International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1090

(05/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

Authentication framework with one-time telebiometric templates

Recommendation ITU-T X.1090

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	**X.1080–X.1099**
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1090

Authentication framework with one-time telebiometric templates

Summary

Recommendation ITU-T X.1090 describes a user-authentication framework that uses one-time telebiometric templates. The framework provides secure user authentication and protection mechanisms for the biometric templates transmitted over open networks. It prevents replay attacks and protects the original biometric template by generating a new template upon each completion of authentication. This Recommendation also addresses the security requirements associated with the framework with one-time telebiometric templates.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1090	2011-05-29	17

Keywords

Biometric authentication, one-time telebiometric template, replay attack, telebiometrics.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1090

Authentication framework with one-time telebiometric templates

1 Scope

This Recommendation describes a user-authentication framework that uses one-time telebiometric templates to implement secure biometric-authentication systems. It specifies the framework in terms of function models and security requirements. Note, however, that this Recommendation does not cover the transformation functions used to generate one-time telebiometric templates (OTTs) because many different kinds of transformation can be adopted to generate OTTs.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ISO 19092] ISO 19092:2008, *Financial services – Biometrics – Security framework*.

[ISO/IEC 18031] ISO/IEC 18031:2011, *Information technology – Security techniques – Random bit generation*.

[ISO/IEC 19784-1] ISO/IEC 19784-1:2006, *Information technology – Biometric application programming interface – Part 1: BioAPI specification*.

[ISO/IEC 19785-1] ISO/IEC 19785-1:2006, *Information technology – Common Biometric Exchange Formats Framework – Part 1: Data element specification*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 biometric [ISO/IEC 19785-1]: Pertaining to the field of biometrics.

3.1.2 biometric authentication [ISO 19092]: Process of confirming an individual's identity, either by verification or by identification.

3.1.3 biometric sample [ISO/IEC 19785-1]: Information obtained from a biometric device, either directly or after further processing.

3.1.4 biometric template [ISO/IEC 19784-1]: A biometric sample or combination of biometric samples that is suitable for storage as a reference for future comparison.

3.1.5 biometric verification [ISO 19092]: Process of comparing a match template against reference based on a claimed identity (e.g., user ID, account number).

3.1.6 biometrics [ISO/IEC 19785-1]: Automated recognition of individuals based on their behavioral and biological characteristics.

3.1.7 biometrics data [ISO/IEC 19785-1]: A biometric sample at any stage of processing, biometric reference, biometric feature, or biometric property.

3.1.8 enrolment [ISO 19092]: Process of collecting biometric samples from a person and the subsequent generation and storage of biometric reference templates associated with that person.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 client: Entity that provides a biometric authentication service using a one-time telebiometric template on a user side in telecommunication environments.

3.2.2 one-time biometric template: Biometric template that is used only once and then revoked.

3.2.3 OTT database: Physical or logical storage device that stores data and information for user authentication and belongs to a server.

3.2.4 one-time telebiometric template: One-time biometric template used in open network environments.

3.2.5 original template: Biometric template that is created directly from a user's biometric sample and is neither transformed nor encoded.

3.2.6 OTT token: Physical storage device that stores data and information for user authentication and belongs to a user.

3.2.7 replay attack: Breach of security in open networks wherein a biometric template from a client is stored without authorization and retransmitted to a server to gain illegal access.

3.2.8 server: Entity that provides a biometric-authentication service using a one-time telebiometric template at the request of a user or a client in telecommunication environments.

3.2.9 synchronization information: Non-biometric data that is used to keep transformation consistent between a client (or user) and a server.

3.2.10 transformation: Process of distorting or converting a biometric template into another domain to protect and conceal its original value.

3.2.11 transformation information: Non-biometric data that is used for transformation of a biometric template.

3.2.12 transformed template: Biometric template that is created through transformation.

3.2.13 user: Receiver of a biometric authentication service through a client and a server.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

OTT	One-time Telebiometric Template
OTT DB	OTT DataBase
SI	Synchronization Information
TI	Transformation Information

5 Conventions

None.

6 One-time telebiometric template for authentication

6.1 Threats in telebiometric authentication

As information technology advances, biometric authentication systems are increasingly employed in many areas to provide efficient and secure access control. Note, however, that this gives rise to privacy concerns as well, since personal information needs to be stored in centralized systems and transmitted over open networks. These threats are not new, but they are more critical in biometric authentication due to the nature of biometric data [b-Ratha]. Biometric data identifies a user as unique, but there are only a few substitutes. Therefore, once they lose their biometric data, they may permanently lose their identities. For example, a user has only one face and ten fingerprints, and it is impossible to change the biometric traits with new ones as if creating new passwords. Moreover, because biometric data is unique, it is much like the same password for multiple systems. Thus, an attacker stealing a user's biometric template from one system can log in to other systems using the stolen template. Unfortunately, conventional encryption will have no effect when coping with such threats. In addition, for template comparison, an encrypted template should be decrypted, and thus an original template is exposed for every comparison. Moreover, without attacking a server directly, an attacker can gain access control by eavesdropping on a communication and simply replaying the encrypted message as if it were generated by any valid client or user.

6.2 Authentication using a one-time telebiometric template

The authentication framework provides secure user authentication and protection for a biometric template transmitted over open networks. It converts a biometric template using transformation functions, and uses a transformed template for user authentication and network transmission instead of an original template. If a template is lost or compromised, a new transformed template is created using a new instance of transforms. Similarly, by generating a new transformed template for each authentication, it effectively prevents a replay attack. Through template transformation, transformation information and biometric data are mixed, and template comparison is performed in a transformed state. Therefore, they are not separated even during template comparison and provide a strong protection for each other.

7 Overview of the authentication framework with a one-time telebiometric template

7.1 Enrolment procedure

Figure 1 shows the outline of the enrolment procedure with a user's biometric data.

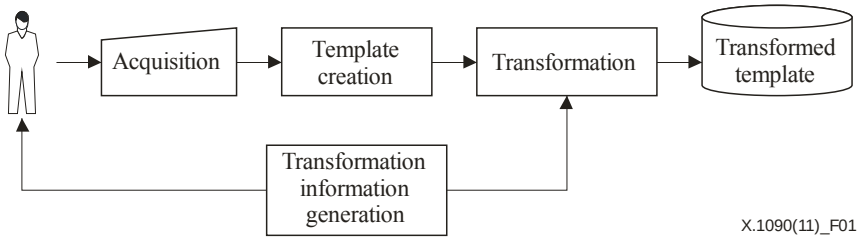

Figure 1 – Enrolment procedure with OTT

a. The user provides his or her biometric data, for example, face or fingerprint.

b. The system extracts the user's biometric features and creates a biometric template.

c. The system generates transformation information randomly.

d. The system converts the biometric template using the random transformation information and stores the transformed template in an OTT DB.

e. The user receives the OTT token that stores the transformation information.

