Study of Cancelable Biometrics in Security Improvement of Biometric Authentication System

Sanggyu Shin, Yoichi Seto

▶ To cite this version:

Sanggyu Shin, Yoichi Seto. Study of Cancelable Biometrics in Security Improvement of Biometric Authentication System. 14th Computer Information Systems and Industrial Management (CISIM), Sep 2015, Warsaw, Poland. pp.547-558, 10.1007/978-3-319-24369-6_46 . hal-01444496

HAL Id: hal-01444496

https://inria.hal.science/hal-01444496

Submitted on 24 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Study of Cancelable Biometrics in Security Improvement of Biometric Authentication System

Sanggyu Shin and Yoichi Seto

Advanced Institute of Industrial Technology,
1-10-40, Higashiooi, Shinagawa-ku, Tokyo, 140-0011, Japan
{shin, seto.yoichi}@aiit.ac.jp

Abstract. Recently, there is a widespread use of biometric authentication systems. This is because biometric systems have become open and large scale and enrolment and authentication systems are separate. Many methods have been proposed for cancelable biometrics technology in biometric systems. However, the security criterion in such is indefinite in cancelable biometrics technology. Moreover, there is still no work on the systematic study of the safety of biometric authentication systems. In this paper, we consider the cancelable biometric techniques from the perspective of the safety of the system. In addition, we also verify the effect on the security precaution of the liveness detection techniques using Fault Tree Analysis, a risk evaluation method about data protection and spoofing prevention techniques.

Keywords: cancelable biometrics, biometric, authentication system

1 Introduction

In biometric authentication systems, the biometric data that becomes the reference for comparison is called template data. A template is biometric information that is used at authentication. The need for template sharing has been recognized because using the same template between applications makes inheriting trust among organizations (e.g., passports and back cards) possible. Furthermore, it enhances stability and reduces cost of system development and operation. Template protection technologies aim at preventing the prediction of raw biometrics data from templates and at preventing leaked templates from being reused by unauthorized users (cancelling leaked templates and reissuing new valid templates).

When the template data leaks, problems such as the spoofing of other users and leakage of private data occur. These problems are usually addressed by the cryptography technology and the system technology of tamper-proof devices such as smart cards.

Various methods have been published for security techniques now known as cancelable biometrics [1]-[7]. However, there has been no systematic study on the criteria for security in biometric authentication systems.

Paul proposed to tackle the problem and present a novel solution for cancelable biometrics in multimodal system. They developed a new cancelable biometric template generation algorithm using random projection and transformation-based feature extraction and selection. The performance of their proposed algorithm was validated on multi-modal face and ear database [11]. They also present a novel architecture for template generation in the context of situation awareness system in real and virtual applications [12]. In addition, Rathgeb presented comprehensive survey of biometric cryptosystems and cancelable biometrics [13].

The purpose of this paper is to discuss and evaluate the cancelable biometrics techniques from the viewpoint of ensuring safety of the systems.

First, the location and the type where the threat is generated on the biometric authentication systems model are explored, and the meaning of cancelable biometrics as the countermeasure technology to those threats is described.

Next, we propose a scheme for evaluating the effectiveness of cancelable biometrics. After that, the effectiveness of the security precaution with the liveness detection techniques is verified by using FTA (Fault Tree Analysis), which is a quantitative risk analysis and is the evaluation approach about the data protection and the proofing prevention technology then the superiority of the liveness detection technique is presented.

Finally, to know the open problems with the current template protection technologies, we summarize our evaluation result, especially from technical and security points of view.

2 Threat medel for a biometric authentication system

Many biometric data is inherently exposed (e.g., faces and fingerprints). It has little value without linking information to person and it is a countermeasure preventing a leak. Liveness detection should be done at sensors and since it has no alternative technologies to it.

Fig. 1 shows the processing diagram of a biometric authentication system. At first, raw biometric data of an individual is captured from the user. For every input, biometric data changes due to the body and sensor device condition in the environment.

In the enrollment process, the correction processing is included in the feature extraction from raw biometric data of an individual, and the extracted characteristics of individual is stored in the database as template data.

