International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1086

Amendment 1

(04/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Telebiometrics

Telebiometrics protection procedures – A guideline to technical and managerial countermeasures for biometric data security

Amendment 1: Multibiometric protection procedures

Recommendation ITU-T X.1086 (2008) – Amendment 1

ITU-T

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.1086

Telebiometrics protection procedures – A guideline to technical and managerial countermeasures for biometric data security

Amendment 1

Multibiometric protection procedures

Summary

Amendment 1 updates Recommendation ITU-T X.1086 to incorporate multiple biometric information in telebiometric protection procedures by modifying the summary, keywords, scope, references, definitions, abbreviations and acronyms, and bibliography.

The amendment defines new vulnerabilities and proposes guidelines for the protection of the multibiometric system at four different fusion levels: the sample-level, the feature-level, the score-level, and the decision-level.

Amendment 1 adds Appendix V to describe techniques to be applied for the protection of multibiometric data.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1086	2008-11-13	17
1.1	ITU-T X.1086 (2008) Amd. 1	2012-04-13	17

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

1) Title 1

2) Summary 1

3) Keyword 1

4) Scope 1

5) References 2

6) Clause 3.1 2

7) Clause 3.2 2

8) Clause 4 3

9) Clause 6 3

10) New clause 19 6

11) Clause I.2.1 – Protection items at the client 9

12) New Appendix V 10

13) Bibliography 12

Recommendation ITU-T X.1086

Telebiometrics protection procedures – A guideline to technical and managerial countermeasures for biometric data security

Amendment 1

Multibiometric protection procedures

1) Title

Change the title as follows:

Telebiometrics protection procedures: A guideline to technical and managerial countermeasures for biometric data security.

2) Summary

Replace the summary with the following new text:

Recommendation ITU-T X.1086 defines the requirements of a guideline to provide security countermeasures for telebiometrics and tele-multibiometrics protection procedures. This Recommendation defines the vulnerabilities and threats in operating telebiometric and tele-multibiometric systems, and proposes a general guideline for security countermeasures, from both the technical and managerial perspectives, in order to establish a safe environment for the use of telebiometric systems and the protection of individual privacy. In particular, this Recommendation focuses on the vulnerabilities and countermeasures in the process of combining multibiometrics data or information by four different fusion schemes: sample-level, feature-level, score-level, and decision-level.

This Recommendation describes countermeasures that allow the protection of biometric devices as related to their installation, removal, and delivery. Countermeasures are proposed for the protection of biometric systems as related to their operational procedures, as well as the roles and responsibilities of personnel involved in system design. It is expected that the proposed countermeasures will ensure the security and reliability of the flow of single and multiple biometric information in a telecommunications environment.

3) Keyword

Replace the keywords as follows:

Multibiometrics, telebiometrics authentication models, telebiometrics countermeasures, telebiometrics protection guideline, telebiometrics vulnerabilities, tele-multibiometrics.

4) Scope

Replace the scope with the following new text:

Recommendation ITU-T X.1086 proposes a general guideline for security countermeasures, from both a technical and a managerial perspective, which would enable the protection of single and multiple biometric systems against various threats (e.g., hijacking, modification, illegal access, etc.) in the entire operation of telebiometrics, from the creation to the disposal of multibiometric data or information. Furthermore, this Recommendation describes the vulnerabilities and proposes countermeasures in the process of combining multibiometric data or information by four different fusion schemes: sample-level, feature-level, score-level, and decision-level. From a technical point of view, this Recommendation proposes the countermeasures to ensure data integrity, mutual authentication, and confidentiality. From a managerial perspective, it describes the countermeasures for the protection of telebiometric systems during their installation, removal, and delivery.

Recommendation ITU-T X.1086 does not cover the security requirements for biometric data, biometric security algorithms or multibiometric systems.

5) References

Add the following references to the existing list of references:

[ITU-T X.1082] Recommendation ITU-T X.1082 (2008), *Telebiometrics related to human physiology.*

[ISO/IEC 19792] ISO/IEC 19792 (2009), *Information technology – Security techniques – Security evaluation of biometrics.*

6) Clause 3.1

Add the following sub-clauses to clause 3.1 in alphabetic order:

biometric features [b-SC37SD2]: Output of a completed biometric feature extraction process.

biometric fusion [b-TR24722]: Combination of information from multiple sources: i.e., sensors, modalities, algorithms, instances or presentations.

biometric modality [b-TR24722]: Biometric characteristic used in a biometric process.

multi-algorithmic [b-TR24722]: Use of multiple algorithms for processing the same biometric sample.

multibiometrics [b-TR24722]: Automated recognition of individuals based on their biological or behavioural characteristics and involving the use of biometric fusion.

multi-instance [b-TR24722]: Use of multiple biometric instances within one biometric modality.

