Possibilities of dynamic biometrics for authentication and the circumstances for using dynamic biometric signature

Frantisek Hortai

Brno University of Technology
Faculty of Business and Management
Czech Republic
hortai@fbm.vutbr.cz

DOI: 10.20470/jsi.v9i1.326

Abstract: *New information technologies alongside their benefits also bring new dangers with themselves. It is difficult to decide which authentication tool to use and implement in the information systems and electronic documents. The final decision has to compromise among the facts that it faces several conflicting requirements: highly secure tool, to be a user-friendly and user simplicity method, ensure protection against errors and failures of users, speed of authentication and provide these features for a reasonable price. Even when the compromised solution is found it has to fulfill the given technology standards. For the listed reasons the paper argues one of the most natural biometric authentication method the dynamic biometric signature and lists its related standards. The paper also includes measurement evaluation which solves the independence between the person's signature and device on which it was created.*

Key words: Authentication, dynamic biometrics, dynamic biometric signature, information system security.

The IS plays one of the key roles in a company's functioning (Koch, Chvátalová, 2017). Secured information system has to prevent its misuse or help to identify and convict its attacker. Findings of security gaps should also serve as an improvement of the security to prevent further attacks or possible cyber-crimes. For this purpose the called logs are the record of the activities of the computer system and all persons (users, administrators, service, etc.) that can be associated with a security incident (Smejkal, 2015). In this case the issue of access control, identification, verification and authentication of people and processes is the key question.

The main terms such as identification, authentication and access control are some of the most frequently used terms of the information system security field. This is where the cornerstones are represented for building a secure information system. The same way they play a significant role in the investigation of cybercrime, the manner in which the crime was committed, i.e. beside other things also the manner in which the perpetrator gained access to the computer system and information medium and what took place in the system. (Porada, Smejkal, 2017)

Generally, by identification we understand the recognition of any entity by the system on basis of a specific identifier which is associated with a particular person or thing, represents their identity, and can be known to other people. As far as humans are concerned it is the first and last name, user name, birth certificate number, social insurance number, identification card - ID number, etc., further for things it can be the car license plate, serial number, officially assigned number (e.g. personal document number), etc. (Mates, Smejkal, 2012). In this case, the identification means finding out the identity of the subject which is done by comparing personal data or expressions of the character of a real person with other persons, while authentication is a verification that the subject is who they poses as through this identity.

Authentication is the process of the verification of the declared identity of the subject. As far as humans are concerned, it is carried out by means of objects (cards, smart cards, mobile phones and others), witnesses, signs of a personal nature (signature, voice, gait, etc.), personal characteristics (fingerprints, iris), knowledge (password, PIN, security question, etc.). As far as things are concerned, it can be authentication against a checklist, sending an automated query and comparing answers with information stored in the system, etc.

Access control is a security arrangement based on the security policy of the authority (organization). Its purpose is to provide access according to the access rights of the authority to authorized users and

prevent unauthorized entities from access. For purpose of security audit or billing, etc. the system can gather information on the made accessions (authentication, logins, etc.), see figure1.

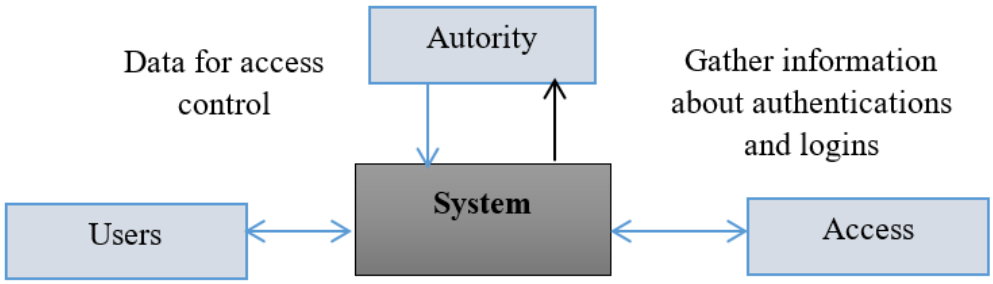


Fig 1. Logics of access control system *(Source: authors' own elaboration)*

1. Methods

The secondary research uses scientific papers as resources which were collected for specified purposes for clarifying the benefits and pitfalls of authentication technologies. The advantages and disadvantages of biometric authentication methods were briefly explained. The law and legislation requirements are also collected and dealt with (regulations and cyber law in biometric technologies). From a wider perspective the focus is then shifted to the dynamic biometric authentication. One of the objectives is to define and isolate the dynamic biometric signature among the other authentication methods. The discussion part mainly argues why the dynamic biometric signature was selected for authentication under these conditions:

- area and space independency;
- to be user-friendly and acceptable for users;
- authentication Process continuity and stability;
- ensure the subject aliveness via automated remote testing.

