



Global Business Dialogue on Electronic Commerce

GBDe 2008 Issue Group Cyber Security

*Issue Chair: Dr. Jyh-Sheng Ke, Senior Fellow,
Information-technology Promotion Agency, Japan*
*Issue Group Members: Mr. Junzo Nakajima,
Vice President and Executive Officer Hitachi, Japan
CyberSecurity, Malaysia (G Member Only)*

1. Introduction

The British government, on September 25, 2008, unveiled a new biometric Identity Card for foreigners in the country, replacing the old paper document identification. The British government hopes that this card will provide protection from identity fraud, illegal workers, multiple identities, etc. Financial institutions have introduced palm or finger vein authentication systems for their Automatic Teller Machines (ATMs) in Japan.

Biometric authentication is attracting a lot of attention. Fingerprint authentication, traditionally used for access control within a company's building or facility, is now also being used at condominium entrances. Personal identification is becoming more important in e-commerce, and biometric authentication is a key technology for personal identification.

With this in mind, the GBDe Cyber Security Issue Group is focusing on biometric authentication systems for IT security. The work is intended for those who are considering the introduction of biometric authentication systems, those who are responsible for information systems or decision-making, and those who are in charge of biometric authentication systems already installed in their organizations.

As far biometric authentication is concerned, there are two opposing opinions: Either biometric authentication is an ultimate authentication method, meaning that it is perfectly secure, or biologic information can be forged and compromised and therefore is not as secure as it seems to be.

This document provides information on biometric authentication systems with the objective of giving a better perspective on the misapprehensions of biometric authentication security. Biometric authentication is neither completely secure nor extremely vulnerable. In order to properly use biometric authentication, it is important to have sufficient understanding of the characteristics and to choose a

system that is suitable for the intended usage. In other words, one can learn how to use biometric authentication in an appropriate fashion by understanding the advantages of introducing and using biometric authentication in the context of greater information security challenges.

2. Overview of Biometrics

2.1. What is Biometrics?

Biometrics is a method of authentication based on the measurement of biologic characteristics. Biologic characteristics are generically called “Biologic Information.” Biologic information includes physiological characteristics (such as fingerprints, faces, etc.) or behavioral characteristics (such as vocal patterns, signature, etc.) Physiological characteristics are related to a part of the human body while behavioral characteristics are related to the person’s mannerisms, which are repeated behavioral characteristics.

Unlike other authentication methods that use passwords or physical cards, biometrics provides an authentication where “keys” can’t be forgotten or known by others, lost, stolen, or left somewhere, because the system takes biologic input directly from the user and compares it to the information on the template. However, there are cases where biometric inputs are used in conjunction with smartcards or keys. In these cases, “false accepts” are still avoidable, but “false rejects” are possible if the user loses their keys or smartcards.

2.2. Advantages of Introducing the Biometric Systems

Introduction of biometric systems brings the following advantages:

i. Provides a convenient identity verification method

Because biometric systems use biologic information that has a unique and permanent characteristic, users do not need to carry identity cards or to remember passwords to prove their identities.

ii. Decreases the likelihood of theft or loss of sensitive information for user authentication

Confidential information used for the biometric systems is biologic information. Use of this biologic information decreases the likelihood of theft and loss of confidential information.

iii. Allows system providers to adjust the level of security and availability based on the purpose of intended usage of the systems

For biometric systems, input on biologic information and enrolled information are verified for authentication. The system providers can set acceptable values or thresholds indicating the degree of similarity between the input data and stored data depending on the level of security and availability required by the intended usage.

Biometric systems do not always assure high security. The advantage of these systems is the decrease in the likelihood of sensitive information being lost, forgotten, or stolen, while providing a relatively high level of reliability. It also enables system providers to adjust the level of security.

2.3. Overview of Biometrics Techniques

2.3.1. Biometric Mechanism

For biometrics authentication, input characteristics data and registered characteristics data are compared to calculate the similarity score. If the score is high, the user is authenticated. The input characteristics data can vary depending on environmental conditions such as humidity and temperature. Therefore, the input characteristic data does not always exactly match the characteristic data stored in the database.

For this reason, the calculated similarity score is compared with the threshold set by the system provider so that the system can determine whether the user is enrolled or not. Figure 1 shows the process flow of the biometrics authentication.