In the authentication process, the identification data that specifies the user is inputted from a sensor device and the corresponding template data is selected from the database. Two sets of features are matched, then the degree of similarity is obtained by a matching process. It is assumed that the authentication succeeds if the degree of similarity exceeds a threshold. As a result, the user can access the application.

The number in Fig. 1 shows the location under the threats of attack in a biometric authentication system. The threats at each location are explained as follows.

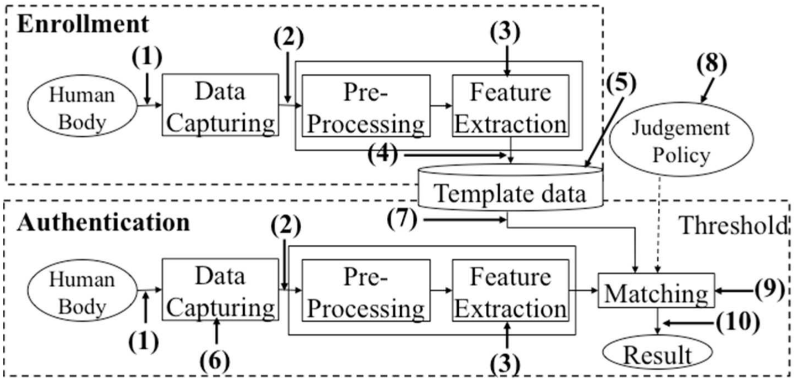

Fig. 1. Possible attack points in a biometric authentication system.

(1) Attack on sensor input of fake biometrics: The photograph of face, counterfeit fingerprint or signature are put on the sensor.

(2) Attack on the transfer data from sensor to feature extraction processing: Biometric data captured from the sensor is replaced with information attacking the network or the bus.

(3) Making replacement of extracted feature data: The feature extraction processing is attacked with the Trojan horse etc., and an arbitrary feature is set instead of an actual feature.

(4) Illegal conversion of body data: Body data is replaced with counterfeit data. It is very difficult to execute this attack because the feature extraction processing and the matching processing are often done in the same system. However, when an extracted feature data is transmitted to the matching processing by the Internet, this attack becomes possible by substituting the packet data.

(5) Tampering with stored template data: An illegal user makes the falsification of a template data stored in the database, such that an unfair user obtains an illegal attestation and gains access or a fair user obtains an illegal attestation and is denied access.

(6) Re-input of stored biometric data: Biometrics that remains on the sensor devices is automatically inputted again without user input.

(7) Attack on the transfer from template data storage to matching processing: When the template stored in the database is transferred to the matching processing through the communication channel, the template data is illegally changed.

(8) Replacement of threshold value: The threshold value is set to the given value by rewriting the judgment policy in order to get the intended result.

(9) Attack on matching process: The matching process is attacked, and the matching result is replaced with an arbitrary score.

(10) Substituting of final decision data: The judgment result of the authentication is substituted.

The countermeasures shown in Table 1 are effective ways to prevent the above-mentioned attacks. The threats in categories (4), (5) and (7) relate to the theft of template data and those in categories (1) and (6) relate to counterfeit use (spoofing) when biometric data is captured and attested.

Table 1. Threats and countermeasures.

No	Threats	Countermeasures
(1)	Attack on sensor input of fake biometrics	Liveness detection
(2)	Attack to transfer data from sensor to feature extraction processing	Encryption
(3)	Making replacement of extracted feature data	Digital signature
(4)	Illegal conversion of body data	Encryption Cancelable biometrics
(5)	Tamper with stored template data	Physical security Cancelable biometrics
(6)	Re-input of stored biometric information	Liveness detection Challenge & Response
(7)	Attack to transfer from template data storage to matching processing	Encryption Cancelable biometrics
(8)	Tampering authentication parameters	Digital signature
(9)	Replacement of threshold	
(10)	Data	

For example, the development of countermeasure techniques for the following attacks will become important in the future.

- Study of fabricating a counterfeit fingerprint with cheap material such as the gelatin, which can be made for a short time.
- A method of the transformation of biometric data of protection and each application of biometric data by the encryption for the template protection and storing.
- A peculiar attack that counters dictionary attack to the biometric authentication.

Another problem includes the copying process when the data used for the biometric authentication loses reliability.

When reliability is lost, the authentic method such as using the key, the token, and the password, etc. can nullify these attestation devices as many times as you want. But, there is a limit in the number of times of nullification for biometrics.