Here mainly empirical comparison of authentication possibilities were performed. It summarises the results of many years of research activities by the authors in the field of the dynamic biometric signature, including experiments. The end research also concludes the comparing of this type of signature with a signature based on cryptographic methods with a view to the current eIDAS Regulation (Regulation (EU) No 910/2014 of the European Parliament and of the Council).

The main goal of this paper is to demonstrate the benefits of the dynamic biometric signature as authenticating method and to explain its standards. In further experiments all the available pads produced by the company Signotec were used. These pads 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 so called on-line DBS was examined. The purpose of the experiments was to show the possible change of the stability of the 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. 8 scanning devices were used (see listed in Table 1). The sampling frequency of the used devices can be set up to 150 Hz, 250 Hz or 500 Hz. The scan rate (sampling) was set up to recommended 250 points/sec. The x, y, time and pressure coordinates were scanned. The experiment was attended by 40 people in one session. The testing was carried out on the following dynamic biometric signature devices with the various technical parameters produced by the company Signotec GmbH in the last five years:

Table 1: Overview of the tested devices *(Source: authors' own elaboration)*

Method of the signature capture	Model of the dynamic biometric signature device
The active pen, display, and pen are mutually synchronized	Signotec Alpha Pad (hereinafter referred to as Alpha – ERT) ST-A4E-2-UFTE100: Color LCD Signature Pad Alpha ERT (Electromagnetic Resonance Technology)
The display is electromagnetic, the pressure is captured on the basis of the outward pressure of the passive pen on the display	Signotec Delta Pad (hereinafter referred to as Delta – ERT) Touch display ST-DERT-3-U100 ERT
The display is electromagnetic, the pressure is captured on the basis of the outward pressure of the passive pen on the display	Signotec Gamma Pad (hereinafter referred to as Gamma – ERT) Touch display ST-GERT-3-U100: 5" Color LCD Signature Pad Gamma ERT
The display is a touch-screen, the pressure is captured on the basis of the outward pressure of the passive pen	Signotec Omega Pad revision B (hereinafter referred to as OmegaOld – TD) Touch display ST-CE1075-2-U100 (old version)
	Signotec Omega Pad revision E (hereinafter referred to as OmegaNew – TD) Touch display ST-CE1075-2-U100 (current version)
	Signotec Sigma Pad revision B (hereinafter referred to as SigmaOld – TD) Touch display ST-ME105-2-U100-B (old version)
	Signotec Sigma Pad revision E (hereinafter referred to as SigmaNew – TD) Touch display ST-ME105-2-U100-B (current version)
There is no display, only the touch area	Signotec Sigma Lite (hereinafter referred to as SigmaLite – WD) Touch area without a display function STLT105-2-U100

1.1 Authentication information and authentication factor

Authentication during direct contact is based on different attributes from personal knowledge. In this case the security of authentication process is directly proportional to the maturity of applied procedure. User authentication in information technologies have to ensure the same conditions as in standard implemented activities, i.e. to ensure the data exchange between authorized users while ensuring the performed actions not being declined etc.

When communicating at a distance (remote communications) as well as in the case of man/machine communication the situation is even more complex than in the case of personal contact (physical presence of both parties – the person being authenticated and the one authenticating) because the possibility of forgery of identity is more risky (Smejkal, Kodl, 2008). For example, in the case of live voice communication (e.g. phone banking / telebanking), the level of the risk is very diversified – from high in the case of the identification of a recurring password or a small set of them (digits of the birth certificate number) to negligible (when using the chart of one-time passwords or the authentication calculator). During authentication by means of technological tools, the risk is usually medium to high while the function is not only the properties of a method or product but also the user's behaviour and properties of the environment, in which the authentication is carried out.

