International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1091

(04/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

A guideline for evaluating telebiometric template protection techniques

Recommendation ITU-T X.1091

ITU-T

ITU
International
Telecommunication
Union

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.1091

A guideline for evaluating telebiometric template protection techniques

Summary

Recommendation ITU-T X.1091 describes a general guideline for testing and reporting the performance of biometric template protection techniques based on biometric cryptosystem or cancellable biometrics. This guideline specifies two reference models for evaluation, which use biometric template protection techniques in telebiometric systems. It then defines the metrics, procedures and requirements for testing and evaluating the performance of the biometric template protection techniques.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1091	2012-04-13	17

Keywords

Biometric cryptosystem, biometric template protection techniques, cancellable biometrics, evaluation, 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 not 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

Page

Introduction

Various valuable applications using password authentication are currently in general use on the open network. However, knowledge-based authentication has some shortcomings; for example, anyone can input a leaked password. Therefore, a number of other authentication methods are considered for application on the open network.

Biometrics technologies are considered as one of the methods of authentication technology. However, they reveal some vulnerability in the open network environment. Once a biometric feature is compromised, it is unable to permanently utilize a secure authentication against the replay attack because of its unique and permanent characteristics. For these reasons, attention is focused on the biometric template protection technique.

The biometric template protection technique has a specific renewal property. If a stored biometric reference has been compromised from the server, the administrator can renew the reference for a secure authentication.

Recently, various protection techniques have been proposed and the following documents have provided standard specifications to protect biometric data, based on these techniques: ISO 24745: *Biometric information protection*, ITU-T X.1088: *Telebiometrics digital key framework (TDK)* and ITU-T X.1090: *Authentication framework with one-time telebiometric templates*.

This Recommendation standardizes the guideline for evaluating protection performance of these techniques.

Recommendation ITU-T X.1091

A guideline for evaluating telebiometric template protection techniques

1 Scope

This Recommendation:

- establishes a general guideline for testing and evaluating the performance of biometric template protection techniques based on biometric cryptosystem or cancellable biometrics;
- clarifies targets of two biometric template protection mechanisms for evaluation reference models in telebiometric systems;
- clarifies evaluation items of each biometric template protection technique;
- defines the protection performance metrics for each biometric template protection technique;
- specifies requirements and procedures of evaluation methods.

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.

[ITU-T X.1086] Recommendation ITU-T X.1086 (2008), *Telebiometrics protection procedures – A guideline to technical and managerial countermeasures for biometric data security*.

[ITU-T X.1090] Recommendation ITU-T X.1090 (2011), *Authentication framework with one-time telebiometric templates*.

[ISO 19792] ISO/IEC 19792:2009, *Information technology – Security techniques – Security evaluation of biometrics*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51521>

[ISO 19795-1] ISO/IEC 19795-1:2006, *Information technology – Biometric performance testing and reporting – Part 1: Principles and framework*.
<http://webstore.iec.ch/webstore/webstore.nsf/ArtNum_PK/42119?OpenDocument>

[ISO 19795-2] ISO/IEC 19795-2:2007, *Information technology – Biometric performance testing and reporting – Part 2: Testing methodologies for technology and scenario evaluation*.
<http://webstore.iec.ch/webstore/webstore.nsf/ArtNum_PK/42120?OpenDocument>

[ISO 19795-3] ISO/IEC TR 19795-3:2007, *Information technology – Biometric performance testing and reporting – Part 3: Modality-specific testing*.
<http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/41184>

[ISO 24745] ISO/IEC 24745:2011, *Information technology – Security techniques – Biometric information protection*.
<http://www.iso.org/iso/catalogue_detail?csnumber=52946>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 attacker [ISO 19792]: Person seeking to exploit potential vulnerabilities of a biometric system.

3.1.2 biometric (adjective) [b-ITU-T X.1084]: Of or having to do with the field of biometrics.

3.1.3 biometric data [ISO 24745]: Biometric sample or aggregation of biometric samples at any stage of processing, biometric reference, biometric probe, biometric feature or biometric property.

NOTE – Biometric data need not be attributable to a specific individual, i.e., Universal Background Models.

3.1.4 biometric reference [ISO 24745]: One or more stored biometric samples, biometric templates, or biometric models attributed to a biometric data subject and used for comparison.

3.1.5 biometric sample [ISO 24745]: Analogue or digital representation of biometric characteristics prior to biometric features being extracted and obtained from a biometric capture device or biometric capture subsystem.

3.1.6 biometrics (noun) [b-ITU-T X.1084]: An automated recognition of individuals based on their behavioural and biological characteristics.

3.1.7 challenge response [b-ITU-T X.1124]: A method of protecting against replay attack. For example, if entity A wants to obtain a new message from entity B, it can first send a challenge in the form of a nonce (e.g., a cryptographic value that is used only once) to B. A then receives a response from B, based on the nonce that proves B was the intended recipient.

3.1.8 evaluator [ISO 19792]: Person or party responsible for performing a security evaluation of a biometric product.

3.1.9 false match rate (FMR) [ISO 19795-1]: Proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template.

NOTE – The measured/observed false match rate is distinct from the predicted/expected false match rate (the former may be used to estimate the latter).

3.1.10 false non-match rate (FNMR) [ISO 19795-1]: Proportion of genuine attempt falsely declared not to match the template of the same characteristic from the same user supplying the sample.

NOTE – The measured/observed false non-match rate is distinct from the predicted/expected false non-match rate (the former may be used to estimate the latter).

3.1.11 key [b-ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

3.1.12 one-way function [b-ITU-T X.509]: A (mathematical) function f which is easy to compute, but which for a general value y in the range, it is computationally difficult to find a value x in the domain such that f(x) = y. There may be a few values y for which finding x is not computationally difficult.

3.1.13 renewability [ISO 24745]: Generic ability to allow the creation of multiple, independent transformed biometric references from one or more biometric samples obtained from the same data subject for the purposes of enhancing security and privacy.

3.1.14 revocability [ISO 24745]: Ability to prevent future successful verification of a specific biometric reference and the corresponding identity reference.

3.1.15 user [ISO 19792]: Person interacting with a biometric system.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Biometric cryptosystem mechanisms

3.2.1.1 biometric cryptosystem mechanism: A mechanism for authentication with a conventional cryptographic protocol using a cryptographic key generated from secret data. The secret data are extracted from helper data that are created from the biometric reference of the user.

3.2.1.2 helper data: Information that depends on biometric reference that enables the restoration of keys in a biometric cryptosystem. If a key is exposed, it can be cancelled and renewed.

NOTE – Synonyms are auxiliary data (AD) in [ISO 24745], help data and other information and data.

3.2.1.3 key control: A part of the key output process that is a method of enabling only a genuine user to create and restore the key.

NOTE 1 – Key generation: a type of key control that is a method of generating helper data by transforming concealment by using biometric reference and a cryptographic key. Only a genuine user can generate a valid key.

NOTE 2 – Key hiding, key release: a type of key control that is a method of generating helper data by encrypting the cryptographic key using a biometric reference. Only a genuine user can decrypt the key.

3.2.1.4 key output: A process to extract a cryptographic key from a biometric feature after fluctuations have been eliminated. The extraction of the key is classified into key generation and key hiding.

3.2.1.5 key regeneration: A function to regenerate a key by modifying helper data.

3.2.1.6 key restoring: A situation where a concealed key is restored from helper data by attackers or through unintended procedures.

3.2.1.7 secret sharing: A method of dividing a key into a number of segmentations and restoring it by assembling the segmentations.

3.2.1.8 verification function: A function to verify the validity of a cryptosystem mechanism by decrypting data created by the cryptosystem mechanism using a verification key.

3.2.1.9 verification key: A key used for verification. A public key in a PKI system is felled into a verification key.

3.2.2 Cancellable biometrics mechanisms

3.2.2.1 cancellable biometrics mechanism: Authentication mechanisms whose matching process utilizes transformed biometric data by using a secret parameter. Renewing the secret parameter can disable a cancellable template.

NOTE – There are similar terms such as "revocable" and "renewable"; however, these terms imply the meaning of a mechanism for protecting templates including biometric cryptosystems. Therefore, "cancellable", which does not imply the meaning of a mechanism for biometric cryptosystems will be used in this Recommendation.

3.2.2.2 cancellable template: Enrolled data in a server that are used for a cancellable biometrics mechanism.

3.2.2.3 cancellable transformation: A function to transform biometric data by using a secret parameter in a cancellable biometrics mechanism.

3.2.2.4 comparison function: A function to compare similarity between a registered cancellable template and transformed biometric data during a verification process.

3.2.2.5 comparison score: A similarity value by comparing a registered cancellable template and transformed biometric data through a comparison function.

3.2.2.6 secret parameter: A parameter to be used in a transformation function to conceal biometric data for a cancellable biometrics mechanism. This parameter should be kept secret from servers and third parties.

3.2.2.7 secret parameter generation function: A function to generate a secret parameter. A general cipher function such as a pseudo-random generator and a symmetry cipher function can be used for this function.

3.2.2.8 transformed biometric sample: Data that are generated by a transformation function using captured biometric data from a sensor in an authentication process.

3.2.3 Evaluation process

3.2.3.1 diversity: The variety of transformed biometric samples generated from a single biometric sample in the cancellable biometrics mechanism. Transformed biometric samples should not match other transformed biometric samples generated from the same biometric sample.

3.2.3.2 restoring rate: The proportion of samples of attacker attempts to be restored from concealed biometric data or a concealed key.

NOTE 1 – Key restoring rate includes both imposter trials and genuine trials.

NOTE 2 – The rate at which biometric data is restored from help information should be an evaluation target in a biometric cryptosystem mechanism. The rate at which biometric data is restored from a transformed biometric template or transformed biometric data should be an evaluation target in a cancellable biometrics mechanism.

3.2.4 General

3.2.4.1 authentication process: A process to check the validity of the claimed identity of an entity.

3.2.4.2 enrolment process: A process to create and store enrolment data for a template protection biometric mechanism.

3.2.5 Template protection techniques (commonly used)

3.2.5.1 concealment of biometric data function: A function to create helper data and a cancellable template to prevent an attacker from restoring biometric data using exposed helper data. Biometric data are transformed so that they can never be restored.

3.2.5.2 dummy information: Information that is in the same form as actual biometric data but is different from a genuine user's biometric data.

3.2.5.3 dummy information scheme: A technique to conceal the biometric data from third parties by adding a lot of dummy information.

NOTE – This is called "chaff" in a biometric encryption mechanism using a fuzzy vault scheme.

3.2.5.4 elimination of fluctuations: A technique to prevent the performance of verification from degrading due to fluctuations in the process of acquiring biometric data through biometric sensors.

3.2.5.5 error correcting code (ECC): Redundant data that are attached to biometric data to eliminate fluctuations. (In this case, the fluctuations are eliminated when the number of errors is within the permissible range.)

3.2.5.6 fluctuation: A variation in biometric samples of the same person that is determined by the capturing environment.

3.2.5.7 quantization function: A function to transform biometric data from continuous values to discrete values. The wider a quantization interval becomes in this process, the larger the quantization error will be.

3.2.5.8 secret partition: A method of storing registered information by dividing the information into several segments.

NOTE 1 – Enrolment data are helper data and act as verification keys for a biometric cryptosystem mechanism.

NOTE 2 – Enrolment data have a secret parameter and a cancellable template for a cancellable biometrics mechanism.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ECC	Error Correcting Code
FMR	False Match Rate
FNMR	False Non-Match Rate
PKI	Public Key Infrastructure

5 Conventions

This Recommendation does not require any specific conventions.

6 Overview of protection techniques for the biometric template on telecommunication systems

6.1 Biometric cryptosystem mechanism

The biometric cryptosystem uses encryption technology to dynamically generate unique encryption keys from the biometric data of each user. Similar to common encryption-based authentication techniques, a hash value of the key data is stored in the server and this hash value is used for comparison (as with password authentication), or a PKI authentication scheme can be utilized with the public key stored on the server and the generated key data can be used as a private key. In both cases, key data cannot be available on the server (i.e., biometric data are concealed), so these methods can be used as a secure method of protecting user privacy.

The basic architecture of authentication systems using the biometric cryptosystem is shown in Figure 1. The authentication mechanism in the client can be divided into two main functions: the first function generates a user's private key K_P created from the user's biometric reference, and the second function verifies the user based on cryptographic technology with the generated key.

In general, biometric data are not the same, due to various factors such as positioning, contamination (e.g., dirt and stains), ageing and environmental noise. However, it is necessary to generate a unique, stable key for each user from this non-uniform data in order to enable people to use authentication with encryption techniques. Helper data, W, that depend on biometric sample, B, are used in the process of generating the key to satisfy this requirement. The user's private key, K_P, is temporarily generated for authentication. The biometric cryptosystem mechanism is able to renew keys K_P and K_v, which correspond to key K_P by regenerating helper data W. Consequently, this mechanism will provide the specific security requirements of "renewability" in [ISO 24745].

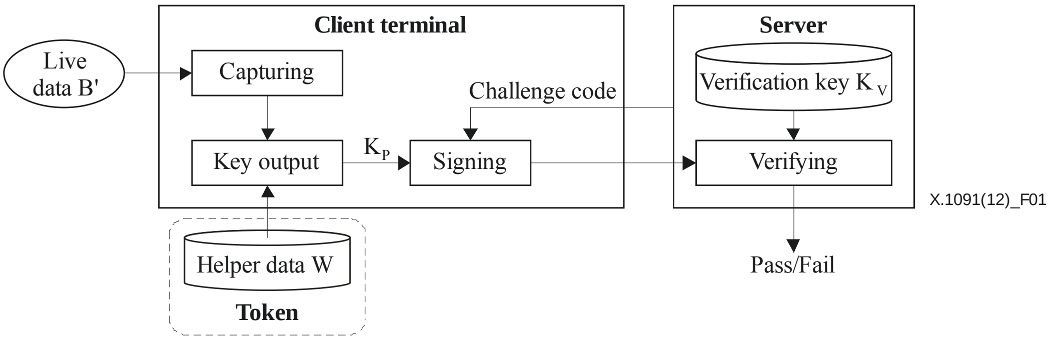


Figure 1 – Functional architecture of the biometric cryptosystem

6.2 Cancellable biometrics mechanism

Cancellable biometrics, proposed in [b-Ratha1], are a method of authentication to protect privacy in biometrics, where biometric data are transformed with a secret parameter before being registered on a server. Consequently, original biometric data are not revealed during the authentication of client/server biometric data.

The basic mechanism underlying a cancellable biometrics system is shown in Figure 2. $F_U(B')$ is obtained from biometric data B' and the transformation function F_U with parameter U which is stored in a client, or in a token. A user's biometric data B have been transformed by the same function F_U in advance in the enrolment process, and $F_U(B)$ also has been obtained. $F_U(B)$ is stored in the server database. The server calculates a score according to the similarity of B' to B by comparing $F_U(B)$ with $F_U(B')$. Where $F_U(B)$ or U is revealed, U can be replaced with U' by deleting $F_U(B)$ and re-registering $F_{U'}(B)$, and security can be retained without a user's biometric data.