Examples: Iris (left) + Iris (right): Fingerprint (left index) + Fingerprint (right index)

multi-modal [b-TR24722]: Use of multiple different biometric modalities.

Example: Fingerprint + Face

multi-presentation [b-TR24722]: Use of either multiple presentation samples of one instance of a biometric characteristic or a single presentation that results in the capture of multiple samples.

Example: Several frames from video camera capture of a face image (possibly, but not necessarily, consecutive).

multi-sensorial [b-TR24722]: Use of multiple sensors for capturing samples of one biometric instance.

7) Clause 3.2

Add the following sub-clauses to clause 3.2 in alphabetic order:

decision-level fusion: Process of combining multiple decisions resulted from individual decision rules into an aggregated decision.

feature-level fusion: Process of combining multiple biometric features produced by individual feature extraction modules into a single feature set or vector.

sample-level fusion: Process of combining multiple biometric samples acquired by individual biometric input devices into a single set of samples.

score-level fusion: Process of combining multiple comparison scores produced by individual classifiers into a single score.

tele-multibiometrics: Application of multibiometrics in the telecommunication environment.

vulnerable point: A weak point where an attacker can reduce the system's information assurance.

8) Clause 4

Add the following abbreviation to the list of abbreviations and acronyms:

SVM	Support Vector Machine

9) Clause 6

Replace clause 6 with the following new text:

6 Components and vulnerabilities of a biometric system

The first step in taking technological protection measures for biometric data is to accurately identify the target and the purpose requiring protection. The second step is to establish biometric data policies. In order to reflect technological protection measures in protection policies, it is essential that technical staff who fully understand and implement the proposed policies, and decision-makers who have the authorization to execute these policies, participate in the process and work together effectively.

When a biometric system is installed with the mechanism for protecting the biometric system, an authorized data auditor is designated to supervise the auditing process in order to make sure that the biometric system is under operation following the protection policies.

One or more sub-processes are executed in a biometric processing unit, and one or more biometric processing units become the biometric verification process. A biometric processing unit is the abstract concept of a security domain, such as a sensor, a smart card, a storage device, or software running on a personal computer. Appendix II describes the functions of five sub-processes in biometric-verification process models.

Figure 1 describes a biometric system based on a network, illustrating how a client acquires personal information and biometric data, thereafter transmitting them to an installed server.

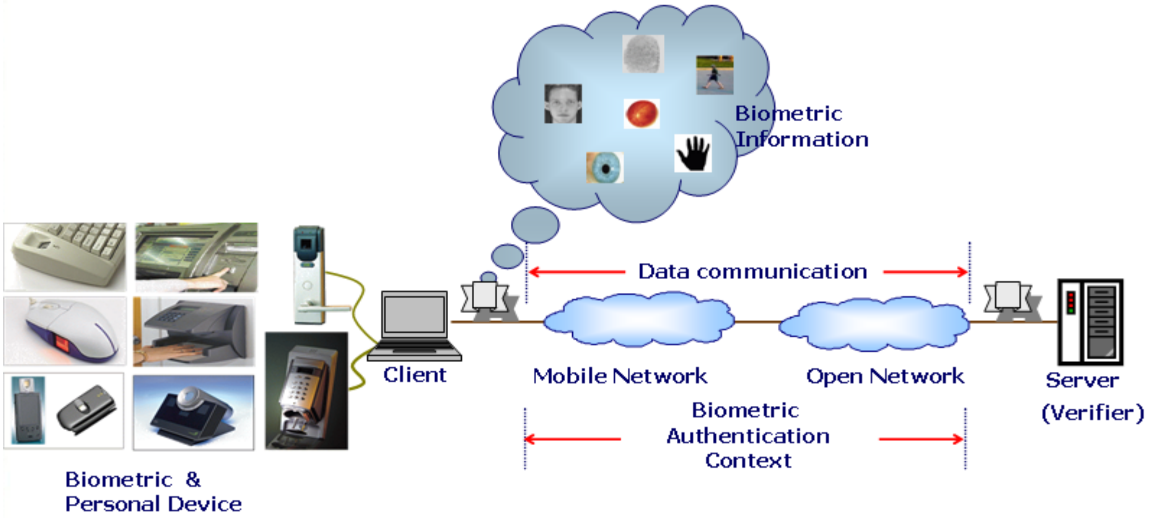

Figure 1 – Telebiometric model

Figure 2 illustrates the threats associated with the biometric component through a network in the biometric-verification process model (see Appendix II). In this model, each component sends processed biometric data to the next component (see clause 5.1 of [ISO/IEC 24761]). Compared to a general biometric functional model, in a telebiometric functional model, processed biometric data can be transmitted among components through telecommunications media, denoted as *NW* in Figure 2. Figure 2 shows that not only each component in the model, but also transmission among components, are vulnerable to outside attacks. Examples of outside attacks are the invasion from outside when biometric data are delivered to the next step or during the modification of processed biometric data.