In the security requirement for a biometric authentication system, the cancelable biometric techniques are not exclusive but are one of the measures technologies.

The problem of the template data leakage is divided into the problem of spoofing due to reuse and privacy concerns. Biometrics was originally exposed, and at 1:1 matching, the individual can be specified if there is a link to other information. Therefore, there is an opinion that biometrics is not privacy.

As for the problem of reuse, the measures technique when reusing such as the liveness detection technique is more effective than the encryption of data and nullification of data if biometrics can specify the individual by the link information.

It is necessary to examine effectiveness compared with the competing measures techniques, for instance, cryptography. T he analysis of the effectiveness of the measures technique is described in Chapter 4.

3 Systematization of the cancelable biometrics technique

3.1 Cancelable biometrics techniques

Cancelable biometrics is a collective term of template protection techniques that nullifies it when an original biometric data is made invisible from the template not to be restorable in the biometric authentication systems.

There are two kinds templates. One is for image (signal) data input from the sensor and the other is for the feature data that used for processing. There are two kinds of nullification methods: based on encryption techniques and on image processing.

Encryption-based approach stores encrypted templates and decrypts templates at authentication time. Image processing-based approach matches encrypted templates without decrypting the data and provides the abilities of invisibility of original biometric data and canceling lost templates. It is also a mixed technology of biometrics and encryption as various mechanisms are used to implement these functionalities. Generally, security strength is unclear.

Fig. 2 shows typical processing flow of the cancelable biometrics.

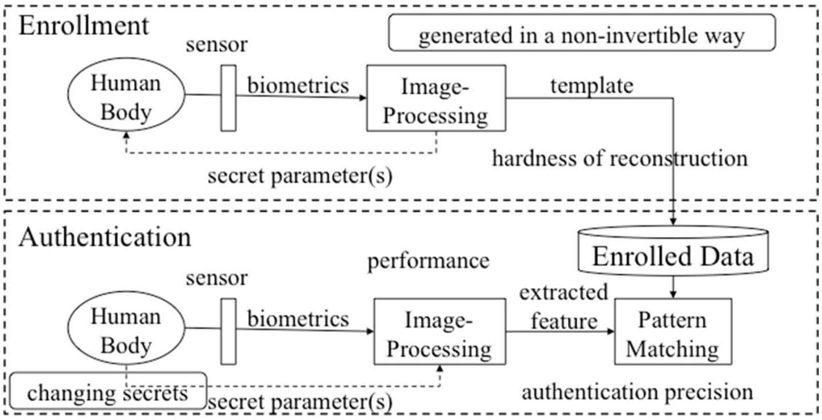

Fig. 2. The processing flow of cancelable biometrics.

The biometric data is distorted by the conversion processing using a one way transformation function in an enrollment or an authentication processing. The template generated by a nonreciprocal method is stored in the smart card and the database.

The biometric data causes a different swerve at each registration. Therefore, when the reliability of biometric information is lost, the misinterpretation method used at that time is changed. Furthermore, it only has to register again based on a new conversion coefficient.

The technical details of a cancelable biometrics based on image processing is discussed thoroughly in [9].

The groupings by PET (Privacy Enhancing Technologies) [8]-[10] are classified techniques of privacy protection that can be applied to the systematization of cancelable biometrics. Techniques of cancelable biometrics and the dynamic key generation algorithm developed now can be classified into four categories (A to D) in reference to the classified techniques of PET, as shown in Table 2.

Table 2. Grouping by PET of template protection techniques.

Principle	Methods	Ref.
One-way function	A1. Non-reversible transformation of images	[6]
	A2. Non-reversible transformation of templates	
	B. Image morphing	
Common key cryptography	NA	
Public key cryptography	D1.	[5] [7]
Secret sharing function	NA	
Blind signature	NA	
Zero knowledge protocol	D2	[4]
Proxy network	NA	
Fake information	C1. Fuzzy vault	[1] [3]
	C2. Convolution random pattern	[2]
Privacy language	NA	

Category A is a method by noninvertible conversion. Conversion can be applied to both image (signal) and feature region. An example of conversion in the image area includes morphing and the block substitution. For example, the block structure is allocated in the block substitution according to a feature point in former image area, it arranges at every the block, and the scramble is done. However, not noninvertible conversion in this case but former image can often be computed reversibly.