However, cancellable biometrics are not effective against replay attacks if $F_U(B')$ is eavesdropped through a communication channel. A technology to protect the template that takes this into account is proposed in [b-Nagai] as an asymmetrical means of authenticating biometrics. This system uses a zero knowledge verification protocol to make it possible to authenticate a user without showing biometric data to the server.

The cancellable biometrics mechanism is able to renew parameter U and transform template $F_U(B)$ without a re-enrolment process. Therefore, this mechanism can provide the specific security requirements of "renewability" in [ISO 24745].

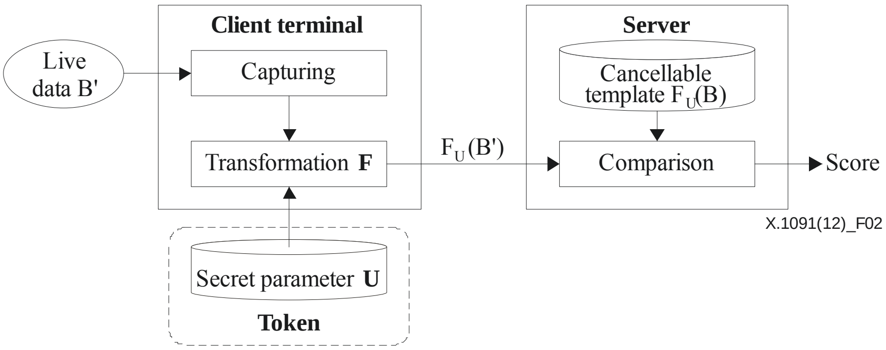


Figure 2 – Functional architecture for cancellable biometrics

7 Reference models of protection techniques for a biometric template

7.1 Reference model of a biometric cryptosystem mechanism

In this Recommendation, biometric template protection techniques are divided into two major types of telebiometric authentication systems. However, each type has some different algorithms. Hence, this Recommendation defines a reference model for each protection technique type. These reference models make it easy for an evaluator to assign functions of an intended mechanism to functional components in the model.

The following clauses describe each reference model, technical components of each protection technique type and specific threats that may arise. Figure 3 shows two fundamental reference models for the biometric cryptosystem mechanism.

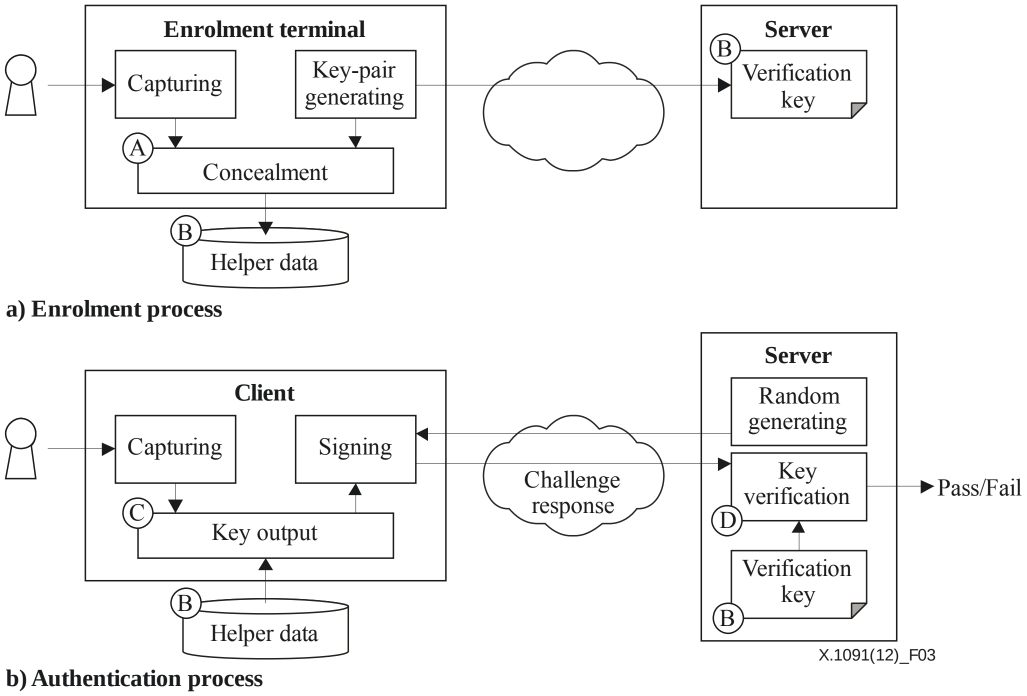


Figure 3 – Reference models for the biometric cryptosystem mechanism

The following list categorizes technical components on the biometric cryptosystem mechanism. Technical components are categorized with respect to functional components in Figure 3 (A) to (D). Technical components can be used for picking up evaluation items and interdependency items in clause 8. Depending on the target of evaluation, one or more technical components are selected for each functional component.

Technical components on the enrolment process

A) Concealment function

1) Secret sharing scheme: A scheme to conceal biometric data by dividing biometric data into a number of segmentations and restoring them by assembling the segmentations.

2) Dummy information scheme: A scheme to conceal the biometric data from third parties by adding a lot of dummy information.

3) One-way function scheme: A scheme to conceal the biometric data x using (mathematical) function f (it is computationally difficult to find a biometric data x in the domain such that $f(x) = y$).

B) Data management function

1) Secret partition scheme: A scheme that will make it difficult to restore biometric data by secure partitioning helper data.

Technical components on authentication process

C) Key output function

a) Elimination of fluctuations

1) Quantization scheme: A scheme to transform biometric data from continuous values to discrete values. The wider a quantization interval becomes in this process, the larger the quantization error will be.

2) Error correcting code scheme: A scheme to attach redundant data to biometric data to eliminate fluctuations. (In this case, the fluctuations are eliminated when the number of errors is within the permissible range.)

b) Key control

1) Key generation scheme: A scheme to generate a valid key using a biometric reference.

2) Key hiding scheme: A scheme to decrypt a key from helper data using a biometric reference.

D) Key verification function

A function to verify whether there is a genuine person on the server side by checking the encryption key generated in the client using a verification key.

7.2 Reference model for a cancellable biometrics mechanism

Figure 4 shows a representative reference model for the cancellable biometrics mechanism.

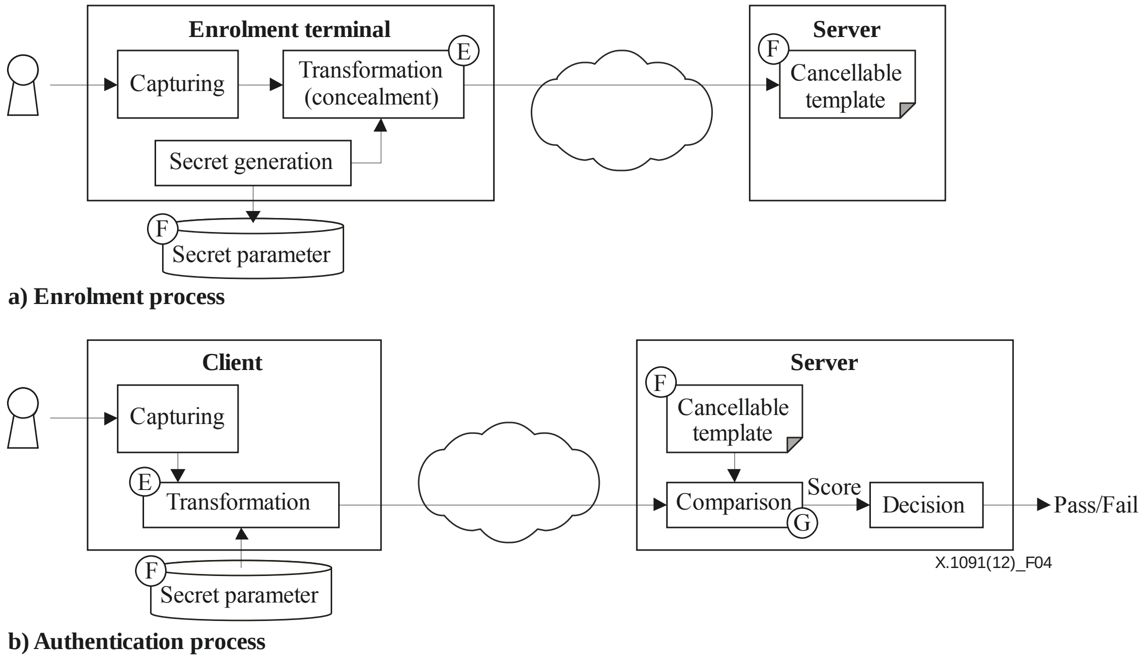


Figure 4 – Reference model for the cancellable biometrics mechanism

The following list categorizes technical components on the cancellable biometrics mechanism. Technical components are categorized with respect to functional components in Figure 4 (E) to (G). Technical components can be used for picking up evaluation items and interdependency items in clause 8. Depending on the target of evaluation, one or more technical components are selected for each functional component.

Technical components on enrolment process

E) Transformation (concealment) function

1) Geometrical deformation scheme: A scheme to conceal biometric data by changing the original shape of biometric data with user specific parameters. It is difficult to find a biometric datum without knowing user specific parameters.

2) One-way function scheme: A scheme to conceal the biometric data *x* using (mathematical) function *f* (it is computationally difficult to find a biometric data *x* in the domain such that *f(x) = y*).

3) Dummy information scheme: A scheme to conceal the biometric data from third parties by adding a lot of dummy information.

F) Data management function

1) Secret partition: A scheme that will make it difficult to restore biometric data by secure partitioning helper data.

Technical components on authentication process

G) Server process

a) Elimination of fluctuations

   1) Quantization scheme: A scheme to transform biometric data from continuous values to discrete values. The wider a quantization interval becomes in this process, the larger the quantization error will be.

   2) Error correcting code scheme: A scheme to attach redundant data to biometric data to eliminate fluctuations. (In this case, the fluctuations are eliminated when the number of errors is within the permissible range.)

b) Comparison

   1) Score calculation scheme: A function to verify whether there is a genuine person on the server side by checking biometric data and the cancellable template, which are both cancellable and transformed through the authentication process.

7.3 Specific threats for reference models

This Recommendation describes the evaluation items of all reference models using template protection techniques. Specific threats are able to indicate the need for evaluating the protection performance.

Specific threats are able to clarify the requirements for protecting the templates of target systems and are also able to clarify the reasons for which evaluation items are employed and their priorities.

This Recommendation excludes threats to a general biometric system that are already described in [ITU-T X.1086]. It should be noted that biometric systems using template protection techniques have threats and vulnerabilities. Consequently, in addition to this Recommendation, other Recommendations and standards such as [ISO 19792], [ISO 19795-1] and [ISO 19795-2] should be referred to for evaluation.

7.3.1 Specific threats for the biometric cryptosystem mechanism

The points at which the biometric cryptosystem mechanism is threatened are presented in Figure 5.

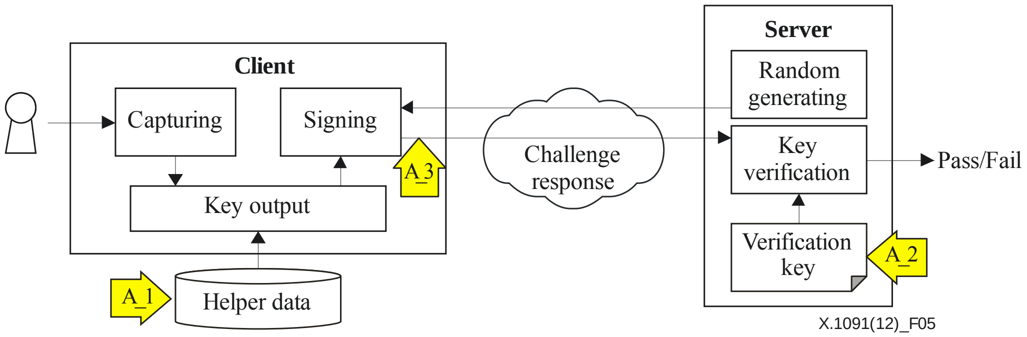


Figure 5 – Points at which the biometric cryptosystem mechanism is threatened

Threat point A_1

- Biometric data are analysed or disclosed by an attacker who has obtained leaked helper data.
- Disclosed biometric data are used for physical/electronic impersonation.
- A signing key is analysed or disclosed by an attacker who has obtained leaked helper data.
- A disclosed signing key is used for electronic impersonation.

Threat point A_2

- A signing key is analysed or disclosed by an attacker who has obtained a leaked verification key.
- A disclosed verification key is used for electronic impersonation.

Threat point A_3

- A signing key is disclosed by an attacker who has eavesdropped a challenge code (random code) and a response code (signature).
- A disclosed signing key is used for electronic impersonation.

7.3.2 Specific threats for the cancellable biometrics mechanism

The points at which the cancellable biometrics mechanism is threatened are outlined in Figure 6.

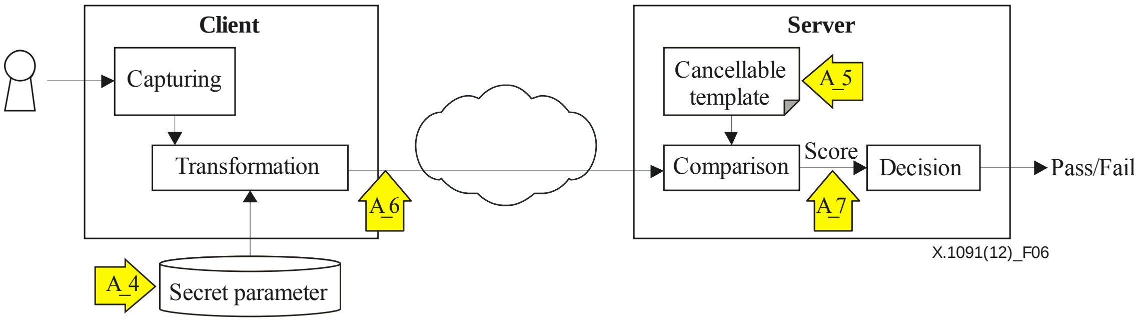


Figure 6 – Points at which the cancellable biometrics mechanism is threatened

Threat point A_4

- An impersonation by an attacker who has obtained a leaked secret parameter.

Threat point A_5

- Biometric data are analysed or disclosed by an attacker who has obtained a leaked cancellable template.
- Disclosed biometric data are used for physical/electronic impersonation.
- A secret parameter is analysed or disclosed by an attacker who has obtained a leaked cancellable template.
- A disclosed secret parameter is used for physical/electronic impersonation.