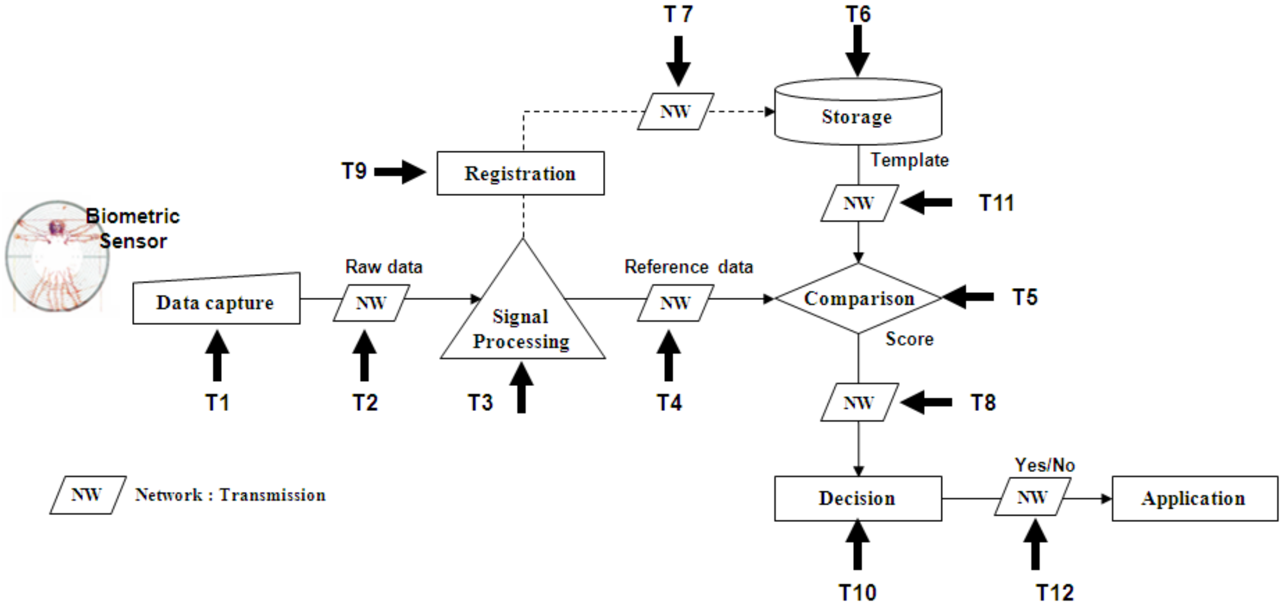

Figure 2 – Vulnerabilities in the telebiometric functional model

The threats associated with each component and transmission in the telebiometric functional model are listed and named as follows:

- T1: Threat to biometric input devices
- T2: Threat to the process of transmitting biometric raw data to the signal processing component
- T3: Threat to the signal processing component
- T4: Threat to the process of transmitting the extracted biometric templates to the comparison component
- T5: Threat to the comparison component
- T6: Threat to the biometric storage component
- T7: Threat to the process of transferring biometric templates from the registration component to the storage component
- T8: Threat to the process of transmitting the matching score from the comparison component
- T9: Threat to the registration component
- T10: Threat to the decision component
- T11: Threat to the process of transmitting the stored biometric template to the comparison component
- T12: Threat to the process of transmitting the decision result to an application system

Table 1 summarizes the relationships between the telebiometric components and the threats described above. For example, T1 can be a replay attack using artificial biometric samples in the data capturing process, and T2 can be a hacking of biometric data being transmitted between the data capturing component and the signal processing component. Appendix III describes the vulnerabilities and threats in the telebiometric system, see clause 6.3 of [ISO/IEC 19792].