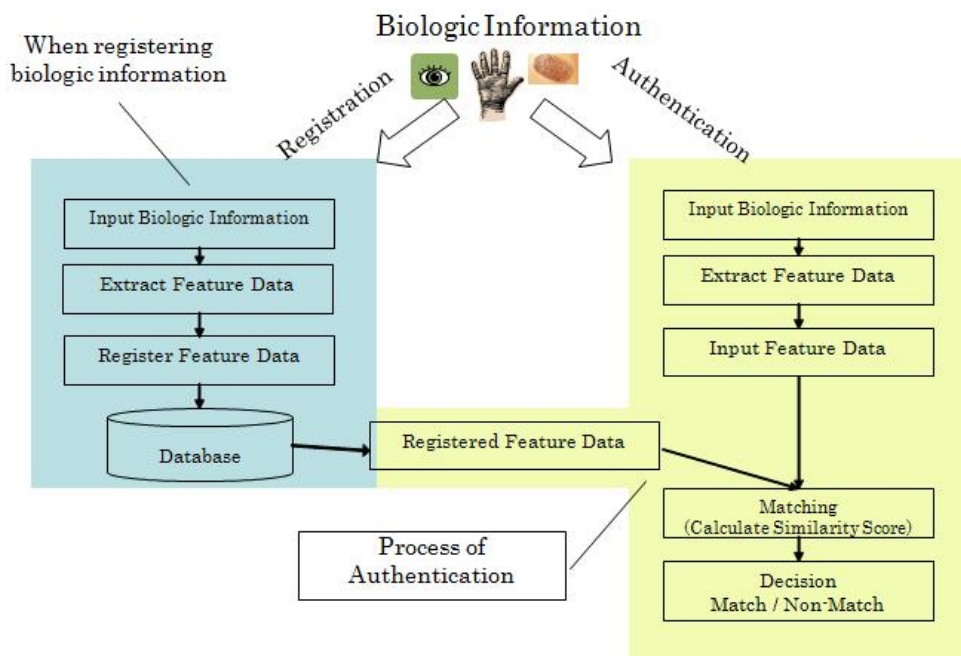


Figure 1 - Processing Flow of Biometric Authentication

2.3.2. Thresholds, False Reject Rate (FRR) and False Accept Rate (FAR)

No matter what value is specified for the thresholds, it is impossible to preclude the possibility that a biometric system fails to identify an enrolled individual or incorrectly accepts an individual who is not enrolled.

Just like any other authentication method, biometric systems can make errors. Based on the operational environment and application, appropriate values should be specified for error rates, taking into account the security risks and convenience. The probability that a biometric system fails to identify an enrolled individual is called False Reject Rate (FRR) while the probability that it accepts an individual who is not enrolled is called False Accept Rate (FAR). Both rates should be included in the security requirements.

2.3.3. Trade-off between Convenience and Security

The lower the FRR, the higher the FAR will be. On the contrary, if you lower the FAR, FRR becomes higher. The former is a convenience-oriented authentication and the latter is a security-oriented authentication.