Threat point A_6

- Biometric data are analysed or disclosed by an attacker who has eavesdropped transformed biometric data.
- Disclosed biometric data are used for physical/electronic impersonation.

Threat point A_7

- Transformed biometric data are analysed or disclosed by an attacker who has obtained a comparison score.

8 Evaluation items for biometric template protection techniques

8.1 Introduction

This Recommendation defines essential components of each protection technique type as described in clause 7. This Recommendation also defines evaluation items for each essential component. The evaluator is then able to point out evaluation items of protection performance for various algorithms when these are applied to a remote authentication system. This clause describes evaluation items for each essential component of the reference models.

The security level of techniques to protect biometric templates depends on the accuracy of biometric authentication, and [ISO 19792] provides steps for "testing security-relevant error rates". The main targeted evaluation items of this Recommendation are the relationship between protection capabilities and error rates. Therefore, clause 8.2 provides more detailed steps to evaluate techniques of protecting biometric templates based on [ISO 19792]. Clauses 8.3 to 8.5 provide evaluation items to be used at step 3 of the evaluation flow diagram described in [ISO 19792].

8.2 Evaluation items for the biometric cryptosystem mechanism

Table 1 lists the evaluation items for each essential component of the biometric cryptosystem mechanism.

Table 1 – Evaluation items for essential components of the biometric cryptosystem mechanism

				Fuzzy vault scheme **[b-Juels2], [b-Clancy], [b-Uludag1], [b-Uludag2], [b-Ohki], [b-Hidano]**	**Bio-hashing** **[b-Monrose], [b-Draper}, [b-Shibata]**	**Fuzzy commitment** **[b-Juels1]**
Client process	A. Concealment			Secret sharing, dummy information	Dummy information	One-way function
	B. Data management		Secret partition	✓		
	C. Key output	a. Elimination of fluctuations	1. Quantization		✓	✓
			2. Error correcting code	✓	✓	✓
		b. Key control	1. Key generation			✓
			2. Key hiding	✓	✓	
Server process	D. Key verification			✓	✓	

(A) Concealment

The following list summarizes the evaluating items for the threat where biometric data or signing keys are analysed or disclosed by an attacker who has obtained leaked helper data. These items correspond to threat point A_1.

- Secret sharing scheme

  The secret sharing scheme should be evaluated in view of the following item:

  – difficulty of restoring the key from secret shared information below the threshold value.

- Dummy information scheme

  The dummy information scheme should be evaluated in view of the following items:

  – difficulty of restoring biometric data from a single piece of information;

  – difficulty of restoring biometric data from a single piece of information after concealment;

  – difficulty of restoring biometric data using the correlativity from multiple pieces of information after concealment.

- One-way function

  The one-way function should be evaluated in view of the following items:

  – difficulty of restoring biometric data from a single piece of information after concealment;

  – difficulty of restoring biometric data using the correlativity from multiple pieces of information after concealment;

  – reduced security due to collision of information after concealment.

(B) Data management – Secret partition

The following list shows an evaluation item for the threat where biometric data or the signing key are analysed or disclosed by an attacker who has obtained part(s) of leaked helper data. This item corresponds to threat point A_1. The pieces of information should be evaluated in view of the following item:

- difficulty of restoring biometric data when parts of partitioned information are leaked.

(C) Key output

Evaluation items are listed in the following for threats where biometric data or signing keys are analysed or disclosed by an attacker who has obtained part(s) of leaked helper data. These items correspond to threat point A_1.

The list also has evaluation items for threats where the signing key is analysed or disclosed by an attacker who has obtained a generated key. These items correspond to threats at points A_2 and A_3.

(C-a-1) Key output – Elimination of fluctuations – Quantization

The quantization function should be evaluated in view of the following items:

– entropy loss of biometric data due to quantization;

– accuracy to restore secret key for a genuine user and difficulty to restore secret key for an imposter.

(C-a-2) Key output – Elimination of fluctuations – Error correcting code

The error correcting code function should be evaluated in view of the following items:

– entropy loss of biometric data due to error correcting code;

– accuracy to restore secret key for a genuine user and difficulty to restore secret key for an imposter.

(C-b-1) Key output – Key control – Key generation

The key generation function should be evaluated in view of the following items:

– difficulty of restoring key using helper data;

– key length;

NOTE – Relationship between key length and encryption strength follows existing encryption protocol;

– difficulty of restoring biometric data using the correlativity between the generated key and biometric data;

– difficulty of restoring biometric data during key regeneration;

– accuracy to restore secret key for a genuine user and difficulty to restore secret key for an imposter.

(C-b-2) Key Output – Key control – Key hiding

The key hiding function should be evaluated in view of the following items:

– difficulty of restoring key using helper data;

– key length;

NOTE – Relationship between key length and encryption strength follows existing encryption protocol.

– entropy loss in key information due to distortion of key space;

– accuracy to restore secret key for a genuine user and difficulty to restore secret key for an imposter.

(D) Key verification

The key verification function should be evaluated in view of the following items:

– possibility of verifying key without exposing its information or biometric data to the network, by following existing security evaluation criteria for encryption protocol;

– security to verify key depends on method used in biometric cryptosystem. Consequently, evaluation items (A)-(C) should be assessed.

8.3 Interdependent evaluation items for the biometric cryptosystem mechanism

This Recommendation describes the requirements for the evaluation items described above. With reference to the evaluation items in Table 1, this Recommendation indicates which items should be treated as interdependent evaluation items. Table 2 lists relationships of interdependency between each essential evaluation item for the biometric cryptosystem mechanism.

Table 2 – Relationship of interdependent evaluation items for the biometric cryptosystem mechanism

Evaluation item		Parameter	Direction of variation	Key restoring rate		Protection performance (easiness to attack)	
				Genuine	Imposter	Biometric information	Key
Elimination of fluctuations	Quantization	Width	More	Up	Up	Difficult	N/E
			Less	Down	Down	Easy	N/E
	Error correcting	Capability of error correcting	More	Up	Up	Easy	N/E
			Less	Down	Down	Difficult	N/E
Key output	Secret sharing	Number of characteristics (without dummy)	More	Down	Down	Difficult	Difficult
			Less	Up	Up	Easy	Easy
	Dummy information	Amount of dummy information	More	Down	Down	Difficult	Difficult
			Less	Up	Up	Easy	Easy
N/E: No effect							

(A) Concealment

- (C-a-1) Key output – Elimination of fluctuations – Quantization

  Interdependency between the concealment function and the quantization function should be evaluated. Biometric data are quantized to make it difficult to restore biometric data from part(s) of shared secret information or from secret partitioned information. Here, it should be ensured that the entropy loss of biometric data is small. If the width of quantization interval is enlarged, biometric data will be better protected. However, since entropy will be lower, the key restoration rate of genuine data will improve, but it will be easier for an imposter to restore the key.

- (C-a-2) Key output – Elimination of fluctuations – Error correcting code

  Interdependency between the concealment function and the error correcting code function should be evaluated. An error correcting code is applied to make it difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information. Here, it should be ensured that the entropy loss of biometric data from using the error correcting code is small.

- (C-b-1) Key output – Key control – Key generation

  The following interdependencies between the concealment function and the key generation function should be evaluated.

- Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, it should be ensured that the generated key is sufficiently long.
- Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-generation-based methods should ensure that it is difficult to restore the key using helper data.
- Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, it should be ensured that it is difficult to restore biometric data using the correlativity between the generated key and biometric data.
- Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-generation-based methods should ensure that it is difficult to restore biometric data using the regenerated key.

• (C-b-2) Key output – Key control – Key hiding

The following interdependencies between the concealment function and the key hiding function should be evaluated.

- Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-hiding-based methods should ensure that it is difficult to regenerate a key from helper data.
- Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-hiding-based methods should ensure that the length of the generated key is sufficiently long.
- Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-hiding-based methods should ensure that entropy loss of biometric data caused by the distortion of key space is small.

(B) Data management – Secret partition

• (C-a-1) Key output – Elimination of fluctuations – Quantization

Interdependency between the secret partition function and the quantization function should be evaluated. Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-hiding-based methods should ensure that entropy loss of quantized biometric data is small.

• (C-a-2) Key output – Elimination of fluctuations – Error correcting code

Interdependency between the secret partition function and the error correcting code should be evaluated. Even though it difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, it should be ensured that the entropy loss of biometric data from using the error correction code is small.

• (C-b-1) Key output – Key control– Key generation

The following interdependencies between the secret partition function and the key generation function should be evaluated.

- Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-generation-based methods should ensure that the key is sufficiently long.
- Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-generation-based methods should ensure that it is difficult to regenerate the key from helper data.
- Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, it should be ensured that biometric

data are difficult to restore using the correlativity between the generated key and biometric data.

– Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-generation-based methods should ensure that it is difficult to restore biometric data during key regeneration.

- (C-b-2) Key output – Key control – Key hiding

  The following interdependencies between the secret partition function and the key hiding function should be evaluated.

  – Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-hiding-based methods should ensure that it is difficult to restore the key using helper data.

  – Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-hiding-based methods should ensure that the generated key is sufficiently long.

  – Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-hiding-based methods should ensure that the entropy loss of biometric data caused by the distortion of key space is small.

8.4 Evaluation items for the cancellable biometrics mechanism

Table 3 lists the evaluation items for all essential components of cancellable biometrics.

Table 3 – Evaluation items for all essential components of the cancellable biometrics mechanism

			Geometrical deformation, functional transformation **[b-Ratha1], [b-Ratha2], [b-Maiorana]**	**Random filtering** **[b-Savvides1], [b-Savvides2] [b-Hirata]**	**Logical addition** **[b-Braithwaite]**
Client process	E. Concealment		Geometrical deformation or functional transformation	One-way function, dummy information	One-way function
	F. Data management	Secret partition	✓	✓	✓
G. Server process	a. Elimination of fluctuations	1. Quantization			✓
		2. Error correcting code			
	b. Comparison	Score	✓	✓	✓

(E) Concealment

The following list contains evaluation items for threats where biometric data or secret parameters are analysed or disclosed by an attacker who has obtained a leaked cancellable template. These items correspond to threat point A_5.

Also listed are evaluation items for threats where biometric data or secret parameters are analysed or disclosed by an attacker who has obtained a leaked transformed biometric sample. These items correspond to threat point A_6.

- Geometric transformation

  The geometric transformation function should be evaluated in view of the following items:

  – difficulty of restoring biometric data from a single piece of information after transformation;

  – difficulty of restoring biometric data using the correlativity from information after multiple transformations;

  – FMR for verifying an imposter by using arbitrary transformation parameter and FNMR for verifying genuine data using the correct transformation parameter;

  – diversity of transformed biometric samples is not considerably reduced due to restriction of geometric deformation;

  – security is reduced due to the number of update processes [ITU-T X.1090] in transformed biometric samples.

- The one-way function

  The one-way function should be evaluated in view of the following items:

  – difficulty of restoring biometric data from a single piece of information after transformation;

  – difficulty of restoring biometric data using the correlativity from multiple pieces of information after transformation;

  – diversity of transformed biometric samples is not considerably reduced due to collision of samples after transformation;

  – FMR for verifying an imposter by using an arbitrary transformation parameter and FNMR for verifying genuine data using the correct transformation parameter;

  – security is reduced due to the number of update processes [ITU-T X.1090] in transformed biometric samples.

- Dummy information

  The dummy information scheme should be evaluated in view of the following items:

  – difficulty of distinguishing between true and dummy information from a single piece of information after transformation;

  – difficulty of restoring biometric data using the correlativity from multiple pieces of information after transformation;

  – diversity of transformed biometric samples is not considerably reduced due to the variety of dummy information;

  – FMR for verifying an imposter by using arbitrary transformation parameter and FNMR for verifying genuine data using the correct transformation parameter;

  – security is reduced due to the number of update processes [ITU-T X.1090] in transformed biometric samples.

(F) Data management – Secret partition

The list that follows contains evaluation items for threats where biometric data or secret parameters are analysed or disclosed by an attacker who has obtained a leaked cancellable template. This item corresponds to threat point A_5. The partitioned information should be evaluated in view of the following item:

- difficulty of restoring biometric data when some partitioned information is leaked.

(G) Server process

Evaluation items for threats of impersonation by an attacker who has obtained a leaked secret parameter, corresponding to threat point A_4, are listed as follows:

(G-a-1) Server process – Elimination of fluctuations – Quantization

The quantization function should be evaluated in view of the following items:

- little entropy loss of biometric data due to quantization;
- FMR for verifying an imposter by using the arbitrary transformation parameter, and FNMR for verifying genuine data using the correct transformation parameter.

(G-a-2) Server process – Elimination of fluctuations – Error correcting code

The error correcting code function should be evaluated in view of the following items:

- little entropy loss of biometric data due to the capability of the error correcting code;
- FMR for verifying an imposter by using the arbitrary transformation parameter and FNMR for verifying genuine data using the correct transformation parameter.

(G-b) Server process – Comparison – Score

The following lists an evaluation item for a threat where transformed biometric data are analysed or disclosed by an attacker who obtained a comparison score. This item corresponds to threat point A_7. The server comparison process should be evaluated in view of the following item:

- difficulty of attack using a comparison score.

8.5 Interdependent evaluation items for the cancellable biometrics mechanism

This Recommendation describes the requirements for the evaluation items of cancellable biometrics and indicates which items should be treated as interdependent evaluation items. Table 4 lists relationships of interdependency between each essential evaluation item for the cancellable biometrics mechanism.

Table 4 – Relationship between interdependent evaluation items for the cancellable biometrics mechanism

Evaluation item		Parameter	Direction of variation	Error rate		Protection performance (easiness to attack)	
				FNMR	FMR	Biometric information	Secret parameter
Elimination of fluctuations	Quantization	Quantization interval	More	Down	Up	Difficult	N/E
			Less	Up	Down	Easy	N/E
	Error correcting	Capability of error correcting	More	Down	Up	Easy	N/E
			Less	Up	Down	Difficult	N/E
Concealment of biometric data	Transformation	Degree of geometric transformation	More	Up	Down	Difficult	Difficult
			Less	Down	Up	Easy	Easy
		Space of cancellable template	More	Up	Down	Difficult	Difficult
			Less	Down	Up	Easy	Easy
	Dummy information	Amount of dummy information	More	Up	Down	Difficult	Difficult
			Less	Down	Up	Easy	Easy
N/E: No effect							

(E) Concealment

- (G-a-1) Server process – Elimination of fluctuations – Quantization

  Interdependency between the concealment function and the quantization function should be evaluated. Biometric data are quantized to make it difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information. Here, it should be ensured that the entropy loss of biometric data is small.

- (G-a-2) Server process – Elimination of fluctuations – Error correcting code

  Interdependency between the concealment function and the error correcting code function should be evaluated. An error correcting code is applied to make it difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information. Here, it should be ensured that the entropy loss of biometric data from using the error correcting code is small.

