Marcin BEDNAREK
Rzeszow University of Technology, Rzeszów
bednarek@prz.rzeszow.pl
Tadeusz DĄBROWSKI, **Michał WIŚNIOS**
Military University of Technology, Warsaw
tdabrowski@wat.edu.pl, mwisnios@wat.edu.pl

CREDIBILITY ANALYSIS OF A MULTI-BIOMETRIC IDENTIFICATION SYSTEM FOR FINGERPRINTS[1]

Key words

Biometrics, multi-biometric identification, the credibility of identification.

Summary

The article contains an example of the credibility estimation of a biometric identification process based on fingerprints. It has been shown that the use of multi-biometric authentication algorithm provides the required level of credibility.

Due to practical tests, probability values of the correct identification of persons determined with the use of the original, self-designed multi-biometric platform are given.

Introduction

An increasing number of access control systems use a variety of identification and/or authentication procedures in their performance. Identification procedure aims at "finding a person" in the system database and is

[1] Scientific work financed from 2010–2012 funds for science as a development project.

commonly carried out with the use of a card, code, or password. In this case, we are not dealing with the identification of a specific person, but his/her specific "parameter" [3]. It might be stated that, by the use of biometric techniques, a specific person, and not just his/her "numerical representation," proceeds to the next stage, which is the authentication process. Authentication should be understood as a mechanism that lets one party ensure that the identity of the other party is true or false. In operations that do not require a very high level of security [1], for example, a sufficient criterion to allow an operator entrance to his work location, a biometric identification procedure system is often used. In this case, we can talk about combined procedures for identification and authentication. In order to increase the security level of the system, it is equipped with multi-biometric identification procedures.

1. Key terms

For the purposes of this article, a few basic terms are presented.

Biometrics – a science that studies the regularity of variability factors in the characteristics of the living organism's population, using the methods of mathematical statistics.

Identification – the comparison of the biometric data of a specific person against the biometric database of all registered individuals.

Verification – the comparison of biometric data of one specific person with a specific pattern contained in a database of different people.

Biometric identifiers (biometrics) can be divided into two groups [4]: *physiological* (e.g., facial image, fingerprints, hand geometry, iris image, DNA, ear shape, scent, retina, skin shine, thermogram) and behavioural (e.g., signature, voice, gait, the pace of writing, mouth motion).

A Biometric identification system includes biometric readers, biometric feature extractors, features comparators (compliance testing modules), and a database of biometric patterns. These elements form the registration subsystem, the authentication subsystem, and the database.

A diagram of biometric identification is shown in Figure 1.

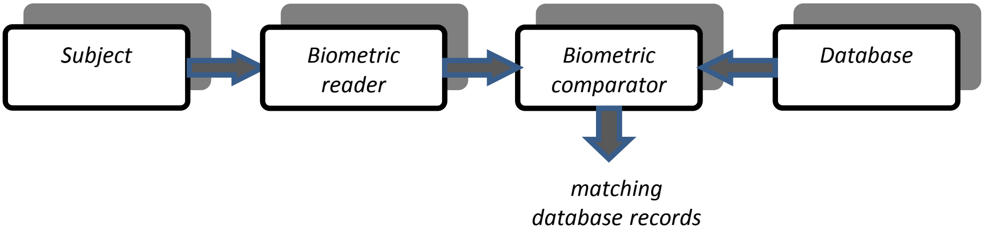

Fig. 1. Diagram of biometric identification

The database contains biometric samples (templates) of registered individuals. A template can contain several biometric samples (not necessarily of the same type).

The result of the identification process is the decision of acceptance or rejection of biometric comparison results by using a specific identification criterion, which is the criterion-based probability value of the identification correctness (Fig. 2).

Methods for determining the criterion-based similarity value can be divided into the following:

– Those based on a threshold (1:1 type of verification is performed for each person in the database and the criterion-based threshold exceeding point is checked);
– Those based on ranks (an ordered list (vector) is created according to values of the similarity of templates); and,
– Hybrids (an ordered list is created but only of those that exceed a certain threshold).