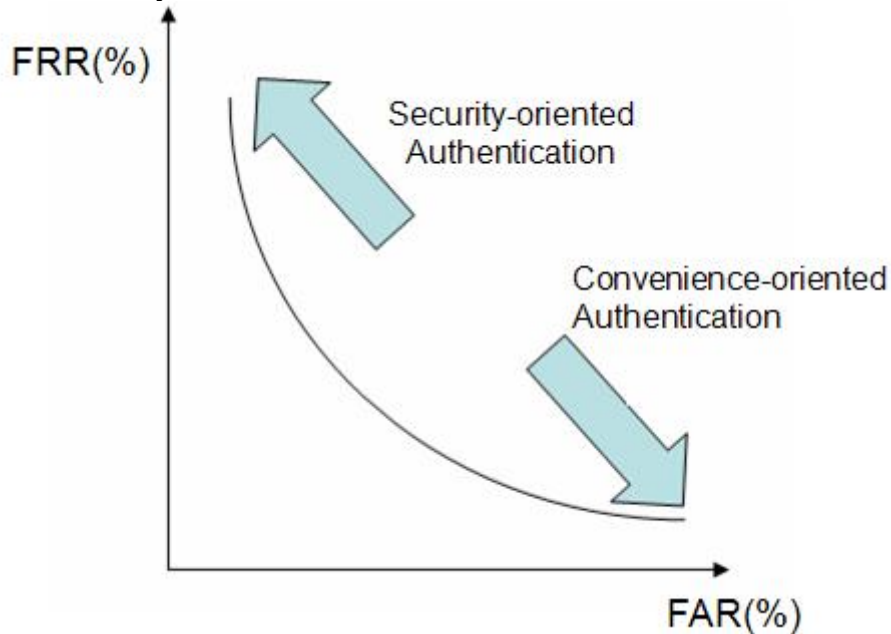


Figure 2 - Correlation between Security and Convenience with Changes to the FRR and FAR

2.3.4. Unrecognizable Rate

There are people whose finger patterns are barely recognizable by fingerprint authentication systems. The same problem can arise when using other biologic information. The rate in which input information is not recognized by the biometric authentication devices or algorithm is called the unrecognizable rate.

There are cases where manufacturers of biometric devices conduct an accuracy evaluation using only biologic information recognized by the devices. System administrators are recommended to check the unrecognizable rate and other information that cannot be recognized by the device.

3. Biometric Technology

In this section, typical authentication technologies using biometrics are discussed.

3.1. Fingerprint Authentication

3.1.1. Overview

A fingerprint is an impression of the friction ridges of all or any part of the finger.

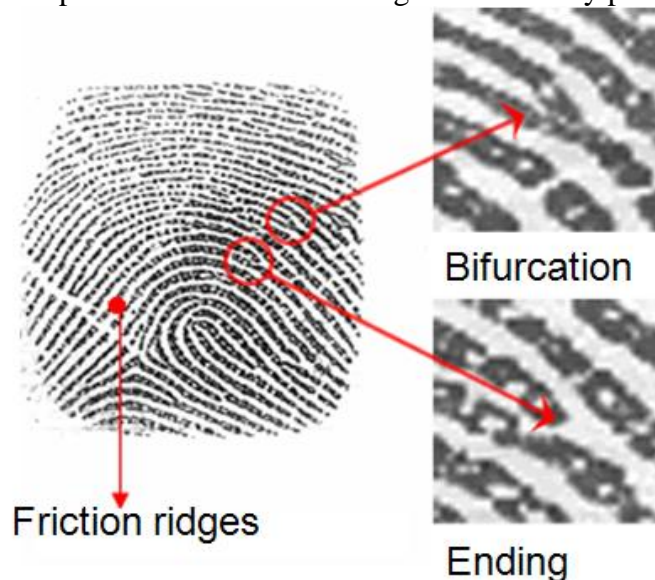


Figure 3 - Friction ridges, Bifurcation, and Ending
Online Magazine “COMZINE,” March 2004 Issue

*Touch-up was done to a picture in
“<http://www.nttcom.co.jp/comzine/no010/dragnet/>”

There are two fingerprint authentication methods, which are the Minutia Method and the Pattern Matching Method. The Minutia Method collects Minutia (ridge ending and bifurcation points) from the user’s fingerprint and calculates data including the coordinates, types, and directions of the Minutia. The Pattern Matching Method converts all the information on the fingerprints into data format and compares with registered data.

3.1.2. Characteristics

Characteristics of a fingerprint authentication system are;

- i. High technical maturity.
- ii. Susceptible to moisture or damage.
- iii. Introduction cost is low.
- iv. Difficulty in registering the fingerprint in some cases.