During authentication of a subject, the verification can be linked into the main authentication groups so called authentication factors which can be:

- knowledge (something that we know) – e.g. password, PIN, secret key;
- ownership (something that we own) – e.g. token, smart card, authentication calculator;
- characteristics (something that we are) – the biometric information which can be obvious (fingerprint, iris, etc.) or hidden (behaviourism or dynamic biometrics e.g. while walking or signing).

However, in the general literature we find one fourth authentication factor (Hortai, 2017). The 4th fact of authentication factor represents the physical location or current geographical position (e.g. personal visit of the bank or known person). In the case of electronic communication this authentication factor can serve e.g. the GPS coordinates (latitude and longitude of the present position) of the device or the location of the workstation (IP address), etc. (Lenzini et al., 2008). This 4th factor can be very useful during the direct contact but in remote communications some situations can provide probability of identity counterfeit (proxy servers, remote hacking, etc.) and so a risk of authentication. For this reason, this paper does not focus on these types of location based authentication.

1.2 Authentication factors combination and multifactor authentication

The basic authentication method is the single-factor authentication. This means that the user proves his identity by one of the three types of evidence - the proof of knowledge, the proof of ownership, the proof of characteristics of the person (or the location based which this paper does not count with).

The most common known method is the proof of knowledge - PIN, password or phrase which are attached to the identifier such as username, sign-in name or login ID. Nowadays however, we need to focus on multidimensional authentication when a solution based on a combination of two or three authentication factors are concerned (Hortai, 2015-a).

The lack of knowledge security based on one-factor authentication highlights the example of authentication failure of iCloud (cloud system from Apple Inc.) in the summer of 2014 (Arthur), when the negligence of its creators allowed hackers to hack into the users' data (big boom caused the nude photos of celebrities).

For higher security it is wise to combine the authentication factors among themselves. Venn diagrams were used for clear representation of authentication factors combinations (see Figure 2). Three basic groups are single-factor authentication where the authentication factors are separate sets of knowledge, ownership/tools and characteristics of the user/person. These factors represent many sub methods. Other variants arise by overlapping these sets (combining them with one another) which in these forms create a multifactor authentications. Option 2F-A is a two-factor authentication by combination of an authentication tool (e.g. bank card, SIM card) and knowledge based authentication (e.g. PIN). It is therefore possible to uniquely identify the owner by the authentication tool and its proper secret code. The 2F-B part comes by overlapping sets of ownership and the user's characteristics, it also represents a two-factor authentication, for example: the use of face recognition and identity cards. The last possibility of two-factor authentication is part 2F-C e.g. it is the use of a fingerprint reader along with a password. The part where all three sets are overlapping is the 3F group which represents three-factor authentication (Huang, 2011). In this issue all three authentication factors are used at least once. This presented orientation leads to a strong multifactor or multiparameter authentication where the successful solution depends upon (to some measure) on the sophisticated process for utilization of these authentication parameters.

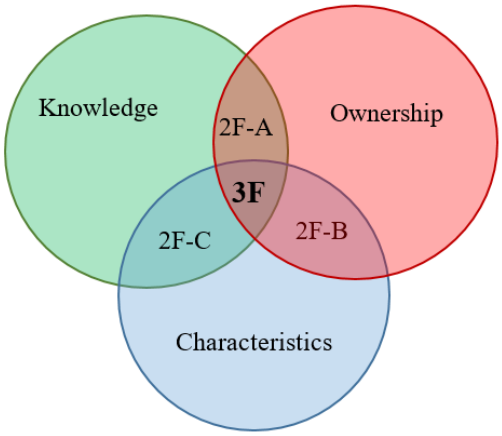


Fig 2. Combination of authentication factors *(Source: authors' own research, own elaboration)*

1.3 Authentication factors combination and multifactor authentication

Biometrics is a set of scientific disciplines which examines the human and other living organisms by measuring their unique characteristics. The recognition of people may be based on their anatomical characteristic features (physiological) or behavioural characteristics (Jain, 2015).

Biometric data are used to uniquely authenticate people. The monitored user's characteristics must be first scanned and then securely saved. The identification is done by comparing the currently measured biometric characteristics of the subject with securely saved records of these characteristics (etalons). The authentication system determines whether the authentication request accepts (the currently measured characteristics and the data of the authentication device are "identical", it is within the tolerance) or rejects it (there is a difference above the set of acceptancy threshold).