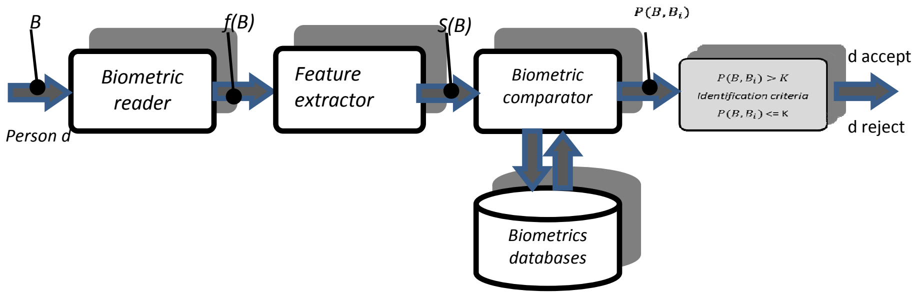

Fig. 2. Identification procedure model

Symbolic representation: *B* – biometrics, *f(B)* biometric sample, *S(B)* – biometric template, Bi – i-th biometric template stored in the database, *P(B,Bi)* – the similarity value between *B* and *Bi* templates, K – the criterion-based similarity value which determines a particular decision (*d* is recognised or unrecognised)

Table 1. The average authentication errors based on the selected biometrics [4, 5, 6,7]

Authentication	False Rejection Rate (FRR)	False Acceptance Rate (FAR)
Fingerprints	(3–7)%	(0.001–0.01)%
Facial image	(10–20)%	(0.1–1)%
Voice	(10–20)%	(2–5)%
Iris image	(2–10)%	≥ 0.001%
Hand geometry	(1–2)%	(1–2)%

Biometrics selection criteria may be created on different bases (Fig. 3). Two mutually exclusive tendencies can be distinguished. The first is to ensure the maximum level of system security by mechanisms that use a biometric identification. The second is to provide a user with a solution that is convenient to use. The final multi-criteria of biometrics selection are always a compromise solution.

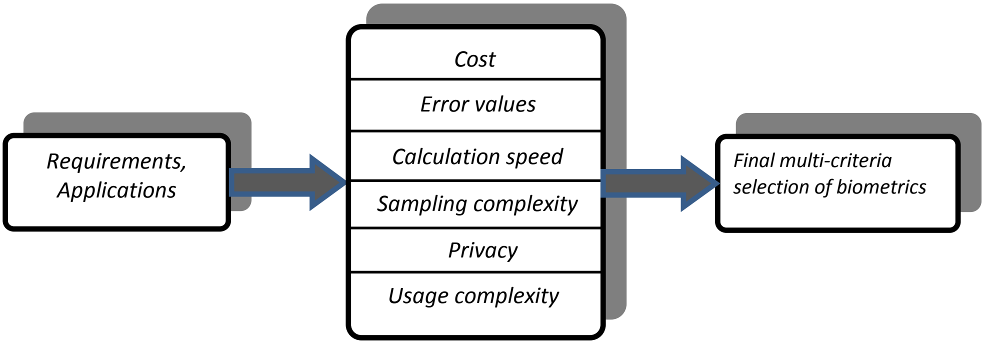

Fig. 3. Factors influencing a rational biometric selection

Integration (combining) of various biometrics identification information includes the use of appropriate methods of biometric information multiplication and the ways of integrating information.

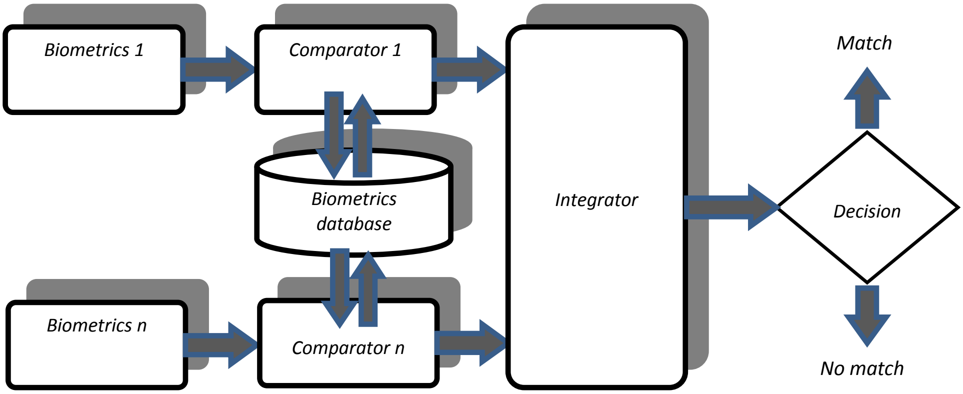

Fig. 4. Identification diagram based on n biometrics and an integrated decision criterion

There is a wide variety of biometric information multiplication methods [4]. For example, one can combine the following:

– A variety of different biometrics (e.g., fingerprint, facial image, voice);
– A variety of samples (multiplied biometrics sampling of the same type from the same person);

- A variety of readers (sampling of the same type with the use of a few readers);
- A variety of comparators (a variety of methods and comparative algorithms for the same sample);
- A variety of biometric identifiers (e.g., fingerprints of several fingers of the same person, iris images of both eyes); and,
- Combinations of the above methods.

