Prototyping Security Test Objects for Use with Advanced Biometric Authentication Systems

Tsutomu Matsumoto
Graduate School of Environment and Information Sciences
YOKOHAMA NATIONAL UNIVERSITY
79-7 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan
tsutomu@ynu.ac.jp

ABSTRACT

The state-of-art methodology to measure or assess security of advanced biometric authentication systems is updated.

Categories and Subject Descriptors

C.4 [**COMPUTER SYSTEMS ORGANIZATION**]: Performance of Systems – *Measurement techniques, Reliability, availability, and serviceability.*

General Terms

Measurement, Reliability, Experimentation, Security

Keywords

Information Security, Biometrics, Test Objects

SUMMARY

Compromise of biometrics will be serious since they are hard to replace because they are intrinsic to person. Therefore, biometric systems must possess the function to effectively reject fake biometric objects or patterns as well as to protect the template data against abuse. We discuss how to measure the security of each biometric system against attacks using fake biometric objects. Existence of such measuring methods is very important for establishing the way to describe the required, the designed, and the really providing level or quality of security of each biometric system.

We will introduce the state-of-art methodology to measure or assess security of advanced biometric authentication systems such as those based on

(1) iris patterns captured by reflected infrared light,

(2) finger prints captured by transmitted visible light,

(3) vein patterns captured by transmitted or reflected infrared light.

As a test object for iris authentication systems (1), so far we introduced the eye-picture-printed paper with punctured pupil part with the method to use it. Today we have purely artificial test objects. Namely there is no need to look through the hole.

In reference [1], we introduced “gummy finger” approach to measure security of fingerprint authentication systems based on optical, capacitive, electric-field, electro conductive, thermal, or pressure sensors. We will update this topic with the latest information. Some system in category (2) is the only --- to the author’s knowledge --- actually commercialized fingerprint authentication system that is claimed "gummy finger" resistant. We confirmed that the system successfully rejects gummy fingers but also proved that there are certain test objects that cannot be rejected by the system. The researchers who developed the system celebrated our results and told the interest to clarify why such vulnerability does exist.

Another result we will present relates to vein pattern authentication systems (3) which deployment is rapidly increasing in Japan. What are suitable test objects and methodology to distinguish security of each biometric system in this category? We can show you some partial answer to the question based on our brand new study using white-box finger and palm vein pattern authentication systems.

The general idea of the security measurement can be depicted as Figure 1.

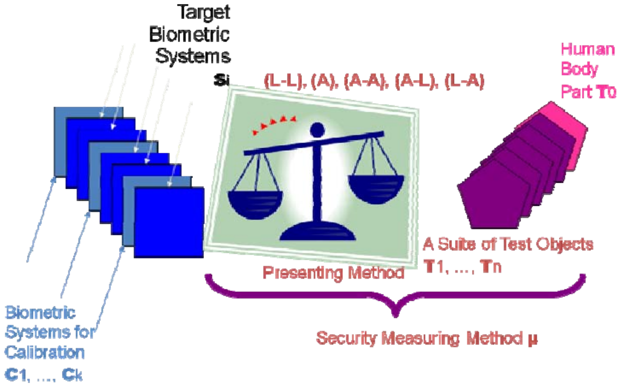

Figure 1. The Security Measuring Method for Biometric Authentication Systems

ASIACCS’08, March 18–20, 2008, Akihabara, Tokyo, Japan.

REFERENCE

[1] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, “Impact of Artificial "Gummy" Fingers on Fingerprint Systems,” *Proceedings of SPIE*, 4677, 2002, pp.275-289.