PhD Magdalena Tomaszewska-Michalak
Faculty of Political Science and International Studies, University of Warsaw, Warsaw
ORCID: 0000-0001-5441-0396

HANDWRITING AS BIOMETRIC FEATURE – PART I

Summary
The aim of the article is to classify the handwriting as one of the biometric feature. In the first part of the article the author deals with the definition of biometric technology, describes a history of biometric devices and points out the areas in which biometric algorithms are being used nowadays. The second part of the paper focuses on using biometric signature for identification and/or verification purposes.
Keywords: biometric technology, biometric verification/identification, handwriting, biometric signature

Introduction

The study aims at the classification of the handwriting as the biometric feature and is divided into three parts. The first part introduces the concepts associated with biometrics technology as well as points to the characteristics allowing the handwriting to be classified as a biometric identifier. The second one refers briefly to the historical context of the development of biometric technology as well as the benefits of biometrics that contribute to the increasing use of biometric devices as a safety protection measure. The examples of areas where biometric technology is implemented are highlighted in this section as well. Consecutively, the third part refers to the possibility of using a signature as a biometric identifier. In this part, the properties resulting from the analysis of the biometric signature for determining its authenticity are discussed. The paper constitutes the first part of the study on the use of handwriting as a biometric feature.

Biometric technology and handwriting

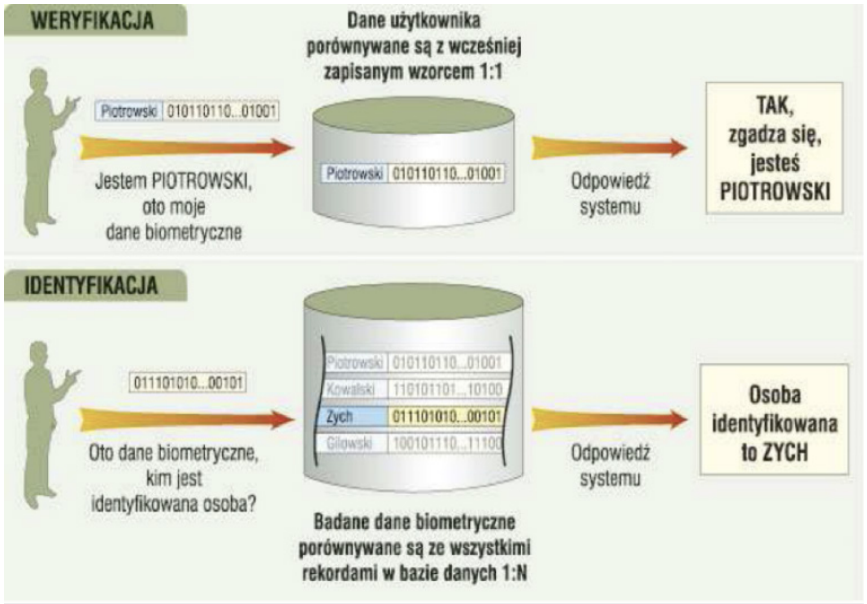
In order to attribute handwritiang to the biometric features, the term *biometrics* needs to be explained in the first place. According to the dictionary definition, *biometrics* is the science involving the study of variability of features among the population of living organisms. The measurement is carried out using mathematical

statistics based methods[1]. As such, the biometrics has been used for many years, also in forensic examination as a tool to aid the identification of the perpetrator. In fact, the first forensic identification systems were based on the assumption on the variability of characteristics of the human body, such as *bertillonage*[2] or dactyloscopy[3]. Starting from the mid-20th century, however, the term biometrics has been attributed a new meaning. This has been due to technological developments allowing the automation and thus significant acceleration of the feature comparison process. Therefore, the biometrics can be defined as a technology used to identify a person or verify someone's identity based on a comparison between individual biological and physical or behavioral characteristics. Various elements of the quoted definition should be briefly discussed. The automation of the comparison relies on the use of appropriate algorithms for identification or verification. In fully automated systems, this means that the human factor is eliminated completely and the comparison is dependent solely on the accuracy of the algorithm. In forensic methods of verification of identity or identification, biometrics often constitutes the first step in the identification and/or verification process. Once the device establishes the similarity between the features being compared, it is the expert who makes the final decision in this regard. An example of such a solution is the AFIS system supporting the work of police experts in the field of fingerprint examination[4].

