BIOMETRIC SECURITY SYSTEMS - PROTECTION VS. PRIVACY

Lukasz Kister [1], Tomasz Serafin [2]

ABSTRACT

Biometrics is getting to be one of the most frequently used identification method in various security systems - from access control through visual monitoring. Along with its popularity increase, many questions of technical as well as legal nature got revealed. This article will try to answer the very essential question: are biometrical data necessary to reach the goal i.e. protection of objects and areas?

Key words: Biometric, Security Systems, Privacy, Identification

ABSTRACT

Biometria je stále najrozšírenejším spôsobom identifikácie v rôznych systémoch technického zabezpečenia - od riadenia prístupu po vizuálny monitoring priestorov. S nárastom popularity použitia biometrie sa objavuje mnoho sporných otázok – technologických i právnych. V článku sa pokúsime odpovedať na základnú otázku: sú citlivé biometrické údaje nevyhnutné na dosiahnutie cieľa, t.j. ochranu objektov alebo priestorov?

Key words: biometria, bezpečnostné systémy, ochrana osobných údajov, identifikácia

[1] Lukasz Kister, Assoc. prof. PhD, Collegium Civitas in Warsaw, mob.: +48 880 147 767, e-mail: lukasz.kister@collegium.edu.pl.

[2] Tomasz Serafin, MA, Editor in Chief of the Specialized Magazine "Ochrona Mienia i Informacji", mob.: +48 606 911 071, e-mail: t.serafin@ochrona-mienia.pl.

1 BIOMETRICS – PROBLEM IDENTIFICATION

Biometrics (gr.: *bio* – life, *metrics* – measure), is a branch of science in the marches of biomedical, technical and mathematical sciences as well as of anthropology and sociology which explores measurable features of human body and all of others biological creatures [1; 5].

Biometrics is a way of extracting mathematical and statistical methods to determine and confirm in an automatic way human identity basing on his individual and unique features – bearing in mind our area of interests [4; 10].

Biometrical features of human being are divided per two main categories [9, 14]:

- Physiological**,** comprising information on physical characteristics of specific person, inter alia:
  - Fingerprint;
  - Hand geometry;
  - Iris anatomy;
  - Retinal anatomy;
  - Ear shape;
  - Lip shape;
  - Face picture;
  - Genetic code (DNA);
  - Handwriting picture,
- Behavioural, comprising mechanisms and ways of performing some repetitive actions by human being, inter alia:
  - Voice and its merits;
  - Manner of walking;
  - Manner of handwriting or typing;
  - Facial expression.

Furthermore you can also find – in some other studies [1; 10] – the third group of biometric features, i.e. **cognitive**, comprising brain reactions on external incentives, f.ex. smell which bring each human being out in specific pulse of brain activity – electroencephalogram (EEG).

At present technologies drawing on biometrics bring very extreme views on. They are very interesting among circles dealing with designing technical protection systems and its interest is still increasing, on the one hand [2; NILES], but they are also strongly criticized by privacy rights defenders, on the other hand [3]. But still there is a lack of broader, scientific and cross-disciplinary overview, bearing in mind arguments of both sides.

This working paper will not bridge this gap, but is an attempt in order to indicate areas of essential interests of researchers, especially those gathered together in ‘Securitology’ circles, who see security through the prism of individual and social groups [11].

2 BIOMETRICS IN TECHNICAL PROTECTION SYSTEMS

2.1 PERSONAL IDENTIFICATION AS A GOAL OF PROTECTION SYSTEMS

As the security environment transforms, and the threats result from terrorist activity reshape in particular, personal identification becomes very meaningful for object protection systems [9].

Nowadays it is assumed that essential determinant of security level is a possibility of strict supervision as to who and when came into protected area. This also the task which is required from integrated technical protection systems, which have to enable unexceptionable identyfication of all persons, who received an access to some objectm, f.ex. office building, airport, sports hall, etc.[12].

The basic division of methods of personal certifying [14]:

- What do you have?
- What do you know?
- Who are you?

