whom, is essentially under the control of cloud service provider. In such a scenario, the authentication of user is very important, so as to guarantee security of data and privacy of data source. Remote user authentication mechanism is useful in distributed domain to identify validity of remote users. There exist several techniques for remote

authentication. Some of the essential requirements for enhancing quality of remote authentication in cloud are given below.

- Third party cloud service provider is not able to retrieve original data, or associated metadata stored in cloud.
- Ensure that an impostor cannot be impersonated as a legitimate user.
- System should be capable to respond to any incoming valid request.
- No intruder is allowed to modify original message.
- If timestamps are used, then it must be synchronized.
- System must optimize bandwidth usage in a cost effective manner.

Password-based authentication with smart card can be used to identify the validity of a remote user. Traditional identity-based authentication mechanisms are mainly based on password, which are very easy to break because of its simplicity. Cryptographic secret keys can also be used in remote authentication framework. Major drawback is that they are difficult to memorize, lost or even be stolen. As a result, it is very difficult to identify valid users accurately. As opposed to traditional password based remote user authentication, biometrics based authentication is increasingly popular because of its reliability [1] and efficiency to authenticate remote users. Cloud based remote authentication provides enhanced security by using biometrics traits [2] such as fingerprint verification, keystroke analysis, ECG analysis, iris analysis, facial analysis, handwritten signature verification etc. Each biometrics trait used in authentication has its own strengths and weaknesses. Biometrics based authentication may be unimodal having single biometrics trait or multimodal, combining multiple biometrics features. Cloud based biometrics technology has high potential market value and attracts interest of many researchers from all around the world.

Cloud framework and remote authentication technique have several challenges of their own. Preserving a balance between security and privacy is a major concern in remote framework of cloud. Privacy is the ability to decide what information should go where. Security acts as significant safeguard for privacy by protecting data. Security and privacy are often considered from two complementary angles. Despite a couple of surveys of biometrics authentication or remote authentication, a comprehensive survey of biometrics based remote authentication in cloud does not exist. The main objective of this paper is to study the balance between security and privacy in biometrics based remote authentication and point out the research gap in this domain. The contributions of this paper are as follows.

- To extensively survey some of the existing schemes that may be used for biometrics based remote authentication in cloud and determine general trends.
- To discuss open issues for future research area.

The rest of the paper contains the following. Section 2 gives a brief introduction of security challenges faced by biometrics techniques. Section 3 presents an extensive survey of some of the existing schemes in this area. Section 4 gives a comparative

analysis of this study. Section 5 presents the open research issues in this area, and section 6 concludes the paper.

2 Security Challenges faced by Biometrics Techniques

The biometrics features, although unique, face several threats in reality [3]. One of the most common threats involves spoofing, whereby users' biometrics templates can be misused. Impostor can produce fake biometrics during enrollment. Genuine templates can be replaced by impostor's template to gain unauthorized access. Spoofing attack involves replay of either raw data or biometrics features extracted from raw data to fool the system into believing an impostor as a real user. User's biometrics features may have extra noise and thus match with incorrect user template, causing false detection. Enhancement of interclass similarity or intra-class variability in the feature sets may cause high false detection rate. Impostors can easily enter into system because of increase in false acceptance rate (zero-effort attack). Data acquisition unit may fail to acquire biometrics trait of user due to limits of capturing technology or adverse environmental conditions. This may lead to failure-to-acquire (FTA) or failure-to-enroll (FTE) errors.

3 Literature Survey

This section provides a literature survey of some of the existing works. There are several works on cloud security and remote authentication. Here, we present a literature survey of existing works depending on the number of biometrics traits used and the additional security features for safeguarding the biometrics template.

