Dynamic Biometric Signature - an Effective Alternative for Electronic Authentication

Vladimír Smejkal[1,*], Jindřich Kodl[2]

[1] Moravian University College Olomouc, Olomouc, Czech Republic.

[2] Authorized Expert of Cryptology and Information Systems Security, Prague, Czech Republic.

Received 07 June 2017; received in revised form 13 June 2017; accepted 23 December 2017

Abstract

The use of dynamic biometric methods for the authentication of people provides significantly greater security than the use of the static ones. The variance of individual dynamic properties of a person, which protects biometric methods against attacks, can be the weak point of these methods at the same time.

This paper summarizes the results of a long-term research, which shows that a DBS demonstrates practically absolute resistance to forging and that the stability of signatures provided by test subjects in various situations is high. Factors such as alcohol and stress have no influence on signature stability, either. The results of the experiments showed that the handwritten signature obtained through long practice and the consolidation of the dynamic stereotype, is so automated and stored so deep in the human brain, that its involuntary performance also allows other processes to take place in the cerebral cortex. The dynamic stereotype is composed of psychological, anatomical and motor characteristics of each person. It was also proven to be true that the use of different devices did not have a major impact on the stability of signatures, which is of importance in the case of a blanket deployment.

The carried out experiments conclusively showed that the aspects that could have an impact on the stability of a signature did not manifest themselves in such a way that we could not trust these methods even used on commercially available devices. In the conclusion of the paper, the possible directions of research are suggested.

Keywords: biometric authentication methods, dynamic biometric signature, electronic signature, authentication

1. Introduction

One negative aspect of the current trend of connecting ever more devices in cyberspace (primarily thanks to the Internet of Things) is the increased risk of them being attacked and exploited. All devices and all information systems must, therefore, be constructed from the very start to be secure against possible risks. The key assumptions for constructing secure information systems are ensuring the quality identification and authentication of people, assets, and events in the system – on the one hand to prevent cyber attacks and other criminal activities in cyberspace, and on the other to record all incidents and their circumstances. This is an important tool for investigation, and also a source of feedback for improving security measures.

The opinion that multifactor authentication is essential to ensure an adequate level of security for information systems is already practically universal [1]. It is also necessary to understand that in open systems we do not ensure proper data protection only through integrity and trust, but a sophisticated authentication process is a very important point in terms of the protection of

[*] Corresponding author. E-mail address: smejkal@znalci.cz.

data, respectively the assets of the subject in question. It is only possible to launch the authorisation process which will provide the authenticated person with access to ICT services after successful and reliable authorization.

The used authentication methods should meet the requirements for variability both from the perspective of the technologies and used systems and from the perspective of the users themselves. The proposed solutions must also respect the legislation in force in different countries and permit the execution of legal acts according to the intentions of both sides.

The authentication methods must provide a high level of protection against their breaking or exploitation, while at the same time remaining user-friendly. They must be secure, easy to use, unobtrusive and also have reasonable implementation costs. The addition of an extra factor for authentication also brings an increase in the technological, organization, and primarily financial demands of such a solution. Hence, this field is still being developed, and the search for the “Holy Grail of Authentication” continues. In particular, at a time when there is more and more emphasis on protection of personal data with concurrent pressure to both simplify and make the process of identification and authentication more pleasant for the user.

For these reasons, it is important to focus on the issue of multifactor authentication, in particular, those where biometric methods play an important role.

2. Biometric Authentication Methods

Biometry is a set of scientific findings, which focuse on the investigation and subsequent practical use of measurable characteristics of living organisms with the aim of unequivocally identifying them (first identification) or verifying them (then authentication) [2]. Biometric authentication methods appear to be a reasonable compromise between demands on users and/or tools for authentication while not reducing the level of security. There are many biometric methods, but they can basically be split into three groups:

(1) static

(2) static with testing for the presence of a person

(3) dynamic

We must make a fundamental distinction between static and dynamic methods, where static methods are basically a continuation of the authentication principle that the user “has something”, even if this means something that is a part of their physiology. This means that there remains a risk of the falsification of biometric information (faking fingerprints, iris image, etc.) or their use through coercion. Hence, for example, at the current time, the authentication methods used for mobile telephones can serve at most only to reassure users or for simple “superficial” protection.

Dynamic authentication methods have been arousing interest. We can assume a higher level of protection from abuse, as we are moving from the variant that the user “has something” to the variant in which the user “knows something” and, what is more, they “do not know what they know”. These are processes where the primary impulse arises in the central nervous system in the human brain with a predefined intensity and duration. The nervous system then activates the relevant muscles in a defined order, so that the user can perform a certain activity a signature, a certain gait, a gesture, and so on. In this case, therefore, biometry is based on the characteristics of a person’s behavior.

The use of static methods connected with a test for the presence of a (living) person is something of an intermediate step. This is usually performed by detecting body temperature or, at a more sophisticated level, by detecting the circulation of blood in vessels or by measuring oxyhaemoglobin concentration.