To use biometry in IT authentication systems is relatively new (compared methods of knowledge based authentication) and faces some basic problems. The main threats are possible attacks with fake biometric models. The attacker could use faked biometry for verification (e.g. authorized person's fingerprints model or rubber mask of the copied face) where the biometric sensor would measure the same biometrics as the original which were copied and so the system would "successfully" authenticate the fraud user. Protections against such attacks could be:

- Use biometrics which are difficult to model, fake or use non hidden-dynamic biometrics.
- Verify that the verified object is actually alive. There are several approaches and measurements: simple thermal readers (hand, face), blood pulse in the veins readers, capturing the visual impact of the human body (dynamics), etc.

The second problem is that there is no 100 percent reliability of biometrics sensors. Errors can occur when an authorised user is rejected from access or when a random user is evaluated as a valid one and then erroneously accesses to the system. The rates of these conditions are expressed with the variables (Banerjee and Woodard, 2012):

- **FAR - false acceptance rate**
  The false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR is typically stated as the ratio of the number of false acceptances divided by the number of identification attempts, see in equation (1) below:

$$FAR = \frac{\text{Number of false acceptances}}{\text{Total number of impostor match attempts}} \qquad \text{(Equation 1)}$$

- **FRR - false recognition rate**
  FRR is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's FRR is typically stated as the ratio of the number of false recognitions divided by the number of identification attempts, see in equation (2) below:

$$FRR = \frac{\text{Number of false recognitions}}{\text{Total number of genuine match attempts}} \qquad \text{(Equation 2)}$$

Each authentication application device puts different demands on the value of these characteristics. To have an idea of the value of these numbers I showed the example of one of the latest technology: technology Fujitsu PalmSecure which captures the unique bloodstream image of the veins in the palm of a person. In the internal research the company Fujitsu has achieved the rate of false accept FAR less than 0.00008% and a false rejection rate of only FRR = 0.01%. Some banking companies think this technology will replace credit cards in the future (Fujitsu, 2014).

1.4 Biometric verification according to the number of comparisons

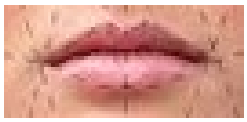
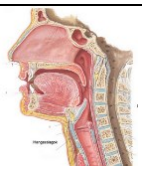
Comparison of **1 to many**: the present verified biometric sample is compared to each one of the given database samples (e. g. used in forensic sciences when the criminal is not known). The disadvantages of this approach are a higher risk of identification errors (wrong evaluations) and higher requirements of computing power of the verification system through comparing more samples.

Comparisons **1 to 1:** the present verified biometric sample is compared to the particular sample of the verified person. In this case preliminary identification (e.g. name, ID) of the verified person is required. This solution provides higher security and eliminates authentication mistakes with other entities.

1.5 Dynamic Biometric characteristics

Each biometric characteristic has its effectiveness and disadvantages, and the choice depends on the specific application. No single biometric is expected to successfully meet all of the requirements (e.g., accuracy, practicality, and cost) of all applications (e.g., digital right management, access control, and welfare distribution) (Pal et al., 2014). Recent years instigated discussions about the use of biometric methods which, in the case of their static form still contain significant execution risk of accepting spurious persons based on the stolen or fraudulent (counterfeit) biometric information (fake fingerprint, iris image, etc.) (Smejkal, Kodl, 2011). Hence in light of the listed reasons, the focus has shifted on the dynamic biometric methods based on the human expressions, such as voice analysis, dynamics of movements, pressing computer keys, walking or writing. Dynamic biometric methods are based on capturing behaviourism or expressions of the authenticated person in the given period of the time. Dynamic biometrics are represented in Table 2 below.

Table 2: Overview of the tested devices *(Source: authors' own elaboration)*

Human expressions, face gesticulations		Dynamics of pressing keyboard or console	
Human eye: pupil / iris movement		Screen touch dynamics	
Mouth movements		Dynamics of mouse movements	
Human voice dynamics analysis		Dynamics of handwritten signature	
Dynamics of walking			

Walking dynamics

The entire method works by comparing the pathways curves that describe the specific points of the body while moving. It is assumed that each person has their own: motion reactions, muscle-skeletal system and dynamic stereotypes, so everyone walks differently. Movement segmentation can be scanned in simple or complex scenes. Movement dynamics are detected at the centre of gravity of the body and at the break points of the body (usually the hips, joints: knee and ankle) (Rak et al., 2008).