3.1 Authentication based on Singular Biometrics Features

Fingerprint based authentication [4] is the most popularly used technique in cloud environment because of its acceptability, uniqueness and immutability. Keystroke pattern analysis is another popular choice to authenticate users. Most important requirement of biometrics based remote authentication is liveliness detection, which is feasible by ECG based authentication. For this reason, a brief idea about some of the existing works on fingerprint, keystroke and ECG is presented here, where template data protection may not be major concern. During fingerprint verification, several image enhancement techniques [4] could be used such as histogram based, frequency transformation based, Gabor filter based enhancement. Gabor filter in wavelet domain improves accuracy level of fingerprint verification. Concept of Toeplitz matrix [5] is considered for fingerprint verification without information loss about fingerprint image. In [6], fingerprint search algorithm was proposed based on database clustering. It speeds up the search process and improves the retrieval accuracy. Fingerprint can be verified by using spectral minutiae representation [7] which can be either location based (SML) or orientation based (SMO). Both techniques have pros and cons in

different scenarios. However, fusion of two techniques shows better result. Fingerprint verifier enables template protection scheme along with fixed length feature vectors. Work on keystroke analysis is vast in the literature [8]. Most of the user authentication techniques are based on measuring the distance between the user keystroke pattern and enrolled keystroke for fixed text or free text. Assessment of keystroke dynamics is based on the traditional statistical analysis or relatively newer pattern recognition techniques such as z-test, Bayesian classifiers, and neural network. Pattern matching may suffer from long search times. This issue can be solved by clustering user profiles. In [9], a combined standard deviation of keystroke duration and degree of disorder for keystroke latency along with disorder for keystroke duration is used for identification and authentication. In pressure-based user authentication system, the discrete time signal is transformed into the frequency domain. It is costly as it requires additional hardware to measure keystroke pressure. In a few cases, instability of typing patterns is reduced by introducing artificial rhythm concept. Keystroke recognition has been investigated for the virtual keyboard that used to interact with the hand held electronic devices, such as PDAs, and mobile phones. In ECG based authentication, correlation coefficient [10] between input image and feature vector stored in database is computed to check authentic person. Confusion matrix is generated to determine False Acceptance Rate (FAR) and False Rejection Rate (FRR). Gurkanet al. [11] proposed ECG authentication technique based on combining AC/DCT features, Mel-Frequency Cepstrum Coefficients (MFCC) features and QRS beat information of the Lead-I ECG signals. According to [12], authentication is possible by collecting ECG signal from fingertips. However, it may contain more noise compared to data collected directly from heart. In [13], feasibility of ECG is tested in a multi-biometric framework where it combines with fingerprint biometrics for individual authentication. Performance is evaluated using Equal Error Rate (EER), Receiver Operating Characteristics (ROC).

3.2 Authentication Systems with Encrypted Biometrics Features

Instead of storing original biometrics, transformed biometrics and transformation are stored in cloud database. Biometrics template protection [14] scheme can be categorized into two ways, (i) Biometric Cryptosystem, (ii) Feature Transformation. Biometric cryptosystem includes key binding (Fuzzy Vault), and key generation (Fuzzy Extractor). Features can be generally transformed either by biometric salting or biohashing and non-invertible transformation or cancellable biometrics template. For data protection, biometrics templates can be encrypted by chaotic encryption method [15], which makes the system more robust against attacks. It becomes dynamic by using the concept of one time biometrics. Blind protocol [16] could be used on any biometrics feature to reveal only identity without any additional information about the user. Real identity of the user is hidden to the server to provide better privacy by making the protocol completely blind. It is also secure under variety of attacks. In blind authentication, focus is on user's privacy, template protection, and trust issue. Cryptobiometric authentication protocol carries out authentication in fully automatic fuzzy vault [17], which aligns transformed template and query minutiae set of fingerprint