Another concept worth explaining in relation to biometric technology is the difference between identification and verification. Identification means the comparison of a specific feature (e.g. friction skin ridges) with a set of features stored in a database. The purpose of the comparison is to reveal the identity of the person. This is the principle behind the *watch lists*, aiming at determination of the identity of undesirable or wanted persons (e.g. at border check). The aforementioned AFIS system operates in a similar way. Verification of the identity, on the other hand, involves comparing the presented feature with a model of that feature previously recorded on a specific medium. It is therefore a mere confirmation that the person declaring his/her identity is, in fact authorized to use the system (e.g. during cash withdrawal from an ATM). The difference between verification and identification is graphically illustrated in Fig. 1.

[1] https://sjp.pwn.pl/, accessed 16.06.2021.
[2] A. Bertillon, *Identification anthropométrique*, Imprimerie Administrative, Melun 1893.
[3] C. Grzeszyk, *Daktyloskopia*, Wydawnictwo Naukowe PWN, Warsaw 1992.
[4] J. Moszczyński, *Z historii polskiej daktyloskopii*, „Studia Prawnoustrojowe" 2014, no. 26.

Fig. 1. Identification of a person and verification of identity



Source: A. Dzwonek, T. Kling, *Biometria w dokumentach podróży,* „Człowiek i Dokumenty" 2008, no. 10.

Another important point needed to comprehend the nature of biometric technology is the explanation in what way the individual features used in the identification/verification process must fulfil certain properties. Biometric comparison can be based on biological and/or physical characteristics inherent to the human body. Therefore the individual has no influence on the process of formation of such characteristics. Currently, the most commonly used biological and/or physical features include fingerprints, iris and facial recognition. Behavioral traits, on the other hand, are formed by a repetitive character of a certain behavior, which consequently leads to the individualization of the feature. Such characteristics include the way someone's moves or the dynamics of hitting on the keyboard. The indicated behavioral criteria are also fulfilled by the manner of writing and, even more importantly, by the characteristics of drawing a signature. Regardless of the type of the feature, the application of biometric technology relies on certain properties they should be characterized. The first one is versatility, meaning that the feature must be universally present in a given community. Failure to meet this condition makes the use of biometrics ineffective due to the fact that a part of the population could not be biometrically compared, and therefore alternative verification and identification methods must be sought. At this point, however, it should be emphasized that versatility is not ruled out by a situation in which only a small percentage of the population is deprived of a particular feature. This may occur, for example, in the case of disease or other circumstances (e.g. diseases resulting

in fading of fingerprints or damage to the iris of the eye). Another prerequisite for the property of the characteristics used is their uniqueness. The purpose of using biometrics involves the ability to distinguish individuals from one another, which can be done if the characteristics being compared are unique. The third highlighted property is the relative invariability over time. The higher invariability is demonstrated by a certain feature, the greater usefulness in the identification or verification process. In cases where a feature changes over time, it is important to note the need to introduce a pattern modification procedure (for example facial geometry). This may also apply to signatures. If the feature is to be utilized for biometric comparison, it should be easily collectable in a non-destructive manner. It is also important that the feature is universally acceptable, which means that the social attitude should be examined *a priori*, with regard to the feasibility of implementing biometric devices of a certain type. An example of social unacceptability of a feature is the requirement to show the face in order to carry out a biometric comparison in countries where religious considerations require veils to be worn.

It should be remembered that not every biometric feature (the so-called biometric identifier) fulfils all the criteria (for instance, face may change over time). On the other hand, the knowledge of the properties of the identifier may help to mitigate the problems arising from its biometric use (e.g. modification of the facial pattern after a certain period of time). Considering these properties in the context of handwriting and signatures in particular, it should be noted that they meet most of the criteria for a biometric identifier, however with certain exceptions. First of all, the signature is universal by nature; the majority of population is capable of putting a signature. According to the literature, handwriting bears the qualities of personal individualization[5]. This statement refers specifically to the signature of an individual. In contrast, it should be noted that a signature is a behavioral trait, meaning that many factors can contribute to its final appearance. The elaboration of a signature relies on the frequency of writing and therefore on a handwriting worked out style. Furthermore, handwriting may change as a result of progressing age or illness. All these factors should therefore be taken into account when creating a biometric template basing on the appearance of handwriting. On the other hand, it goes without saying that taking a handwriting sample for biometric analysis requires the cooperation of the writer, but at the same time it is non-invasive. Apparently, given the habit of frequent signing the documents, the implementation of biometric devices based on handwriting (signatures in particular) comparison does not pose a problem in terms of social acceptability of such a solution.