Methods of information integration include the following:

- Tight integration (at the level of biometric readers and features extraction), and
- Loose integration (at the level of the score of biometric templates comparators and at the level of decision).

Methods of integration at the decision level are implemented on the basis of the following:

- Boolean algebra (the principle of conjunction, the logical sum principle),
- Filtering (the use of additional non-biometric information) and bucket sort (the use of additional biometric information such as an additional template), and
- Dynamic authentication protocols (e.g. conversation with the object being identified).

Methods of integration at the level of score can be divided into the following:

- Those based on the assumption of a normal distribution of biometric template parameters,
- Those based on the distances between the biometric templates being compared, and
- Those based on threshold criteria of FAR and FRR errors.[2]

2. Estimating the credibility of identification based on a biometric type – "fingerprints"

Assumptions

1. The person (**PerA**) who has their biometric templates in the biometric database system and persons without such templates (**PerB**) are subjected to the identification procedure.
2. The sets of elements PerA and PerB comprise at least 25 people.
3. Symbolic representation: A biometric PerA person sample: $\mathbf{B_A}$,

[2] FAR – (*False Acceptance Ratio*) ratio of incorrect acceptance (here: incorrectly accepted as compatible with an invalid biometric pattern). FRR – (*False Rejection Ratio*) ratio of incorrect rejection determines the percentage of results in which the sample that is consistent with the pattern was rejected as inconsistent (here: incorrect rejection – accepted as inconsistent with a valid biometric pattern).

A biometric PerA person template: $\mathbf{B_{AS}}$,
A biometric PerB person sample: $\mathbf{B_{B}}$.

4. The identification is based on sets of samples and biometric templates of all right hand fingerprints.
5. Multimodal biometric identification comprises the following:
   a) Performing the identification procedure based on a specific finger biometrics at least twice (e.g. fingerprint of a thumb, fingerprint of an index finger, etc.);
   b) Performing the identification procedure based on the biometrics of two specific fingers (e.g., fingerprints of a thumb and an index finger); and,
   c) Performing the identification procedure based on the biometrics of all five fingers.
6. The result of each comparison is independent.
7. The following results of comparison are the only possible options (Figure 5):
   - A positive recognition indicating that the compared sample and the template are identical – ***Wp***,
   - A negative recognition indicating that the compared sample and the template are not identical – ***Wn***.

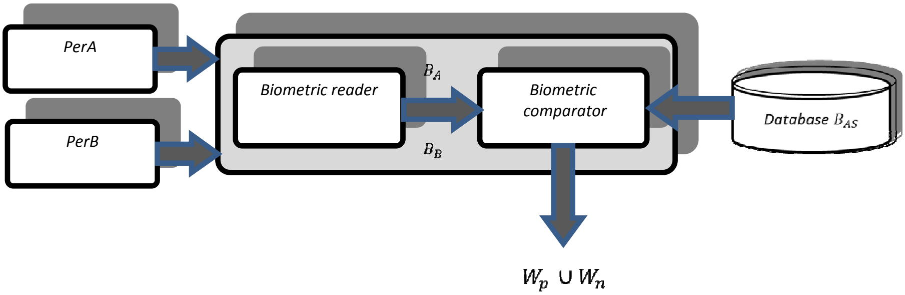

Fig. 5. Illustration of the identification procedure under scrutiny

8. Each result of a comparison can be true or false with a certain probability as follows:
   - The probability of correct acceptance – $\boldsymbol{P_{p+}}$ *(TA)*,
   - The probability of an incorrect (false) acceptance – $\boldsymbol{P_{n+}}$ (*FA*),
   - The probability of a correct rejection – $\boldsymbol{P_{p-}}$ *(TR)*,
   - The probability of an incorrect (false) rejection – $\boldsymbol{P_{n-}}$ (*FR*[3]).
9. The probabilities of the possible results of the biometrics comparison:

$$\begin{array}{lll} & \boldsymbol{B_A{:}B_{AS}} & P_{p+}+P_{n-}=1 \\ & \boldsymbol{B_B{:}B_{AS}} & P_{p-}+P_{n+}=1 \\ \text{Therefore:} & P_{p+}=1-P_{n-} & P_{p-}=1-P_{n+} \end{array}$$

[3] TA – True Accept; TR – True Reject; FA – False Accept; FR – False Reject.