without leaking data. Bio-capsule [18] is user-friendly technique adaptive to any environment. It provides security even if authentication server is compromised. It can be applied to several biometrics. This irreversible cryptographic hash function [19] is completely independent from any operating threshold. Non-invertible Gabor transform [20] is resistant to minor translation error and rotation distortion. In [20], user can be given number of cancellable biometric identifiers created from fingerprint image according to the requirement by issuing a new transformation key. The identifiers can be cancelled and replaced when compromised. User's biometrics can be verified using bio-hashing [19]. This scheme is efficient due to usage of one-way hash function and XOR operations. Remote user authentication use nonce or long pseudo-random numbers and timestamps for better security and strong mutual authentication between user and server. Sometimes accuracy level of biometrics can be enhanced by fusing it with multiple factors. Smartcard based authentication uses biometrics along with password and smart card. According to Li et al.'s two factor authentication scheme [21] , user tries to login to remote server by inserting smart card into card reader and input personal biometrics for verification. It fails to provide strong authentication. Fan et al. [22] proposed a three-factor authentication scheme by fusing password, smart card and biometrics. Yeh et al. [23] proposed an elliptic curve cryptography-based authentication scheme that is improved according to security requirements. However, it is seen from the comparative study of different multi-factor biometrics authentication schemes, that Huang et al.'s proposal [24] on generic framework based on three factor remote user authentication provides better results from the aspects of security and privacy. This type of authentication is flexible in nature. User's biometrics traits are kept secret from the server to enhance privacy and to avoid single point of failure.

4 Analysis

From the above study, it is observed that the following parameters are generally used as performance metrics for biometric systems.

- **True Acceptance Rate (TAR)** - Probability to correctly match input pattern to a matching template. It measures the percent of valid inputs which are correctly accepted.
- **True Rejection Rate (TRR)** - Probability to correctly detect non-matching input pattern to any template stored in the database. It measures the percent of invalid inputs which are correctly rejected.
- **False Acceptance Rate (FAR)** - Probability to incorrectly match input pattern to a non-matching template stored in the database. It measures the percent of invalid inputs which are incorrectly accepted. It is more dangerous than FRR.
- **False Rejection Rate (FRR)** - Probability to fail to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
- **Receiver Operating Characteristic (ROC)** - ROC plot is a visual characterization of the trade-off between FAR and FRR.

- **Equal Error Rate or Crossover Error Rate (EER or CER)** - Rate at which both acceptance and rejection errors are equal. Value of EER can be easily obtained from ROC curve. Lowest EER represents high accuracy.
- **Accuracy** - Percentage of ratio of true detection (TAR+TRR) and overall detection (TAR+TRR+FAR+FRR).
- **Peak Signal to Noise Ratio (PSNR)**–It is a measure of peak error in decibels between two images. It is used as a quality measurement between original and reconstructed image.
- **Computation Time (CT)** –It estimates processing time involved in computation (e.g. enhancing the image).

Table 1 gives a quantitative analysis of few biometrics traits based on previously discussed performance metrics. It compares the estimated values of several existing works based on evaluation metrics and checks whether additional security features affect the performance of those works or not. It gives an idea about the security and privacy trade-off in biometric authentication level.

Table 1. Quantitative Analysis of Few Biometric Features

Topic	Additional Security Features	Evaluation Metrics	Estimated Values
Fingerprint verification with image enhancement [4]	No	Equal Error Rate (EER), Peak Signal to Noise Ratio (PSNR), Computation Time (CT)	9.345% EER 41.56db PSNR 0.894 sec CT
Fingerprint verification using spectral minutiae representation [7]	Yes Template Protection	Equal Error Rate (EER), Fused EER	6.4% EER for SML; 6.1 % EER for SMO; 4.8% EER for Fusion of SML and SMO
Continuous Dynamic Authentication for Identification [25]	No	False Acceptance Ratio (FAR), False Rejection Ratio (FRR)	20.25% FAR 4.18% FRR
Bio Password (keystroke fused with password) [26]	No	EER	3% EER
ECG based authentication by high frame rate system for imaging [27]	No	True Acceptance Rate (TAR), True Rejection Rate (TRR)	84.97% TAR 99.48% TRR
ECG based authentication using predefined signature and envelope vector sets [11]	No	TAR, TRR	97.25% TAR 99.91% TRR
Fingertips based ECG [12]	No	EER	9.1 % EER
ECG plus Fingerprint	No	TAR	95% TAR