Therefore, security strength is low, and the conversion in the image space is classified into category B.

Category C is the method to use information on fake data such as Fuzzy Vault.

Category D is the method of the data protection using the public key cryptography and zero knowledge proof technology. Furthermore, category D also proposes data protection techniques that use a general cryptographic protocol in ISO TC68 that is the technical committee intended for financial services.

Currently, data protection technologies in biometric data are perceived to be immature. Therefore, the empty column in Table 2 represents template protection technologies that could be proposed in the future.

3.2 Evaluation of validity of the cancelable biometrics

There are two technologies for the protection of template data: image processing based methods and cryptographic based methods.

Cryptographic template protection technology is open to the public, which allows evaluation of security strength by third parties. For example, FIPS140-2 is maintained as a safety standard at the implementation level.

Application Existence of an application where image processing-based template protection methods have the precedence over cryptographic-based.

On the other hand, from a technical point of view, image processing-based template protection methods have the following problems..

- Proper evaluation of the template protection technique is insufficient.
- The third party evaluation cannot be done because the algorithm and the interface are unpublished.
- The security strength evaluation scheme is not established, and an objective evaluation concerning a one way transformation, accuracy preservation and the processing performance is not done (Refer to Table 3).
- There is a possibility that it is technically immature as described in paragraph 3.1, and a more effective method will be developed in the future.

Table 3. Evaluation axis of the cancelable biometrics.

Items	Description
Hardness of reconstructing original data	Proof of being essentially unable to reconstruct original biometric data from converted data by a one-way function etc.
Preservation of authentication precision	Proof that authentication precision over converted data is no lower than that over pre-converted (original) data
Performance	Demonstration of the performance of a conversion algorithm for practical use
Application	Existence of an application where image processing-based template protection methods have the precedence over cryptographic-based.

- There is no appropriately applied actual case.
- The individual data not in the database but in the smart card model is general from a viewpoint of a restriction of law and safety.
- Cancelable biometrics is a technology that assumes storage in a database, and a powerful application that can demonstrate superiority over template protection technology of cryptography based methods is not known.
- The priority is low in the viewpoint of the security risk. Details are presented in Chapter Chapter 4. Therefore, it is enough not to ensure that the template data is kept secret and discuss the safety of the system.

As a solution to these problems, security evaluation techniques will be established and an appropriate application will be developed.

4 Evaluation of countermeasure techniques for securing the system

Two points should be considered: technical validity and standardization. If biometrics have been exposed. the possibility that it is acquired by a malicious person without the consent of the user is high. Therefore, for the safety of a biometric authentication system, measures against reuse are more important than those against theft.

In reusing the template data, there are two kinds of abuse such as the capturing of the biometrics of the counterfeit and spoofing due to hacking to the system. The liveness detection function is necessary for the former and it is necessary for data transfer to be secure for the latter.

Applying the standardized cryptography technology for the data protection in the channel is an advantage in terms of cost and safety. Moreover, liveness detection measures that should be carried out when body information is acquired from the sensor, and image processing techniques become indispensable, as no alternative technology exists.

Therefore, from a practical viewpoint, it is thought that the development of liveness detection technology is a higher priority than the data protection technique of the image processing based cancelable biometrics.

In this chapter, the liveness detection technique is discussed as a spoofing prevention in the sensor aiming to prove the above-mentioned hypothesis quantitatively. Then, encryption and cancelable biometrics are taken up as data protection techniques in the channel and the database. The effectiveness of each technique is evaluated with respect to safety.

In this study, FTA (Fault Tree Analysis) is adopted as a quantitative risk evaluation method. FTA is a technique for making a logic diagram with a tree structure known as the Fault Tree that shows the causal relation of the generation process of the threat, the calculation of the probability of occurrence of the threat based on this logic diagram, and evaluation of the risk.

Applied to the security measures in the information system, FT is composed of making the threat a root[8], and uniting events derived according to the causal relation hierarchically by using the logic gate of the logical add and the logical product. The probability of occurrence of the root threat can be obtained by giving the probability of occurrence for each lower event after the FT is made.

