

ICS 35.240
CCS L 70



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 45910-2025

**Information technology - Performance testing of biometric
template protection schemes
(English Translation)**

Issued on: June 30, 2025

Implemented on: January 1, 2026

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms and Definitions
4 Abbreviations
5 Compliance
6 Biometric identification template protection method (informative)
6.1 Overview
6.2 General Architecture of Biometric Template Protection System
6.3 Data Separation
6.4 Typical Architecture Example of Template Protection System
7 Overview of Performance Evaluation of Biometric Template Protection Schemes
7.1 Methods of attacking biometric template protection systems
7.2 The need for metrics beyond traditional recognition performance
7.3 Technical Assessment
7.4 Theoretical and Experimental Evaluation
7.5 Threat Model
8 Performance metrics of biometric template protection systems
8.1 General Principles
8.2 Multi-biometric access control system case
8.3 Registration and Verification Performance Metrics
8.4 Security and Privacy Protection Performance Metrics
Appendix A (Informative) Performance Evaluation Using Algorithms or Publications
Reference

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting.

This document is equivalent to ISO/IEC 30136:2018 "Information technology - Performance

testing of protection schemes for biometric templates".

Introduction

The protection method and protection scheme performance evaluation in the field of biometric recognition template protection, and stipulates the accuracy, the confidentiality and privacy assessment method aims to scientifically and objectively evaluate the biometric recognition template protection scheme.

A biometric template is a set of reference biometric features obtained from an individual's biological and behavioral characteristics and stored in a registration database.

The general system allows a limited number of times to revoke and update the biometric registration information that has been violated. However, the unique information that an individual can extract is the number of unique biometric features is limited, so biometric registration information cannot be revoked indefinitely like a credit card number or password.

and update. The infringement of biometric registration records stored in the registration database is a serious problem.

In a control system, an attacker can obtain biometric data of registered individuals by invading the registration database.

If the attacker can perform a presentation attack or replay attack, the attacker can disguise himself as an individual through the biometric data of the individual registered database that he has hacked into.

Furthermore, if the biometric registration database contains unprotected patterns, If the same biometric recognition modality is used in multiple applications, the attacker can link individual accounts in these applications.

Therefore, we need to adopt various methods and procedures to reduce the risk of infringement and protect the individual biometrics in the registration database.

Confidentiality of object feature recognition templates.

Currently, biometric recognition template protection technology has achieved the goal of not needing to store individual biometric items directly in access control devices.

The basic principle of this method is that the access control system does not store the biometric items directly, but obtains the biometric information from the biometric information.

The system derives some data from the item and stores the extracted derived data on the device.

Individuals collect biometric samples, which are then compared with derived data to

produce biometric verification results. Derivative data has almost or completely the key features of the biometric information collected during the registration phase are not revealed. Even if the access control device is compromised by an attacker, only the derived data falls into the hands of an attacker, but this data does not enable the attacker to recover the biometric characteristics of the individual in the registration database.

In addition, if an attacker attempts to access the user's biometric sample through forged biometric samples, system, then a well-designed biometric recognition system can identify forged biometric samples by comparing derived data, thus Therefore, this technology not only protects the confidentiality of individuals in the registration database, but also realizes the security of biometric verification.

Feature verification.

Principle of the new measure There are many ways to achieve biometric template protection. Regardless of the method used to construct the derived data, Consider the following issues when selecting a template protection system.

a) What is the probability that the system will reject the real individual and accept the imposter? This is an inevitable consideration for any biometric verification system.

FNMR and FMR are two metrics used to measure the performance of traditional biometric systems (see GB/T 29268.1), biometric recognition template protection systems also continue to use these measurement items.

b) What is the probability that an attacker with knowledge of the database of registered individuals can successfully authenticate as one of the registered individuals?

c) How much information can an attacker obtain by attacking an access control device and stealing the derived registration information stored on the device?

In traditional biometric recognition systems, attackers can obtain important information, including biometric information stored on the device.

The goal of the biometric template protection system is to ensure that these derived data stored on the device it does not reveal too much information about the registered individual.

d) After the attacker successfully breaches one or more access control devices and steals the data stored on the devices, he or she may use the information obtained to What is the probability of successful authentication on the access control device?

These questions form the basis for evaluating the accuracy, confidentiality, and privacy of biometric template protection systems and are successfully introduced.

A new set of metrics that differ from those previously used to evaluate traditional biometric systems.

The need for standardization There are many architectures of biometric template-based

protection systems, such as fuzzy safe-based systems, security profile-based systems, Therefore, it is necessary to define a system that is applicable to various biometric recognition systems.

The template protection architecture key metrics and answers the above questions, thus providing a common basis for comparing systems based on different architectures.

The goal of this document is to define these new metrics for use in evaluating template-based biometric authentication and identification systems.

Chapter 8 provides theoretical and empirical definitions for each metric.

Information technology biometric recognition template protection Performance testing of the solution

1 Scope

This document supports the evaluation of accuracy, confidentiality, and privacy of biometric template protection schemes.

Definitions, terminology, and metrics for the performance of signature recognition template protection schemes. This document specifically specifies the testing and reporting requirements for.

--- Theoretical and experimental accuracy of biometric template protection schemes;

--- Theoretical and experimental probabilities of successfully attacking biometric template protection schemes (single or multiple);

---Information about the original biometrics that is leaked when one or more biometric template protection schemes are violated.

This document is suitable for evaluating the accuracy, confidentiality and privacy of biometric template protection schemes.

This document does not apply to.

---Establish template protection plan;

---Tests for traditional encryption schemes.

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document.

For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to this document.