- (G-b) Server process – Comparison – Score

  The following interdependencies between the concealment function and the score function should be evaluated.

  – While making it difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information that is above the threshold value, ensure that it is difficult to attack using the score.

  – Even though it is difficult to restore biometric data by using the score, it should be ensured that the diversity of the transformed biometric sample is high.

  – Even though it is difficult to restore biometric data using the score, it should be ensured that security due to the number of update processes [ITU-T X.1090] of transformed biometric samples is enhanced.

(F) Data management – Secret partition

- (G-a-1) Server process – Elimination of fluctuations – Quantization

  Interdependency between the secret partition function and the quantization function should be evaluated. Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, methods of quantizing biometric data should ensure that the entropy loss of quantized biometric data is small.

- (G-a-2) Server process – Elimination of fluctuations – Error correcting code

  Interdependency between the secret partition function and the error correcting code function should be evaluated. An error correcting code is applied to make it difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information. Here, it should be ensured that the entropy loss of biometric data from using the error correcting code is small.

- (G-b) Server process – Comparison – Score

  Interdependency between the secret partition function and the score function should be evaluated. Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, it should be ensured that it is difficult to restore biometric data using the score.

(G-a-1) Server process – Elimination of fluctuations – Quantization

- (G-b) Server process – Comparison – Score

  Interdependency between the quantization function and the score function should be evaluated. Even though the entropy loss of quantized biometric data is small, it should be ensured that it is difficult to restore biometric data using the score.

(G-a-2) Server process – Elimination of fluctuations – Error correcting code

- (G-b) Server process – Comparison – Score

  Interdependency between the error correcting code function and the score function should be evaluated. Even though the entropy loss of biometric data using error correcting is small, it should be ensured that it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information.

9 Evaluation steps of protection techniques for the biometric template

9.1 General

The evaluation steps are given in Figure 7 and refer to [ISO 19792].

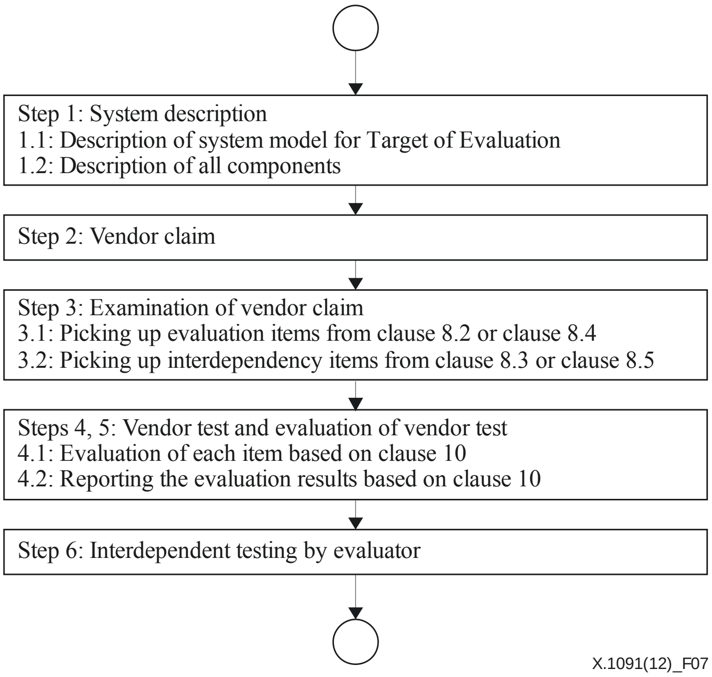

Step 1: System description
1.1: Description of system model for Target of Evaluation
1.2: Description of all components
Step 2: Vendor claim
Step 3: Examination of vendor claim
3.1: Picking up evaluation items from clause 8.2 or clause 8.4
3.2: Picking up interdependency items from clause 8.3 or clause 8.5
Steps 4, 5: Vendor test and evaluation of vendor test
4.1: Evaluation of each item based on clause 10
4.2: Reporting the evaluation results based on clause 10
Step 6: Interdependent testing by evaluator
X.1091(12)_F07

Figure 7 – Flow of evaluation steps for biometric protection techniques based on [ISO 19792]

Step 1: System description

1.1: Description of system model for the target of evaluation

A vendor who offers evaluations should describe the reference model for evaluation and evaluation targets based on the selected reference model.

1.2: Description of all components

The vendor should describe functional components of a selected reference model.

Step 2: Vendor claim

The vendor provides performance claims in the form of set(s) of maximum values of security-relevant error rates that can be simultaneously achieved. For each claimed value of security relevant error rates, the vendor provides the threshold(s) that the claim is based on.

Step 3: Examination of vendor claims

The vendor should list the evaluation items for the selected reference model in clause 8.2 or clause 8.4. The vendor should also list interdependent evaluation items with the functional components of the selected reference model in clause 8.3 or clause 8.5.

Where the protection of performance claimed by a vendor is included in the list, go to the next step.

Steps 4 and 5: Vendor test and evaluation of vendor test

The vendor should design parameters to be determined, such as the number of samples, evaluate them and write test reports based on clause 10. The evaluator should assess the justification for the report in terms of the test scenario and statistical approach.

Step 6: Independent testing by other evaluators

In a case where objectivity is strongly needed in the evaluation, outside evaluator(s) should validate the evidence or independently test it.

10 Requirements and procedures of protection performance testing

10.1 General

This clause describes requirements and procedures on testing and reporting for each evaluation item in clause 8. These requirements and procedures can provide the evaluator with benchmarks for validity and repeatability of the testing report.

10.2 Biometric cryptosystem

10.2.1 Requirements and procedures for individual evaluation items

(1) Difficulty of restoring key information

Requirements:

- The information-theoretic security or computational security of the key for the adopted mechanism should be proven, and the proof should be documented.
- Any elements that would facilitate key restoring should be clarified.

Procedures:

1. Prove the information-theoretic security or computational security for the adopted mechanism. At this time, the preconditions of this proof should be given. These become the preconditions for achieving security in the use of a template protection technique. Additionally, the number of attacks that an attacker would have to make for key restoring by brute-force attack should be given.
2. List the elements, if any, that would facilitate key restoring, and for each element. For key restoring in which the attacker takes such elements into account, the least number of attacks required for key restoring should be given.
3. Document the results of proving security. Specify the following items in the documentation:
   – preconditions for proving security;
   – procedure for proving security;
   – number of attacks that an attacker would have to make for key restoring by brute-force attack;
   – elements that facilitate key restoring and the least number of attacks required for key restoring when taking each of those elements into account;
   – preconditions that become constraints in actual use.

(2) Difficulty of restoring biometric data

Requirements:

- The information-theoretic security or computational security of the biometric sample for the adopted mechanism should be proven, and the proof should be documented.
- Any elements that would facilitate biometric-sample restoring should be clarified.
- For a biometric sample protection mechanism that adds dummy information, the amount of dummy information should be defined.
- For a biometric sample protection mechanism that adds dummy information, any elements that would facilitate differentiation between dummy information and the genuine user's biometric data should be clarified.

Procedures:

1. Prove the information-theoretic security or computational security for the adopted mechanism. Any preconditions that become constraints in actual use should be indicated. Additionally, the number of attacks that an attacker would have to make for biometric sample restoring by brute-force attack should be given.
2. List the elements, if any, that would facilitate biometric-sample restoring. For biometric sample restoring, in which the attacker takes such elements into account, the least number of attacks required for biometric-sample restoring should be given.
3. For a biometric sample protection mechanism that adds dummy information, decide on the amount of dummy information to be provided.
4. For a biometric sample protection mechanism that adds dummy information, list the elements, if any, which would facilitate differentiation between dummy information and the genuine user's biometric data. Then, for each element, compute the least number of attacks that an attacker would have to perform for biometric-sample restoring that takes that element into account.
5. Document the results of proving security. Specify the following items in the documentation:
   – preconditions for proving security;
   – procedure for proving security;
   – number of attacks that an attacker would have to make for biometric-sample restoring by brute-force attack;
   – elements that facilitate biometric-sample restoring and the least number of attacks required for biometric-sample restoring when taking each of those elements into account;
   – preconditions that become constraints in actual use.

NOTE – In a biometric cryptosystem mechanism, the key and the genuine user's biometric sample have a dependency relation: clarifying one makes it easy to clarify the other. Consequently, the security of (1) key information or (2) the biometric sample is determined by the weaker of the two.

(3) Authentication accuracy

Requirements:

- Based on the results of (1) and (2), a parameter (key information, dummy information, etc.) of the template protection technique should be fixed to a value that can achieve the desired security level, and biometric samples conforming to [ISO 19795-1] should be gathered and evaluated.

Procedures:

1. Based on the results of (1) and (2), fix a parameter (key information, dummy information, etc.) of the template protection technique to a value (key length, amount of dummy information, etc.) that can achieve the desired security level.
2. Gather biometric samples according to [ISO 19795-1].
3. Assuming identical keys, create helper data based on gathered biometric samples for enrolment, and compute the key restoring rate for both the genuine user and imposter using matching samples for evaluation purposes.
4. Document evaluation results. Specify the following items in the documentation:
   - evaluation procedure conforming to [ISO 19795-2];
   - number of gathered samples;
   - template protection parameter (key length, number of items of dummy information, etc.) used in the evaluation and its value.

(4) Diversity

Requirements:

- In a mechanism that protects a biometric sample or key information using dummy information and that uses a single biometric sample and single key, the maximum number of items of helper data that can be created by modifying dummy information should be given.

Procedures:

1. In a mechanism that provides protection by adding dummy information, select a single biometric sample and a single key.
2. Determine the maximum number of mutually different items of helper data that can be created by modifying dummy information.
3. Perform procedures 1 and 2 using multiple biometric samples and calculate the average number of items of helper data.
4. Document evaluation results. Specify the following items in the documentation:
   - template protection parameters (key length, etc.) excluding number of items of dummy information;
   - number of times procedures 1 and 2 were performed and the average number of items of helper data obtained.

10.2.2 Evaluation of interdependent items for the biometric cryptosystem mechanism

Template protection performance should be evaluated in conformance with the method in [ISO 19795-3] for evaluating accuracy with respect to environmental fluctuation. Specifically, the effect on the accuracy of varying an environmental parameter, as one type of environmental fluctuation, should be evaluated.

That is, one of the template protection performance parameters should be fixed and the other should be varied to evaluate robustness with respect to the varied factor as in [ISO 19795-3].

On documenting evaluation results, the following items should be specified:

- fixed factor and varied factor;
- security of biometric sample for each value of the varied factor;
- security of the key for each value of the varied factor;
- diversity for each value of the varied factor;

– authentication accuracy (false match rate, false non-match rate) for each value of the varied factor.

10.3 Cancellable biometrics

10.3.1 Requirements and procedures for individual evaluation items

(1) Difficulty of restoring biometric data

Requirements:

- The information-theoretic security or computational security for the adopted mechanism should be proven, and the proof should be documented.
- Any elements that would facilitate restoring of biometric samples should be clarified.

Procedures:

1. Prove the information-theoretic security or computational security for the adopted mechanism. At this time, the preconditions of this proof should be given. These become the preconditions for achieving security in the use of a template protection technique. Additionally, the number of attacks that an attacker would have to make to restore a biometric sample by brute-force should be given.
2. List the elements, if any, which would facilitate restoring biometric samples. For biometric sample restoring in which the attacker takes such elements into account, the least number of attacks required to restore a biometric sample should be given.
3. Document the results of proving security. Specify the following items in the documentation:
   - preconditions for proving security;
   - procedure for proving security;
   - number of attacks that an attacker would have to make to restore a biometric sample by brute-force attack;
   - elements that facilitate biometric-sample restoring and the least number of attacks required for key restoring when taking each of those elements into account;
   - preconditions that become constraints in actual use.

(2) Authentication accuracy

Requirements:

- A parameter of the template protection technique should be fixed to a value that can achieve the level of desired security, and biometric samples conforming to [ISO 19795-1] should be gathered and evaluated.

Procedures:

1. Based on the evaluation of (1), fix the secret parameter of the template protection technique to a complex value (in terms of length and randomness) that can achieve the level of desired security.
2. Gather biometric samples according to [ISO 19795-2].
3. Transform the gathered biometric samples using the same secret parameter, and evaluate FMR and FNMR using the transformed biometric samples.
4. Document evaluation results according to [ISO 19795-2], specifying the following items:
   - evaluation procedure conforming to [ISO 19795-2];
   - number of gathered samples;
   - value of the fixed secret parameter used in the evaluation.

(3) Diversity

Requirements:

- The number of transformed biometric samples that can be created from a single biometric sample should be given.
- All transformed biometric samples that can be created from a single biometric sample should be created, and the false non-match rate (FNMR) among those samples should be given. This evaluation should be performed for multiple biometric samples and the average FNMR given.

Procedures:

1. Compute the number of transformed biometric samples that can be created from a single biometric sample (within the range of values that can be taken on by the secret parameter).
2. Create mutually different transformed biometric samples in only the quantity computed in step 1 by transforming a single biometric sample in the range of values that can be taken on by the secret parameter.
3. Compare the transformed biometric samples and measure the FNMR according to the appropriate genuine user rejection rate threshold clarified in (2) above.
4. Perform procedures 2 and 3 using multiple biometric samples and calculate the average FNMR.
5. Document evaluation results. Specify the following items in the documentation:
   - number of biometric samples;
   - number of transformed templates that can be created from a single biometric sample;
   - base threshold for assessing a match in procedure 3;
   - number of times procedures 2 and 3 were performed, and the average FNMR calculated.

(4) Number of update processes

Requirements:

- For an algorithm that enables a transformed biometric sample to be updated, evaluate the relationship between the number of update processes and authentication accuracy (FMR and FNMR), referring to [ISO 19795-3].

Procedures:

1. Based on the evaluation of (1), fix the secret parameter of the template protection technique to a complex value (in terms of length and randomness) that can achieve the level of desired security.
2. Gather biometric samples according to [ISO 19795-2].
3. Transform the gathered biometric samples using the same secret parameter, update each biometric sample using the same update parameter and evaluate the authentication accuracy (FMR and FNMR) for each update step as the number of template updates.
4. Denote the relationship between the number of updates and authentication accuracy (FMR and FNMR) in graph and table form.
5. Document evaluation results. Specify the following items in the documentation:
   - number of biometric samples;
   - value of the secret parameter applied to each sample;
   - relationship between the number of updates and authentication accuracy (FMR and FNMR).

10.3.2 Evaluation of interdependent items for the cancellable biometric mechanism

Evaluation of template protection performance should conform to the method in [ISO 19795-3] for evaluating accuracy with respect to environmental fluctuation. Specifically, the effect on the accuracy of varying an environmental parameter as one type of environmental fluctuation should be evaluated.