The 'What do you have' method – consists in authentication of somebody by object to which this person has an access, f.ex. key, magnetic stripe card, identity card. It is a most common method at present, but it is also the least effective and the most fallible, i.e. loss, thievery, making available.

The 'What do you know?' method consist in using individual password, f.ex. code or cipher. It is less exposed on intrusive activity, like thievery, but it is prone to pathologic behaviors such as saving or making something available for somebody else.

The 'Who are you' method rests on identification of specific person, based on its unrepeatable biometrics features. You don't need any additional item using this method – **'**an individual is a key/password'**.** Therefore it is assumed that the method is the least subject to intrusive activity [4; 12].

Choosing the identification method in access control systems dealing with protected objects you have to bear in mind its effectiveness first of all. The parameters of this effectiveness are listed as follows [14]:

- Quickness of process control
- Forgeries vulnerability,
- Credibility, which consist of coefficients:

– False Acceptance Ratio (FAR);
– False Rejection Ratio (FRR).

2.2 BIOMETRICS AS A TOOL OF IDENTIFICATION

Employing of biometric features in identification systems most of all requires to choose the feature which will enable the highest level of effectiveness. You have to take the following requirements on a board in this respect [4; 6]:

- **Commonness** – feature has to appear among all people;
- **Individuality** – feature has to be unrepeatable;
- **Measurability** – it is easy to measure and compare a feature;
- **Permanence** – feature can't be changeable during human development;

- **Forgery difficulty –** feature can't be easily replicated and be subject to replicate.

Thereupon, biometrics features and features having physiological characteristics are the features which meet very much the rules above, i.e. fingerprint, hand geometry or iris anatomy. These features are most commonly used by protection systems [13].

'Fingerprint – fingerprint scheme' –is the most popular biometric feature employed to identify people, not only when access control to protected area is needed (see: notebook computers, cash machines).

This technology is based on identification and codifying one or a few fingers, so-called minutia, inside of the system of characteristic points for fingerprint scheme. The amount of needed points of reference depends on identified measurement accuracy needs. Nevertheless it is assumed that to make unambiguous comparison it is enough to have 10 – 12 points [ŚLOT].

Protection measures drawing on **'iris picture'** are also becoming increasingly popular.

Systems like those also doesn't use full mapping of iris, but its specific characteristic elements – even 300 points, which then are codified. The most often applied method is designing of 'iris digital map' (256 bits), which allow to distinguish it among population in unquestionable way. To make measurement efficient it is enough to draw up the map of one eye, but methods employing codifying of two eyes are used increasingly [4; 8].

Interest in authorization technics employing biometrics, as a **'hand geometry'** doesn't give away to methods listed above.

Systems using measurements of geometric features of hand are the easiest solution bearing in mind technical regard. The method rests on making 3-D picture of upper part of hand, then measure it – by length, width, thickness and then vectorial classifying – about 90 points. In addition it is applied complementary measurement of temperature distribution of hand [4; 8].

Biometric technology enables to accomplish tasks of access control system in two dimensions [7]:

- Personal authorization;
- Personal identification.

The former rests on answering the question **'**Is this X?**'**. Some person put on sensor its biometrics, fingerprint for instance, and enter to reader the object containing master in addition, f.ex. microprocessor card. After converting, both biometrics are compering to each other by the system, beyond central database.

The latter by contrast is attempting to answer the question **'**Who is X?**'**. Person put on a sensor its biometrics, hand for instance and after converting it, system compares it with all other masters gathered before in central database.

3 BIOMETRIC SYSTEMS – EFFICIENCY VS. PRIVACY

Fast development of biometric technologies, and its increasingly broader applying as a tool of people identification within security systems generate array of questions concerning its consistency with human rights. As a consequence they must be analyzed in details bearing in mind its impact on right of individual to privacy [3].

The most relevant attempt to determine whether this interference with privacy is justified may form an **efficiency level** of systems based on biometric data, i.e. are they more than other methods immune to intrusive activity and characterize a higher level of credibility.