For each method, there are several characteristics that will determine its usefulness. These are, in particular: accuracy and reliability (expressed through parameters such as FRR, FAR, FER, FIR, FMR, FNMR [3]), security (protection against forgery and coercion, as well as against attacks on biometric images and samples), user acceptability, costs of acquisition and operation, etc. Sometimes, these qualities can be directly in opposition a simpler, and more accurate method might be easier to attack (e.g. the faking of fingerprints).

Depending on the number of features used for recognition biometric systems, we can use a unimodal method (if only one of the biometric characteristics is used), or a multimodal one (if more than one characteristic is used).

3. Dynamic Biometric Signature

A dynamic biometric signature appears increasingly appropriate to authenticate people and also documents containing important information. It contains information about how the signature was created, and thus reflects characteristics of the signers, their habits and behavior, as well as the fact that they made the signature consciously. These characteristics represent a biometric footprint that is unique for each person and cannot be reproduced by a forger (unlike the actual image of the signature itself, which only makes up one of the parameters of the biometric footprint).

These include the basic features of a handwritten signature:

- the duration of the signature process, including the periods between strokes
- points and curves in different parts of the signature
- the pressure exerted by the pen on the pad during different parts of the signature
- the overall size of the signature
- the form and shape of the signature
- the length and angle of lines, arcs and curves, the number of loops
- the speed of individual stokes, acceleration and deceleration

One of the important attributes of a DBS is that it contains not only the element that the writer is alive, but also the fact that the signature was created by the writer consciously. Therefore, there is no need to develop additional mechanisms to test whether the subject is present, alive, or not - unlike with static biometric methods (checking the print of a finger, palm, iris etc.). It is also legally beneficial, in that we can rely on the (theoretically rebuttable) assumption that people knew what they were signing [4].

A special tablet (pad) is currently used for scanning a DBS. When acquiring signature data, biometric data [mostly x(t), y(t), p(t), t)] are also acquired. This biometric information is also used to calculate additional parameters, defined using the ISO/IEC 19794-11 standard [5]. This standard contains a description of the mandatory parameters and formats of the biometric data. The system then scans the parameters of the signature, adds them to the information from the signed document, for example, the user name, current time and date, and about the device used. These data are encrypted and create the so-called biometric data that are sent for further processing.

In this way, we acquire authentication data for the signer with subsequent securing against forgery. At the same time, the process simulates the standard process of a traditional signature. A DBS may be used as a handwritten signature, but it is also possible to use it in the form of a one-off password or graphical pattern that the user writes on the sensor or shows with a gesture - for example using a mobile phone. A DBS would appear to be an effective alternative to the only technology used for electronic signatures to date - a signature based on asymmetric cryptography. It can be used with an advantage in cases when the implementation of certificates (partly due to their limited validity period) and the secure "concealment" of private keys significantly interfere with the normal activities of signers. From the perspective of users, it is also the most pleasant method, as the act of signing is something we do today and every day without needing any special knowledge, skills or the ownership of any secret. Handwritten signatures are also one of the most socially accepted biometric features.

4. Risks Involved with the Use of a Dynamic Biometric Signature

Recently, the static authentication tools provided by the makers of mass-used devices (mobile phones, laptops, etc.), such as fingerprint, palm or face scanners have been accepted in a sickly optimistic way. At the same time, the successful cases of attacking these devices are known. E.g. [18-21]. (New authentication tool Face ID on iPhone X has also been subjected to attacks since it was released. They have been unsuccessful so far [22], but according to the authors, it is only a matter of time (and money). Perhaps, the attacks failed because of the fact that Face ID is not a mere static method.

Greater safety of the new authentication method is based on the fact that Face ID revolutionizes authentication on iPhone X, using a state-of-the-art TrueDepth camera system made up of a dot projector, infrared camera, and flood illuminator, and is powered by A11 Bionic to accurately map and recognize a face. These advanced depth-sensing technologies work together to securely unlock iPhone, enable Apple Pay, gain access to secure apps, and many more new features. Face ID projects more than 30,000 invisible IR dots. The IR image and dot pattern are pushed through neural networks to create a mathematical model of your face and send the data to the secure enclave to confirm a match while adapting to physical changes in appearance over time. All saved facial information is protected by the secure enclave to keep data extremely secure, while all of the processing is done on device and not in the cloud to protect user privacy. Face ID only unlocks iPhone X when customers look at it, and it is designed to prevent spoofing by photos or masks [23].

An infrared camera, then, captures the distortion of that grid as the user rotates his or her head to map the face's 3-D shape a trick similar to the kind now used to capture actors' faces to morph them into animated and digitally enhanced characters. [24].

Despite the high level of quality of Face ID that greatly eliminated the possibility of forgery (falsifying the sample), the weaknesses of static biometric methods remain the same.