7.2 Verification procedure

Figure 2 shows the outline of the biometric verification procedure with an OTT.

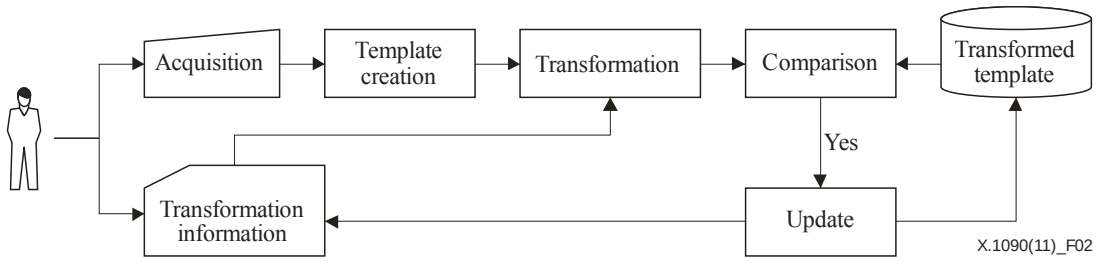

Figure 2 – Verification procedure with OTT

a. The user provides his or her biometric data and OTT token.

b. The client creates a biometric template from the given biometric data and transforms the template using the transformation information stored in the user's OTT token.

c. The client sends the transformed template to the server.

d. The server compares the template from the client with a transformed template in the OTT DB.

e. If the user is verified as genuine, the server generates updated data for new transformation information and a new transformed template.

f. The server creates a new transformed template using the updated data.

g. The server sends the client the updated data.

h. The client checks the validity of the updated data and creates new transformation information using the updated data.

i. At the next authentication, the client uses the new transformation information to create a new transformed template.

8 Authentication framework with a one-time telebiometric template

8.1 OTT generation model

8.1.1 Overview

Figure 3 illustrates an OTT generation model. The OTT generation module takes two inputs, an input template and transformation information, and produces the OTT.

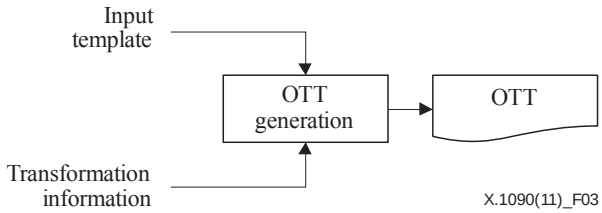

Figure 3 – OTT generation model

8.1.2 Input template

The input template can be an original template, a transformed template or an OTT.

8.1.3 Transformation information

The transformation information can be a transformation function or a set of parameters for a transformation function. Ideally, transformation information should be created independently of biometric data or input templates; otherwise, a user's biometric information could be leaked when transformation information is disclosed. For maximum security and protection, it should be kept secret

8.1.4 OTT generation

The OTT generation module or process generates an OTT by transforming an input template using transformation information. It shall generate a completely different OTT from the same input template if different transformation information is used, so that various transformed templates can be made from the same biometric data.

OTT generation with transformation information shall increase the randomness of biometric templates and conceal the range and distribution of biometric features so that an attacker cannot exploit prior knowledge about biometric data. Note, however, that the process and transformation information shall not affect biometric recognition performance. If the process and transformation information affect biometric recognition performance, authentication may depend on transformation information rather than a user's biometric data, and then an attacker may gain illegal access to a system without a user's biometric data. An attacker may gain illegal access to a system with transformation information only, which can be lost or compromised relatively easily compared to biometric data [b-Kong].

8.1.5 OTT

The OTT is a transformed template from an input template. The OTT shall have the same structure as its input template but with different values, since the OTT is used again as input to OTT generation to generate a new OTT.

8.2 User enrolment model with OTT

8.2.1 Overview

Figure 4 illustrates the user enrolment model with OTT. A user provides his or her biometric sample, and a system creates a user's original template and transforms it into an OTT. A system also generates TI and SI randomly and independently.

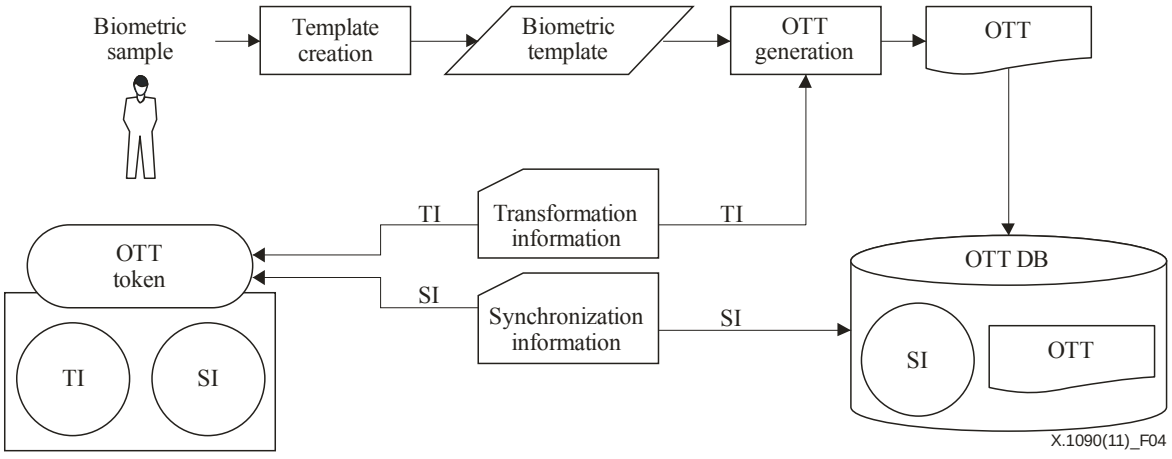

Figure 4 – User enrolment model with OTT

8.2.2 Template creation

The template creation module or process creates an original template from a user's biometric sample. The template shall not be stored in a permanent storage device since it is unprotected raw data, which is almost equivalent to a user's biometric sample.

8.2.3 Synchronization information

The synchronization information is information that is shared between a client (or user) and a server. It is used to synchronize a transformation information generation module or process between a client and a server. For practical purposes, it can be used as a seed to generate new transformation information. For enrolment, initial synchronization information shall be created independently of transformation information. Otherwise, transformation information can be reconstructed from synchronization information; it can then be used to recover an original template from OTT.