3.2. Vein Authentication

3.2.1. Overview

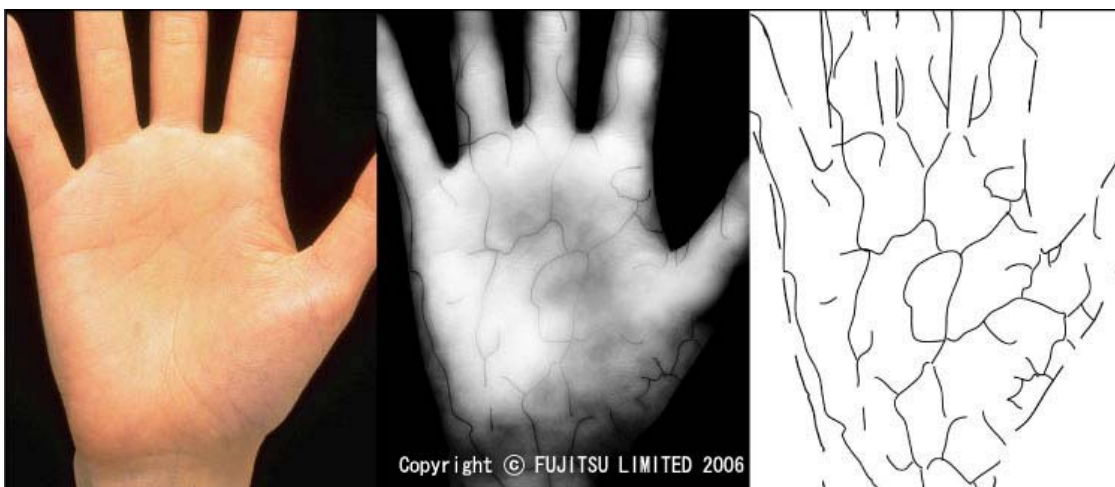
Vein patterns, which include veins and arteries, are unique and permanent. Since this information resides inside the human body, it cannot be seen by others and is hardly changed by external factors.

Vein Authentication includes;

- i. palm vein authentication
- ii. backhand vein authentication, and
- iii. finger vein authentication.

A number of financial institutions are introducing palm vein and finger vein authentication.

Vein Authentication uses an infrared camera to capture the vein pattern on one's palm or finger and extracts these patterns from the picture. As in the case of fingerprint authentication, the extracted vein patterns are compared to the registered patterns, using the Minutia Method or Pattern Matching Method.



(a) An Image taken with a normal camera (b) An Image taken with an infrared camera (c) Outline of one's palm and vein patterns extracted

Figure 4 - Palm Vein Patterns

3.2.2. Characteristics

Characteristics of a vein authentication system are:

- i. Difficult to counterfeit.
- ii. Only a few people are likely unrecognizable or cannot be registered.
- iii. Has a high level of authentication accuracy.
- iv. Introduction cost is high.

3.3. Iris Authentication

3.3.1. Overview

The human eye has a flat colored part called the Iris, which has tiny muscles that enlarge and reduce the size of the pupil. These muscles have creases that become permanent after the age of two. Crease patterns are captured using a camera and compared with the registered information.

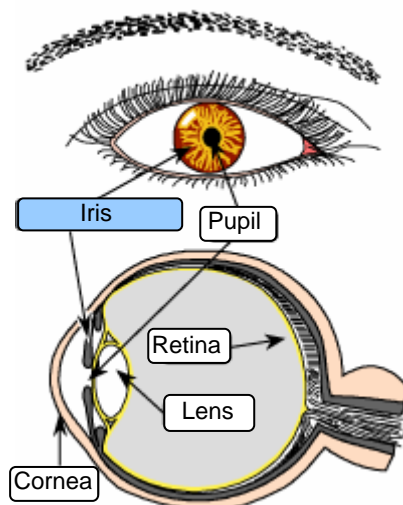


Figure 5 - Iris

Presented by Japan Automatic Identification Systems Association

*This diagram is quoted from

<http://www.jaisa.or.jp/action/group/bio/Technologies/Iris/Irs-00.htm>

3.3.2. Characteristics

Characteristics of an Iris authentication system are;

- i. Has a low level of FAR.
- ii. Hard to counterfeit.
- iii. Introduction cost is high.

3.4. Face Authentication

3.4.1. Overview

A face authentication system scans one's face and extracts data including coordinates of the characteristic points that outline the face and the points indicating the relative position of the eyes, nose, and other parts of the face. The distance between these points and angles, curvature, surface color, and shading are used for verification.

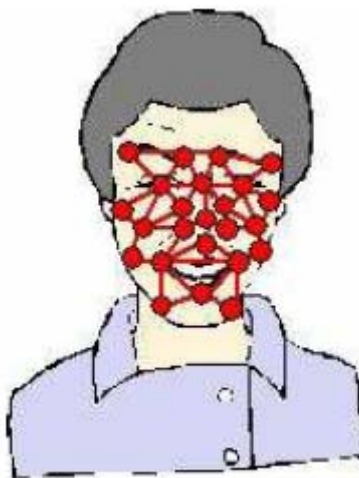


Figure 6 - Example of Characteristic Points Used for Face Authentication

See Section 5-1-1-3-2 “Screening facial characteristic points extraction,” in the “Input and recognition of biometric verification systems,” in the FY2004 Standard Technologies.