[13]			
Crypto-biometric verification protocol for fingerprint [17]	Yes, Blind Authentication	Accuracy	84.45% Accuracy
Blind protocol [28] for fingerprint	Yes, Fuzzy Vault	Accuracy	96% for Accuracy
Bio-capsule [18] for iris	Yes, Feature Transformation	EER	0.029 EER
Bio salting[19]	Yes, Addition of Noise	EER	6.68% EER in worst case, 0.1% in best case
Non-invertible Gabor transform for fingerprint [20]	Yes, Cancellable Biometrics	FAR, FRR	0% FAR, 4.5% FRR

After analyzing major biometrics traits like fingerprint, keystroke and ECG, it can be said that accuracy level of fingerprint is better than keystroke and ECG. Keystroke is better than other two because of its simplicity and cost-effectiveness. ECG is better than other two because of its capacity to prove liveliness which is a major issue in biometric authentication. However, ECG suffers from several limitations. Time variation nature of ECG enhances interclass similarity of sample. Few random traces of abnormality can exist in a normal user, resulting into misclassification. Data acquisition is costly and it takes longer time. As ECG data acquisition needs to go through ethical approval, accuracy level is affected due to lack of data sample. Only fingerprint is capable to authenticate users accurately provided fingerprint scanner has very high resolution. However, this type of scanner is very costly and may not be affordable for all type of applications. So fingerprint verification can be fused with other factors to enhance accuracy level using low resolution fingerprint scanner. Keystroke dynamics gains its popularity among the behavioral biometric solutions for providing feasible authentication in distributed environment, because of its simple and natural way to enhance security. Keystroke biometrics is cheaper to implement in distributed framework than other biometrics. It has been studied that performance of keystroke based bio-password is better than vein pattern recognition [26] and is similar to fingerprint and voice recognition. Keystroke does not depend upon the location of the user as data can be collected from anywhere using Internet. It is a globally accepted mechanism which is easy to deploy and use. Keystroke analysis cannot be used alone because of its low permanence in data collectivity. Therefore, physiological trait fingerprint and behavioral trait keystroke analysis can be considered for remote authentication in cloud.

5 Open Issues

From the above analysis, several research gaps are identified and presented as open issues which need to be solved in near future for better performance.

5.1 Design of Effective Framework for Achieving Balance between Security and Privacy

At present, most of the remote authentication techniques are based on either biometrics traits such as iris, fingerprints, voice or the traditional authentication proof such as passwords. It is found through the analysis that remote user authentication schemes become useless if user-id is compromised. In the present social structure, it is very important to focus on balancing security and privacy while designing remote authentication schemes using individual biometrics features. Acceptable limit of security and privacy trade-off need to be determined. There is no privacy implementation without sufficient security. Privacy issues have different meanings in different cases and protection levels are provided according to state laws.

5.2 Design of Energy Efficient Multi-Modal Biometrics based Authentication Scheme for Different State-of-the-Art Applications

At present, pervasive computing has given way to Internet of Things domain, where the application may demand recording of the user's each and every move, in order to assist in remote applications such as healthcare. However, these type of data are confidential to the user, and need to be protected from unauthorized access. Sensors used for sensing and data collectors used for sending information are rather low on energy and hence the authentication schemes involving them have to be highly energy efficient. The use of single biometrics features also fail to sufficiently safeguard the data, hence a fusion of different biometrics traits need to be used for effective protection [29].

5.3 Consideration of Psychological or Other Environmental Effects on Biometrics Features of an Individual for better Authentication

As has been noticed earlier, keystrokes based authentication is an easy to implement technique. However, not much have been researched about the effect an individual might have on the typing pattern when he or she is either sick or depressed. There comes the effect of humidity, temperature, etc. to be considered with fingerprints.

5.4 Design of Cost-Effective Means to Record Biometrics Features

The devices available for recording the features need to be engineered so as to achieve energy efficiency and accuracy. As such, usage of any specialized device itself is often considered as an addditional overhead. This overhead can be justified only by improved efficiency in terms of biometrics feature extraction.