8.2.4 OTT DB

The OTT DB stores the OTT and SI. It is a storage device that belongs to a server. For security and protection of a user's biometric template, the OTT DB shall not keep TI together with an OTT since TI can be used as informative data for recovering an original template from the OTT when the OTT DB is compromised.

8.2.5 OTT token

The OTT token stores TI and SI. It is a personal storage device that belongs to a user. For positive verification, a user shall provide both his/her biometric data with his/her OTT token issued during enrolment.

8.3 Biometric verification model with an OTT

8.3.1 Overview

Figure 5 illustrates biometric verification with an OTT. A client creates an OTT and sends it to a server, which then performs template comparison. If a user is verified as genuine, a server performs the OTT DB update process or module, which is specified in the next clause.

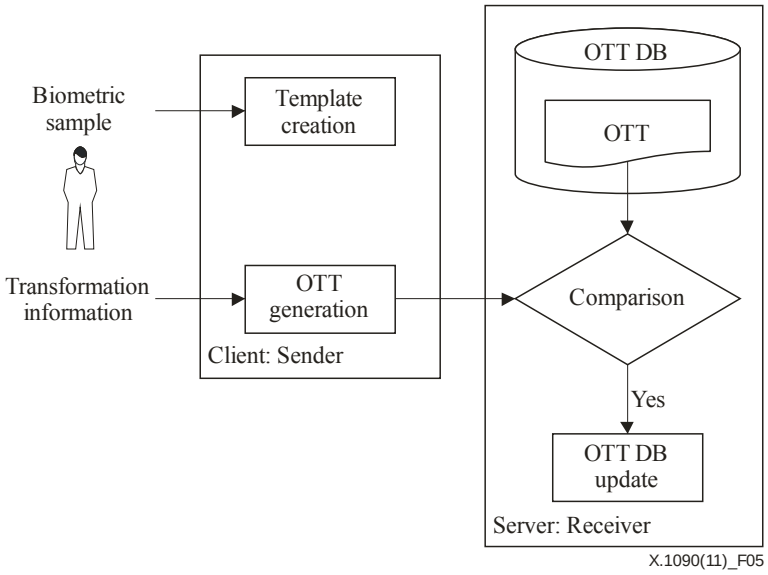

Figure 5 – Biometric verification model with an OTT

8.3.2 Comparison

The comparison module or process performs template comparison by comparing a template received from a client with a template stored in the OTT DB.

8.4 OTT DB update model

8.4.1 Overview

Figure 6 illustrates an OTT DB update model on a server side. If a user is verified as genuine at the verification stage, a server updates SI and the OTT stored in the OTT DB. The updated model on a client side is specified in the next clause.

A new template, OTT_{New}, is created from OTT and TI′, which is intermediate transformation information. TI′ is generated based on SI through transformation information generation. New synchronization information, SI_{New}, is generated from SI and a random number, R_{SI}. The OTT is then replaced by the OTT_{New}, and SI by SI_{New}.

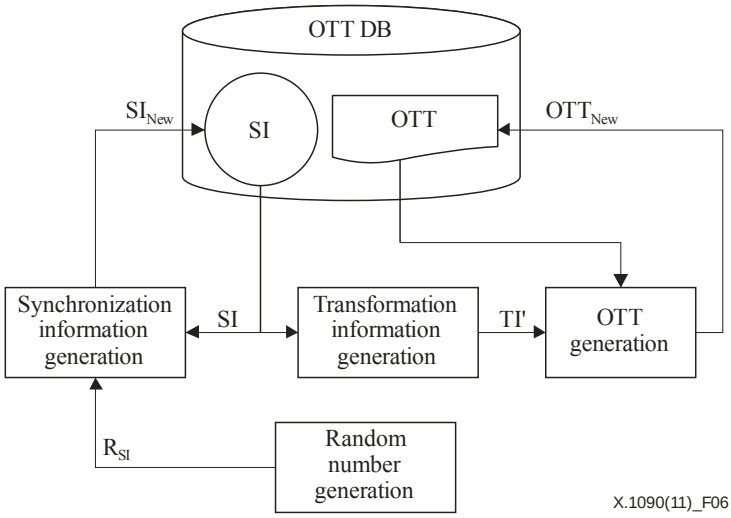

Figure 6 – OTT DB update model

8.4.2 Transformation information generation

The transformation information generation module or process generates transformation information based on its input. For example, it can generate a set of parameters for the transformation function from a random number generator, using its input as a seed.

8.4.3 Random number generation

The random number generation module or process generates a random number. For example, a random number generator specified in [ISO/IEC 18031] can be used.

8.4.4 Synchronization information generation

Synchronization information generation module or process generates new synchronization information by combining its two inputs. For example, SI_{New} can be created such that $SI_{New}: = H(SI \oplus R_{SI})$, where H() represents a one-way hash function, and ⊕, an exclusive OR operator.

8.5 Synchronization model

8.5.1 Overview

Figure 7 illustrates a synchronization model to keep transformation consistent between a client and a server. After updating data in the OTT DB, a server sends a client a signal so that the client confirms verification and updates the data stored in a user's OTT token through the OTT token update process or module, which is specified in the next clause. A random number, R_{SI}, which is used to update synchronization information, is sent to a client with a checksum, C.

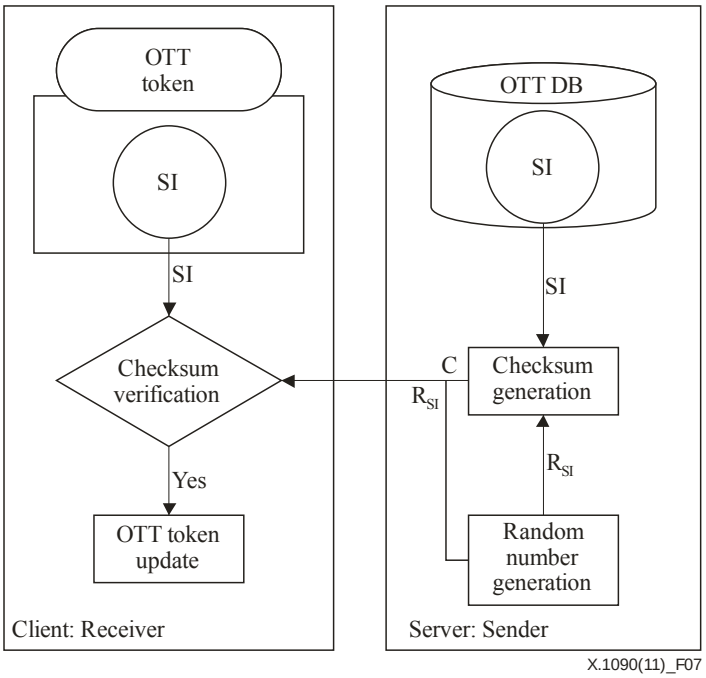

Figure 7 – Synchronization model

8.5.2 Checksum generation

The checksum generation module or process generates C from R_{SI} and SI stored in OTT DB. Because C and R_{SI} could be exposed during transmission, recovering SI from C and R_{SI} shall be computationally impossible. For example, C can be generated from SI and R_{SI} using a secure hash function H() such that C:=H(SI||R_{SI}), where || represents a concatenation operator. A standard hash algorithm can be used.