Quoted from

http://www.jpo.go.jp/shiryou/s_sonota/hyoujun_gijutsu/biometric/5-1-1.pdf

3.4.2. Characteristics

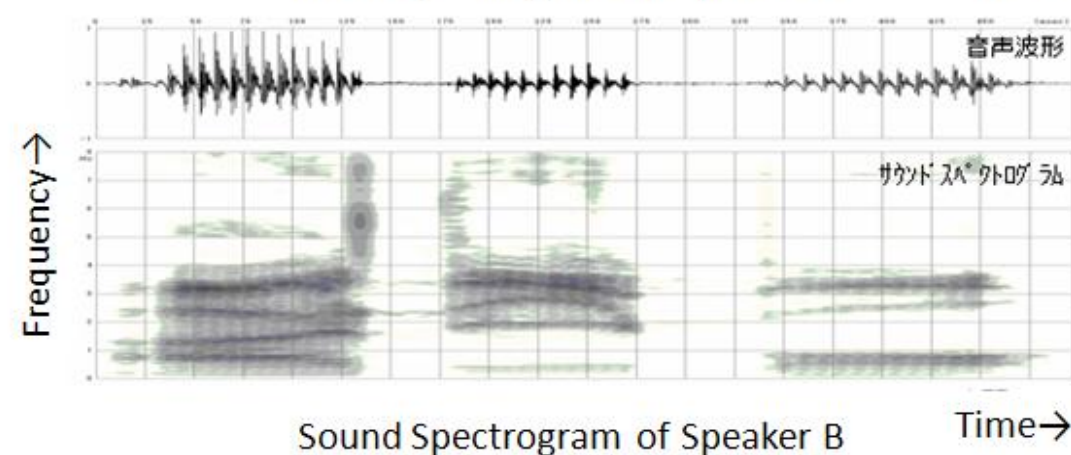
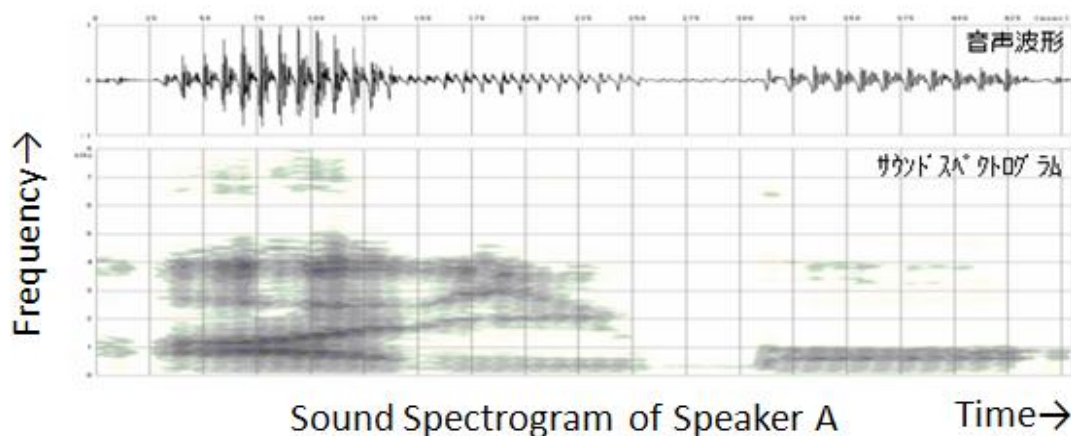
Characteristics of a face authentication are:

- i. Users do not need to go through cumbersome procedures when they need to be enrolled or authenticated.
- ii. May fail to identify and enroll an individual depending on the face angle.
- iii. Re-registering is necessary every few years.

3.5. Voice Authentication

3.5.1. Overview

Voice authentication takes voice signals and visually represents them as a spectrogram, in which frequency is plotted against time, or transforms them into other data formats that contain equivalent information. During the identity verification process, input data and registered data is compared.