In [ITU-T X.1082], the biometric modality is defined as one of the classifications of the interaction of a human body with its environment, based on the physical nature of the interaction or on the human sensory system that it affects, or based on a property of the human body that is determined, or changed, using one or more of the base modalities. Some of the limitations imposed by single biometric systems can be overcome by using multiple biometric modalities (see [b-JAIN]). Multibiometrics use a number of biometric traits and several algorithms for feature extraction, comparison, and decision (see [b-KISKU]). The advantages of multibiometrics are: non-universality encountered by single biometrics, facilitation of the filtering or indexing of large-scale biometric databases, and the difficulty for impostors to spoof using multiple biometric traits and fault tolerant systems (see [b-MOHAMED]). Multibiometric fusion occurs during the fusion in multiple biometric components, and increases the reliability of a biometric system by integrating comparison scores or features obtained from multiple biometric input devices (see [b-ROSS]).

Since sample-level fusion in the tele-multibiometric system can take place at various stages after the data capture until the application, multibiometric verification is used to represent multibiometric processing (see Figure 3). All the components are the same as in the generic telebiometric system (see [b-RATHA]), except that the multibiometric verification module replaces the biometric verification module. As a result, the possible vulnerable points in the multibiometric system coincide with those in the general biometric system.

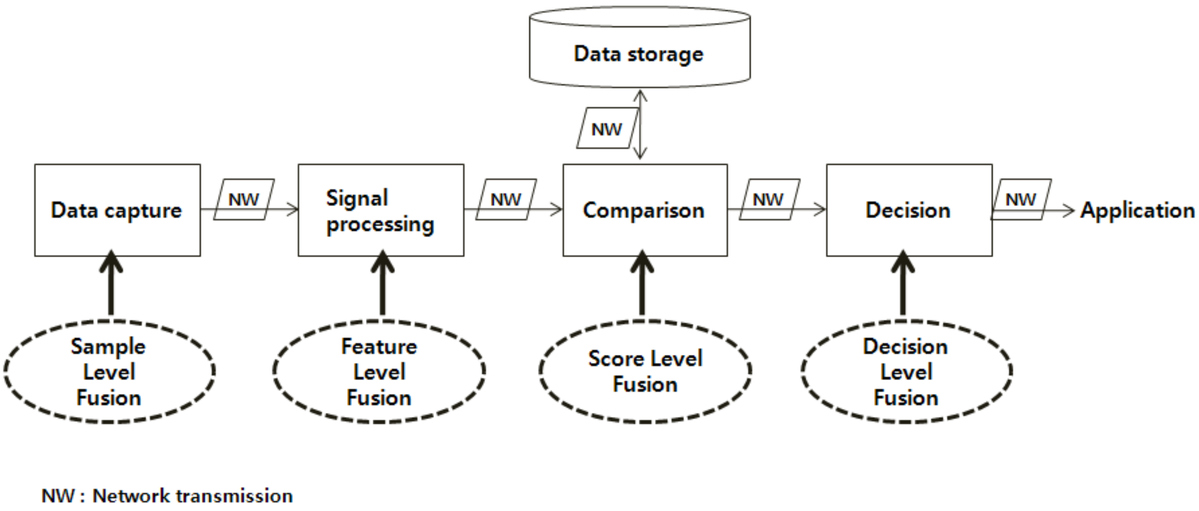

Figure 3 – Fusion level of the multibiometric system

Multibiometric verification is classified according to the fusion of the processing level: sample-level fusion, feature-level fusion, score-level fusion, and decision-level fusion. Each kind of multibiometric system has some fusion module in the proper level (see clause 19). For example, the sample-level fusion operates on several data capturing units because of threats in more than one biometric trait.

10) New clause 19

Add a new clause 19 as follows:

19 Protection on the fusion process of the tele-multibiometric system

Multibiometrics can overcome some of the limitations and reduce the failure rates of single biometrics. However, it should be noted that multibiometrics increases the processing time and add a level of complexity in combining multiple biometric data. Processing of multibiometrics involves acquiring multiple samples, extracting features from the samples, generating a set of comparison scores, and decision-making over the set of comparison scores.

Threats to a multibiometric system can occur during processing of multibiometric components in the telecommunication environment. Multiple biometric data can be fused in any processing module, data capture, signal processing, comparison, and decision, depending on the type of biometric information. Thus, threats existing in tele-multibiometrics are very similar to those in general biometrics. For example, biometric raw data and template can cause serious problems when leaked outside, i.e., the data can be utilized for replay attack.