Fig. 3 shows FT made for the spoofing attack. The probability of occurrence of a basic event of the liveness detection, the encryption, and the cancelable biometrics was given to FT under assumption that each technology was applied, and the probability of occurrence of the threat was calculated.

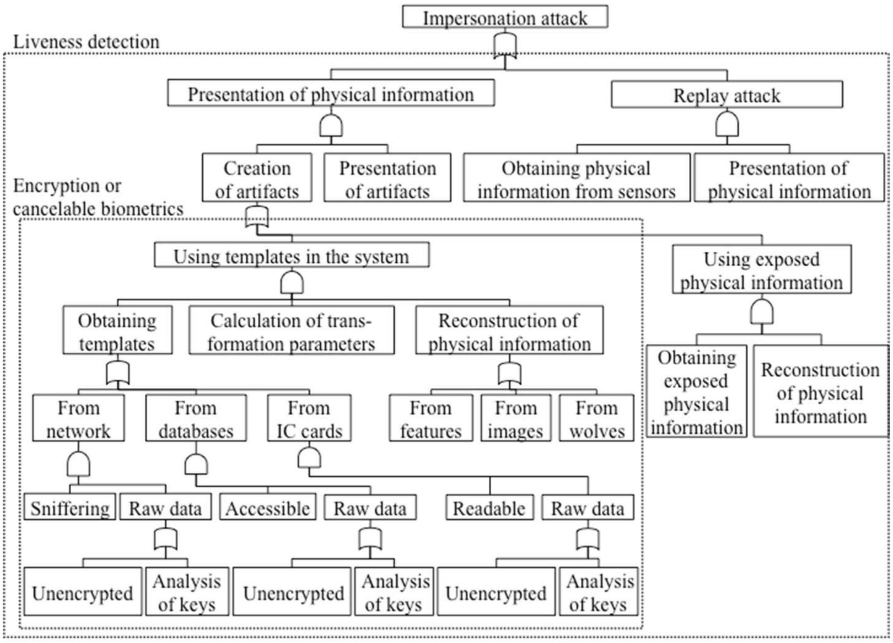
Impersonation attack
Liveness detection
Presentation of physical information
Replay attack
Creation of artifacts
Presentation of artifacts
Obtaining physical information from sensors
Presentation of physical information
Encryption or cancelable biometrics
Using templates in the system
Using exposed physical information
Obtaining templates
Calculation of trans-formation parameters
Reconstruction of physical information
Obtaining exposed physical information
Reconstruction of physical information
From network
From databases
From IC cards
From features
From images
From wolves
Sniffering
Raw data
Accessible
Raw data
Readable
Raw data
Unencrypted
Analysis of keys
Unencrypted
Analysis of keys
Unencrypted
Analysis of keys

Fig. 3. Fault tree for an impersonation attack.

Table 4 shows the probability of occurrence of the basic event used by this analysis. It was roughly distinguished that the probability of occurrence obtained an actual figure in three stages because it was difficult. The living body detection technology was assumed to be the one that it was possible to detect it surely when body information not to be alive was presented.

Table 5 shows the numerical results. The risk type is usually defined by the product of the probability of occurrence and the size of the loss. Here it was assumed that the loss that occurred as a result of the spoofing was the same for each threat, and so the risk is evaluated only by the probability of occurrence.

It is understood to have lowered the liveness detection in addition while the cryptography and the cancelable biometrics lower the probability of occurrence (0.15 and 0.13, respectively) under the situation in which measures are not done

Table 4. Occurrence probabilities of basic events.

Events	Event probability (When a measure is applied)			
	Nothing	Cryptography	Cancelable biometrics	Liveness detection
Obtaining physical information from sensors	0.1	0.1	0.1	0.1
Obtaining exposed physical information outside the system	0.3	0.3	0.3	0.3
Reconstruction of physical information from exposed biological information	0.3	0.3	0.3	0.3
Derivation of transformation parameters of cancelable biometrics	-	-	0.1	-
Reconstruction of physical information from features	0.1	0.1	0.1	0.1
Reconstruction of physical information from images	0.3	0.3	0.3	0.3
Analysis of encryption keys	-	0.01	-	-
Data Encryption	1.0	0	1.0	1.0
Interception of communication	0.1	0.1	0.1	0.1
Database Access	0.2	0.2	0.2	0.2
Unauthorized reading of IC card	0.1	0.1	0.1	0.1
Presentation of not physical information that is not live	1.0	1.0	1.0	1.0

Table 5. Probability of occurrence of threats.