8.5.3 Checksum verification

The checksum verification module or process checks the validity of R_{SI} transmitted from a server. It calculates a checksum using R_{SI} from a server and SI stored in a user's OTT token and compares it with a checksum transmitted from a server. If the validity of R_{SI} is confirmed, a client updates data stored in a user's OTT token through the OTT token update process or module, which is specified in the next clause.

8.6 OTT token update model

8.6.1 Overview

Figure 8 illustrates an OTT token update model on a client side. After confirming verification, a client updates data stored in a user's OTT token. The updated data are used to generate a new transformed template for the next authentication.

New transformation information, TI_{New}, is generated through the transformation information update module or process. New synchronization information, SI_{New}, is created from SI and R_{SI}, which is sent from a server. Then, TI and SI are replaced by TI_{New} and SI_{New}, respectively.

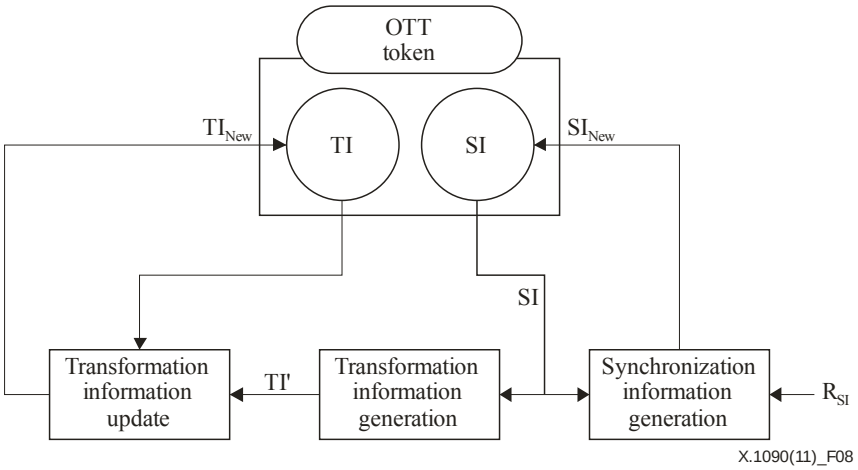

Figure 8 – OTT token update model

8.6.2 Transformation information update

The transformation information update module or process creates TI_{New} from TI and TI′, which is intermediate transformation information generated from SI. For example, TI_{New} can be generated through the function composition of TI′ and TI, such that TI_{New}:= TI′○TI, where ○ represents a function composition operator.

9 Requirements in authentication with OTT

9.1 General requirements

In general, data security concerns confidentiality, integrity, and availability. Besides these security requirements for general data, however, a one-time telebiometric template concerns additional requirements in security and privacy aspects as follows:

a. Retrieving or decoding an input template from an OTT shall be impossible without transformation information.

b. Linking an OTT across databases or applications shall be impossible.

9.2 Requirements in an OTT generation

The following conditions are required for secure biometric authentication and template protection:

a. A completely different OTT shall be generated from the same input template if different transformation information is used.

b. OTT generation with transformation information shall increase the randomness of biometric templates and conceal the range and distribution of biometric features.

9.3 Requirements in user enrolment

At a user enrolment process, the following guidelines should be observed to enhance security of a user's private data:

a. User enrolment should be performed face-to-face.

b. A user's identity should be validated by checking legal ID cards, for example passport and driver's license.

c. A system shall discard a user's biometric sample and original template immediately after enrolment.

9.4 Requirements in biometric verification

For secure biometric authentication, the following shall be considered:

a. A user shall provide both his/her biometric sample and valid OTT token to be verified as a genuine user.

b. The loss and misuse of a user's personal OTT token by an attacker shall not increase the possibility of false biometric authentication.

9.5 Security requirements in the authentication system

In order to protect a user's original biometric data, individual information or data, whose combination can possibly recover a user's original template, shall be distributed among the components, and each of them shall not store more data than they need. Moreover, each component shall provide proper protection for the data stored in it.

For higher security, a user's OTT token should conform to the following requirements:

a. An OTT for verification should be generated within the OTT token rather than within a client.

b. Transformation information and synchronization information should be updated within the OTT token rather than within a client.

c. An OTT token should be as directly and physically connected as possible to prevent an information leak and to make any outside attack difficult.

A client shall conform to the following requirements:

a. A client shall not keep biometric data and any other information provided by a user and transmitted from a server.

b. A biometric sensor shall be directly and physically connected to a client to prevent an information leak and to make any outside attack difficult.

A server shall conform to the following requirements:

a. An authentication server shall not keep a user's original template.

b. An authentication server shall not keep transformation information.

Annex A

OTT authentication with robust synchronization

(This annex forms an integral part of this Recommendation.)

A.1 Introduction

The synchronization module or process between a client and a server plays an important role in the authentication framework using a one-time telebiometric template. If information between a client and a server is inconsistent, the user-authentication service will stop. For example, during the transmission of a random number and a checksum from a server to a client, an attacker could generate a jamming signal so that the client will be unable to receive the message and update the transformation information, while the server will update the OTT. After this, the transformation information in the user's OTT token and the template in the OTT DB will be inconsistent, and the next user-verification service will fail. This annex presents user authentication with a robust synchronization technique. In the technique, a server keeps two OTTs and two SIs: the current OTT (OTT_{Curr}) and previous OTT (OTT_{Prev}); and current the SI (SI_{Curr}) and previous SI (SI_{Prev}). It is recommended that the scheme be employed if a transmission channel is unstable and unprotected.

A.2 User enrolment model with OTT

Figure A.1 illustrates the user enrolment model with OTT. A user provides his or her biometric sample and a system generates TI, SI and an OTT for enrolment. A user keeps TI and SI in his or her OTT token. A system assigns the OTT to OTT_{Curr}, and random values to OTT_{Prev}. Similarly, it assigns SI to SI_{Curr} and a random number to SI_{Prev}.