That is, one of the template protection performance parameters should be fixed, and the other should be varied, to evaluate robustness with respect to the varied factor as in [ISO 19795-3].

On documenting evaluation results, the following items should be specified:

- fixed factor and varied factor;
- security of biometric sample for each value of the varied factor;
- diversity for each value of the varied factor
- authentication accuracy (false match rate, false non-match rate) for each value of the varied factor.

Appendix I

Algorithm list of template protection techniques

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

This appendix provides algorithm lists of template protection techniques to enable them to be evaluated with this Recommendation. The algorithm list for the biometric cryptosystem is presented in Table I.1, and the algorithm list for the cancellable biometrics system is presented in Table I.2.

Tables 2 and 4 in clause 8 classified major techniques of template protection; they gave an approximate but sufficient number of frames for main-body classifications. However, they did not clarify all details. This appendix provides a new table with all the details of the techniques, which take into consideration future expansion, general evaluation and ease of use. Therefore, the tables are designed to match component functions to each technique.

Table I.1 – Algorithm list of the biometric cryptosystem mechanism

Algorithm	Place of function or process						
	Client						Server
	A. Concealment	B. Data manage-ment	C. Key output				D. Key verification
			a. Elimination of fluctuations		b. Key control		
		Secret partition	1. Quantization	2. Error correcting	1. Key generation	2. Key hiding	
[Fuzzy vault scheme]							
[b-Juels2]	Secret sharing, dummy information	✓		✓	✓		✓
[b-Clancy]							
[b-Uludag1]							
[b-Uludag2]							
[b-Ohki]							
[b-Hidano]							
[b-Yang]							
[b-Nandakumar]							
[b-Sutcu]							
…							
[Fuzzy commitment]							
[b-Juels1]	Dummy information		✓	✓	✓		
[Bio-hashing]							
[b-Monrose]	Secret sharing		✓			✓	✓
[b-Draper]	One-way function						
[b-Shibata]	One-way function		✓	✓		✓	

Table I.2 – Algorithm list of the cancellable biometrics mechanism

Algorithm	Place of function or process				
	Client		Server		
	E. Concealment	F. Data management	G. Process partition		
			a. Elimination of Fluctuations		b. Comparison
		Secret partition	1. Quantization	2. Error correcting	Score
[Geometrical deformation]					
[b-Ratha1]	Geometrical deformation	✓			✓
[Functional transformation]					
[b-Ratha2]	Functional transformation	✓			✓
[b-Maiorana]	Functional transformation				
[b-Chikkerur]	Functional transformation				
[Random filtering]					
[b-Savvides1]	One-way function, dummy information	✓			✓
[b-Savvides2]					
[b-Hirata]					
…					
[Logical addition]					
[b-Braithwaite]	One-way function	✓	✓		✓
…					

Appendix II

Evaluation example for a biometric cryptosystem mechanism using a fuzzy vault scheme

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

II.1 System description (Step 1)

II.1.1 Description of the target of the evaluation

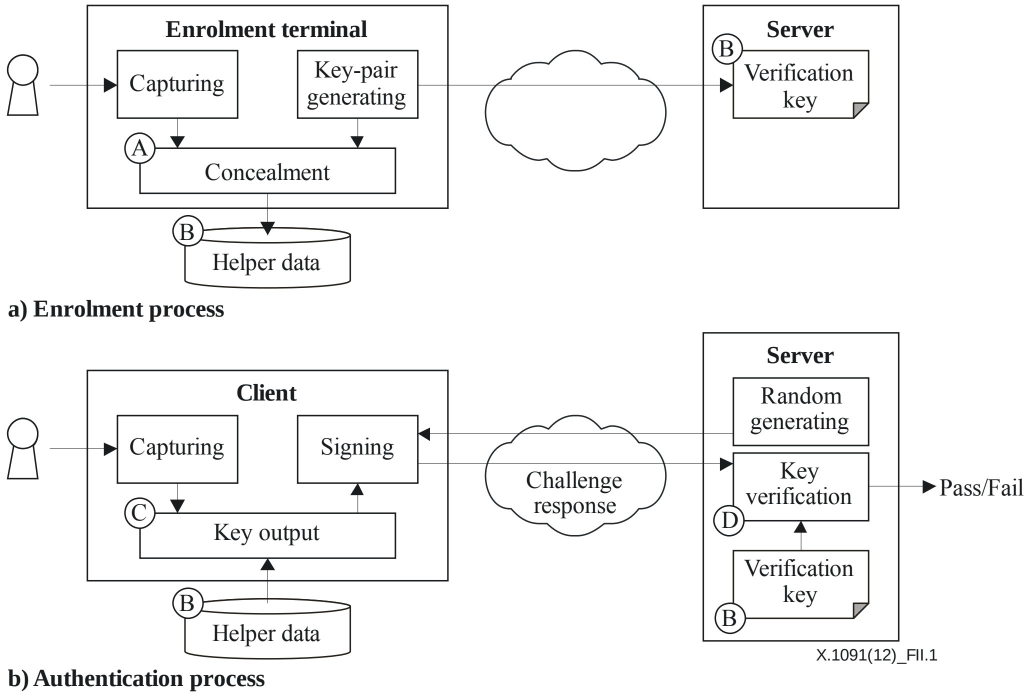


Figure II.1 – Description of the target of the evaluation system

II.1.2 Description of all essential components

A) Concealment

- Secret sharing: A function to conceal biometric data using secret sharing.
- Dummy information: A function to conceal biometric data using dummy information.

B) Data management

- Secret partition: A function that will make it difficult to restore biometric data by secretly partitioning helper data.

(C-a-2) Key output– Elimination of fluctuations – Error correcting code

- A function to eliminate fluctuations using the error correcting code.

(C-b-1) Key output – Key control – Key generation

- A function that will output the concealed key from the helper data of the genuine user, using the key generation method.

II.2 Vendor claim (Step 2)

The vendor provides performance claims in the form of a set(s) of maximum values of security-relevant error rates that can be achieved simultaneously.

II.3 Examination of vendor claim (Step 3)

In this step, evaluation items using this contribution are clarified. As defined in Table 1 and clause 8.2, evaluation items for the fuzzy vault scheme can be listed as follows:

(A) Concealment of biometric data

- Secret sharing scheme:
  - difficulty to restore key from a single information share;
  - difficulty to restore key from secret shared information below the threshold value.
- Dummy information:
  - difficulty to restore biometric data from a single information part;
  - difficulty to restore biometric data from a single information part after concealment;
  - difficulty to restore biometric data using the correlativity obtained from multiple parts of information after concealment.

(C-a-2) Key output – Elimination of fluctuations – Error correcting code

- Entropy loss of biometric data by using the error correcting code
- Accuracy to restore the secret key for a genuine user and difficulty to restore the secret key for an imposter.

(C-b-1) Key output – Key control – Key generation

- Difficulty to restore key using only helper data.
- Key length is sufficient. However, the relationship between key length and encryption strength follows the existing encryption protocol.
- Difficulty to restore biometric data using the correlativity between the generated key and biometric data.
- Difficulty to restore biometric data during key regeneration.
- Accuracy to restore the secret key for a genuine user and difficulty to restore the secret key for an imposter.

As defined in Table 2, interdependencies for each evaluation item can be listed as follows:

(A) Concealment of biometric data

- (C-a-2) Key output – Elimination of fluctuations – Error correcting code

  When it is difficult to restore biometric data from a part/parts of secret shared information, or from secret partitioned information, an error correcting code is applied. In this case, it should be ensured that entropy loss of biometric data by using an error correcting code is small.

  - When the capability of an error correcting code is high, the FNMR becomes lower. At the same time, entropy loss of biometric data becomes bigger, so the risk related to restoring biometric data becomes higher. On the other hand, when the capability of the error correcting code is low, the FNMR becomes higher. At the same time, entropy loss of biometric data becomes smaller, so the risk related to restoring biometric data becomes lower.

- (C-b-1) Key output – Key control – Key generation

  Although it is difficult to restore biometric data from a part/parts of secret shared information, or from secret partitioned information, it should be ensured that the length of the generated key is sufficiently long.

- Even if it is difficult to restore biometric data from a part/parts of secret shared information, or from secret partitioned information, if the length of the generated key is too short, there is the threat that the key can be easily restored.

- (C-b-1) Key output – Key control – Key generation

  Although it is difficult to restore biometric data from a part/parts of secret shared information or from secret partitioned information, in key-generation based methods, it should be ensured that it is difficult to restore the key using helper data.

  - Even if the length of the key generated from helper data is sufficiently long, if the possible patterns of the restored key derived from the same helper data are few, there is the threat that the key can be easily restored from helper data.

- (C-b-1) Key output – Key control – Key generation

  Although it is difficult to restore biometric data from a part/parts of secret shared information or from secret partitioned information, it should be ensured that it is difficult to restore biometric data using the correlativity between the generated key and biometric data.

  - Even if it is difficult to restore biometric data from a part/parts of secret shared information or from secret partitioned information, if the generated key or secret partitioned information is exposed, there is the threat that it is possible to restore biometric data using the exposed information or data.

- (C-b-1) Key output – Key control – Key generation

  Although it is difficult to restore biometric data from a part/parts of secret shared information or from secret partitioned information, in key-generation based methods, it should be ensured that it is difficult to restore biometric data using a regenerated key.

  - Even if it is difficult to restore biometric data from a part/parts of secret shared information or from secret partitioned information, there is the threat that it is possible to restore biometric data using the correlativity between the regenerated and exposed helper data.

(B) Data management – Secret partition

- (C-a-2) Key output – Elimination of fluctuations – Error correcting code

  Although it is difficult to restore biometric data from a part/parts of secret shared information or from secret partitioned information, it should be ensured that entropy loss of biometric data by using the error correction code is small.

  - When the capability of an error correcting code is high, the FNMR becomes lower. At the same time, it becomes possible to restore original biometric data using a part/parts of secret shared information or from secret partitioned information. On the other hand, when the capability of an error correcting code is low, the FNMR becomes higher. At the same time, if the entropy of helper data is inadequate, biometric data cannot be restored.

- (C-b-1) Key output – Key control– Key generation

  Although it is difficult to restore biometric data from a part/parts of secret shared information or from secret partitioned information, in key-generation based methods, it should be ensured that the key length is sufficiently long.

  - Even if it is difficult to restore biometric data from a part/parts of secret shared information or from secret partitioned information, if the length of the generated key is too short, there is the threat that the key can be easily regenerated from helper data.

- (C-b-1) Key output – Key control – Key generation

  Although it is difficult to restore biometric data from a part/parts of secret shared information, or from secret partitioned information, in key generation-based methods, it should be ensured that it is difficult to regenerate the key from helper data.

  – Even if the length of the key generated from helper data is sufficiently long, if possible patterns of the restored key derived from the same helper data are few, there is the threat that the key can be easily restored from helper data.

- (C-b-1) Key output – Key control – Key generation

  Although it is difficult to restore biometric data from a part/parts of secret shared information, or from secret partitioned information, it should be ensured that it is difficult to restore biometric data using the correlativity between the generated key and biometric data.

  – Even if it is difficult to restore biometric data from a part/parts of secret shared information, or from secret partitioned information, if the generated key or secret partitioned information is exposed, there is the threat that it is possible to restore biometric data using the correlativity between the generated key and secret partitioned information.

- (C-b-1) Key output – Key control – Key generation

  Although it is difficult to restore biometric data from a part/parts of secret shared information, or from secret partitioned information, in key generation-based methods, it should be ensured that it is difficult to restore biometric data during key regeneration.

  – Even if it is difficult to restore biometric data from a part/parts of secret shared information, or from secret partitioned information, there is the threat that biometric data can be restored using the correlativity between exposed helper data.

An example of the evaluation process is described in clause II.4.1, and evaluation results are described in clause II.4.2

II.4 Vendor test and evaluation of vendor test

II.4.1 Evaluation methods for each item

(1) Evaluation items for key restoring rate

Evaluation items for key restoring rate can be listed as follows:

(C-a-2) Key output – Elimination of fluctuations – Error correcting code

- Accuracy to restore the secret key for a genuine user and difficulty to restore the secret key for an imposter.

(C-b-1) Key output – Key control – Key generation

- Key length is sufficient. However, the relationship between key length and encryption strength follows existing encryption protocol.
- Accuracy to restore the secret key for a genuine user and difficulty to restore the secret key for an imposter.

As shown in Table 2, there is a trade-off between a genuine key restoring rate and an imposter key restoring rate [ISO 19795-2]. The biometric performance testing method is applied to this evaluation. However, the interdependencies shown in Table 2 should be taken into consideration.

(2) Evaluation items for difficulty to restore key/biometric data

Evaluation items for difficulty to restore key/biometric data can be listed as follows:

(A) Concealment of biometric data

- Secret sharing scheme:
  - difficulty to restore key from a single information share;
  - difficulty to restore key from secret shared information below the threshold value.
- Dummy information:
  - difficulty to restore biometric data from a single information part;
  - difficulty to restore biometric data from a single information part after concealment;
  - difficulty to restore biometric data using the correlativity from multiple parts of information after concealment.

(C-a-2) Key output – Elimination of fluctuations – Error correcting code

- Entropy loss of biometric data by using the error correcting code.

(C-b-1) Key output – Key control – Key generation

- Difficulty to restore key using helper data.
- Difficulty to restore biometric data using the correlativity between the generated key and biometric data.
- Difficulty to restore biometric data during key regeneration.

(3) Example of an evaluation method for (C-b-1) Key output – Key control – Key generation

A security evaluation method using the estimated entropy is described here as an example of methods to evaluate this point. An attacker is able to guess the secret key without the biometric data of a genuine user by using statistical bias, such as the pattern and the appearance frequency of the secret key restored from helper data, including dummy information, by the brute-force attack. In this instance, the security against the threat that an attacker who has no knowledge of the biometric data of a genuine user can estimate the secret key illegally is evaluated by (C-b-1), difficulty of guessing key using helper data.

Here, key information that is output from helper data is defined as restored information, regardless of whether or not it is the secret information of a genuine user. A summary of the secret-key-guessing attack using the statistical bias of the restored information is described.

It is not possible to guess the secret key from the restored information alone. However, the frequency of the appearance of restored information is not uniform if it is acquired many times from the same helper data.

An attack is now considered under the conditions that the number of secret information symbols is denoted by k, the number of helper data elements is denoted by r, and the number of dummy data elements is denoted by d, and g is defined by $r - d$.

(1) Derive k elements from the exposed helper data.

(2) Acquire secret data by error correction of the derived helper data elements.

(3) Repeat (1) and (2) above many times, and create statistical data on the pattern and restoring rate of the restored information. It is assumed that the probability that the restored information output in (1) and (2) equal to the secret key is the secret key restoring rate P_b by the brute-force attack, where the theoretical value of P_b is given by:

$$P_b =_g C_k /_r C_k$$

where ${}_gC_k$ is the number of *k*-combinations from *g* elements.