10. Normalised credibility of a 1-fold process of comparison:

$$W^{1}_{(B)} = \frac{P_T}{P_T + P_F} \tag{1}$$

where:

$\boldsymbol{P_T}$ – the indicator of a correct result of the identification process (the truth indicator):

$\boldsymbol{P_T} = P_{p+} + P_{p-}$

$\boldsymbol{P_F}$ – the indicator of an incorrect result of the identification process (the falsity indicator):

$\boldsymbol{P_F} = P_{n+} + P_{n-}$

11. Normalised credibility of an n-fold comparison process:

$$W^{n}_{(B)} = \frac{\prod_{i=1}^{n} P_{Ti}}{\prod_{i=1}^{n} P_{Ti} + \prod_{i=1}^{n} P_{Fi}} \tag{2}$$

where:

$\boldsymbol{P_{Ti}}$ – the indicator of a correct i-th result of the identification process (the truth indicator): $\boldsymbol{P_{T\,i}} = P_{pi+} + P_{pi-}$

$\boldsymbol{P_{Fi}}$ – the indicator of an incorrect i-th result of the identification process (the falsity indicator): $\boldsymbol{P_{Fi}} = P_{ni+} + P_{ni-}$

12. Numerical representation of fingerprints: a thumb: 1; an index finger: 2, a middle finger: 3; a ring finger: 4; a small finger: 5.
13. Symbolic representation of comparison results:
    - A fingerprint of a thumb, 1-fold comparison: $W^{1}_{(op1)}$; 2-fold: $W^{2}_{(op1)}$
    - A fingerprint of an index finger, 1-fold comparison: $W^{1}_{(op2)}$; 2-fold: $W^{2}_{(op2)}$
    - Fingerprints of the other fingers are represented in an analogous way
    - Fingerprints of a thumb and index finger, 1-fold comparison: $W^{1}_{(op12)}$
    - Fingerprints of a thumb and index finger, 2-fold comparison: $W^{2}_{(op12)}$
    - Fingerprints of all fingers, 1-fold comparison: $W^{1}_{(op1\text{-}5)}$
    - Fingerprints of all fingers, 2-fold comparison: $W^{2}_{(op1\text{-}5)}$.

3. Examples of test results

Case 1: Identification credibility based on an ("averaged") fingerprint in a single test:

Data (based on Table 1):

– for a biometric: "fingerprint"
$P_{n+} = 0.0001$; $P_{n-} = 0.07$; therefore, $P_{p+} = 0.93$; $P_{p-} = 0.9999$

Calculations

Based on (1):

$$W^{1}_{(op)} = \frac{P_{p+} + P_{p-}}{P_{p+} + P_{p-} + P_{n+} + P_{n-}} \tag{3}$$

where:
$W^{1}_{(op)}$ – the credibility (probability of the truth) of 1-fold comparison of biometric type: "fingerprint."

After substituting the values of probabilities, we obtain the following:

$$W^{1}_{(op)} = 0.96495$$

Case 2: Identification credibility based on a thumb fingerprint in a single test:

Data (based on self-performed analyses, Table 2) for a biometric: ‘a thumb fingerprint’:
$P_{n1+} = 0.0$, $P_{n1-} = 0.1333$; therefore, $P_{p1+} = 0.8667$, $P_{p1-} = 1.0$.

Calculations:

Based on (1):

$$W^{1}_{(op1)} = \frac{P_{p1+} + P_{p1-}}{P_{p1+} + P_{p1-} + P_{n1+} + P_{n1-}} \tag{4}$$

Which reduces to $W^{1}_{(op1)} = 0.93335$

Case 3: Identification credibility based on a 2-fold test of a thumb fingerprint

Data: (as in case 2):

Calculations:
Based on (2):

$$W^{2}_{(op1)} = \frac{\prod_{i=1}^{2} P_{Ti}}{\prod_{i=1}^{2} P_{Ti} + \prod_{i=1}^{2} P_{Fi}} = \frac{\left(P_{p1+} + P_{p1-}\right)^{2}}{\left(P_{p1+} + P_{p1-}\right)^{2} + \left(P_{n1+} + P_{n1-}\right)^{2}} \qquad (5)$$

After substituting the values of probabilities, we get

$W^{2}_{(op1)} =$ **0.99493.**

4. Summary of test results

Note: These results relate to the case of full credibility of identification in a finger-fingerprint match.