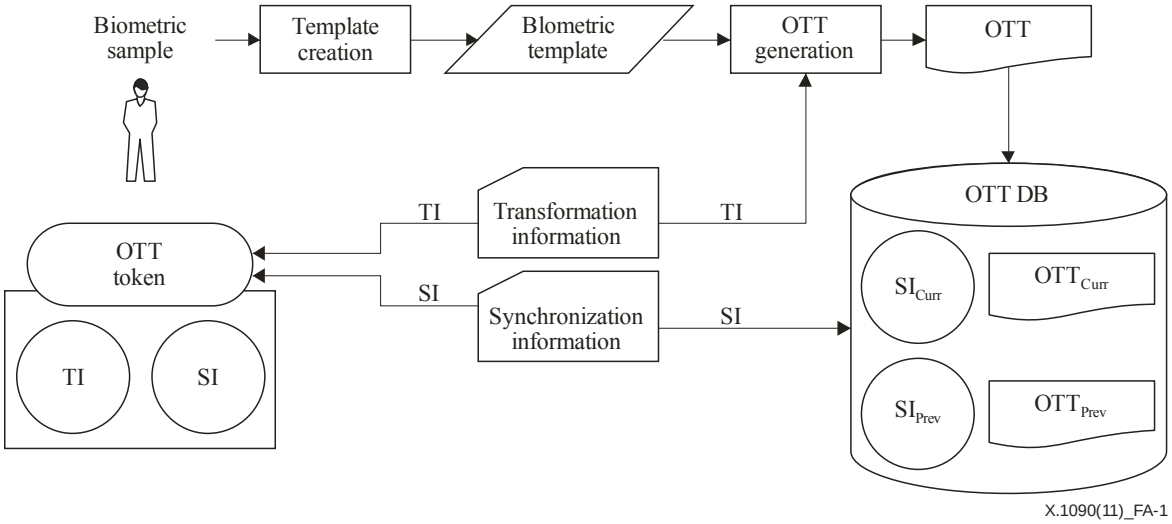

Figure A.1 – User enrolment model with OTT

A.3 Biometric verification model with an OTT

Figure A.2 illustrates biometric verification with an OTT. A client creates an OTT and sends it to a server, which then performs template comparison. The server first performs comparison between the OTT from a client and OTT_{Curr} in the OTT DB. If the comparison fails, it performs a comparison using OTT_{Prev}. If both of the trails fail, user authentication is terminated. Depending on a matched template, data in the OTT DB are updated in a different way.

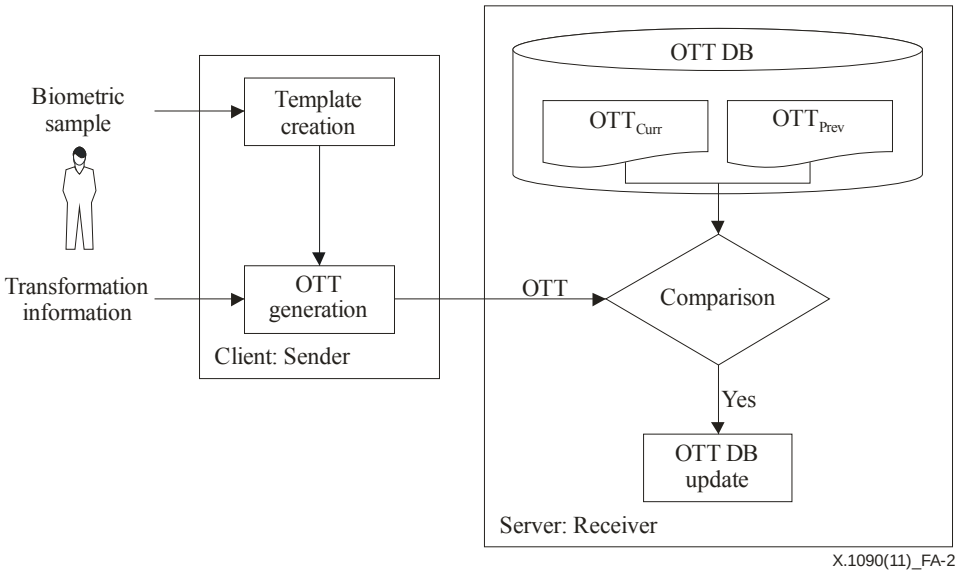

Figure A.2 – Biometric verification model with an OTT

A.4 OTT DB update model

If a user is confirmed positively at the verification stage, a server generates a new transformed template. The server performs the updating process in a different way, depending on the matched template, OTT_{Curr} or OTT_{Prev}.

Figure A.3 illustrates an OTT update model on the server side when the OTT from a client is matched with OTT_{Curr} in the OTT DB. A new template, OTT_{New}, is created from OTT_{Curr} and TI′, which is intermediate transformation information. TI′ is generated from SI_{Curr}. New synchronization information, SI_{New}, is created from SI_{Curr} and R_{SI}. Then, OTT_{Prev} is replaced by OTT_{Curr}, and OTT_{Curr} by OTT_{New}. Similarly, SI_{Prev} is replaced by SI_{Curr}, and SI_{Curr} by SI_{New}.

After updating the data, the server sends R_{SI} to the client so that the client will update the data stored in the user's OTT token.

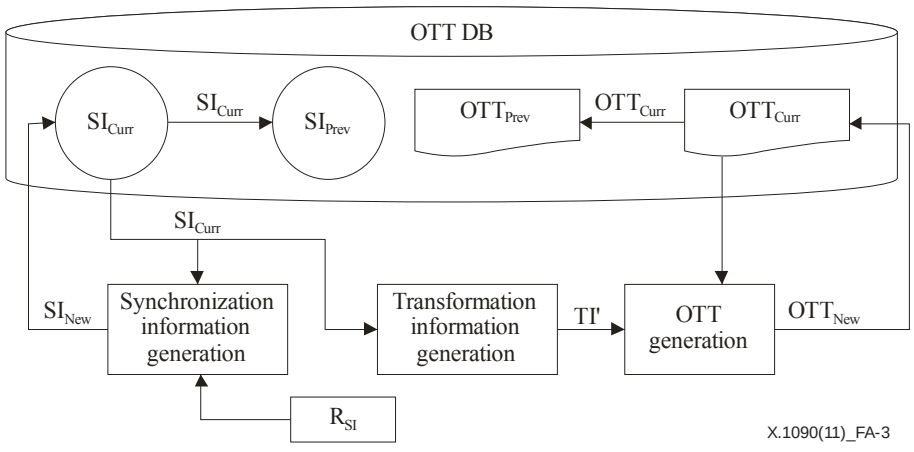

Figure A.3 – OTT DB update model when matched with OTT_{Curr}

Figure A.4 illustrates an OTT update model on the server side when an OTT from a client is matched with OTT_{Prev} in the OTT DB. Note that OTT_{Prev} and SI_{Prev} are not replaced. OTT_{New} is created from OTT_{Prev} and TI′, and then OTT_{Curr} is replaced by OTT_{New}. TI′ is generated from SI_{Prev}. SI_{New} is created from SI_{Prev} and R_{SI}, and then SI_{Curr} is replaced by SI_{New}.