(4) Note the pattern of the restored information in the decreasing order of the probability, starting with approximating the P_b.

That is to say, an attacker uses the statistical bias that the appearance probability of the restored information that is different from the secret key is not always equal to P_b, because different keys from the secret key are restored only when dummy information is derived. Consequently, it can be easier to guess the secret key with a few trials rather than with brute-force attacks.

Estimated entropy is used as a baseline for evaluating security against such an attack method. Let *X* be the random key and *P(X=x)* be the probability of each possible key *x* of *X*. The estimated entropy $H_\infty(X)$ is defined as follows:

$$H_\infty(X) := -\sum_x P(X=x)\log_2 P(X=x) \qquad \text{(II-1)}$$

In this case, it is computationally difficult to derive elements from the helper data by trying all combinations of these elements because the number of trials increases as the number of the secret-key symbols and the helper-data elements increases. Therefore, in this instance, only *N* samples of elements are derived from the helper data and the estimated entropy is calculated from these samples. If it is assumed that *N* samples have an independent distribution, the estimated entropy takes a maximum value max $H_\infty(X)$ given by:

$$\max H_\infty(X) = -\log_2 \frac{1}{N} \qquad \text{(II-2)}$$

However, the estimated entropy obtained from the results of experiments involves a decrease in entropy, without necessarily matching max $H_\infty(X)$. In this case, the rate of decrease in entropy from max $H_\infty(X)$ is assumed to be an estimated entropy loss H_{loss}, where H_{loss} is defined as follows:

$$H_{loss} = \frac{\max H_\infty(X) - H_\infty(X)}{\max H_\infty(X)} \qquad \text{(II-3)}$$

This shows that as H_{loss} decreases, the recovery results approach an independent distribution, and it is difficult to restore the key.

II.4.2 Evaluation results

(1) Evaluation results for the genuine/imposter key-restoring rate

Experiments should be performed to investigate the genuine/imposter key-restoring rate, taking the number of parity code elements *g* to be 20, and the number of dummy data elements to be 50, 150 and 250.

Reed-Solomon codes on a Galois extension field $GF(2^8)$ are used as error correcting codes in the experiments. Thus, if *k* symbols on $GF(2^m)$, the size of secret data that can be stored is $m \times k$ [bits]. The fingerprint data and other simulation data used in the experiments are shown in Table II.1.

Table II.1 – Condition of the simulation

Fingerprint data	140 subjects × 5 prints (3 for registration, 2 for verification)
Feature-point extraction algorithm	NFIS2
Number of obtained minutiae data *n*	20
Error correcting code	Encoding with $GF(2^8)$, $g = 20$
Number of dummy data elements *d*	50, 150, 250
Number of secret data elements *k*	4, 5, 6, 7, 8, 9, 10

The secret data-restoring rate is shown in Figure II.2, with the horizontal axis showing the number of secret data elements and the vertical axis showing the results of the secret data-restoring rate.

The false non-match rate (FNMR) and false match rate (FMR) are generally used in evaluating biometrics, but in this case, the authorized person acceptance rate and false acceptance rate are used for indicating the probability that the secret data is correct (called "recovery rate").

Taking $k = 6$ and $d = 150$ as an example, the recovery rate for a genuine user was about 98%, and the restoring rate for a third party was only about 3%.

The relationship between evaluation items and evaluation results is as follows:

(C-a-2) Key output – Elimination of fluctuations – Error correcting code

- Accuracy to restore the secret key for a genuine user, and difficulty to restore the secret key for an imposter.
  - The relationship between the genuine key-restoring rate and the imposter key-restoring rate is shown in Figure II.2.

(C-b-1) Key output – Key control – Key generation

- Key length is sufficient. However, the relationship between key length and encryption strength follows existing encryption protocol.
  - The horizontal axis of Figure II.2 shows the length of the secret key.
- Accuracy to restore the secret key for a genuine user, and difficulty to restore the secret key for an imposter.
  - The relationship between the genuine key restoring rate and the imposter key restoring rate is shown in Figure II.2.

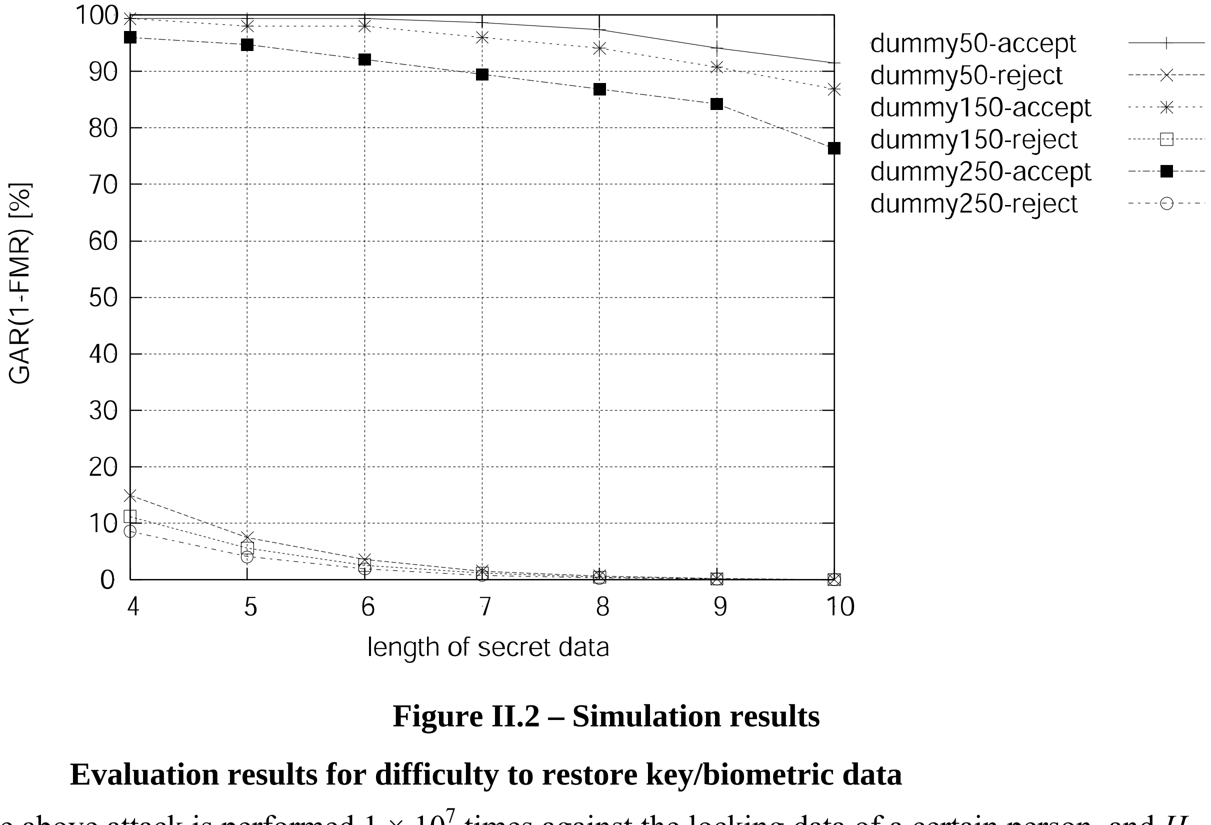


Figure II.2 – Simulation results

(2) Evaluation results for difficulty to restore key/biometric data

The above attack is performed 1 × 10^7 times against the locking data of a certain person, and H_{loss} is calculated from the distribution of restored information. Note that the number of secret data elements k was fixed at 4, and the number of dummy data elements added to the locking data was varied during the evaluation in steps of 20, 40, 60, 80, 100.

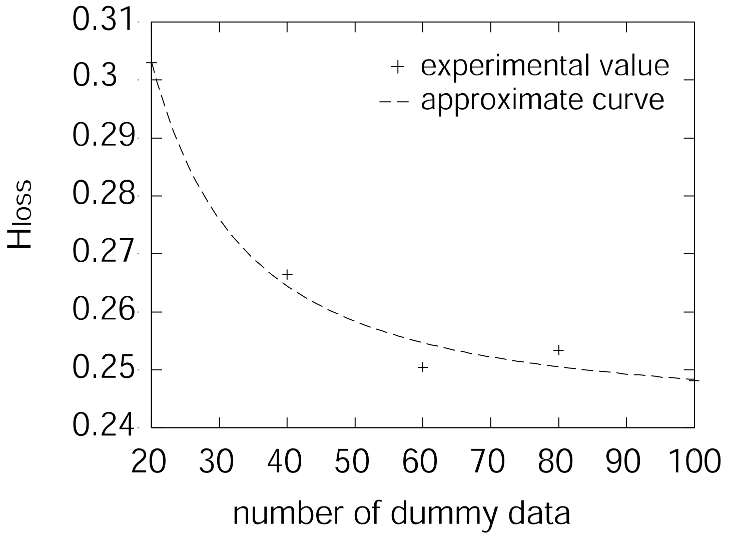


Figure II.3 – Estimated entropy loss H_{loss}

The relationship between the number of dummy data elements and H_{loss} is shown in Figure II.3, with the vertical axis showing H_{loss} and the horizontal axis showing the number of dummy data elements. The approximate curve, calculated from least square method, is also shown in Figure II.3.

If there are few dummy data elements, H_{loss} reaches a maximum of approximately 30%, but that value decreases to approximately 25% as the number of dummy data elements increases. As H_{loss} decreases, the key restoring rate approaches an independent distribution. Even if H_{loss} is low, in the case that P_b is high, there is the threat that the key can be easily restored by brute-force attack. Thus, both P_b and H_{loss} should be considered.

Here, the number of brute-force attacks to restore the key is defined as B_f. The rate of decrease in B_f can be represented using H_{loss} and Equation II-4. The rate of decrease in B_f is shown in Figure II.4.

$$(1-\frac{1}{2^{(H_{loss}\times\max H_{\infty}(X))}})\times 100(\%) \qquad \text{(II-4)}$$

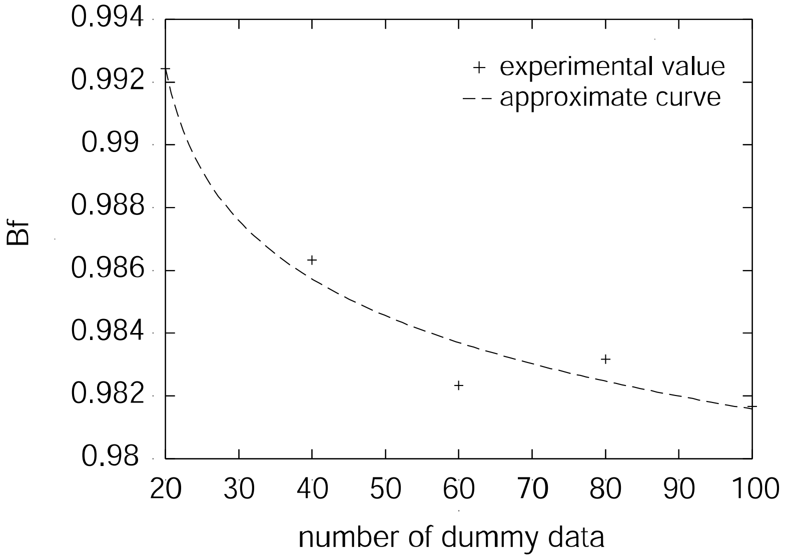


Figure II.4 – Rate of decrease in B_f

Figure II.4 and Equation II-4 show that increasing the number of dummy data makes it more difficult to restore key from helper data.

(3) Evaluations of interdependencies

The interdependencies are evaluated with the results from Equations II-1 and II-2.

(A) Concealment of biometric information

- (C-a-2) Key output – Elimination of fluctuations – Error correcting code

  An error correcting code is applied to make it difficult to restore biometric data from part(s) of secret shared information, or from secret partitioned information. It should be ensured that the entropy loss of biometric data by using the error correcting code is small.

  – When the capability of the error correcting code increases, the FNMR decreases. As the entropy loss of biometric data simultaneously increases, the risk related to restoring biometric data increases. However, when the capability of the error correcting code decreases, the FNMR increases. As the entropy loss of biometric data simultaneously decreases, the risk related to restoring biometric data decreases.

  The relationship between the capability of the error correcting code and the key restoration rate is plotted in Figure II.2.

- (C-b-1) Key output – Key control – Key generation

  Even though it is difficult to restore biometric data from part(s) of secret shared information, or from secret partitioned information, it should be ensured that the generated key is sufficiently long.

  – Even if it is difficult to restore biometric data from part(s) of secret shared information, or from secret partitioned information, where the generated key is too short there is a threat that the key can be easily restored.

  The relationship between the length of the key and the key restoration rate is plotted in Figure II.2.

- (C-b-1) Key output – Key control – Key generation

  Even though it is difficult to restore biometric data from part(s) of secret-shared information, or from secret-partitioned information, key-generation-based methods should ensure that it is difficult to restore the key using helper data.

  – Even if the key generated from helper data is sufficiently long, where there are few possible patterns for the restored key derived from the same helper data, there is the threat that the key can be easily restored from helper data.

  Where the key length is fixed, the difficulty of restoring the key is determined by the amount of dummy data. The relationship between the length of the key and the key restoration rate is plotted in Figure II.2. The relationship between the difficulty of restoring the key and the amount of dummy data is plotted in Figure II.3.

- (C-b-1) Key output – Key control – Key generation

  Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, it should be ensured that it is difficult to restore biometric data using the correlativity between the generated key and biometric data.

  – Even if it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, where the generated key or secret partitioned information is exposed, there is the threat that it will be possible to restore biometric data using the exposed information or data.

  The difficulty of restoring biometric data using the correlativity between the generated key and biometric data was not evaluated.

- (C-b-1) Key output – Key control – Key generation

  Even though it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, key-generation-based methods should ensure that it is difficult to restore biometric data using the regenerated key.

  – Even if it is difficult to restore biometric data from part(s) of secret shared information or from secret partitioned information, there is the threat that it will be possible to restore biometric data using the correlativity between the regenerated and exposed helper data.

  The difficulty of restoring biometric data using the regenerated key was not evaluated.

(B) Data management – Secret partition

- (C-a-2) Key output – Elimination of fluctuations – Error correcting code

  Even though it is difficult to restore biometric data from part(s) of secret shared information, or from secret partitioned information, it should be ensured that the entropy loss of biometric data by using the error correction code is small.

  – When the capability of error correction increases, the FNMR decreases. It simultaneously becomes possible to restore original biometric data using part(s) of secret shared information, or from secret partitioned information. However, when the capability of error correcting decreases, the FNMR increases. If the entropy of helper data is simultaneously insufficient, biometric data cannot be restored.

  The relationship between the capability of the error correcting code and the key restoration rate is plotted in Figure II.2.