This method needs to create the pattern of the user's movement and to scan it enough space of the movement parameters is required. The advantage in this method is the simple deployment of cameras for example in public places (useful for forensic application) or for better resolution specialized room is required for the authentication. The disadvantage is that it is difficult to determine the biometric pattern through the influence of psychological and physical condition of the individual. Movement of the individuals are unique and are suitable for comparison and for 1:1 identification. Identification through

walking is more solved in the field of forensic science (Straus, Jonák, 2008) than solved as authentication technology.

Human voice dynamics analysis

The verification is based on the analysis of sound, vibration, pronunciation and speed of the human voice/speech. The voice characteristics depend on the person's vocal cords size, mouth, nasal cavity, and further human parts in creation of the voice. These analyses can be divided into two main groups:

- Statistical analyses - independent of the text, working with long-term mean values, histograms, using only voiced segments - basic tone (frequency) of speech, long-term spectrum of the speech coefficients LPC (Linear Predictive Coding), correlation and covariance matrix of individual symptoms (Han et al., 2006).
- Dynamical analyses - suitable for the recognition of the speaker according to the text, to the determination of the time profiles of the selected speech parameters (Trevisan et al.,2015) - the basic tone of the speech, frequency spectrum, the first formant, cylindrical vocal tract model, etc.

Some authentication technologies make their decision on an analysis of words and whole sentences which are know only to the authenticated spokesman. Thus, this is a two-factor authentication based on speech recognition and the validation of the knowledge (password or paraphrase). It is mainly used for authentication through voice communications: phone, VoIP (voice over internet protocol), etc. The advantage is that there is no need to implement any additional hardware. The user speaks into a device's microphone and that is well known and acceptable for users. The downside is that the verification may be affected by the user's health status (colds, fever, mental state of the speaker), ambient noise etc. In remote communication there is high risk of counterfeit: speech records, learned voice imitator algorithm, etc. (Smejkal, 2015).

Human face movements

This part summarizes the dynamics of human face expressions, gesticulations, eyes and mouth movements. Each of these have to be captured by a camera for a period of time and evaluated by specified algorithm so called computer vision methods (Hortai, 2015- b).

The Literature on face recognition technology discusses the issue of face spoofing which can bypass the authentication system by placing a photo/video/mask of the enrolled person in front of the camera. This problem could be minimized by detecting the liveness of the person by using eye and mouth movements (Singh, 2014).

Dynamics of pressing keyboard or console

Each person writes otherwise (speed, time of presses key/button, frequency of keystroke, the length of the pause etc.) In this method it is difficult to create a precise etalon - it is necessary to re-write the text samples while capturing its dynamics (type more words several times, thereby reducing the error rate in afterwards verifying).

The advantage in this method is that it doesn't require any additional hardware. It uses the already implemented hardware (e.g. console, keyboard) (Banerjee and Woodard 2012). In IT systems, to verify the user they have to login first, and then they can be verified by scanning their key strokes. This method can be used as further verification of users which are already logged into the system and reveal unusual behaviour (no or too fast typing means that it is using an algorithm and not a real person), protecting the computer from children, etc.

This activity can be interrupted, or the user's dynamics can be affected with fatigue or stress and by hand injuries this method is unusable for authentication (Tresner, Salykin, 2016). This solution represents a less accurate method (volatility of typing and high values of FRR) and should serve just as an additional authenticating method.

Dynamics of mouse movements

The user had to draw a determined shape which has been drawn in creating the reference etalon. To create user's etalon, it is necessary to draw the image a few times. By identification the drawn patterns specific features are extracted such as position, speed, strength and roundness, etc. which are then compared with the user's standard etalon. Properties are similar to the dynamics of typing and are rather useful for verification (Zheng et al, 2011) after the user logs into the system.

Screen touch dynamics

Touch-screens, such as smartphones and tablets have the signs of user's behavioural reflection. In this case the screen touch parameters can be measured (speed, touch frequency, time and force of pressure, the length of the pauses, etc.). (XI Zhao et al, 2014)

Dynamics of handwritten signature

The biomechanical processes involved in the production of the human signature are very complex and not yet fully understood. In vastly simplified terms, the primary excitation is thought to occur in the central nervous system, more specifically in the human brain, with predefined intensity and duration describing the intent of the movement. The signal of the intent (or the movement plan) is passed through the spinal cord to the particular muscles which are activated in the intended order and intensity. As a result of such activation and loosen of the muscles and whilst holding a pen, the resultant of the arm movement is recorded in the form of a trail on the paper – the handwritten signature. Each individual person has an individual set of component movements (Smejkal et al., 2013).