After updating the data, the server sends R_{SI} to the client so that the client will update the data stored in the user's OTT token.

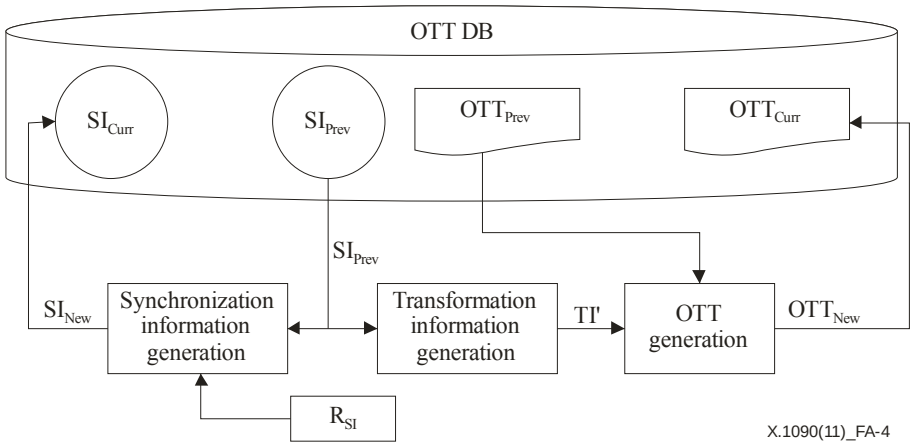

Figure A.4 – OTT DB update model when matched with OTT_{Prev}

A.5 Synchronization model

A.5.1 Overview

After updating the data in the OTT DB, the server sends to the client a signal so that the client will confirm authentication and will update the data stored in the user's OTT token. Figure A.5 illustrates a synchronization model between a client and a server. Note that SI in the OTT DB denotes SI_{Prev} when the OTT updating process is completed.

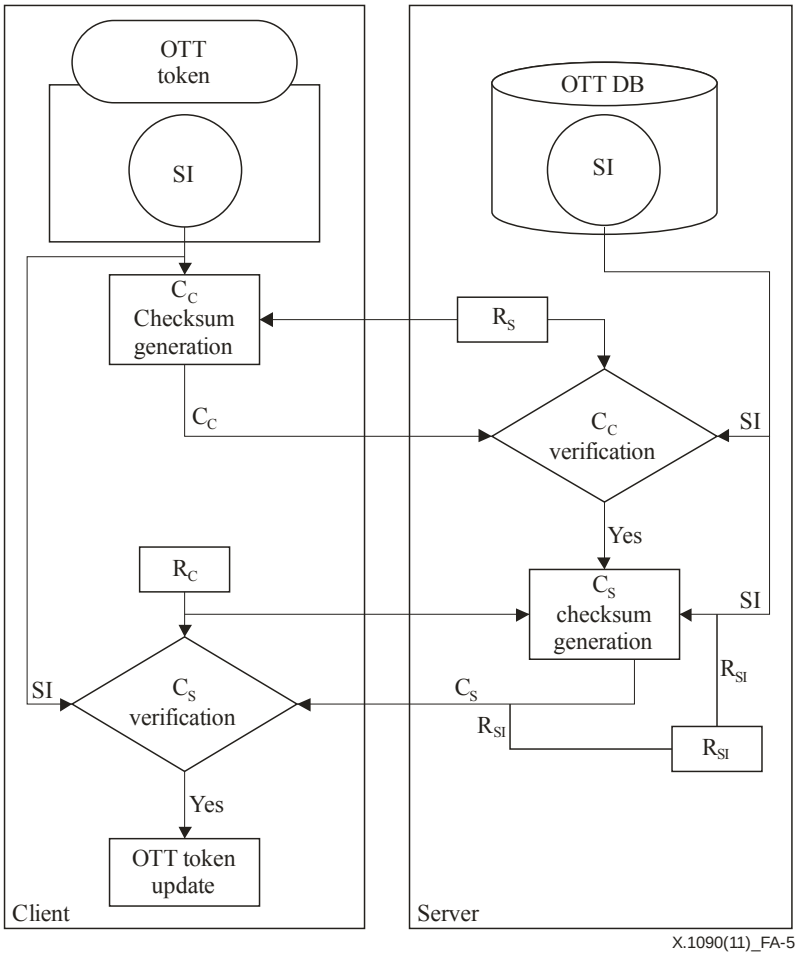

Figure A.5 – Synchronization model

A.5.2 Random number R_S

R_S is a random number generated from a server and sent to a client, which then generates a checksum using R_S to prove its validity to the server.

A.5.3 C_C checksum generation

The C_C checksum generation module or process generates a checksum from SI stored in a user's OTT token and R_S from a server. For example, a checksum can be generated using a secure hash function such that C_C:=H(SI|| R_S). A client sends a checksum to a server, which in turn checks the validity of the client using the checksum.

A.5.4 C_C verification

The C_C verification module or process verifies a client by comparing two checksums: the checksum from a client and that generated by itself.

A.5.5 Random number R_C

R_C is a random number generated by a client and sent to a server, which then generates a checksum using R_C to prove its validity to the client.

A.5.6 C_S checksum generation

The C_S checksum generation module or process generates a checksum from SI stored in the OTT DB and random numbers R_{SI} and R_C. For example, a checksum can be generated using a secure hash function such that C_S:=H(SI||R_{SI}||R_C). A server sends a client the checksum with R_{SI}.

A.5.7 C_S verification

The C_S verification module or process verifies a server by comparing two checksums: the checksum from a server and that generated by itself. If a client confirms the validity of a server, it updates data stored in the user's OTT token using R_{SI}.

A.6 OTT token update model

After confirming successful authentication, a client updates data stored in a user's OTT token. The updated data is used to generate a new OTT for the next authentication. Figure A.6 illustrates an OTT token update model.