- (C-b-1) Key output – Key control – Key generation

  Even though it is difficult to restore biometric data from part(s) of secret shared information, or from secret partitioned information, key-generation-based methods should ensure that the key is sufficiently long.

  – Even if it is difficult to restore biometric data from part(s) of secret shared information, or from secret partitioned information, where the generated key is too short, there is the threat that the key can easily be regenerated from helper data.

  The relationship between the length of the key and the key restoration rate is plotted in Figure II.2.

- (C-b-1) Key output – Key control – Key generation

  Even though it is difficult to restore biometric data from part(s) of secret-shared information, or from secret-partitioned information, key-generation-based methods should ensure that it is difficult to regenerate the key from helper data.

  – Even if the key generated from helper data is sufficiently long, where there are few possible patterns for the restored key derived from the same helper data, there is the threat that the key can be easily restored from helper data.

  Where the key length is fixed, the difficulty of restoring the key is determined by the amount of dummy data. The relationship between the length of the key and the key restoration rate is plotted in Figure II.2. The relationship between the difficulty of restoring the key and the amount of dummy data is plotted in Figure II.3.

- (C-b-1) Key output – Key control – Key generation

  Even though it is difficult to restore biometric data from part(s) of secret shared information, or from secret partitioned information, it should be ensured that it is difficult to restore biometric data using the correlativity between the generated key and biometric data.

- Even if it is difficult to restore biometric data from part(s) of secret shared information, or from secret partitioned information, where the generated key or secret partitioned information is exposed, there is the threat that it will be possible to restore biometric data using the correlativity between the generated key and secret partitioned information.

The difficulty of restoring biometric data using the correlativity between the generated key and secret partitioned information was not evaluated.

- (C-b-1) Key output – Key control – Key generation

Even though it is difficult to restore biometric data from part(s) of secret shared information, or from secret partitioned information, key-generation-based methods should ensure that it is difficult to restore biometric data during key regeneration.

- Even if it is difficult to restore biometric data from part(s) of secret shared information, or from secret partitioned information, there is the threat that biometric data can be restored from the correlativity between exposed helper data.

The difficulty of restoring biometric data using the correlativity between exposed helper data was not evaluated.

Appendix III

Evaluation example for cancellable biometrics using correlation-based matching

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

III.1 Introduction

This appendix clarifies evaluation requirements in cancellable biometrics based on this Recommendation and presents an evaluation example.

III.2 Clarification of evaluation requirements

Evaluation requirements are clarified in accordance with the procedure in clause 8.

III.2.1 System description

The system targeted for evaluation is shown below (cancellable biometrics system).

Target technology is reproduced from [b-Hirata].

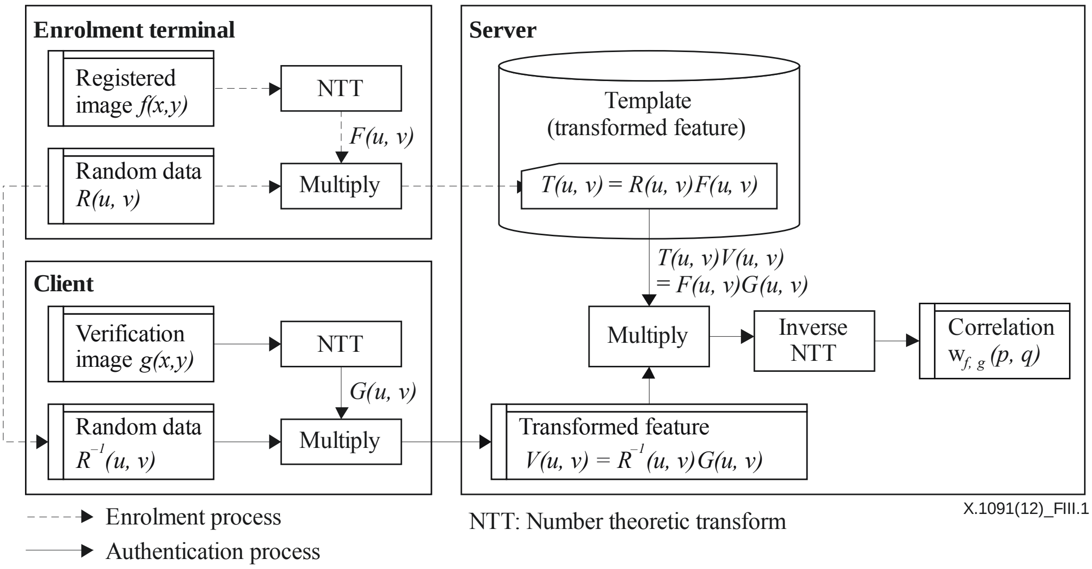

Enrolment terminal
Registered image $f(x,y)$
NTT
$F(u, v)$
Random data $R(u, v)$
Multiply
Server
Template (transformed feature)
$T(u, v) = R(u, v)F(u, v)$
$T(u, v)V(u, v) = F(u, v)G(u, v)$
Client
Verification image $g(x,y)$
NTT
$G(u, v)$
Random data $R^{-1}(u, v)$
Multiply
Multiply
Inverse NTT
Correlation $w_{f,g}(p, q)$
Transformed feature $V(u, v) = R^{-1}(u, v)G(u, v)$
Enrolment process
Authentication process
NTT: Number theoretic transform
X.1091(12)_FIII.1

Figure III.1 – Process flow of evaluation target

As the authentication system using template protection techniques that is targeted for evaluation is classified as cancellable biometrics, the reference model in Figure III.2 is used to define evaluation targets.

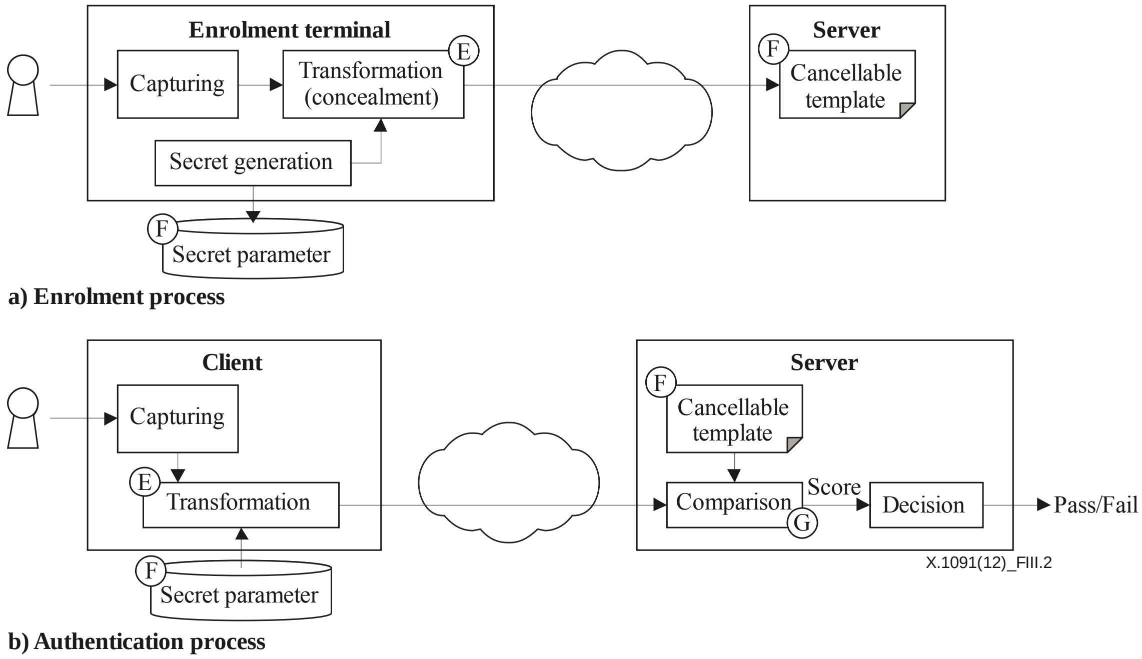


Figure III.2 – Reference model of evaluation targets

The following outlines each elemental technology that is targeted for evaluation.

E) Transformation (Concealment)

The one-way function is achieved by multiplying the random-number filter, *R(u,v)*, by the results, *F(u,v)*, of transforming the registered image *f(x,y)* through a number-theoretic transform (NTT).

Alternatively, the one-way function is achieved by multiplying $R^{-1}(u,v)$, the inverse of the random-number filter *R(u,v)*, by the results *G(u,v)* of transforming the input matching image *g(x,y)* by a number-theoretic transform (NTT).

F) Data management

- Secret parameter
- Random number filter *R(u,v)* is used as dummy information. This parameter is managed in a distributed manner with the cancellable template.
- Cancellable template

  The results *F(u,v)R(u,v)* of multiplying the random-number filter, *R(u,v)*, by the results, *F(u,v)*, of transforming the registered image *f(x,y)* through a number-theoretic transform (NTT), are managed in a distributed manner with the secret parameter.

G) Comparison

- The results of multiplying the cancellable template, *F(u,v)R(u,v)*, by the results, *G(u,v)* $R^{-1}(u,v)$, by transforming the input matching image, are subjected to an inverse number-theoretic transform (inverse NTT), and the ratio between the correlation average and the peak value is calculated.

III.2.2 Clarification of evaluator (vendor) requested items

Evaluator-requested items governing authentication accuracy conforming to the evaluation steps in this Recommendation are extracted from [b-Hirata] and are described in clause III.2.1.

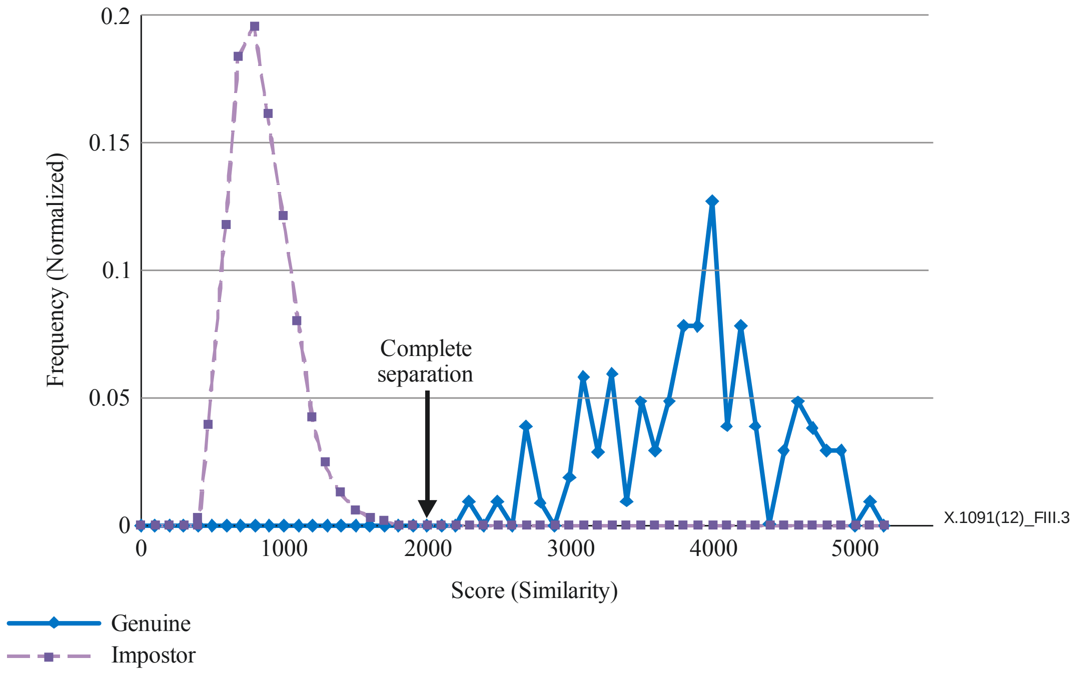


Figure III.3 – Requirements in accuracy evaluation

In [b-Hirata], accuracy is evaluated using 102 finger samples from 17 volunteers. In the evaluation, the score distribution for genuine users and that for imposters is completely separated, and the number of samples is less than that recommended by the accuracy evaluation standard. In the document, however, accuracy evaluation in conformance with the standard is not stressed, and here as well, evaluation is performed by a simplified similarity distribution in the comparison process, as described above.

III.2.3 Test of vendor-required items

Evaluator tests vendor-required items conforming to the evaluation steps in this Recommendation. Given that the target of evaluation in the reference document is a cancellable biometrics system, the evaluator extracts evaluation items from clause 8.4, as follows.

i) Concealment (E)

- One-way function:
  – difficulty of restoring biometric data from post-transformation information;
  – drop in security due to a conflict in transformed information;
  – comparison of the FMR for any transformation parameter and comparison of the FNMR for the correct transformation parameter.
- Dummy information:
  – difficulty of separating dummy information and biometric data from post-transformation information;
  – FMR for comparison by any transformation parameter, and the FNMR for comparison by the correct transformation parameter.

ii) Data management (F)

– Difficulty of restoring biometric data in the event that other data are leaked.

iii) Server management (G-b)

– Difficulty of attacks using scores.

The evaluator also extracts evaluation items governing mutual dependency from clause 8.5, as follows.

i) Concealment (E)

- Server processing, comparison, scores:
  - the difficulty of restoring divided information and the difficulty of performing attacks using scores should be evaluated.

ii) Data management, secret sharing (F)

- Server processing, comparison, scores:
  - the difficulty of restoring biometric data in the event of an information leak and the difficulty of attacks using scores (biometric restoration) should be evaluated.

III.3 Requirements of evaluation tool

Focusing on evaluation guidelines for biometric template protection technologies indicated by standardization policies, the purpose of an evaluation tool is to develop a programme for evaluating the relationship between template-protection security and items having a dependency relation with that security, and to perform security-evaluation trials with that programme on existing technologies and products. The results of these trials can then be used to test the validity of those standardization policies, and to extract and organize points for improvement and problems to be addressed.

The following items are targeted for evaluation.

- Effect of security-related parameters in the concealment function on authentication accuracy:
  - security-related parameters;
    - ○ bit length of secret parameter (32 bits, 64 bits, 128 bits);
  - authentication accuracy (FAR, FRR).
- Drop in security due to a conflict in transformed information after transformation by the concealment function:
  - security-related parameters;
    - ○ number of concealment transformations (1, 10, 100);
  - authentication accuracy (FAR, FRR).

In the evaluation, biometric samples must be gathered to test authentication accuracy. The following requirements have therefore been specified for a data-gathering tool, currently under development, that can be used for gathering biometric samples.

- It should be displayed as a document asking for user consent to an experiment, and must move to a data-gathering screen once that consent option has been selected.
- It should be displayed as the ID of the experiment volunteer and prompt for entry of notes.
- It should allow the number of times that data are gathered (input) for each finger to be specified (minimum: three inputs).
- It should enable the gathering of enrolment images from a maximum of six fingers (left and right index fingers, middle fingers and ring fingers) to a minimum of two fingers.
- It should generate an enrolment template from the set of enrolment images after data gathering.
- It should allow the number of trials for verifying whether matching can be performed to be specified and must enable images for this number of trials to be gathered as matching images.