Automatic signature verification can be divided into two main areas depending on the data acquisition method (Lopez-Garcia, 2014):

- offline (off-line),
- online (on-line) signature verification.

Off-line systems utilize the classic method of on-paper signature for the verification of a person. The obtained signature is digitized by an optical scanner or camera. There is an alternative to input the image through a tablet or any other suitable device. Subsequently, respective application determines the match of the person's signature with a reference sample by comparing the overall trace (image) of the signature (Diaz et al., 2015). These methods are based on this particular principle and used to verify handwritten signatures. These methods are very unreliable and commonly practiced for example in retail and banking, where they are relying on the human factor in the form of a calligraphy expert (Smejkal, Kodl, 2011).

On-line systems analyze the dynamical characteristics of handwriting which are obtained in real time, using specialized tablets, touch screens, PDAs, or other suitable devices (Francis et al., 2015). The verified person signs with their signature like on some paper or on the scan surface of the device or can use a specialized pen (the sensors are embedded in the pen). The dynamics, i.e. the whole process of creation of the signature in time is monitored. The handwriting's dynamic properties are scanned i.e. the speed of the signature, acceleration of movements, timing, pressure and direction of the thrust, which are recorded in a multi-dimensional coordinate system (Galbally et al., 2015). The two dimensions of the signature movement are used to determine the speed and direction of the thrust, the third basic coordinate determines the contact pressure (Smejkal et al., 2013). The sensing units may vary from various manufacturers by the number of the monitored biometric vectors information (Lopez-Garcia, 2014) and also the value of reliability may differs (values of FRR and FAR).

The System after loading the parameters of the signature joins other information of the signed user such as user's name, current time and date, the size of the document, etc. All the data are then encrypted, and the so-called biometric marker is created and is sent for further processing (including in the signed document, login audit).

2. Discussion

The authentication methods should meet the variability in terms of applied technologies and systems, and in terms of users themselves. The proposed solution must also fulfill the requirements of the legal rights of the involved communication parties and authorized users. In the case of official or banking operations it has to meet the proper conclusion of the contract for transactions execution.

Passwords can only be used at the lowest level of security. They are relatively easily observable, transferable and hackable by attacks (He and Wang, 2015). Tokens can be used for higher degrees of security. They are transferable and can be lost or stolen. The combination of token and password can be used for a relatively high degree of security (2 factor authentication). The combination of knowledge (password) and ownership (token) based authentication is highly resistant when the authentication tool is lost or stolen but again the human factor can fail and cause "inadvertent" disclosure of password or lending/borrowing the token to others (it is transferable). A key assumption

for constructing secure information systems is ensuring the proper identification and authentication of people, assets and events in the system (Smejkal, Kodl, 2016). It is only after high quality authentication that we can move to the next essential step, which is authorisation. For these reasons, it is important to focus on the issue of multifactor authentication, in particular where biometric methods play an important role.

Biometric characteristics of humans are not transferable (by the mean of originality) and so they cannot be lost by normal circumstances. Biometrics can be used as authentication for the highest security level especially the hidden forms of biometrics. The demands for biometric verification were clarified (see the corresponding section). Static biometric samples still contain significant security risk of accepting frauds which use fraudulent (counterfeit) biometric samples (fake fingerprint, iris image, etc.). Static biometric authentication even has the risk of the user physically forced authentication. Users can be authenticated against their will by putting their biometrics into scanners, or even drastically steal the original biometry of the user, e.g. cut down the user's finger and use it to bypass the authentication (this can be partially eliminated by checking the biometric sample aliveness). For these reasons the focus has shifted on the dynamic biometric methods which capture the hidden parameters of the human expression and the behaviourism of a particular person in time (see listed in Table 2).

The final decision of authentication method is selected from the listed dynamic biometric methods. The decision is based on the following conditions and circumstances (gradually eliminated by the selection of dynamic biometric methods):

Area and space independency

Walking dynamics is eliminated because for accurate walk sensing fine-tuned circumstances and enough space is required. Voice / speech is not applicable for the surrounding area noise/buzz.