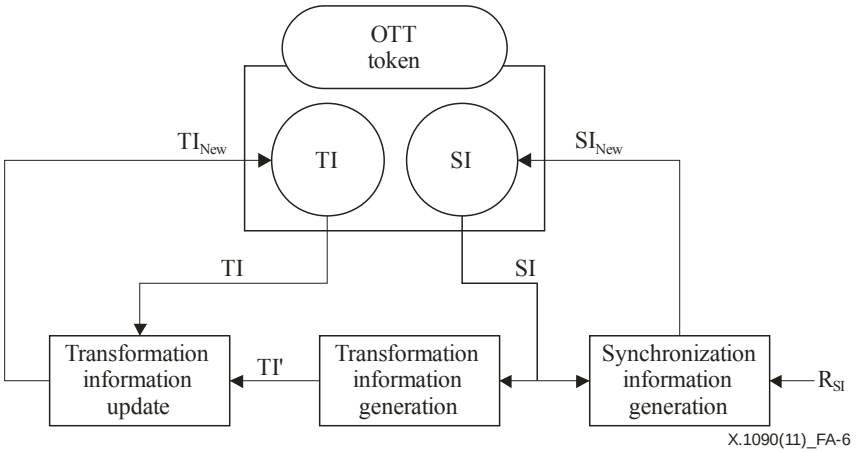

Figure A.6 – OTT token update model

Appendix I

Example of implementing OTT generation

(This appendix does not form an integral part of this Recommendation.)

I.1 Introduction

This appendix provides an example of OTT generation with transformation functions. It also describes how to update a template in a server and transformation information in a client. More details and examples can be found in [b-Lee].

I.2 Template transformation and comparison

Assume that a user's biometric template is in a vector of real numbers, and that comparison between two templates is performed using Euclidean distance. For convenience, suppose that $\mathbf{x}$ and $\mathbf{y}$ denote a gallery (enrolled template) and a probe (query template), respectively. They represent original templates, which are created directly from a user's biometric sample. Similarly, $\mathbf{g}$ and $\mathbf{p}$ represent their corresponding transformed templates.

At an enrolment stage, a user provides his or her biometric sample, and an authentication system generates original template $\mathbf{x}$ as well as a random transform. A transformed template is then created as follows:

$$\mathbf{g} := \mathbf{A}\mathbf{x} + \mathbf{b}$$

where $\mathbf{A}$ is a random orthogonal matrix and $\mathbf{b}$ is a random vector. An orthogonal matrix has properties as shown in the following equation:

$$\mathbf{A}^T\mathbf{A} = \mathbf{A}\mathbf{A}^T = \mathbf{I}$$

where $\mathbf{A}^T$ represents the transpose matrix of $\mathbf{A}$ and $\mathbf{I}$ is an identity matrix with the same size as $\mathbf{A}$. The variation and randomness of the transformed templates can be adjusted by controlling the variance of $\mathbf{A}$ and $\mathbf{b}$.

Instead of $\mathbf{x}$, $\mathbf{g}$ is stored in an authentication system, and $\mathbf{A}$ and $\mathbf{b}$ are kept with a user in a personal token, such as a smartcard. If $\mathbf{g}$ is (or $\mathbf{A}$ and $\mathbf{b}$ are) lost or compromised, a new template $\mathbf{g}$ is created using new $\mathbf{A}$ and $\mathbf{b}$. A new template $\mathbf{g}$ can be generated for each authentication by updating $\mathbf{A}$ and $\mathbf{b}$.

At a verification stage, a user provides his or her biometric sample and a token storing $\mathbf{A}$ and $\mathbf{b}$. A client then creates probe $\mathbf{p}$ as follows:

$$\mathbf{p} := \mathbf{A}\mathbf{y} + \mathbf{b}$$

Instead of sending $\mathbf{y}$, the client sends $\mathbf{p}$ to a server over the network, and the server performs template comparison. Comparison can be performed directly using Euclidean distance on $\mathbf{g}$ and $\mathbf{p}$ without $\mathbf{x}$ and $\mathbf{y}$ if a user provides accurate $\mathbf{A}$ and $\mathbf{b}$ as shown in the following equation:

$$\begin{aligned} \|\mathbf{g} - \mathbf{p}\|^2 &= (\mathbf{g} - \mathbf{p})^T (\mathbf{g} - \mathbf{p}) \\ &= (\mathbf{A}\mathbf{x} + \mathbf{b} - \mathbf{A}\mathbf{y} - \mathbf{b})^T (\mathbf{A}\mathbf{x} + \mathbf{b} - \mathbf{A}\mathbf{y} - \mathbf{b}) \\ &= (\mathbf{A}\mathbf{x} - \mathbf{A}\mathbf{y})^T (\mathbf{A}\mathbf{x} - \mathbf{A}\mathbf{y}) \\ &= (\mathbf{x} - \mathbf{y})^T \mathbf{A}^T \mathbf{A} (\mathbf{x} - \mathbf{y}) \\ &= \|\mathbf{x} - \mathbf{y}\|^2 \end{aligned}$$

Comparison itself does not change after the transformation of templates. Thus, even if an attacker obtains a user's token with transformation information, the possibility of false authentication does not increase compared to verification based on comparison between original templates. It means that he or she stills needs a valid biometric template to gain access to the system.

If a user provides the wrong $\mathbf{A}$ and $\mathbf{b}$, the difference between $\mathbf{g}$ and $\mathbf{p}$ is larger than that between $\mathbf{x}$ and $\mathbf{y}$ due to the mismatch of $\mathbf{A}$ and $\mathbf{b}$. This means that a user should provide his or her own biometric data and the correct $\mathbf{A}$ and $\mathbf{b}$ for positive authentication.

I.3 Update of template and transformation

Assume that just before the *nth* authentication, a server has $\mathbf{g}_n$ and synchronization information K_n, and a user has transformation information, $\mathbf{A}_n$ and $\mathbf{b}_n$, and synchronization information K_n.

At the *nth* authentication, a user provides his or her biometric data and a token storing $\mathbf{A}_n$ and $\mathbf{b}_n$; a client then creates *nth* probe $\mathbf{p}_n$, as follows, and sends it to a server:

$$\mathbf{p}_n := \mathbf{A}_n\mathbf{y} + \mathbf{b}_n$$

A server performs comparison between $\mathbf{p}_n$ and $\mathbf{g}_n$. If comparison is performed positively, the server updates $\mathbf{g}_n$. Using K_n as a seed number for a random number generator, the server generates the intermediate transforms $\mathbf{A}'_n$ and $\mathbf{b}'_n$, where $\mathbf{A}'_n$ is a new random orthogonal matrix and $\mathbf{b}'_n$ is a new random vector. A server then updates $\mathbf{g}_n$ into new template $\mathbf{g}_{n+1}$ as follows:

$$\mathbf{g}_{n+1} := \mathbf{A}'_n\mathbf{g}_n + \mathbf{b}'_n$$

After confirming the authentication result, a client generates intermediate transform $\mathbf{A}'_n$ and $\mathbf{b}'_n$ using K_n as a seed number in the same way as a server. The client then updates the current transformation information, $\mathbf{A}_n$ and $\mathbf{b}_n$, into new transformation information, $\mathbf{A}_{n+1}$ and $\mathbf{b}_{n+1}$, as follows:

$$\mathbf{A}_{n+1} := \mathbf{A}'_n\mathbf{A}_n$$

$$\mathbf{b}_{n+1} := \mathbf{A}'_n\mathbf{b}_n + \mathbf{b}'_n$$

I.4 Proof of consistency in comparison

Through mathematical induction, comparison can be proven to be performed consistently; comparison itself does not change as a template and transformation information are updated successively.