Table 1 Comparison of dynamic and static biometric authentication methods

Property	Static Methods	Dynamic Methods
Forgery (imitation)	Yes	No
Stealing (reuse)	Yes	No
Compulsion	Yes	Complicated
Possibility of revocation (substitution by a different sample)	No	Partially
Impact of the internal state of an organism	No	No
Impact of the environment	No	No
Ageing	Very little	Has not been studied
Change as a result of illness or injury	Yes	Yes
Inability to use (for objective reasons)	Improbable	In the case of a serious disorder, e.g. inability to write (agraphia or dysgraphia).

Critics of this method of identification, respectively authentication of people point to the lower credibility of a DBS arising from insufficient uniqueness of generated signature samples - in particular in connection with the possible change in the motor skills of people as they age or due to stress, the "rationalization" (simplification) of the signature due to the increasing skill of the writer after numerous repetitions, etc. The experiments described below show that this is not true. Table 1 contains the comparison of selected properties of dynamic and static biometric authentication methods in terms of safety and protection against abuse.

The second main counterargument is the need for high security for the database of signature samples, respectively biometric samples when signing. This is another separate issue [6].

4.1. DBS credibility

Regarding the first objection, it is important to state that the DBS rests on the repeated performance of the same movement. It means a handwritten signature, which is considered to be a highly-qualified movement, during which some general laws apply, and where the latest research shows that some basic characteristics of a signature, respectively its characteristic parameters, can be determined and described mathematically:

- The 2/3 PL (Power Law) states the known effect of the curvature of trajectory on the speed of movement, and the momentary angular velocity is proportionate to the momentary curvature with a 2/3 power relationship. A study focusing on the issue of handwriting, and its compliance with the 2/3 PL has confirmed the relationship between the trajectory of the curvature of the writing and the speed of movement [7, 17].

- The principle of isochrony applies to the temporal characteristics of human movement and describes the invariance of the time to perform a movement in relation to its amplitude, meaning that the duration of a movement remains almost the same irrespective of its scope. This fundamental also applies for smaller parts of the assessed movement, which means that this part of the movement can be geometrically changed (for example enlarged), while the time to complete this sub-movement remains the same.

- Another easy to observe a feature of human movement is its smoothness. The minimum jerk model enables the assessment of trajectory creation, where the sections of a movement are examined in relation to the maximized smoothness. (Jerk is a vector-based physical quantity characterizing movement, and describes the rate of change of acceleration.)

The natural laws indicated above, which are discussed in studies for activities connected with writing, can also be naturally applied to the handwritten signature. Studies have also shown that for samples of a signature or even of only its part, the time pattern of determined sections remains the same, irrespective of changes in geometry. Hence, changes in movement caused by emotions or stress will not impact the overall timing of the movement (in our case the signature). Thus, as soon as identification points are determined for a handwritten signature, the time relationship between them will always remain the same [8-11].

4.2. DBS forgery

When trying to forge a signature, the forger must contend with the speed profile of the original. Even if the image is the same, the velocity profile will differ with a level of probability approaching one. It is important to note that a certain variability is actually permitted for the coordinates (x, y), while the time relationship between these through points must remain unchanged. Small changes in the geometric shape of the signature (amplitude, scale) are not significant compared to the actual timing of the movement. An attempt at forging a signature must always be visible at the time level, and this especially if the forger only has access to the visual form of the signature [6].

As a part of the research performed by the authors in 2014, the characteristics of a DBS during an attempt at forging the signature of another person whose signature sample was available as an image were examined, *inter alia*. 102 university students of different ages took part in the test. The test subjects were supplied with a sample of the signature of a bank client, who had made the signature during a standard transaction. The forgers were given both the first and second names of the signer. In this phase of the test, the test subjects had the chance to practice the signature before imitating it and thus create as convincing copies as possible. The signature training was done on paper, and also on a signing pad (in this phase the result of the signing was not scanned). After the training, the test subjects were tasked with imitating the signature sample five times with the maximum possible accuracy.

Fig. 1 shows that the attempt at imitating the client's signature according to the sample reveals diametrical differences in terms of the time taken to create the sample and the forgery, while at first glance they appear very similar:

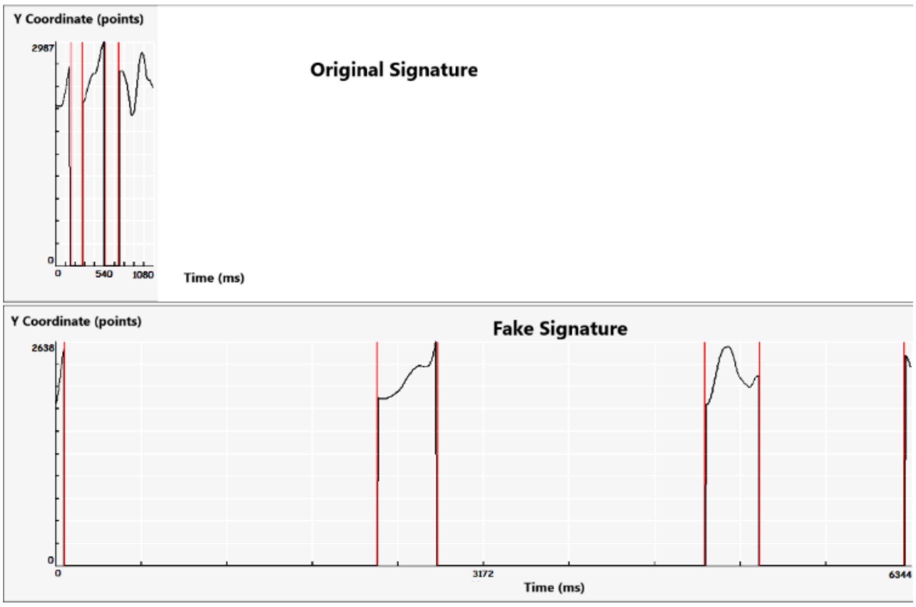

Fig. 1 Time: the original signature above, the forgery below

It is clear at first glance how long it took to create the forged signature; without mentioning the detailed differences in the individual time sections. When analyzing the scope of the performed signature (according to the number of image points), we see the different progress of the individual characteristics – for example, speed in Fig. 2:

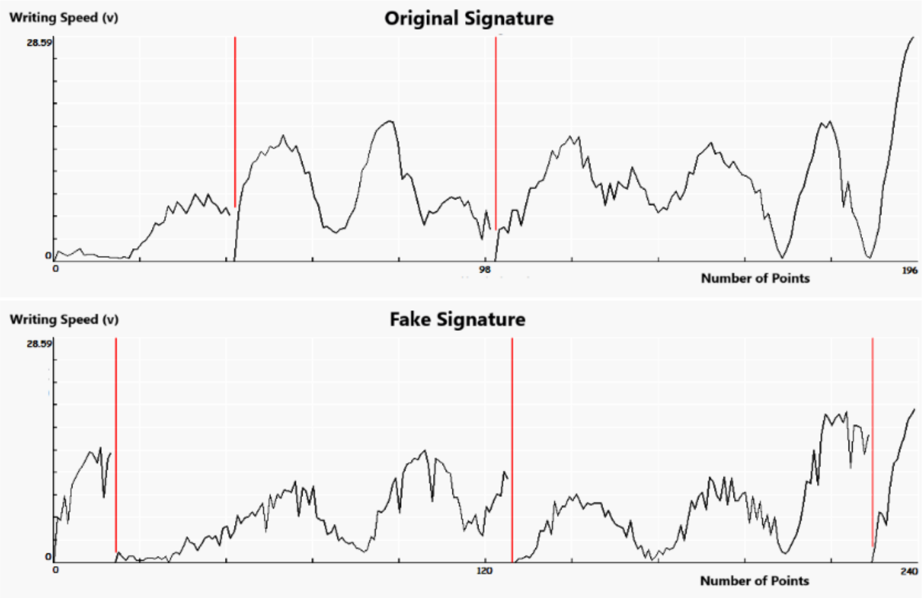

Fig. 2 Writing speed: the original signature above, the forgery below

A handwriting expert was also involved in the experiments and was provided with the forgery attempts produced by the test subjects. The analysis focused on assessing the compliance between the signatures created by the test subjects and the bank client's signature. The results confirmed the conclusions arising from the data acquired by the validation server. The results of the examined set of signatures showed that out of the 190 forgeries, not even a short-term rehearsal of the signature to be forged was successful [12].

The experiments showed that the biometric data acquired during the creation of the signature provide such a set of information that enables an unequivocal opinion during subsequent verification in the case of a dispute over the authenticity of a signature. It was shown that the manufacturer's software can be used to process these data. The configuration of the data that influences the amounts of the calculated indicators cannot – with the exception of the acceptance level – be changed in the programs delivered by the manufacturer. The configuration of the compliance level that results in agreement/rejection/non-rejection of a validated DBS will have to be addressed in the validation server, where it is possible to set the acceptable level according to the determined policy of the DBS operator.

One interesting result of the experiments is that it will only be necessary to use the results and conclusions of an analysis of biometric data performed by a handwriting expert in extreme cases of the verification of the authenticity of a signature, while it is usually enough to deploy the validation server. In such a case, the biometric data are an ideal source of information for the handwriting expert compared to a situation in which they can only use two short texts, namely signatures on paper, for a comparison [12].

4.3. DBS stability for different people

Other research assessed the stability of a DBS across a heterogenous set of tested people.

Three hypotheses were formulated:

I. When using a standard (routine) signature, there is a high degree of similarity among individual signatures. The signatures are stable and display a small degree of variability.