19.1 Guideline for protection at the sample-level fusion

At the sample-level fusion in the multibiometric system, the module receives multiple biometric raw data from biometric input devices, and produces single biometric data derived from combination of the raw data. The fused biometric data are then transferred to the signal processing module for feature extraction (see Figure 4). Upon receiving raw data from the biometric input devices directly, the sample-level fusion module shall check whether the input data are genuine or not, because reproduced biometric raw data (e.g., fake finger, copy of a signature, fake face, etc.) can be used to attack the system. Furthermore, unacceptable raw data can be produced by input devices due to undetected defects of the devices.

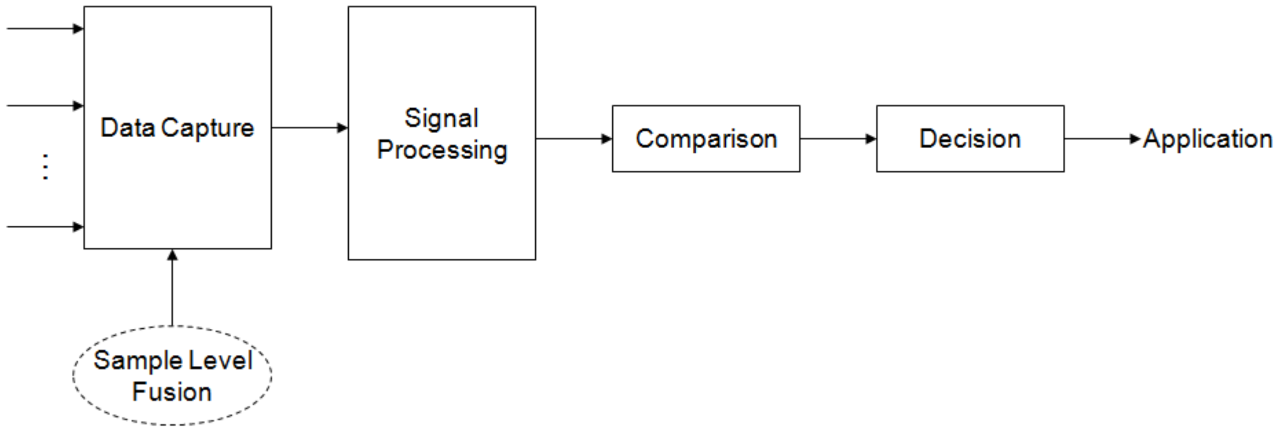

Figure 4 – Vulnerable points of the sample-level fusion

It is an important concern that when biometric raw data are captured by biometric devices, not only the unchangeable biometric raw data but also the user's private information can be exposed. Therefore, the fusion module at the sample-level shall be able to prevent the biometric raw data from being leaked out.

Possible attacks at the sample-level fusion of the tele-multibiometric system are as follows:

1) creation of incorrect fusion data by a malicious program

2) theft or modification of biometric data when acquiring biometric data by different input devices

3) absence of clear fallback in the case of an unfamiliar user, unless a special guideline is provided.

Protection methods against the above attacks are as follows:

1) provision of a firewall or a vaccine program to detect any malicious program

2) provision of a protection scheme to assure individual biometric raw data captured by each input device

3) provision of a proper fallback scenario for unfamiliar users.

19.2 Guideline for protection at the feature-level fusion

The feature-level fusion receives multiple sets of biometric sample data as inputs, transforms them to a set of features, and then combines the multiple features into a single feature or a feature vector. The combined feature set or vector is then, sent to the comparison module (see Figure 5).