Copyright (C) ANIMO LIMITED 2007

Figure 7 - Example of voice patterns used during voice authentication

3.5.2. Characteristics

Characteristics of voice authentication system are;

- i. Introduction cost is low, since the system can be built using just a microphone and software program.
- ii. The false acceptance error or false rejection error can be high depending on the health condition of the user because of changes in sound waveform.
- iii. FRR might also increase due to noise.

3.6. Signature Authentication

3.6.1. Overview

Signature authentication collects data such as the coordinates of pen tips or writing pressure, etc. from a signature written on a tablet or other coordinates input devices at regular intervals. During the identity verification process, the input data and the registered data are compared.

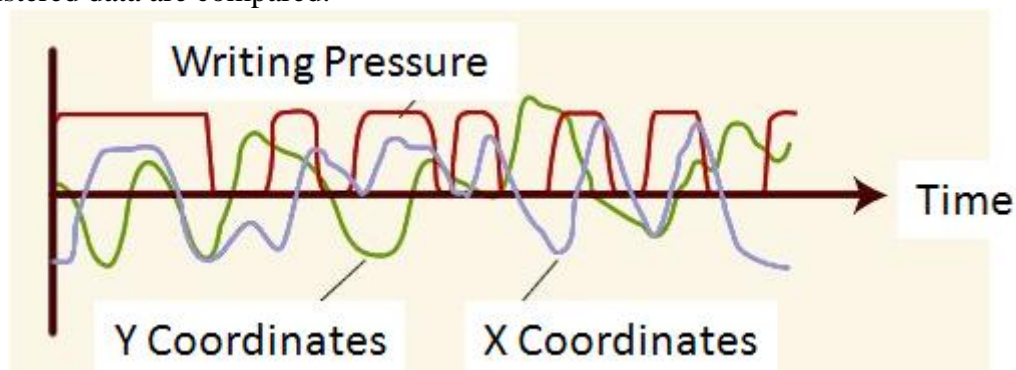


Figure 8 - Changes in the positions and pressure of a pen; this data is used during the signature authentication process
Quoted from the Website of Witswell Consulting & Services Inc.
See <http://www.witswell.co.jp/cybersign/wm/syogo.htm>

3.6.2. Characteristics

Characteristics of a signature authentication system are;

- i. Registered data (signature) can be changed based on the user's request.
- ii. Users who cannot hold the pen for reasons such as injury cannot use the system.
- iii. Relatively easy for an attacker to copy an authorized user's handwriting, as compared to other authentication methods

4. Challenges for Application of Biometric Authentication Technology

In this section, we look into typical fields where biometric authentication technology is applied and challenges for its implementation.

4.1. Where Biometric Authentication Technology is Applied

4.1.1. Used in Various Fields where Personal Identification is Required

Fields where biometric authentication technology are applied can be classified into logical and physical access. Logical access is access to a system or IT device and physical access is access to a building or other areas. Typical fields where biometric authentication technology is applied are as follows:

- i. Logical access
 - Private sector: financial transactions, settlement service (access to ATM)
 - Public sector: criminal investigation
 - Both in private and public sector: information security (access to a PC or server)
- ii. Physical access
 - Private sector: personal assets (access to shared space in a condominium)
 - Public sector: national security (immigration control)
 - Both in private and public sector: valuable goods/regulated items/important installations (access to a building or facility)

4.1.2. Fields where Biometric Authentication Technology is Applied (in Japan)

In Japan, biometric authentication technology is applied in files listed below. In particular, finger vein authentication is widely used for ATMs.

- i. Information security: users log on to a PC by presenting their finger print. Use of finger vein authentication is also increasing.
- ii. Access control for those entering and leaving a specific area: finger print, face, iris, vein etc.
- iii. Financial transactions: palm and finger veins have begun to be used for authentication. To prevent ever-increasing incidents caused by falsification and stolen cards, city and regional banks installed ATMs with vein authentication devices attached, which are used for depositors' personal identification.
- iv. Mobile Phones: mainly, finger print is used for authentication.

