Konovalova Varvara Petrovna
Student
Ural Federal University
Russia, Yekaterinburg
Research advisor: Tkacheva Marina Viktorovna

BIOMETRICS SECURITY SYSTEMS: GENERAL OVERVIEW

Abstract: *This article briefly describes the definition and the purpose of biometrics security systems. After the description of this security field, a brief overview of existing iris recognition system in automated teller machines was given.*

Keywords: *biometrics technology, identification technique, iris verification, ATM, PIN.*

Коновалова Варвара Петровна
Студент
Уральский федеральный университет
Россия, г. Екатеринбург
Научный руководитель: Ткачева Марина Викторовна

БИОМЕТРИЯ В СИСТЕМАХ БЕЗОПАСНОСТИ: ОБЩИЙ ОБЗОР

Аннотация: *В данной статье кратко описывается предназначение биометрии в системах безопасности. После описания этой области защиты данных, был представлен краткий обзор аутенфикации по радужной оболочке глаза в банкоматах.*

Ключевые слова: *биометрия, методы идентификации, аутенфикация по радужной оболочке глаза, банкомат, PIN-код.*

I. INTRODUCTION

There are hundreds of security methods to save the personal data and confident information in today's world. But at the same time not all of them are reliable and safe.

In addition, existing authentication methods based on PINs and passwords are not convenient for some users. They can forget their passwords, secret words or even share this information with their friends or family members. Because of this fact those people can become attackers and read the sensitive information that the owner doesn't want to share.

Moreover, one of the most important security systems is connected with the finance. Banks provide people with a special four-digit PIN code in order to ensure the protection of confident information. However, an attacker can also hack it and steal money from a bank account in case of loss of the credit card.

Following a brief introduction to biometrics technology, we want to present the research work of American scientists about the iris verification technology in ATM.

II. THE DEFINITION OF BIOMETRICS

What is the biometrics? Maybe this word sounds too novel, the meaning of it is simple: the human recognition.

First of all, it is the science of recognizing individuals based on their behavioral and biological characteristics such as face, fingerprints, iris, voice, gait, and signature [1, c. 17]. This kind of security method is becoming more and more popular nowadays. Scientists and people from security services pay attention to this sphere. Because of this fact this field of activity develops daily. The term of this system for recognizing people refers to a variety of identification techniques. It is based on physical, or behavioral characteristics of the individual. Here is the list of them:

1. Physical characteristics:
   - fingerprints
   - iris recognition
   - hand geometry
   - skin pores

- face recognition
- etc.

2. Behavioral characteristics:

- voiceprint
- gesture models
- typing behavior
- handwritten signature
- etc.

All biometrics approaches follow a similar operation. First a digital template is created after the finish of an enrollment process by the user. Then the electronic template is stored in a database (Figure 1). The form of this template depends on a kind of biometric security system: it can be the features that were extracted out of the photograph of person's iris, fingerprint or it can be a bio-crypto key (cryptographic key from the biometric data of a user). [2, c. 465]

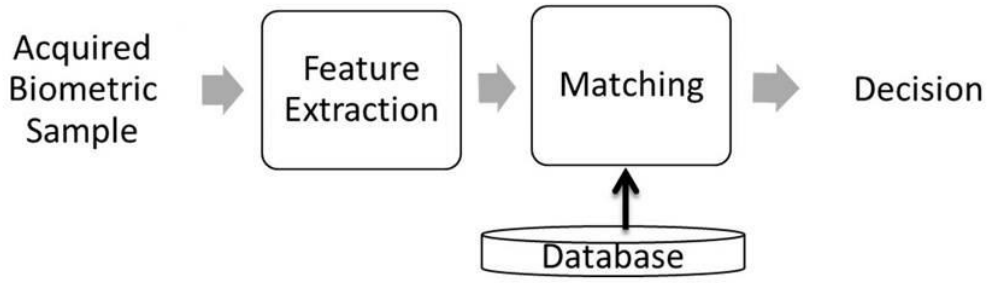

Figure 12 Flowchart of a Typical Biometric Systems

The performance of biometrics is measured using statistical techniques to predict their technical accuracy. The following are used as performance metrics for biometric systems:

- false accept rate (FAR) – the likelihood that the wrong person is accepted;
- false reject rate, (FRR) – the likelihood that a legitimate person is rejected form the basis for comparisons;
- true acceptance rate (TAR) - the proportion of attempts of a legitimate user correctly accepted by the system;

- true rejection rate (TRR) - the proportion of attempts of an adversary correctly rejected by the system.
- failure to acquire rate (FTAR) - the proportion of failed recognition attempts (due to system limitations). A reason for this failure could be the inability of the sensor to capture, insufficient sample size, number of features, etc. [3, c. 279]

III. BIOMETRIC VERIFICATION AT THE ATM INTERFACE

As an example, we would like to present how the biometrics security system works in the ATM's. Banks are starting using this kind of verification process in their security systems.