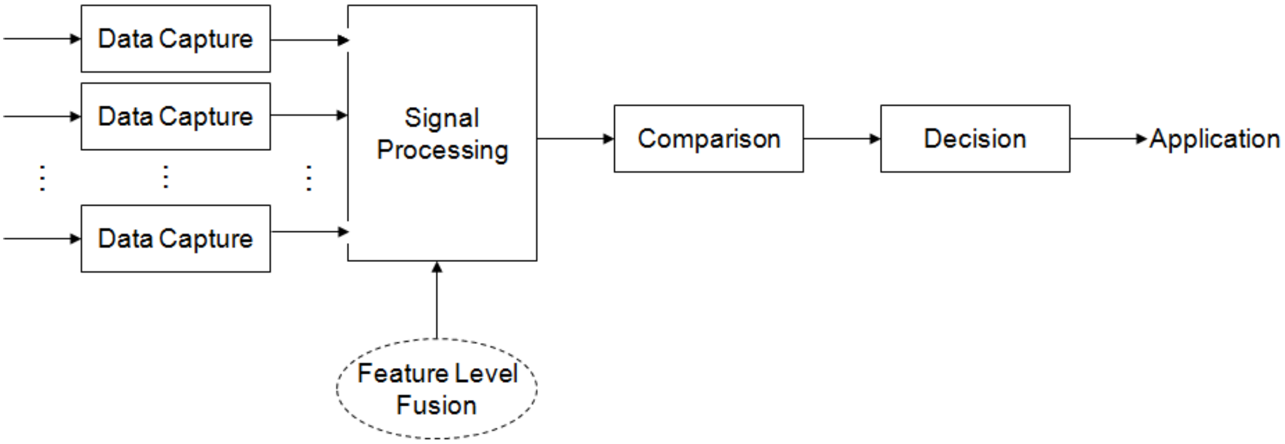

Figure 5 – Vulnerable points of the feature-level fusion

The following are possible attacks at the feature-level fusion:

1) incorrect fusion data can be created by a malicious program or an attack launched by the attacker

2) forged biometric raw data can be input to the feature-level fusion scheme.

Protection methods against the above attacks are as follows:

1) provision of a firewall or a vaccine program to detect any malicious program

2) provision of an appropriate method for checking whether the input raw data are forged or not.

19.3 Guideline for protection at the score-level fusion

The score-level fusion module accepts multiple features from more than one feature extraction module, produces a set of comparison scores based on individual features, and then either fuses the multiple scores into a single score or forms a vector of scores (see Figure 6). The result of the score-level fusion is to be transmitted to the decision module to make the final decision.

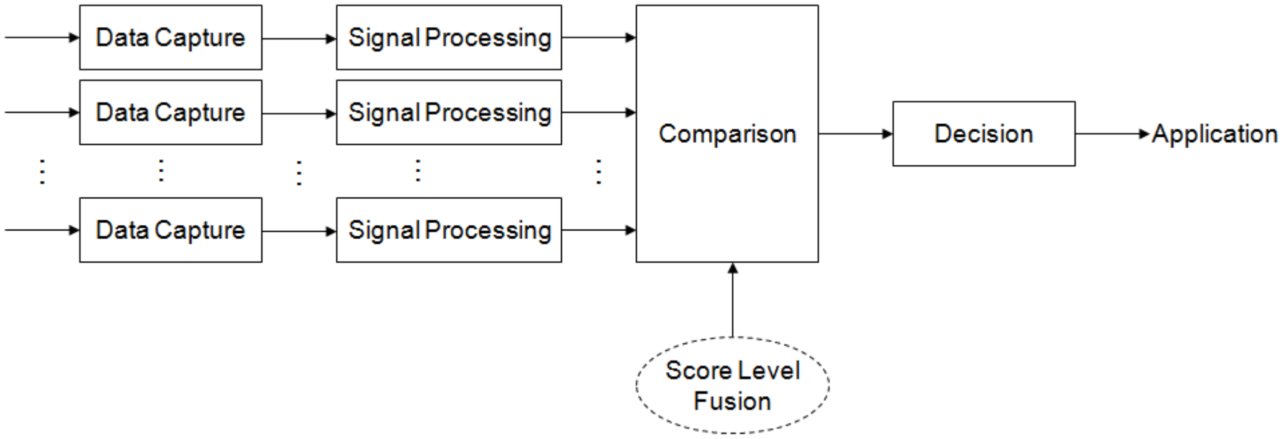

Figure 6 – Vulnerable points of the score-level fusion

The following are possible attacks at the score-level fusion:

1) Creation of incorrect fused matching data by a malicious program

2) Input of a forged feature to the score-level fusion module.

Protection methods against the above attacks are as follows:

1) provision of a firewall or a vaccine program to detect any malicious program

2) provision of an appropriate method for checking whether the input feature is forged or not.

19.4 Guideline for protection at the decision-level fusion

Decision-level fusion occurs after multiple comparisons are made for individual biometric features (see Figure 7). There are two different schemes in decision-level fusion. In the first scheme, the decision module formulates the set of multiple scores obtained from the multiple comparison modules as a single vector and dichotomizes it into ACCEPT or REJECT. In the second scheme, the decision module converts each comparison score individually into a Boolean value by thresholding, and aggregates the set of Boolean values using a voting function or a logical operation such as AND or OR.