[5] A. Feluś, *Podpisy – studium z pismoznawstwa*, Uniwersytet Śląski, Katowice 1987; Z. Czeczot, *Badania identyfikacyjne pisma ręcznego*, Wydawnictwo Zakładu Kryminalistyki KG MO, Warsaw 1972.

Table 1. Characteristics of handwriting as a biometric feature

Characteristics of biometric identifier	Identifier as handwriting (signature)
Versatility	present
Uniqueness	partially present
Invariability	partially present
Possibility to collect	present
Acceptability	present

Source: own elaboration.

Possibilities of using biometric technology based on handwriting

Although contemporary forensic examination methods used individual characteristics to confirm the identity of the suspect as early as the 19th century, the development of biometric comparison was significantly related to the technological opportunities being explored in the mid-20th century[6]. The biometrics started to develop most extensively after the attacks on the World Trade Center and the Pentagon on 11 September 2001.[7] Following the WTC attacks, the US administration commenced exploration of more effective ways to control the identity of people entering the US territory. In this respect, the biometrics development trends were indicated by the so-called Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001)[8]. The Patriot Act envisaged the development of a technological standard that would contribute to quick and effective identification or verification of a foreign national when, for example, applying for a visa to enter the United States. Also, at the beginning of the 21st century the European Union became interested in the possibilities of using biometrics. The implementation of the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States[9] can serve as the example. Over the past few years, the market for biometric security has been growing steadily, which demonstrates the popularity of the use of biometric identifiers in various areas of life; this can be seen in the growth of the biometric technology market in the United States (Fig. 2).

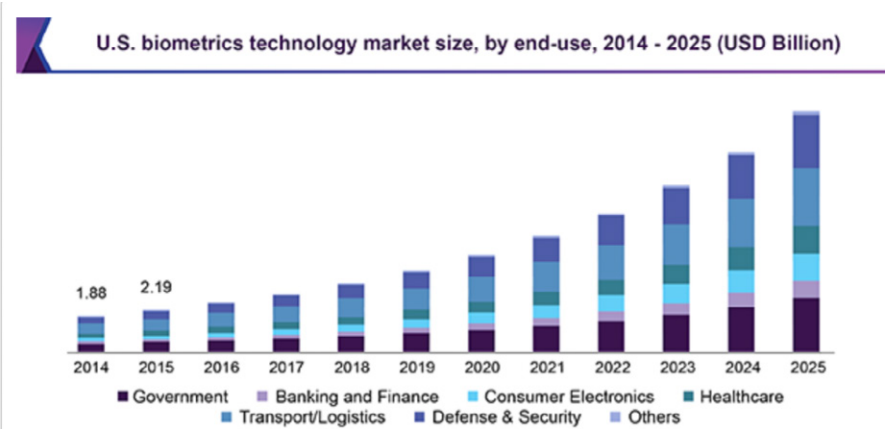
[6] M. Tomaszewska-Michalak, *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*, Difin, Warsaw 2015.

[7] K. Gates, *Identifying the 9/11 'faces of terror'. The promise and problem of facial recognition technology*, „Cultural Studies" 2006, vol. 20 (4–5), pp. 417–440.

[8] Public Law Pub.L. 107-56.

[9] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L. 385.

Fig. 2. The US biometrics technology market by end-use



Source: https://www.grandviewresearch.com, accessed 30.09.2022.

In addition to the opportunities granted to biometrics due to global technological development over the last 20 years, the widespread use of identifiers has been determined by the benefits of biometric comparison. The first and foremost advantage is the speed of the verification and/or identification process, especially when compared to conventional methods, as performed by a clerk or officer. Nowadays, a biometric comparison can take less than a second, thus a person can receive relevant authorization significantly more effectively. This is accompanied by the accuracy of the measurement. Biometric comparison has the advantage over traditional verification and/or identification due to the fact that the error rate of the device algorithms has already been examined. Additionally, biometrics can replace other methods of verification or identification of someone's credentials. Conventional security measures are based on a "something that I know" or "something that I have" concept. Passwords or PIN numbers can be classified to first category, while tokens or cards fall into the second one. Biometrics, on the other hand, belongs to the third security group – "something that I am". The use of identifiers can therefore be convenient for the user, who does not have to remember passwords or have a card with code number[10]. Furthermore, biometric identifiers do not carry the risk that they will be stolen from the authorized

[10] The advantages of biometrics in this respect have been recognized by the EU legislation; the Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending the Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Payment Services Directive), pointed to the need of introducing a mechanism for so-called robust customer authentication in the financial sector, which means authentication based on the application of at least two elements belonging to the categories of knowledge (something that only the user knows), possession (something that only the user has) and customer characteristics (something that the user is), independent in the sense that the breach of one of them does not undermine the

person. This increases the safety of correct identification of the authorized person, as the identifier is irrevocably linked to the person's identity. Today, the biometric identifiers have numerous applications and are used, among others, for the following purposes:

1) as an element of document security. An example is the passport issued in EU Member States, which contains a biometric photo and a chip with an encoded fingerprint;

2) verification of the identity/identification of wanted persons and/or criminal offenders. The Polish AFIS or the European SIS II system may be included in this category;

3) verification of the identity of the customer of financial institution in order to obtain authorization to execute a transaction. Examples include biometric cash dispensers or verification of an identity based on facial recognition system;

4) increased security during mass events. Examples include biometric verification of people trying to enter the Olympic village;

5) security measure for mobile phones or computers;

6) a means of preventing unauthorized entry to a specific area (e.g. installation of biometrically secured door handles).

The above list constitutes only an example of the application of biometrics. On the other hand, the list illustrates the versatility of biometrics technology and the possibility to implement comparison algorithms across many areas of life. Regarding the use of the signature as a biometric identifier, apparently this feature will prove useful in places where a traditional signature is already used in order to verify identity, including such examples as all transactions carried out in banks or with a payment card. A similar purpose for the biometric signature can also be found in documents.

The purpose of application of signature as biometrics identifier

Signature constitutes the most unique handwriting element. The more often the signature is drawn, the more automated this process becomes, which allows it to be included in the group of behavioral biometric identifiers. The signature represents an important element in the confirmation of someone's identity. The importance of signature is highlighted by the need to place it on all documents with legal implications, such as contracts, financial documents or wills. Although, according to police

reliability of the others, which authentication is designed to protect the confidentiality of the authentication data (Article 4, point 30).

statistics, the number of offences under Article 270 of the Penal Code (document forgery)[11] is gradually decreasing, it still remains at a fairly high level[12].

Table 2. Crime statistics pertaining to Art. 270 of the Penal Code

Year	Number of initiated proceedings	Number of criminal offences
2020	9350	17 546
2019	11 910	19 880
2018	12 667	22 474
2017	13 667	23 690
2016	15 129	28 324
2015	16 707	26 988
2014	16 652	30 392
2013	17 579	30 331
2012	17 148	29 588
2011	15 888	36 025

Source: https://statystyka.policja.pl, accessed 30.09.2022.

According to literature reports, many types of signature forgery can be distinguished, which include, among others:

• forgery as a result of copying the signature,

• forgery through the so-called intellectual imitation, i.e. when the counterfeiter does not know the picture of a genuine signature,

• forgery resulting from the imitation of a genuine signature known to the counterfeiter,

[11] "Article 270 of the Penal Code. § Whoever counterfeits or forges a document for the purpose of using it, or uses such a document as authentic, shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for a term of between 3 months and 5 years.

§ 2. The same punishment shall be imposed on anyone who fills in a blank document bearing another person's signature contrary to the will of the signatory and to his detriment, or uses such a document.

§ 2 a. In the case of lesser gravity, the perpetrator shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.

§ 3. Whoever makes preparations for the offence specified in § 1, shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years".

[12] It should be noted, however, that Article 270 of the Penal Code in general relates to the offence of forging or altering a document and not only to the offence of signature forgery, which is of interest in this study.

• self-forgery, the purpose of which is to disguise someone's own handwriting so as to undermine the authenticity of the signature at the later stage[13].

A traditional method of determining the authenticity of a signature involves the opinion of a document examiner. On the other hand, it would be very helpful to introduce, if possible, drawing a signature on a tablet used for biometric verification. In this case, in addition to the conventional graphical and comparative method used for forensic analysis of signature, it is also possible to verify additional characteristics inherent to the signature drawing[14]. The first characteristics is the time required to generate the signature. If drawing a comparative (reference) signature takes too much time, this may indicate that the signature is not authentic, and there has been an attempt to copy or reproduce someone's signature. The dynamics of writing is one of the properties that a counterfeiter cannot learn by merely looking at the graphic picture (appearance) of a signature. The other advantage of using the biometric tablet is that the device is capable of storing the information on the writing pressure distribution. This is helpful in traditional forensic examination of handwriting, as the pressure distribution which deviates from the individual habit may indicate an attempt to forge a signature. The third noteworthy characteristics involves the measurement of the angles of the stylus as well as recording each removal of the stylus from the tablet surface. The abovementioned possibilities of biometric algorithms in the case of signatures provide significant opportunities in identification of potential forgeries of signatures. Naturally, in order to be able to carry out biometric verification of the signature, appropriate reference material must be previously saved in the system. It is impossible to perform biometric verification when the signature was drawn in a conventional manner. The self-forgery is the case when the discussed properties (writing dynamics, pressure, pen angle) may prove insufficient to point to an attempted fraud. In such situation, however, the conventional handwriting examination should be able to demonstrate an attempt to mask the handwriting by revealing the habitual characteristics in the signature. Apparently, after appropriate conditions have been met, the biometric algorithms could be used to verify not only the authenticity of signatures, but also other handwritten entries. In contrast, it should be remembered, that the signature reveals the highest level of automatic drawing, and hence this handwritten element constitutes the basis for creating its biometric equivalent.