With iris verification, for application at ATMs, a wide-angle camera finds the head of the person to be identified. A zoom lens then targets in on the user's iris and takes a digital photo. A template of concentric lines is laid on the iris image and a number of specific points are recorded and the information converted into a digital template. This can then be compared with others for verification and identification purposes. (Figure 2)

Iris verification is becoming popular in banking security systems nowadays because of its accuracy, fast speed of the process and the fact that the biometric itself can be acquired without the individual having to come into physical contact with the «end-point». [4, c. 154]

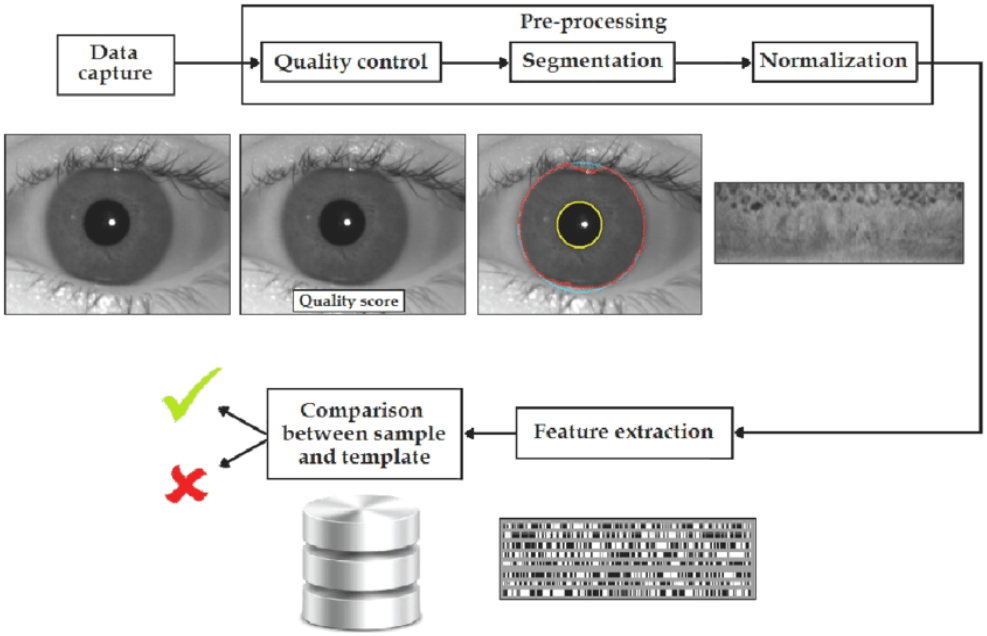

Figure 13 Components of an iris biometric system.

IV. CONCLUSION

In conclusion, we would like to point out that biometrics has great future in various fields of security systems. This field of activity is very popular in security sphere. That is why programmers and scientists develop it and try to make it better. It provides enormous benefits in data protection in different fields from smartphones to banks. The development of these sphere is important because it is directly related to the development of the whole security sphere.

REFERENCES

1. Evans, N.; Marcel, S; Ross, A; Beng Jin Teoh, A; Biometrics Security and Privacy Protection, IEEE Signal Processing Magazine, 12 August 2015, 17-18.

2. Panchal, G.; Samanta, D.; A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security, Computers and Electrical Engineering, 2018, 461–478.

3. Buriro, A.; Crispo, B.; DelFrari, F.; Wrona, K.; Hold & Sign: A Novel Behavioral Biometrics for Smartphone User Authentication, IEEE Security and Privacy Workshops, 2016, 276-285.

4. Coventry, L.; De Angeli, A.; Johnson, G.; Usability and Biometric Verification at the ATM Interface, CHI 2003: NEW HORIZONS, Ft. Lauderdale, Florida, USA, April 5-10 2003, 153-160