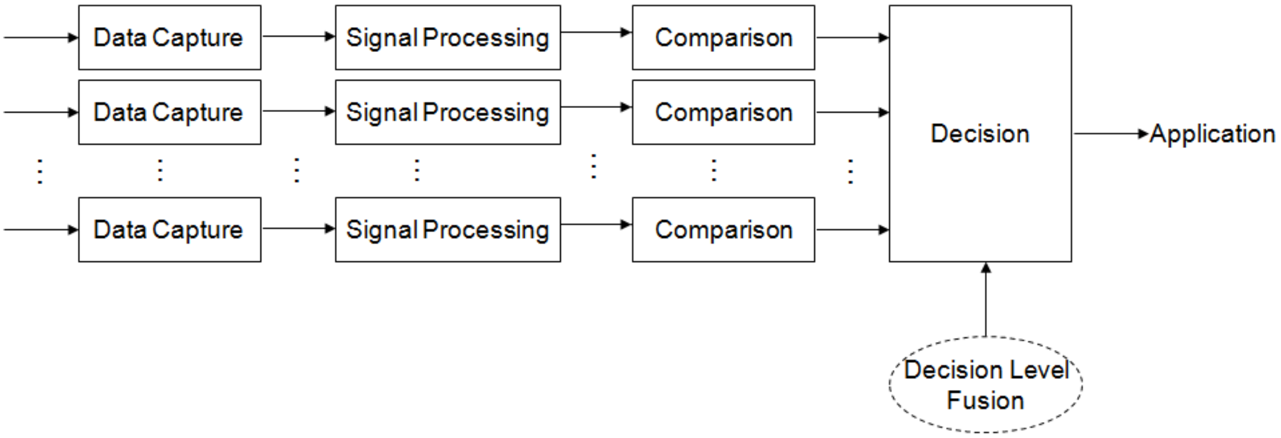

Figure 7 – Vulnerable points of the decision-level fusion

The following are possible attacks at the decision-level fusion:

1) incorrect decision can be created by a malicious program

2) a manipulated score can be entered from the comparison module.

Protection methods against the above attacks are as follows:

1) provision of a firewall or a vaccine program to detect any malicious program

2) provision of an appropriate method for checking whether the input score is manipulated or not.

11) Clause I.2.1 – Protection items at the client

Add the following sentences to item 3) Developer list:

3) Developer list

- Does the fusion module of the tele-multibiometric system provide any feature for examining whether the biometric data entered are genuine?
- Does the fusion module of the tele-multibiometric system provide any feature to examine whether or not the biometric data entered is from genuine input devices?

- Does the fusion module of the tele-multibiometric system provide any feature to prevent reuse of leaked multibiometric data?
- Does the fusion module of the tele-multibiometric system prevent malicious outside programs from handling multibiometric data?
- Does the tele-multibiometric system provide any feature to protect multibiometric data during transmission, such as the embedding of biometric data into host data?
- When enrolling a new user, does the tele-multibiometric system examine the recognition accuracy of each biometric modality and adjust its weight of reliability?

12) New Appendix V

Add a new Appendix V as follows:

Appendix V

Technical issues for multibiometric data protection

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

Recommendation ITU-T X.1086 defines the requirements and countermeasures for a secure and reliable telebiometric system, challenge-response, and time stamp, etc., in telebiometrics. In order to assure secrecy and privacy of biometric raw data, several techniques are possible, such as cryptography (see [b-PETITCOLAS]), digital watermarking (see [b-PETITCOLAS]), and cancellable biometrics (see [b-TEOH]). The use of standard cryptographic techniques can be a straightforward approach to guaranteeing the confidentiality and integrity of biometric raw data. Once decrypted, however, biometric data can be opened. Digital watermarking can be considered as a complement to cryptography. Data, called "watermark", is embedded within the content called "cover work", using digital watermarking. An embedded watermark is never removed during normal usage and can be designed to survive various attacks, such as decryption and compression.

Tele-multibiometrics utilize multiple sets of biometric data delivered through transmission channels, and should thereby be able to protect the biometric data in the fused manner. A general digital watermarking method can be used for fusion of multibiometric data. Embedding biometric raw data into other biometric raw data, or other unrelated data, has some advantages as follows:

- hiding information being transmitted
- protecting embedded data
- transmitting efficiently by reducing the amount of transmitted data.

To protect biometric data, a data-hiding method, such as steganography, can be applied (see [b-CHEN]). The purpose of steganography is covert communication, to hide the existence of a message from a third party. By hiding biometric raw data within arbitrary host data, the hidden biometric raw data does not attract attention and can be protected from attackers.