II. This also applies to special circumstances, such as drunkenness, stress or other influences.

III. For some people, even the falsified (intentionally changed by them) signatures display a high degree of stability.

A total of 10 signatures were recorded on the form from each person within the framework of the testing of the group of heterogeneous people. People signed in the usual standard manner during the first six signatures (hereafter simply referred to as the "authentic signatures"). They were, then, called upon during the next four signatures to try to change the signatures in such a way so that they could object that they were not the authors of the signatures during any eventual verification of authenticity (hereafter simply referred to as the "inauthentic signatures" or the "falsified signatures"). This involves a fairly typical variant where the first 6 signatures are completely routine, while the signatures starting with the seventh are falsifications of the person's own signature (the person was asked to sign the same name, but different) with certain variability.

After testing the group of 24 people which included:

- people aged 12 to 92.
- people with a primary, secondary and tertiary education (university students and graduates, including postgraduate education).
- people working both manually and mentally.
- the following evaluation was performed.

A total of 240 results were acquired when comparing the authentic signatures, 138 when comparing the inauthentic signatures and 444 when comparing the authentic and inauthentic signatures with each other. The first finding involved the fact that in most people the first signature undertaken on the sensor showed a high degree of variance of compliance in relation to the other signatures, which is a consequence of the necessity of getting used to the method of signing on the sensor. For this reason, the first signature of each person was always omitted from the evaluation which resulted in the evaluated set of data being more homogeneous (with a smaller variance and standard deviation).

It was found that the degree of compliance (stability) for authentic signatures is substantially higher than for inauthentic signatures, and this with a level of significance of 0.01.

4.4. The influence of the consumption of alcohol on a DBS

The testing of influences on the biometric signature's dynamic was carried out on a group of 9 university educated people with an average age of 35.2 ± 14.2 (for 22 to 60). The measurement (signatures and filling in the tests) was carried out in a restaurant during its regular operations, i.e. in an environment with significant background noise. All 9 people carried out 2 x 10 signatures (before and after drinking alcohol).

People who did not reach a breath alcohol concentration of at least 1‰ were eliminated from further processing. During the course of the experiment, which lasted 4 hours, 6 people reached an average breath alcohol level of 1.4 ± 0.2 ‰ (from 1.0 to 1.7‰). The measurements were taken using an AlcoScan AL9000L (Korea) digital alcohol tester.

People took the Brickemkamp-Zillmer variant d2 attention test at the beginning and the end of the measuring. The d2 selective attention test is a widely used test in psychological diagnostics. It enables the evaluation of the attention, performance (speed) and error rate under time pressure. It is appreciated for its stable results and the high mutual correlation of the individual evaluated parameters. We used the Brickenkamp-Zillmer d2 test, published in association with the Hogrefe Gottingen publishing house [13].

The speed of performance after the consumption of alcohol did not change in a demonstrable manner. On the other hand, the number of errors after the consumption of alcohol increased by more than twice (2.4x). The error rate with consistent results was statistically evaluated using a paired t-test and Welch's test comparing the characteristics before (b as before) and after (a as after) the consumption of alcohol and a significant difference was found in the error rate (Ch%) and in the attention variability (VS) at a level of significance of 0.05.

The degree of compliance of the signatures after the consumption of alcohol at a level of significance of 1% does not differ from the degree of compliance of the signatures before the consumption of alcohol, not even in the case of people who displayed a significant increase in errors during the attention test.

It has been demonstrated that:

I. When using the standard (routine) signature, there is a high degree of similarity between the individual signatures for a particular person. The signatures of individual persons are stable and they display only a small degree of variability. The signature is a stable tool for the identification and authentication of a person.

II. (a) In some people, even their falsified (intentionally changed by them) signatures display a high degree of stability.

(b) In some people, these falsified signatures are not sufficiently distinguishable from the authentic signatures.

III. The influence of alcohol on the realization of routine (authentic) signatures has not been proven.

Even in cases where people displayed a high degree of stability in their inauthentic signatures, the dynamic parameters of the data which were received during the creation of the DBS provide sufficient room for their analysis by a trained person or a handwriting expert, who has a significant amount of information available of the sort which is simply unable to be acquired when comparing classic signatures on paper [14].

It is common for the person providing a signature to be exposed to stress, and one reason for this is the importance of the situation in which they are appending the signature. After all, stress and very often negative stress are the most common emotions in human life. For this reason, we were interested in whether and in what way stress influences the quality and constancy of a DBS.

In our experiments, we used the extreme situations in which test subjects in survival courses (”X-TREAM” course) at the University of Defence of the Czech Republic found themselves [15]. Test subjects undertook a series of demanding tasks and gradually reached a level of stress and physical and mental exhaustion, hunger, sleep deprivation and therefore stress.