4.2. Challenge for Biometric Authentication

In spite of the advancement made in biometric systems, there are concerns and issues that need to be addressed. Biologic features are permanent - therefore any breach on the biometric database causing biometric information to be stolen will render the biologic input useless for a long time. To mitigate this, database administrators usually encrypt the database. Other main issues are:

- i. Authentication accuracy
 - False Rejection Rate (FRR) (usability) and False Acceptance Rate (FAR) (security) are trade-offs that need to be balanced with regards to the intended use of the system.
- ii. Counterfeiting
 - Biometric authentication methods can allow malicious users to counterfeit biometrics information. This can be handled by having 'Difficulty in making a

copy' and 'Difficulty in acquiring' biometrics samples. In short, authentication methods requiring no specific technique for creating imitations and easily available items are easy to exploit as compared to those using hard-to-imitate biometric samples and items difficult to be obtained in daily life.

iii. Information Security

Vulnerabilities may exist in any process stage for biometric authentication. Those vulnerabilities can allow malicious users to easily imitate or falsify functions or data, or compromise data.

iv. Vulnerability inherent in biometrics

There are three factors that can be the sources of vulnerabilities in biometrics;

- It is not easy to consciously keep biometric information confidential
- Biometric information cannot be created an infinite amount of different ways
- Biometric information is personal information

5. Points to Remember when Implementing and Operating Biometrics Systems

This section is intended for system administrators and integrators involved in the implementation of biometric systems. The contents include basic knowledge and individual measures pertaining to the implementation and operation of biometric systems.

5.1. Implementation Phase

i. Clarify the Purpose of the System and Usage of Biometrics

At the beginning of the implementation phase, it is important to clarify the purpose of the system and the use of biometrics.

For example, for the access control system of a server room within a data center which requires a high level of confidentiality, priority should be given to preventing unauthorized access through impersonation, even if the system may force users to go through complex procedures to enter the room. On the other hand, for an organization's attendance management systems, priority should be given to confirming employees' identities in a quick and accurate manner. The purpose of the system and how to use biometrics can be clarified by adjusting FRR and FAR as follows:

Table 1 - Purpose of the System and How to Use Biometric Authentication

Purpose of the System	How to use Biometric Authentication
Confidentiality-oriented systems (i.e. primary objective is to prevent impersonation and allow only those having permission to enter the room.)	Focused on keeping FAR low.
Convenience-oriented systems (i.e. primary objective is to prevent FRR)	Focused on keeping FRR low.

ii. Ensure the Accuracy of Authentication

Accuracy of biometrics varies depending on a number of conditions. Although there are differences between each type of biologic information, the following

information extracted from each biometric device is checked:

- Number of people who can be enrolled
- Validity period for biologic information (Year)
- Whether users can modify their registered personal information
- Whether the device is outdoor-safe
- Water resistance
- Temperature
- Humidity
- Illumination intensity

iii. Biologic Information Registration

As for the registration of biologic information, the following points should be noted:

- Provide a facility to check and prevent unnecessary information, attached to the biologic information, from being registered.
- Provide a facility to show the difference between biologic information registered in the past and the one the user is going to register.

In general, the above points:

- are required for a system that needs to ensure a high level of confidentiality by keeping FAR low, and
- are required for any biometrics device regardless of their purpose of usage.

iv. Biologic Information Management

To appropriately manage sensitive biologic information, the following functions should be provided;

- Access control to distinguish the system administrators from other users.
- Preventing users other than the system administrators from accessing biologic information stored in the database.
- Preventing falsification of biologic information.
- Allowing the system administrators to delete biologic information.
- Encrypting biologic information when registering.

v. Alternate Functions

When providing substitute functions for biometrics, the following points should be noted;

- Select an appropriate method to realize the function (the method should also be applicable to individuals whose information cannot be handled by biometrics.)
- Change of the accuracy level of authentication (it is preferable to keep the same level of authentication accuracy.)

5.2. Operation Phase

i. Verification in the Real Operational Environment

Before beginning the operation of the biometric system, conduct an exhaustive test of the system in the real operational environment so that changes in authentication accuracy can be observed and specify the appropriate value for thresholds based on the purpose of the system.

For system verification, the following points should be noted;

- Enroll the same number of people as in the case of the real operation.