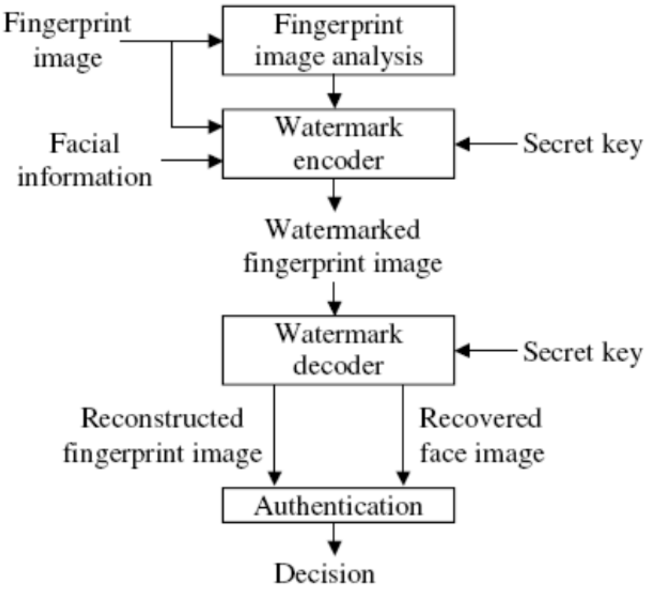

Figure V.1 – Embedding face information into fingerprint image

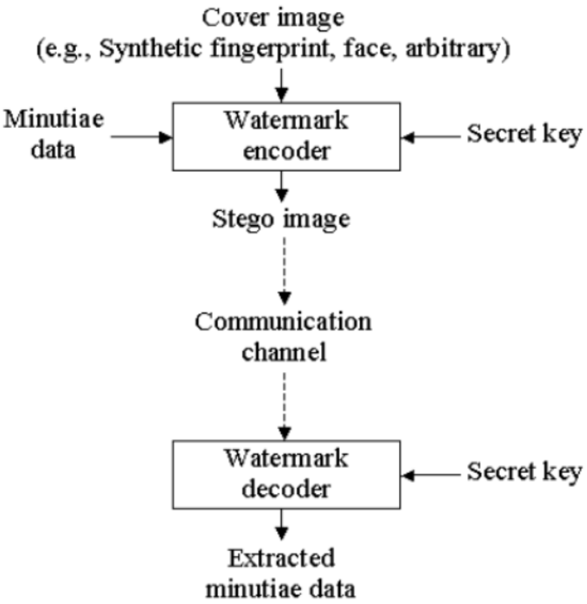

Figure V.2 – Hiding fingerprint information by embedding it within the cover image

13) Bibliography

Add the following bibliography:

Bibliography

[b-TR24722] ISO/IEC TR 24722 (2007), *Multi-Modal and Other Multi-Biometric Fusion.*

[b-TR29794-4] ISO/IEC TR 29794-4 (2010), *Information technology – Biometric sample quality – Part 4: Finger image data.*

[b-TR29794-5] ISO/IEC TR 29794-5 (2010), *Information technology – Biometric sample quality – Part 5: Face image data.*

[b-SC37SD2] ISO/IEC JTC 1/SC 37, Text of Standing Document 2, Version 7 (2007) – *Harmonized Biometric Vocabulary.*

[b-CHEN] Mei-Ching Chen, Agaian S.S., Chen C.L.P. (2008), *Generalized collage steganography on images, Systems, Man and Cybernetics*, pp. 1043-1047.

[b-JAIN] Anil K. Jain, Arun Ross, Multibiometric systems (2004), *Communications of the ACM*, Vol. 47, No. 1, pp. 34-40.

[b-KISKU] Dakshina Ranjan Kisku, Jamuna Kanta Sing, Phalguni Gupta (2009), *Multibiometrics Belief Fusion*, 2009 Second International Conference on Machine Vision, pp. 37-40.

[b-MOHAMED] Deriche Mohamed (2008), *Trends and Challenges in Mono and Multi Biometrics, Image Processing Theory, Tools and Applications*, IPTA 2008, pp. 1-9.

[b-PETITCOLAS] Petitcolas, Fabien A.P., Anderson, Ross J., and Kuhn, Markus G. (1999), *Information hiding-a survey*, Proceedings of the IEEE, Vol. 87, No. 7, pp. 1062-1078.

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

[b-ROSS] Arun Ross and Anil Jain (2003), *Information fusion in biometrics, Pattern Recognition Letters*, 24, pp. 2115-2125.

[b-TEOH] Andrew B.J. Teoh, YipWai Kuan and Sangyoun Lee (2008), *Cancellable biometrics and annotations on BioHash, Pattern Recognition*, Vol. 41, No. 6, pp. 2034-2044.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2012