We originally formulated two hypotheses:

I. stress does not influence the stability of a signature.

II. there is a significant correlation between performances achieved in a d2 attention test and the stability of a DBS.

The tests incorporated in our experiment included a Brickenkamp-Zillmer d2 attention test and provided ten signatures on a Signotec tablet that reads the biometric characteristics of a signature. Equipment and procedures were the same as before. [14] Each test subject undertook the tests before the load commenced (at the beginning of the survival course), in the middle of the course and at the end – indicated as S(tart), M(iddle), F(inish). A total of 26 people took part.

The results of our experiments showed that even though the physical and mental load on the test subjects rose, the stability of their dynamic biometric signatures was high or actually improved during the experiment. The variability of the signatures of most individual people did not differ significantly at individual stages. It was also again confirmed that the use of a 1st signature as “practice”, not included in the results, reduces the variability of signatures among all the test subjects.

Hypothesis I., that stress has no influence on the stability of a signature, was confirmed, at a significance level of 0.01. Hypothesis II., that there is a significant correlation between performances achieved on a d2 attention test and the stability of a DBS, was not confirmed. It can be assumed that a signature, as a stereotype embedded in the central nervous system over the long-term, can be influenced by outside factors to a lesser extent than specific activity performed at a stage of stress.

We consider the stability of a DBS to be confirmed to such an extent by the range of experiments which we conducted [4, 6, 12, 14] to be able to use this method to identify and authenticate people or the documents which they have signed with a high degree of reliability and verifiability.

4.5. Stability of a dynamic biometric signature created on various devices

Within further experiments, we focused on examining whether the use of various devices for DBS scanning affects the stability of a DBS of the signer.

In our experiments, we used all the available pads produced by Signotec, which differ from each other in terms of their design, the size of the signature field, resolution, sampling rate, and even the scanning method used – a regular pen or a special pen using the ERT (Electromagnetic Resonance Technology). The purpose of the experiments was to show the possible change of the stability of a DBS of a signer depending on the scanning device. As the sample represented people of both sexes aged 20 to 65, the size of the heterogeneous sample used was statistically representative enough.

The following hypotheses were formulated:

I. The participants will cope with the difficulties connected with the changing circumstances of the signing depending on the technical design of the pad in a different way:

H_0 the stability of signatures of a particular person on each device does not significantly change (mean and variance of the degree of compliance of signatures for each device belonging to the same basic set).

H_1 there is a statistically significant difference in the means and variances of the degree of compliance of signatures of a particular person on individual devices.

II. The stability of signatures achieved on individual devices will statistically significantly differ:

H_0 the mean degree and variance of compliance of signatures for each device do not significantly change (mean and variance of the degree of compliance of signatures for each device belonging to the same basic set).

H_1 there is a statistically significant difference in the means and variances of the degree of compliance of signatures on individual devices.

4.5.1. Testing of hypothesis I

The result characterizing the technology as a whole, i.e. without differentiation of types of devices and signers (i.e. for all people on all devices) is as follows - see Table 2:

Table 2 Summary results on the degree of compliance of signatures

x [%]	M_2	σ [%]
79.330	173.290	13.164

The selective mean of the degree of compliance of signatures came under an accepted level of compliance of biometric signatures 60% only in case of two people.

In order to test the homogeneity of variances of the degree of compliance of signatures of each participant on all devices, the Bartlett's test was used [25]. The values in the B test ranged from 20.341 to 609.934, i.e. the P-value was between 0.000 and 0.005. For all participants, the null hypothesis was, therefore, rejected at the significance level 0.01 and thus at the significance level 0.05 (as the P-value was <0.01 for all participants).

Using the Cochran-Cox test [26], a pair of devices, where the hypothesis on the compliance of means of the degree of compliance was rejected at the significance level 0.01, was found for each participant. The simple sorting test (analysis of variance, ANOVA) that would keep the probability of error of the first kind at the level 0.05 or 0.01 could not be used with regard to the results of the Bartlett's test.

We can conclude that the participants coped badly with various designs of devices. This is due to the fact that selective variances of the degree of compliance are significantly different for all participants on individual devices, and there are also differences in means of compliances.

4.5.2. Testing of hypothesis II

The following values of selective means and unbiased estimates for variances of the degree of compliance of signatures were detected on the stated devices - see Table 3 below:

Table 3 Selective means and unbiased estimates for variances of the degree of compliance

The Signotec device and scanning method	x [%]	S^2
Alpha - ERT	80.342	113.019
Delta - ERT	76.749	238.268
Gamma - ERT	78.971	232.027
OmegaNew - TD	76.022	228.052
OmegaOld - TD	83.002	125.844
SigmaLite - WD	77.097	148.574
SigmaNew - TD	85.233	139.194
SigmaOld - TD	77.195	120.338

Compliance of variances was verified by the Bartlett's test (B = 13.597, k-1 = 7, α = 0.01 and 0.05, P-value = 0.059), so the hypothesis on the compliance of all variances was accepted at the significance level 0.01 and at the significance level 0.05.