Summary

The aim of the study was to demonstrate the possibility of using handwriting as a biometric identifier. With regard to the abovementioned definition of biometric technology, it can be concluded that handwriting belongs to the behavioral biometric characteristics that are shaped and become individualized proportionally to the

[13] M. Goc, *Badania podpisów w kryminalistycznej ekspertyzie pismoznawczej – wybrane zagadnienia metodyczne*, „Problemy Kryminalistyki" 2009, vol. 263, pp. 19–27.

[14] A. Czajka, A. Pacut, *Biometria podpisu odręcznego*, in: P. Zając, S. Kwaśniowski (ed.), *Automatyczna identyfikacja w systemach logistycznych*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004, pp. 244–260.

frequency of writing. The contemporary use of tablets, which is limited to the comparison of individual signatures, can support the work of forensic document examiner in determination of the authenticity of handwritten entry.

The study does not address any legal issues related to the possibility of processing biometric data nor the problems that may arise in connection with the use of algorithms to verify the identity on the basis of a signature. Due to the importance of this matter, a due discussion will be comprised in the second part of the study.

Bibliography

Literature

Bertillon A., *Identification anthropométrique*, Imprimerie Administrative, Melun 1893.

Cieśla R., *Współczesne wyzwania wobec badań dokumentów*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2021.

Czajka A., Pacut A., *Biometria podpisu odręcznego*, w: P. Zając, S. Kwaśniowski (red.), *Automatyczna identyfikacja w systemach logistycznych*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004.

Czeczot Z., *Badania identyfikacyjne pisma ręcznego*, Wydawnictwo Zakładu Kryminalistyki KG MO, Warszawa 1972.

Feluś A., *Podpisy – studium z pismoznawstwa*, Uniwersytet Śląski, Katowice 1987.

Gates K., *Identifying the 9/11 'faces of terror'. The promise and problem of facial recognition technology*, „Cultural Studies" 2006, t. 20 (4–5).

Goc M., *Badania podpisów w kryminalistycznej ekspertyzie pismoznawczej – wybrane zagadnienia metodyczne*, „Problemy Kryminalistyki" 2009, nr 263.

Grzeszyk C., *Daktyloskopia*, Wydawnictwo Naukowe PWN, Warszawa 1992.

Mendyk-Krajewska T., *Biometryczne metody sprawdzania tożsamości w nowych zastosowaniach*, „Roczniki SGH" 2019, nr 54.

Moszczyński J., *Z historii polskiej daktyloskopii*, „Studia Prawnoustrojowe" 2014, nr 26.

Sikora K., *Technologie biometryczne sposobem uwspółcześnienia przepisów o formie testamentu holograficznego*, „Studia Prawnicze. Rozprawy i Materiały" 2020, nr 2 (27).

Tomaszewska-Michalak M., *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*, Difin, Warszawa 2015.

Sources of law

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 1997 Nr 88, poz. 553 ze zm.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Public Law Pub.L. 107-56.

Rozporządzenie Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie, Dz. Urz. L. 385.

Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniającej dyrektywę: 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylającej dyrektywę 97/5/WE (Payment Services Directive).

Internet sources

https://sjp.pwn.pl/
https://statystyka.policja.pl

Conflict of interest

None

Source of funding

The article was written in the framework of the project no. DOB-SZAFIR/06/A/042/01/2020 titled "Intelligent system for the recognition of forgery of biometric features of handwriting", funded by the National Center for Research and Development, implemented within the "Development of modern, breakthrough technologies for the state security and defense – SZAFIR" programme, Competition No. 1/SZAFIR/2020. The project is implemented in the period between 2021–2024 by the following project consortium: Central Forensic Laboratory of the Police, Institute of Criminalistics of the Polish Forensic Association Ltd. and JAS Technology Ltd.