Applied technology	Probability of occurrence of threats	Range of Reduction Probability
Nothing	0.33	-
Cryptography	0.18	0.15
Cancelable biometrics	0.20	0.13
Liveness detection	0	0.33

compared with the probability 0.33 that the threat is generated from the results in Table 5. The following conclusions can be derived from above.

- In these technologies, the liveness detection is the most effective.
- From viewpoint of prevention of reuse to effectiveness of this level cryptography and cancelable biometrics that is data protection technology.
- The cryptography technology is standardized, and it is an advantage if an objective evaluation approach for safety has been established.

The template protection technology currently proposed is still immature but it is possible that it would evolve sufficiently in the future. Technical merits and demerits can't be judged objectively because the precision and the security strengths aren't estimated enough.

5 Conclusions

Living body measure is most effective in these technologies. However, encryption technology is standardized and there is a merit by which objective evaluation technique is established about safety.

The viewpoint of an effective methodology that secured the safety of biometric authentication systems was considered. The cancelable biometrics technique was systematized based on Privacy Enhancing Technology, and the possibility that a new technology will be developed in the future was shown in Chapter 4.

It proposed the evaluation items such as one way transformation, accuracy preservation and processing performance that clarified the effectiveness of the cancelable biometrics. The effectiveness of the technologies were quantitatively compared by using FTA method for the reuse problem in a biometric authentication system, when biometrics data had been leaked and exposed. According to the FTA analysis, when compared the cryptography and liveness detection, the effect of cancelable biometrics on the safety of biometric authentication systems was small.

References

1. Clancy, T., Kiyavash, N., Lin, D.: Secure smartcard based fingerprint authentication. In: WBMA '03 Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, pp.45–52 (2003)
2. Hirata, S., Takahashi, K., Mimura, M.: Vulnerability analysis and improvement of cancelable biometrics for image matching. In: The 2007 Symposium on Cryptography and Information Security, 3C1-2, Japan (2007)
3. Juels, A., Sudan, M.: A fuzzy vault scheme. In: Proc. IEEE Int. Symp. Inf. Theory, pp.408–413 (2002)
4. Kikuchi, H.: On security of asymmetric biometrics authentication. In: The 2006 Symposium on Cryptography and Information Security, 2D3-2, Japan (2006)
5. Kwon, T., Lee, J.: Practical digital signature generation using biometrics. In: Computer Science and Its Applications, LNCS (Lecture Notes in Computer Science), vol. 3043, pp.728–737. Springer-Verlag (2004)

6. Ratha, N., Connell, J., Bolle, R.: Enhancing security and privacy in biometrics-based authentication systems. IBM systems J., Vol.40, No.3, pp.614–634 (2001)
7. Soutar, C., Roberg, D., Stoianov, A., Gilroy, R., Kumar, V.: Biometric encryption, http://www.bioscrypt.com/assets/Biometric_Encryption.pdf
8. Shimizu, S., Seto, Y.: A study on the effectiveness of cancelable biometric technology in biometric authentication systems. In: The 2008 Symposium on Cryptography and Information Security, 2B3-2, Japan (2008)
9. Shimizu, S., Seto, Y.: An evaluation of biometric template protection methods. In: The Asian Biometrics Consortium Conference and Exhibition 2007 (ABC2007), Invited talk, Singapore (2007)
10. Seto, Y.: Proposal to develop and operate for useful biometric application systems. The Journal of the Institute of Electronics, Information and Communication Engineers, Vol.90, No. 12, pp.1025–1030 (2007)
11. Paul, P. P.,: Multimodal Cancelable Biometrics. In:Cognitive Informatics and Cognitive Computing (ICCI*CC), pp.43–49, Kyoto (2012)
12. Paul, P. P., Gavrilova, M., Klimenko, S.: Situation awareness of cancelable biometric system. In:The Visual Computer, Volume 30, Issue 9, pp 1059–1067 (2014)
13. Rathgeb, C and Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security (2011)