- It should encrypt gathered image data and create and store file names on the basis of volunteer IDs uniquely assigned to experiment volunteers. Additionally, it must separately prepare a function for decrypting image data for evaluation purposes (this may be done in evaluation-tool source code).
- It should enable an individual experiment volunteer to use this ID to delete his or her data.

The following requirements are also imposed on the evaluation tool, so that the evaluation items described above can be evaluated with respect to gathered data.

- With respect to the protection function, it should be possible to input the same protection parameter for both enrolment data and matching data and to store that data accordingly.
- With respect to the protection function, it should be possible to generate and store enrolment data for any number of transformations (same transformation history), and to generate and store matching data using the protection parameters resulting from that transformation history.
- It should be possible to compare by brute-force attack, enrolment data and matching data achieved by transformation in the above two ways and to output score lists.

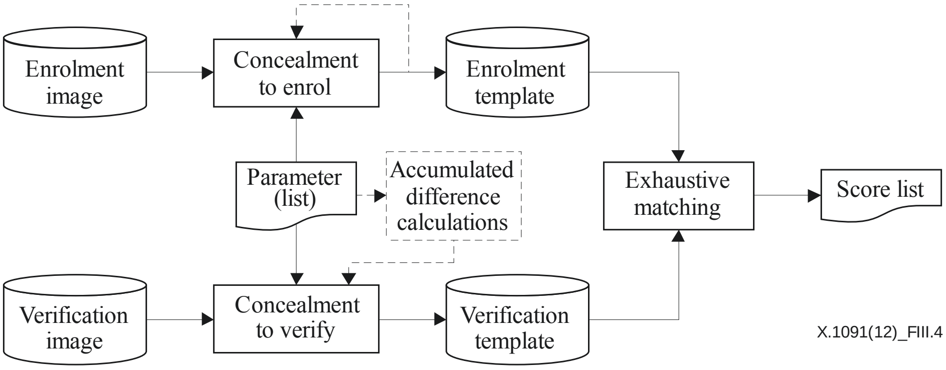


Figure III.4 – Function block diagram of evaluation tool

III.4 Evaluation experiment

An evaluation was performed by developing the tool and using it to perform an experiment.

Evaluation data

The following data were gathered and used in the evaluation by the data-gathering tool.

- Number of volunteers assembled by the gathering tool: 10 people.
- Data for six fingers (left and right index fingers, middle fingers and ring fingers) were gathered from each volunteer.
- Three enrolment images and three input matching images were gathered from each volunteer.

Experiment 1

Evaluate the effect of different secret-data bit lengths (32 bits, 64 bits, 128 bits) on authentication accuracy.

Method 1

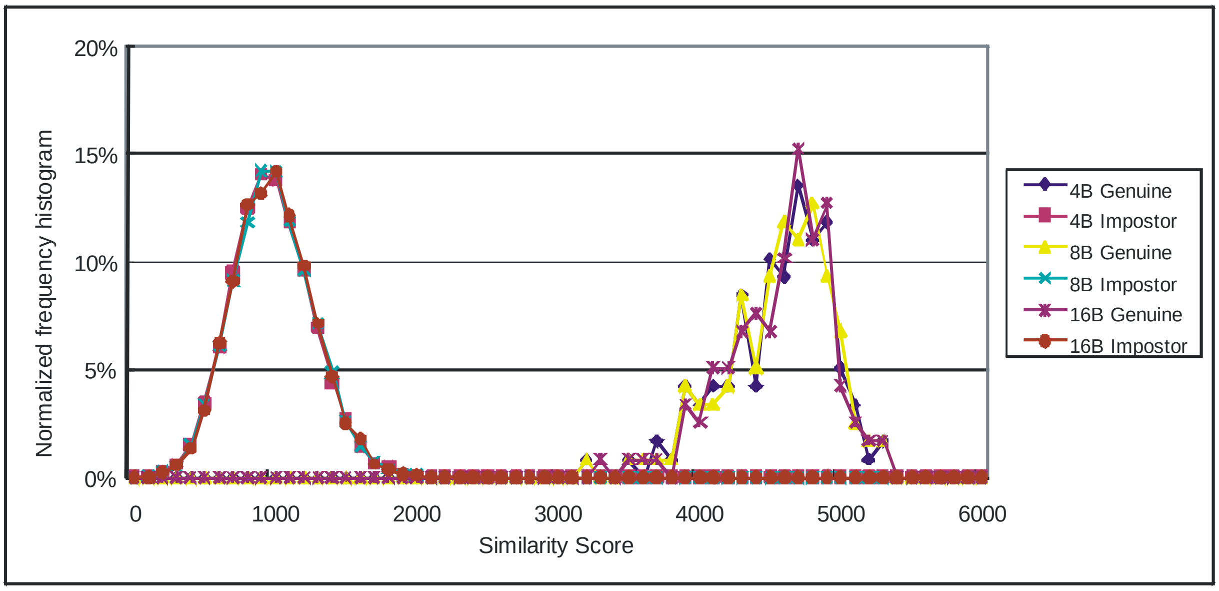
(1) Set 4-byte, 8-byte, and 16-byte secret data in the parameter file and create respective enrolment templates for gathered enrolment images.

(2) Using the same parameter file, create matching templates with respect to input matching images gathered by the data-gathering tool.

(3) Compare enrolment templates and matching templates by brute-force attack and obtain a score list.

Result 1

See Figure III.5.



X.1091(12)_FIII.5

Figure III.5 – Experiment 1: evaluation results

Conclusion 1

- The similarity distribution for comparison in the biometric template protection technology targeted here for evaluation was found to be independent of the strength of secret data.

Experiment 2

- Evaluate the effect of a different number of secret-data updates (1, 10 and 100) on authentication accuracy. Here, the length of secret data was 64 bits.

Method 2

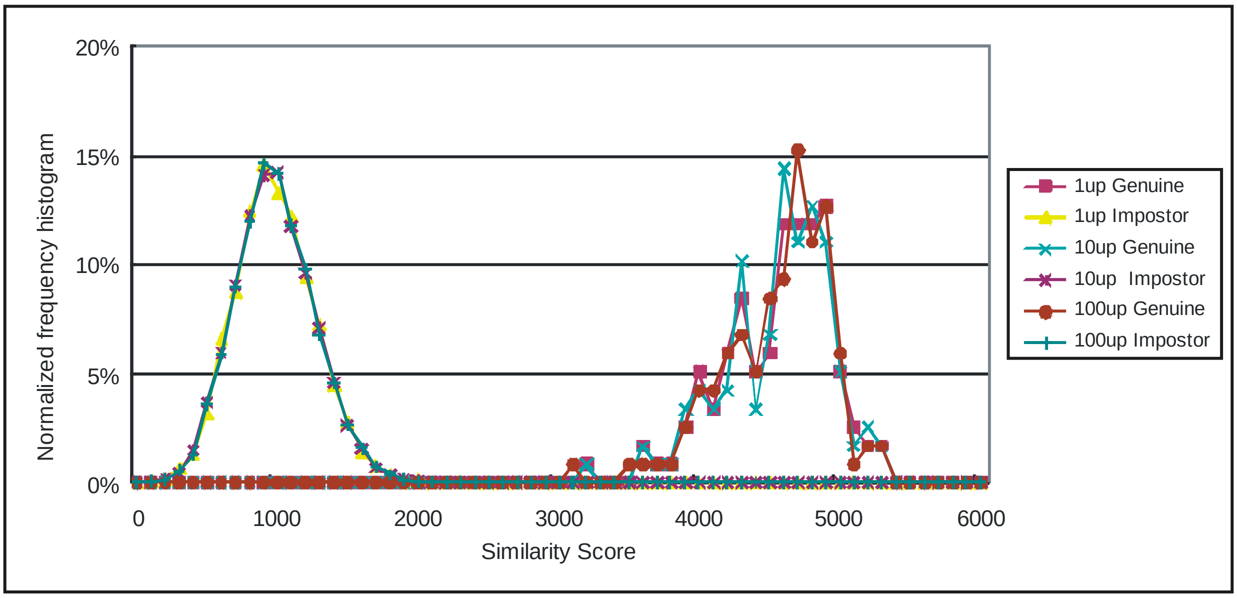
(1) Prepare a list of secret data for each update (1, 10 and 100) in the parameter file, and create enrolment templates with respect to gathered enrolment images by repeatedly performing updates for only the number of secret-data items set in the parameter file.

(2) Create matching templates with respect to input matching images gathered by the data-gathering tool, using the last parameter in the same parameter file.

(3) Compare enrolment templates and matching templates by brute-force attack and obtain a score list.

Results 2

See Figure III.6.



X.1091(12)_FIII.6

Figure III.6 – Experiment 2: evaluation results

Conclusion 2

- The similarity distribution for comparison in the biometric template protection technology targeted here for evaluation was found to be independent of the number of secret data updates.

Bibliography

General

[b-ITU-T X.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1084] Recommendation ITU-T X.1084 (2008), *Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems*.

[b-ITU-T X.1088] Recommendation ITU-T X.1088 (2008), *Telebiometrics digital key framework (TDK) – A framework for biometric digital key generation and protection*.

[b-ITU-T X.1124] Recommendation ITU-T X.1124 (2007), *Authentication architecture for mobile end-to-end data communication*.

Biometric cryptosystem

[b-Clancy] Clancy, T.C., Kiyavash, N., Lin, D.J. (2003), Secure Smartcard-Based Fingerprint Authentication. In: *Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications*, NY, ACM; pp. 45-52.

[b-Draper] Draper, S. *et al.* (2007), *Using Distributed Source Coding to Secure Fingerprint Biometrics*, Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Vol. 2; pp. 129-132.

[b-Hidano] Hidano, S. *et al.* (2008), On Biometric Encryption using Fingerprint and Its Security Evaluation. In: *Proceedings of the 10th International Conference on Control, Automation, Robotics and Vision*; pp. 950-956.

[b-Juels1] Juels, A., and Wattenberg, M. (1999), A Fuzzy Commitment Scheme. In: *Proceedings of the 6th ACM Conference on Computer and Communications Security*, NY, ACM; pp. 23-36.

[b-Juels2] Juels, A., and Sudan, M. (2002), A Fuzzy Vault Scheme. In: Lapidoth, A., Teletar, E., eds. *Proceedings of the IEEE International Symposium on Information Theory*, Lausanne, Switzerland, IEEE Press; p. 408.

[b-Monrose] Monrose, F. *et al.* (2001), Cryptographic Key Generation from Voice. In: *Proceedings of the 2001 IEEE Symposium on Security and Privacy*, Washington, DC, IEEE Computer Society; pp. 202-213.

[b-Nandakumar] Nandakumar, K., Jain, A.K., Pankanti, S. (2007), *Fingerprint-based fuzzy vault: Implementation and Performance*, IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4; pp. 744-757.

[b-Ohki] Ohki, T., Komatsu, N., Kasahara, M. (2006), Fingerprint Authentication Using a Fuzzy Vault Scheme for Security. In: *Proceedings of the 1st Joint Workshop on Information Security*; pp. 235-249.

[b-Shibata] Shibata, Y. *et al.* (2007), A Study on Biometric Key Generation from Fingerprints: Fingerprint-Key Generation from Stable Feature Value. In: *Proceedings of the International Conference on Security & Management*, Las Vegas, CSREA Press; pp. 45-51.

[b-Soutar] Soutar, D. *et al.* (1998), Biometric Encryption. In: Nicholls, R.K., ed. *ICSA Guide to Cryptography*, Columbus, OH, McGraw-Hill Companies; pp. 649-675.

[b-Sutcu] Sutcu, Y., Li, Q., Memon, N. (2007), *Protecting Biometric Templates with Sketch: Theory and Practice*, IEEE Transactions on Information Forensics and Security, Vol. 2, No. 3, part 2; pp. 503-512.

[b-Uludag1] Uludag, U. *et al.* (2004), *Biometric Cryptosystems: Issues and Challenges*. Proceedings of the IEEE, Special Issue on Multimedia Security for Digital Rights Management, Vol. 92, No. 6; pp. 948-960.

[b-Uludag2] Uludag, U., Pankanti, S., Jain, A.K. (2005), Fuzzy Vault for Fingerprints. In: *Audio- and Video-Based Biometric Person Authentication*, Berlin-Heidelberg, Springer-Verlag; pp. 310-319.

[b-Yang] Yang, S. *et al.* (2005), *Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme*, Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, Philadelphia, Vol. 5; pp. 609-612.

Cancellable biometrics

[b-Braithwaite] Braithwaite, M. *et al.* (2002), *Application-Specific Biometric Templates*, IEEE Workshop on Automated Identification Advanced Technologies, Tarrytown, NY, 14-15 March; pp. 167-171.

[b-Chikkerur] Chikkerur S. *et al.* (2008), *Generating Registration-Free Cancelable Fingerprint Templates*, 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems; pp. 1-6.

[b-Hirata] Hirata, S., Takahashi, K. (2009), *Cancelable Biometrics with Perfect Secrecy for Correlation-based Matching*. In: Tistarelli, M., Nixon, M.S., eds. *Advances in Biometrics Lecture Notes in Computer Science Vol. 5558*, Berlin Heidelberg, Springer-Verlag; pp. 868-878.

[b-Maiorana] Maiorana, E., Campisi, P., Neri, A. (2009), *Multi-Matcher Dynamic Signature Recognition with Protected and Renewable Templates*, 2009 International Conference on Biometrics, Identity and Security; pp. 1-8.

[b-Ratha1] Ratha, N.K., Connell J.H., Bolle, R.M. (2001), *Enhancing Security and Privacy in Biometric-based Authentication Systems*, IBM Systems Journal, Vol. 40, No. 3; pp. 614-634.

[b-Ratha2] Ratha, N.K. *et al.* (2007), *Generating Cancelable Fingerprint Templates*, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 4; pp. 561-572.

[b-Savvides1] Savvides, M., Kumar, B.V., Khosla, P.K. (2004), *Authentication Invariant Cancellable Biometric Filters for Illumination-Tolerant Face Verification*, Proceedings of SPIE, Vol. 5404; pp. 156-163.

[b-Savvides2] Savvides, M., Kumar, B.V., Khosla, P.K. (2004), *Cancelable Biometric Filters for Face Recognition*, Proceedings of the 17th International Conference on In Pattern Recognition, Vol. 3; pp. 922-925.

Other

[b-Nagai]	Nagai, K. *et al.* (2007), *ZeroBio – Fingerprint Authentication System Using Oblivious Neural Network Evaluation Protocol*, The Second International Conference on Availability, Reliability and Security, 10-13 April; pp. 1155-1159.

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, 2013