6 Conclusion

In today's world, use of third party cloud environment has become mandatory for the organizations handling huge amount of data cost-effectively. Securing data stored in cloud is a big challenge. Therefore, one of the most important challenges is to how to control access of data stored in cloud from remote location. Authentication is necessary step in security implementation for remote data access. It is studied that biometrics authentication is feasible solution in cloud. With growing popularity of biome-

trics features, database containing biometrics template and user details are also stored in cloud and vulnerable to various threats. Authentication mechanism has no significance without security. Similarly, complex security mechanism affects usability and accuracy of authentication. In this paper, we present a survey of security and privacy issues of biometrics based remote authentication in cloud after analyzing existing works from different angles. An insight into the open research issue is also presented. The objective of this survey is to determine the challenges in biometrics based remote authentication in cloud; so that more effective user authentication could be proposed to resist attacks in remote environment besides identifying users accurately.

References

1. Tang, Q., Bringer, J., Chabanne, H., Pointcheval, D.: A Formal Study of the Privacy Concerns in Biometric-based Remote Authentication Schemes. In: Proceedings of International Conference on Information Security Practice and Experience, ISPEC 2008, LNCS, pp. 56–70 (2008).
2. Jain, A.K., Ross, A., Pankanti, S.: Biometrics: A Tool for Information Security. IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, pp. 125-143 (2006).
3. Ignatenko, T., Willems, F. M. J : Biometric Systems: Privacy and Secrecy Aspects. IEEE Transactions on Information Forensics and Security, Vol. 4, No. 4, pp. 956-973(2009).
4. Arora, K., Garg, P.: A Quantitative Survey of Various Fingerprint Enhancement Techniques. International Journal of Computer Applications, Vol. 28, No. 5, pp. 24-28 (2011).
5. Surmacz, K., Saeed, K.: Robust Algorithm for Fingerprint Identification with a Simple Image Descriptor. In: Proceedings of International Conference on Computer Information Systems and Industrial Management Applications, CISIM 2011, CCIS, pp. 137-144 (2011).
6. Liu, M., Jiang, X., Kot, A. C.: Efficient Fingerprint Search based on Database Clustering. Elsevier Journal, Pattern Recognition, Vol. 40, No. 6, pp. 1793 – 1803 (2007).
7. Xu, H., Veldhuis, R. N. J. , Bazen, A. M. , Kevenaar, T. A. M. , Akkermans, T. A. H. M., Gokberk, B. : Fingerprint Verification using Spectral Minutiae Representations. IEEE Transactions on Information Forensics and Security, Vol. 4, No. 3, pp. 397-409 (2009).
8. Karnan, M., Akila, M., Krishnaraj, N.: Biometric personal authentication using keystroke dynamics: A review. Elsevier Journal of Applied Soft Computing, Vol. 11, No. 2, pp. 1565–1573 (2010).
9. Rudrapal, D., Das, S., Debbarma, S.: Improvisation of Biometrics Authentication and Identification through Keystrokes Pattern Analysis. In: International Conference on Distributed Computing and Internet Technologies. ICDCIT 2014, LNCS, pp. 287–292 (2014).
10. Hegde, C., Prabhu, H. R., Sagar, D.S., Shenoy, P. D., Venugopal, R., Patnaik, L.M. : Human Authentication Based on ECG Waves using Radon Trans-