Let $\mathbf{g}_0$ be an initial enrolled template and $\mathbf{p}_0$ a first authentication template after enrolment.

$$\mathbf{g}_0 := \mathbf{A}_0\mathbf{x} + \mathbf{b}_0$$

$$\mathbf{p}_0 := \mathbf{A}_0\mathbf{y} + \mathbf{b}_0$$

where $\mathbf{A}_0$ and $\mathbf{b}_0$ are transformation information used at an enrolment stage. The following holds, as shown previously:

$$||\mathbf{g}_0 - \mathbf{p}_0||^2 = ||\mathbf{x} - \mathbf{y}||^2$$

When $n = 1$, a gallery and a probe are written as follows:

$$\mathbf{g}_1 := \mathbf{A}'_0\mathbf{g}_0 + \mathbf{b}'_0$$

$$\mathbf{p}_1 := \mathbf{A}_1\mathbf{y} + \mathbf{b}_1$$

where $\mathbf{A}_1 = \mathbf{A}_0^{'}\mathbf{A}_0$ and $\mathbf{b}_1 = \mathbf{A}_0^{'}\mathbf{b}_0 + \mathbf{b}_0^{'}$. With the updating rule, $\mathbf{p}_1$ can be written in terms of $\mathbf{p}_0$:

$$\begin{aligned}\mathbf{p}_1 &= \mathbf{A}_1\mathbf{y} + \mathbf{b}_1 \\ &= \mathbf{A}_0^{'}\mathbf{A}_0\mathbf{y} + \mathbf{A}_0^{'}\mathbf{b}_0 + \mathbf{b}_0^{'} \\ &= \mathbf{A}_0^{'}\left(\mathbf{A}_0\mathbf{y} + \mathbf{b}_0\right) + \mathbf{b}_0^{'} \\ &= \mathbf{A}_0^{'}\mathbf{p}_0 + \mathbf{b}_0^{'}\end{aligned}$$

Using the relation, the following can be derived:

$$\begin{aligned}\left\|\mathbf{g}_1 - \mathbf{p}_1\right\|^2 &= \left(\mathbf{g}_1 - \mathbf{p}_1\right)^T\left(\mathbf{g}_1 - \mathbf{p}_1\right) \\ &= \left(\mathbf{g}_0 - \mathbf{p}_0\right)^T\mathbf{A}_0^{'T}\mathbf{A}_0^{'}\left(\mathbf{g}_0 - \mathbf{p}_0\right) \\ &= \left\|\mathbf{g}_0 - \mathbf{p}_0\right\|^2 \\ &= \left\|\mathbf{x} - \mathbf{y}\right\|^2\end{aligned}$$

At time *n*, a gallery and a probe are defined as follows:

$$\mathbf{g}_n := \mathbf{A}_{n-1}^{'}\mathbf{g}_{n-1} + \mathbf{b}_{n-1}^{'}$$

$$\mathbf{p}_n := \mathbf{A}_n\mathbf{y} + \mathbf{b}_n$$

Assume that for the *nth* authentication, the following equation holds:

$$\|\mathbf{g}_n - \mathbf{p}_n\|^2 = \|\mathbf{x} - \mathbf{y}\|^2$$

Based on the assumption, the following equation can be proven to be true as well for *(n+1)th* authentication:

$$\|\mathbf{g}_{n+1} - \mathbf{p}_{n+1}\|^2 = \|\mathbf{x} - \mathbf{y}\|^2$$

According to the definition and updating rule, $\mathbf{g}_{n+1}$ and $\mathbf{p}_{n+1}$ can be written as follows:

$$\mathbf{g}_{n+1} = \mathbf{A}_n^{'}\mathbf{g}_n + \mathbf{b}_n^{'}$$

$$\begin{aligned}\mathbf{p}_{n+1} &= \mathbf{A}_{n+1}\mathbf{y} + \mathbf{b}_{n+1} \\ &= \mathbf{A}_n^{'}\mathbf{A}_n\mathbf{y} + \mathbf{A}_n^{'}\mathbf{b}_n + \mathbf{b}_n^{'} \\ &= \mathbf{A}_n^{'}\left(\mathbf{A}_n\mathbf{y} + \mathbf{b}_n\right) + \mathbf{b}_n^{'} \\ &= \mathbf{A}_n^{'}\mathbf{p}_n + \mathbf{b}_n^{'}\end{aligned}$$

By inserting the two equations into, $\|\mathbf{g}_{n+1} - \mathbf{p}_{n+1}\|^2$ the following can be derived:

$$\begin{aligned}\left\|\mathbf{g}_{n+1} - \mathbf{p}_{n+1}\right\|^2 &= \left(\mathbf{g}_{n+1} - \mathbf{p}_{n+1}\right)^T\left(\mathbf{g}_{n+1} - \mathbf{p}_{n+1}\right) \\ &= \left(\mathbf{g}_n - \mathbf{p}_n\right)^T\mathbf{A}_n^{'T}\mathbf{A}_n^{'}\left(\mathbf{g}_n - \mathbf{p}_n\right) \\ &= \left\|\mathbf{g}_n - \mathbf{p}_n\right\|^2 \\ &= \left\|\mathbf{x} - \mathbf{y}\right\|^2\end{aligned}$$

Therefore, comparison is performed consistently from the beginning, and the updating rules are said to be valid.

Bibliography

[b-Kong] Kong A., Cheung K. H., Zhang D., et al. (2006), *An analysis of BioHashing and its variants, Pattern Recognition*, vol. 39, No. 7, pp. 1359-1368.

[b-Lee] Lee, Y., Lee, Y., Chung, Y., and Moon, K. (2010), *Secure face authentication framework in open networks*, ETRI Journal, Vol. 32, No. 6.

[b-Ratha] Ratha N. K., Connell J. H., and Bolle R. M. (2001), *Enhancing security and privacy in biometrics-based authentication systems*. IBM Systems Journal, Vol. 40 No. 3, pp. 614-634.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012