The simple sorting test (ANOVA) [26] gave the following results F = 2.565, k = 7, n-k = 306, P-value = 0.014, $\alpha = 0.01$ and 0.05, $F_{0.01}$= 2.700 and $F_{0.05}$= 2.039, where $F_{1-\alpha}$ (k-1, n-k) is (1-α) quantile of the Fisher-Snedecor distribution for the significance level α, so compliance of all means was accepted at the significance level 0.01 and rejected at the significance level 0.05.

The results of the Scheffe's test of multiple comparisons [27] would enable to determine between which two above-mentioned means the statistically significant differences exist. The Scheffe's test accepts the equality of all 28 pairs of means of the degree of compliance of signatures at the significance level 0.01 and 0.05 (28 is the number of possible options for all pairs of devices).

When using different devices, there were found no differences between the mean values of the degree of compliance (x) and values of the variance of the degree of compliance (σ^2) that is at the significance level 0.05 for variances and at the significance level 0.01 for means. It can, therefore, be noted that, despite the technological differences between individual devices, the stability of signatures (indicated by variance) does not change when changing the device. Also, the degree of compliance of signatures on all devices does not statistically significantly differ at the significance level 0.01.

The experiment brought the following results:

Hypothesis I. – The participants will cope with the difficulties connected with the changing circumstances of the signing depending on the technical design of the pad in a different way: The null hypothesis H_0 claiming that the stability of the signatures of a particular person on each device does not significantly change that is at the significance level 0.01 and thus at the significance level 0.05, was disproved. A pair of devices, where the hypothesis on the compliance of means of the degree of compliance was rejected at the significance level 0.01, was found for each participant. Therefore, the hypothesis H_1 claiming that there is a statistically significant difference in the means and variances of the degree of compliance of signatures of a particular person on individual devices was confirmed.

Hypothesis II. – The stability of signatures achieved on individual devices will statistically significantly differ: The null hypothesis H_0 claiming that the mean degree and variance of compliance of signatures for each device do not significantly change, because there were found no differences between the values of means and variances of the degree of compliance when using different devices, that is at the significance level 0.05 for variances and at the significance level 0.01 for means, was confirmed.

A detailed description of the experiment can be found in the report from [28].

5. Conclusions

DBS has been an important alternative to classic electronic signatures based on cryptographic methods. It can be used with an advantage in cases when the implementation of certificates (partly due to their limited validity period) and the secure “concealment” of private keys significantly interferes with the normal activities of signers. From the perspective of users, it is also the most pleasant method, as the act of signing is something we do today and every day without needing any special knowledge, skills or the ownership of any secret. Handwritten signatures are also one of the most socially accepted biometric features[16].

Through the implemented tests, the authors of this paper have shown that the level of compliance, stability, and imperviousness to influence during the creation of signatures performed by the test subjects in different situations is high. A DBS shows practically absolute resistance to imitation, and the stability of signatures made by the test subjects in different situations is high. Factors such as alcohol and stress have no influence on signature stability either. The results of the experiments have shown that a handwritten signature acquired through long practice and the compaction of the dynamic stereotype, which is composed of the physiological, psychological, anatomical and motor characteristics of each person, is automatic to such an extent and stored deep in the human brain, that its involuntary performance enables other processes to take place concurrently in the cortex.

A DBS is not a replacement for a cryptographic electronic signature, but an important alternative that can be used in cases when the use of certificates, the secure storage and "policing" of private keys, etc. would significantly impact routine and stable processes, and potentially form a barrier discouraging normal users (contracting parties). Its advantage over a cryptographic electronic signature, when a computer de facto does the signing, is the existence of this "handwritten" quality, which is only ensured through a legal declaration when a private key is used.

In further research, the authors want to focus on other possible impacts occurring as a result of the external factors that can influence the process of signing, e.g. a change in the body position. They will also take into account the additional authentication options and abilities to imitate a DBS, this time not as a static image of the signature, but in a process of monitoring and imitating its dynamics.

References

[1] V. Smejkal and J. Kodl, "Development trends of electronic authentication," Proc. of the 42nd Annual Conf. 2008 IEEE International Carnahan Conf. on Security Technology, IEEE Press, October 2008, pp. 1-6.

[2] R. Rak, V. Matyáš, and Z. Říha, "Biometry and identity in forensic and commercial applications," Grada Publishing, 2008.

[3] M. Gamassi, M. Lazzaroni, M. Misino, V. Piuri, D. Sana, and F. Scotti, "Accuracy and performance of biometric systems," Proc. of the 21st IEEE Instrumentation and Measurement Technology Conf. (IEEE Cat. No. 04CH37510), IEEE Press, November 2004, pp. 510-515.

[4] V. Smejkal and J. Kodl, "Strong authentication using dynamic biometric signature," Proc. of 45th Annual 2011 IEEE International Carnahan Conf. on Security Technology (ICCST), IEEE Press, October 2011, pp. 340-344.