- Use the same system configurations and functions as in the case of the real operation.
 - Collect and analyze environmental data, i.e. temperature, humidity, illumination intensity, whether the system is used indoors or outdoors, etc., on a daily, weekly, monthly, and yearly (if possible) basis.
- ii. Operation manual for the system administrators should include how to handle biologic information and points to be noted regarding the use of the system
The operation manual for the system administrators should include;
- Procedures for registering personal information including biologic information
 - Tasks to be completed by system administrators (identity verification through face-to-face communication or signed documents.)
 - Rules to be followed by general users when using the system.
 - Procedures for referring to personal information including biologic information
 - Requirements for enabling reference to the information.
 - Procedures for referring to the information.
 - Procedures for modifying personal information including biologic information
 - Requirements for enabling modification of the information.
 - Procedures for modifying the information.
 - Procedures for deleting personal information including biologic information
 - Requirements for deleting the information.
 - Procedures for deleting the information.
 - Procedures for testing modification to the system configuration
 - Requirements for modifying the system configuration.
 - Procedures for modifying the system configuration.
 - Procedures for verifying the system
 - Requirements for system verification when necessary
 - Items and procedures for verification.
 - Frequency of verification
 - Procedures for auditing the system
 - Timing for auditing the system
 - Items and procedures for auditing
 - Points to be noted regarding the use of the system
 - Alternatives used in case the system fails to identify an enrolled individual.
 - How to respond to incidents (such as when false acceptance is detected, or when a system failure occurs.)
- iii. Security in System Settings and Modifications
When making system settings and modifications, consider security issues and note the following points:
- Allow only the system administrators to make system settings and modifications through an access control.
 - Select an appropriate method to authenticate the system administrators.
 - To prevent from looking over one's shoulder, choose a safe place for setting work.
- iv. Creation of Manuals for Users
For the appropriate operation of the system, create manuals for users and revise when necessary. The manual should include:
- The Purpose of the System

Whether the system is used where high level confidentiality is required or a high level of convenience is required.

- How to Use the System
 - How to register biologic information (Describe the procedures for registering the information in detail)
 - How to authenticate biologic information (Describe how the system conducts authentication of the information in detail)
 - How to respond to failures in the biometrics (such as FRR)
- Other Points to be noted
 - What may happen during normal operation (i.e. the system may fail to identify an enrolled an individual depending on the environmental conditions, i.e. weather conditions)
 - Biologic information is not permanent, therefore, it should be updated as and when needed.

v. User Training on How to Use the System based on the Users' Manual

For appropriate operation of the system, users should be trained on how to use the system following the instructions in the users' manual. The training should be done in the real operation environment and the training program should include:

- How to register biologic information
- How the authentication is done in detail
- How to respond to failure in the biometrics (such as FRR)

vi. Audit

A system audit should be carried out after a lapse of several months (since the beginning of operation.)

The following items should be examined during the audit of biometrics systems:

- Comparison with system purpose and the items described in the administrator's manual.
- Comparison with items described in the administrator's manual and the real operation.
- FAR, FRR, and others.

6. Conclusion

The type of biometrics authentication that is being used in various fields has two major characteristics:

- Levels of security and convenience pertaining to biometric systems vary depending on how the device is used and the level of authentication accuracy required by the user. These levels are affected by:
 - The part of the human body that will be presented as the biometric information.
 - The location where the system is installed.
 -
- Configuring the system in a way that best suits the user's environment may provide "accessible security", however, inappropriate settings can result in a lower level of security than expected.
- Using biometric information for user authentication significantly reduces the

probability of information being forgotten, lost or stolen. In case of other authentication mechanisms, users would not be able to get through the authentication process if they forget the information to be presented (e.g. password) or if they lose their cards containing such information, or even worse, their information might be abused by others to gain unauthorized access if the information was stolen. On the other hand, since biometric information is invariant, even if the system containing the biometric information was compromised and modified, the owner of the information would simply not be able to use it for authentication. However, if the user is injured or sick in a way that would change the biometric information presented, it will not match the one contained in the system. As a result, the user might not be able to use their biometric information temporarily.

In conclusion, the GBDe Cyber Security Issue Group recommends the promotion of using biometric authentication mechanisms to ensure secure e-commerce. Since biometric authentication does not require user to hold special knowledge, memorize information or possess cards containing identity, it can be used for various purposes. To promote a secure use of biometric authentication systems as a convenient tool, security awareness training should be given to the users so as not to use them in an inappropriate manner. In addition, tools that provide them with adequate information should also be developed.