form. In: Proceedings of International Conference on Disaster Recovery and Business Continuity, DRBC 2010, CCIS, pp. 197–206(2010).
11. Gurkan, H., Guz, U., Yarman, B.S., Modeling of Electrocardiogram Signals using Predefined Signature and Envelope Vector Sets. EURASIP Journal on Advances in Signal Processing, Springer Open journal, pp. 1-12 (2007).
12. Da Silva, H. P, Lourenço, A., Fred, A. L. N. Raposo, N., De-Sousa, M. A. : Check Your Biosignals Here: A New Dataset for Off-The-Person ECG Biometrics. Elsevier Journal, Computer Methods and Programs in Biomedicine, Vol. 113, No. 2, pp. 503-514 (2014).
13. Singha, Y.N., Singh, S.K., Gupta, P : Fusion of Electrocardiogram with Unobtrusive Biometrics: An Efficient Individual Authentication System. Elsevier Journal, Pattern Recognition Letters, Vol. 33, No. 14, pp. 1932–1941 (2012).
14. Isobe, Y., Ohki, T., Komatsu, N : Security Performance Evaluation for Biometric Template Protection Techniques. International Journal of Biometrics, Vol. 5, No.1, pp. 53-72 (2013).
15. Gao, H., Zhang, Y., Liang, S., Li, D: A New Chaotic Algorithm for Image Encryption. Elsevier Journal, Chaos, Solitons and Fractals, Vol. 29, No. 2, pp. 393–399 (2006).
16. Nandakumar, K., Jain, A., Pankanti, S.: Fingerprint-based Fuzzy Vault: Implementation and Performance. IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4, pp. 744–757 (2007).
17. Upmanyu, M., Namboodiri, A. M., Srinathan, K., Jawahar, C. V. : Blind Authentication: A Secure Crypto- Biometric Verification Protocol. IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, pp. 255-268 (2010).
18. Sui, Y., Zou, X., Du, E. Y., Li, F.: Design and Analysis of a Highly User-Friendly, Secure, Privacy-Preserving, and Revocable Authentication Method. IEEE Transactions on Computers, Vol. 63, No. 4, pp. 902-916 (2014).
19. Jin, A. T. B., Ling, D.N. C., Goh, A.: Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number. Elsevier Journal, Pattern Recognition, Vol. 37, No. 11, pp. 2245–2255 (2004).
20. Ratha, N. K., Chikkerur, S., Connell, J. H., Bolle, R. M.: Generating Cancelable Fingerprint Templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 4, pp. 561-572 (2007).
21. Li, C. T., Hwang, M. S.: An Efficient Biometrics based Remote User Authentication Scheme using Smart Cards. Elsevier Journal, Journal of Network and Computer Applications, Vol. 33, No. 1, pp. 1-5 (2010).
22. Fan, C.I., Lin, Y. H.: Provably Secure Remote Truly Three-Factor Authentication Scheme with Privacy Protection on Biometrics. IEEE Transactions on Information Forensics and Security, Vol. 4, No. 4, pp. 933-945 (2009).
23. Yeh, H. l., Chen, T. H., Hu, K. J., Shih, W. K.: Robust Elliptic Curve Cryptography-based Three Factor User Authentication Providing Privacy of Biometric Data. IET Information Security, Vol. 7, No. 3, pp. 247-252 (2013).
24. Huang, X., Xiang, Y. Chonka, A. Zhou, J., Deng, R. H.: A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed

Systems. IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 8, pp. 1390-1397 (2011).
25. Monaco, J.V., Bakelman, N., Cha, S., Tappert, C.C: Developing A Keystroke Biometric System for Continual Authentication of Computer Users. In: Proceedings of European Intelligence and Security Informatics Conference, EISIC 2012, pp. 210-216 (2012).
26. Bio Password White Paper: Authentication Solutions through Keystroke Dynamics (2007). Available at: http://www. infosecurityproductsguide.com/ technology/ 2007/ BioPassword_Authentication_ Solutions_ Whitepaper Final. pdf
27. Wang, S., Lee, W. N., Provost, J., Jianwen, L., Konofagou, E. E.: A Composite High-Frame-Rate System for Clinical Cardiovascular Imaging. IEEE Transaction on Ultrasonics, Ferroelectrics and Frequency Control, Vol. 55, No. 10, pp. 2221-2233 (2008).
28. Moon, D., Chung, Y., Seo, C., Kim, S. Y., Kim, J.N.: A Practical Implementation of Fuzzy Fingerprint Vault for Smart Cards. Springer, Journal of Intelligent Manufacturing, Vol. 25, No. 2, pp. 293-302 (2014).
29. Nagar, A., Nandakumar, K., Jain, A.K.: Multibiometric Cryptosystems Based on Feature-Level Fusion. IEEE Transactions on Information Forensics and Security Vol. 7, No.1, pp. 255-268 (2012).