[5] ISO/IEC 19794-11:Information technology. Biometric data interchange formats, Part 11: Signature/sign processed dynamic data, IEEE Standard, 2013.

[6] V. Smejkal, J. Kodl, and J. Jr. Kodl, "Implementing trustworthy dynamic biometric signature according to the electronic signature regulations," Proc. of 47th Annual 2013 IEEE International Carnahan Conf. on Security Technology (ICCST), IEEE Press, October 2014, pp. 165-170.

[7] F. Lacquaniti, C. Terzuolo, and P. Viviani, "The law relating the kinematic and figural aspects of drawing movements," vol. 54, no. 1-3, pp. 115-130, October 1983.

[8] F. Lacquaniti, "Central representations of human limb movement as revealed by studies of drawing and handwriting," vol. 12, no. 8, pp. 287-291, 1989.

[9] S. Kandel, J. P. Orliaguet, and P. Viviani, "Perceptual anticipation in handwriting: The role of implicit motor competence," Perception & Psychophysics, vol. 62, no. 4, pp. 706-716, January 2000.

[10] A. J. Thomassen and H. L. Teulings, "Time, size and shape in handwriting: Exploring spatio-temporal relationships at different levels," Time, mind, and behavior, Springer Berlin Heidelberg, pp. 253-263, 1985.

[11] Y. Wada and M. Kawato, "A theory for cursive handwriting based on the minimization principle," Biological Cybernetics, vol. 73, no. 1, pp. 3-13, June 1995.

[12] V. Smejkal and J. Kodl, "Assessment of the authenticity of dynamic biometric signature," The results of experiments. Proc. of 48th Annual 2014 IEEE International Carnahan Conf. on Security Technology (ICCST), IEEE Press, October 2014, pp. 45-49.

[13] R. Brickenkamp and E. Zillmer, D2-Test of attention, Seattle: Hogrefe & Huber, 1998.

[14] V. Smejkal, J. Kodl, L. Sieger, D. Novák, and J. Schneider, "The dynamic biometric signature. Is the biometric data in the created signature constant?" In Proc. of 49th Annual 2015 IEEE International Carnahan Conf. on Security Technology (ICCST), IEEE Press, September 2015, pp. 385-390.

[15] E. Ambrozová, J. Koleňák, D. Ullrich, V. Okorný, and D. Cibulka, "X-tream index and multi-parameter personality dimension for managers cognition and decision-making in the modern corporate environment," Global Journal for Research Analysis, vol. 4, no. 3, pp. 1-7, 2015.

[16] R. Tolosana, R. Vera-rodriguez, J. Ortega-Garcia, and J. Fierrez, "Increasing the robustness of biometric templates for dynamic signature biometric systems," In Proc. of 49th Annual IEEE International Carnahan Conf. on Security Technology (ICCST), IEEE Press, September 2015, pp. 229-234.

[17] J. KODL Jr., "Mechanisms of human arm motion planning in the presence of multiple solutions," Imperial College, 2010.

[18] A. Rattani and A. Ross, "Automatic adaptation of fingerprint liveness detector to new spoof materials," 2014 IEEE International Joint Conf. on Biometrics (IJCB), IEEE Press, December 2014, pp. 1-8.

[19] A. AL-AJLAN, "Survey on fingerprint liveness detection," 2013 International Workshop on Biometrics and Forensics (IWBF), Lisbon, IEEE Press, April 2013, pp. 1-5.

[20] L. Ghiani, D. Yambay, V. Mura, S. Tocco, G. L. Marcialis, F. Roli, and S. Schuckers, "Livdet 2013 fingerprint liveness detection competition 2013," 2013 International Conf. on Biometrics (ICB), IEEE Press, September 2013, pp. 1-6.

[21] M. Drahanský, O. Kanich, and E. Březinová, "Challenges for fingerprint recognition-spoofing, skin diseases and environmental effects," In Handbook of Biometrics for Forensic Science, Advances in Computer Vision and Pattern Recognition, 2017.

[22] A. Greenberg, "We tried really hard to beat face id-and failed (so far)," https://www.wired.com/story/tried-to-beat-face-id-and-failed-so-far/.

[23] The future is here: iPhone X. Apple Inc. Press release, September 2017.

[24] A. Greenberg, "How secure is the iphone x's faceid? Here's what we know," https://www.wired.com/story/iphone-x-faceid-security/.

[25] G. W. Snedecor and W. G. Cochran, "Statistical methods. eighth edition," Iowa State University Press, 1989.

[26] W. G. Cochran and G. M. Cox, Experimental & designs, 2nd ed. New York: John Wiley and Sons, 1957.

[27] H. Scheffé, The Analysis & Variance, New York: John Wiley and Sons, 1999.

[28] V. Smejkal, J. Kodl, L. Sieger, F. Hortai, and P. Tesař, "Stability of a dynamic biometric signature created on various devices," IEEE Press, December 2017.