Table 2. Identification errors based on individual fingers biometrics of the right hand

Fingerprint	False rejection (*FR*, P_{n-})	False acceptance (*FA*, P_{n+})	Correct acceptance (*TA*, P_{p+})	Correct rejection (*TR*, P_{p-})
Thumb	0.1333	0.0	0.8667	1.0
Index	0.1	0.0	0.9	1.0
middle	0.1333	0.0	0.8667	1.0
Ring	0.3333	0.0	0.6667	1.0
Small	0.3333	0.0	0.6667	1.0

Table 3. Identification credibility of an individual based on fingerprints

Fingerprint	1-fold procedure	2-fold procedure
thumb	0.93335	0.99493
index	0.95	0.99724
middle	0.93335	0.99493
ring	0.83335	0.96155
small	0.83335	0.96155
thumb and index	0.996255	0.99998587
all right hand fingers	0.999989	0.9999999998

Summary

The following are the conclusions based on the conducted analysis and calculations:

1. A single biometric sampling and a 1-fold comparison of this sample against the template stored in the biometric database do not give a credible result of identification.
2. The credibility of identification can be significantly improved by
   – multiple tests based on the same type of biometric feature and
   – multiple tests based on different types of biometric features.
3. The credibility of the identification process result depends not only on the multiplicity of biometric testing but also (among others) on the following:
   – The quality of biometric samples,
   – The quality of the biometric feature extraction methods,
   – The quality of the algorithm used to create biometric templates,
   – The quality of the methods and criteria that are applied for deduction in terms of similarity between the compared samples and biometric templates, and
   – The level of disturbance (accidental and intentional) influencing the system of biometric identification.

Each of these issues requires a separate analysis and relevant actions.

References

1. Bednarek M., Będkowski L., Dąbrowski T.: Bezpieczeństwo użytkowe systemu antropotechnicznego w ujęciu potencjałowym, XXXVIII Zimowa Szkoła Niezawodności 2010, Szczyrk, 10–16 stycznia 2010, CD.
2. Będkowski L., Dąbrowski T.: Wpływ komparacyjnego diagnozowania efektu na niezawodność systemu, XXXIV Zimowa Szkoła Niezawodności „Niekonwencjonalne metody badania niezawodności”, Szczyrk, 9÷14.01.2006, s. 41÷53.
3. Muszyński J.: Identyfikacja, uwierzytelnienie i autoryzacja. www.netword.pl, 1 maja 2003.
4. Bolle Ruud M., Connel Jonathan H., Pankanti Sharath, Ratha Nalini K., Senior Andrew W.: Biometria, WNT 2008.
5. Maio D., Maltoni D., Cappelli R., Wayman J.L., Jain A.K.: Fingerprint verification competition, Pattern Analysis and Machine Intelligence, IEEE Transactions on (Volume: 24, Issue: 3), 2002, pp. 402–412.
6. Delac K., Grgic M.: A survey of biometric recognition methods, Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium, 2004, pp. 184–193.

7. Yilong Yin, Yanbin Ning, Zhiguo Yang: A hybrid fusion method of fingerprint identification for high security applications, Image Processing (ICIP), 2010 17th IEEE International Conference on.

Analiza wiarygodności identyfikacji multibiometrycznej typu „odciski palców”[4]

Słowa kluczowe

Biometria, identyfikacja multibiometryczna, wiarygodność identyfikacji.

Streszczenie

Artykuł zawiera przykład oszacowania wiarygodności wyniku procesu identyfikacji biometrycznej osób w oparciu o odciski palców. Wykazano, że zastosowanie multibiometrycznego algorytmu uwierzytelniania zapewnia wymagany poziom wiarygodności.

Podano (wynikające z praktycznych testów) wartości prawdopodobieństwa poprawnej identyfikacji osób poddanych badaniom na autorskiej, oryginalnej platformie multibiometrycznej.

[4] Praca naukowa finansowana ze środków na naukę w latach 2010–2012 jako projekt rozwojowy.