Biometric systems are more significantly **immune** to such threats as thievery of an item, which may confirm eligibility or its **unauthorized access** – key, magnetic stir card or document [BEŁDYCKI].

The situation is similar for biometrics forgery. Although it is possible to make artificial imitation of biometrics or different attempt in order to cheat metrological system reader [3], it is still difficult to enlist master and cost and other activities – essential to replicate it and these activities are so demanding that they seem to be **unreal** today in other place than lab environment [6].

Unfortunately biometric systems yield **much worse** in **credibility** area. In general assessment merits of False Acceptance Rate – FAR (from 0,001 % for iris picture to 2% for hand geometry) as well as merits of False Recognition Rate – FRR (2% for iris to 0,7% for fingerprint) are **unacceptable**. Although this results are minimal in micro scale, in macro scale they have essential meaning for success of authorization procedures, and they overly increase probability of frauds or problems with maintaining expected access control level [10].

Nevertheless there is a scant probability of doubling physical biometric within human population, i.e. two individuals having the same fingerprints or iris haven't been identified so far [2].

Summing up it should be absolutely affirmed that security systems based on biometric data are inevitable future within object protection. And even though its criticism which is often justified will not lead to ban them it should be impulse to persistent development increasing effectiveness and nullifying threats for privacy.

REFERENCES

[1] ASHBOURN J.: Biometrics: Advanced Identity Verification: The Complete Guide. Springer. London, 2000.

[2] BAŁDYCKI K.: Nieuprawnionym wstęp wzbroniony!. "Patrol", 4/2008.

[3] BODNAR A., MICHALSKI J.: Dokument biometryczny a prawa człowieka. In: GRUZA E. (ed.): Dokumenty we współczesnym prawie, Wydział Prawa i Administracji Uniwersytetu Warszawskiego. Warszawa, 2009.

[4] BOULGOURIS N.V., PLATANIOTIS K.N., MICHELI-TZANAKOU E.M. (ed): Biometrics: Theory, Methods, and Applications. Wiley-IEEE. New Jersey, 2010.

[5] CALIŃSKI, T.: Rozwój i osiągnięcia biometrii polskiej. "Przegląd Statystyczny", 1/2012.

[6] DACIUK J.: Biometria. [online]. KSI ETI Politechniki Gdańskiej. http://galaxy.eti.pg.gda.pl/katedry/kiw/dydaktyka/Multimedialne_Systemy_Interaktywne/biometria.pdf, [30.03.2015].

[7] JAIN A. K., BOLLE R., PANKANTI S. (ed.): Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, Norwell, 1999.

[8] KASZUBSKI R.: Biometria w bankowości i administracji publicznej. Związek Banków Polskich. Warszawa, 2009.

[9] KIEŁBUS A., FURYK K.: Nowe technologie i zastosowania w biometrii - analiza rynku. in: KNOSALA R. (ed.): Innowacje w zarządzaniu i inżynierii produkcji. Tom II. Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją. Opole, 2014.

[10] KIRPSZA A.: Biometryczna identyfikacja tożsamości ludzkiej w świetle standardów praw człowieka: przykład paszportu biometrycznego. In: JASKIERNIA J. (ed.): Wpływ standardów międzynarodowych na rozwój demokracji i praw człowieka, Tom I. Wydawnictwo Sejmowe, Warszawa, 2013.

[11] KORZENIOWSKI L.F.: Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych. European Association for Security. Kraków, 2008.

[12] NILES S.: Zabezpieczenia fizyczne w obiektach o znaczeniu krytycznym. White Paper nr 82. American Power Conversion., ver. 1, 2004.

[13] PACUT A. et al.: Metody biometrii. "Biuletyn NASK", nr 3/2006.

[14] ŚLOT K.: Wybrane zagadnienia biometrii. Wydawnictwa Komunikacji i Łączności. Warszawa, 2008.

Článok recenzovali dvaja nezávislí recenzenti.