Process continuity and stability:

Generally: in static systems the variables can be uniquely determined by the present values of control/input variables, in contrast to the dynamic systems whose output (status) is dependent not only on the present value of the input but also on previous values of inputs and conditions of the system (depending on the depth of memory). The more time is scanned the more accurate the system could be (in this case a person identification).

Empirically: the idea that the user should be pursued in a long time for authentication is absurd (too time-consuming). In dynamic behaviour the longer time perspective additionally integrates mistakes by ambient conditions. There can be signs of interruption of routine behaviour while the person authentication which could be then detected as a fake user (in the case of circumstances ignorance) and causes errors. So we are looking for a main authentication method which could be done at once and without ambient disturbance. Discontinuous process could be stumbling while walking (so it eliminated from the final selection) or interrupted by a conversation of another person, mood symptoms, interruption with a non-standard idea or thought: dynamics of keyboard or console pressing, mouse movement dynamics, dynamic touch screens. These methods were eliminated from the selection this way. Partly the methods of: facial gestures, eye movements and lips movements could be eliminated from the final selection due to the impact of the surrounding circumstances (physical, psychical state of the user). This remaining method mostly serve as additional authentication e.g. whether the subject is alive (discussed further).

The handwritten signature can be done at once. It is common for the person providing a signature to be exposed to stress, one reason for this being the importance of the situation in which they are appending the signature. After all, stress and very often negative stress, is one of the most common emotion in human life. In a different experiment it was examined whether and in what way stress influences the quality and constancy of DBS. In the experiments made by Smejkal, Kodl and Sieger (2016) extreme situations were used in which test subjects in survival courses (X-tream course) at the University of Defence of the Czech Republic found themselves, while used the d2 Test of Attention and signature stability at the start, in the middle, and at the end of the course. The results of the experiments showed that irrespective of the stress levels of the participants, the stability of their DBS was high, respectively actually improved.

To be user-friendly and acceptable for users

This is a subjective matter of each of individual. Empirically, to encourage the users to make grimaces (facial gestures), sticking out her tongue (lip movements) or move the eyes may not be acceptable for

all the users. These methods could be used rather than complementary methods (voice / speech-lip movements as aliveness check of the user). Signature is a natural, easily available, well-known tool for users to prove their identity. Earlier experiment showed that DBS is also well accepted by the users (see Hortai, 2017) so we can presume it is also user-friendly.

Test the subject aliveness via automated remote testing:

In personal contact the aliveness is obvious. When remotely communicating occurs the aliveness of the user has to be checked. Voice/speech is transmittable via electronical communication channels but forgeries with sound recordings, etc. still represent security risks. Aliveness test could be solved by interactivity of the verified person that goes on spite of the above conditions (can be used independently from space - ambient noise, noise, process continuity - can be interrupted; acceptability to users - to answer questions of a personal nature by proving knowledge).

When remotely communicating occurs in the case of DBS we can assume an axiom that each signature is unique (empirically: two similar created signatures from the same person will never be 100% identical). This topic is solved in the conclusion part.

3. Paper results

To use biometric authentication a measurable biometry is demanded. Biometric data must undergo the legislation of the given country which is mostly regulated by the law of protection of personal data. Table 3 collects the regulations and standards for biometric methods and technology, mainly the joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) whose purpose is to develop, maintain and promote standards in the fields of information technology (IT) and Information and Communications Technology (ICT).

Table 3: List of standards related to biometrics *(Source: authors' own elaboration)*

Label	Name
ISO/IEC 2382-37	Information technology –Vocabulary - Part 37: Biometrics
ISO/IEC 7816-11	Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods
ISO/IEC 19792	Information technology -- Security techniques -- Security evaluation of biometrics
ISO/IEC 19794-1	Information technology – Biometric data interchange formats – Part 1: Framework
ISO/IEC 19794-10	Information technology -- Biometric data interchange formats -- Part 10: Hand geometry silhouette data
ISO/IEC 19794-11	Information technology -- Biometric data interchange formats -- Part 11: Signature/sign processed dynamic data
ISO/IEC 19794-14	Information technology -- Biometric data interchange formats -- Part 14: DNA data
ISO/IEC 19794-2	Information technology -- Biometric data interchange formats -- Part 2: Finger minutiae data
ISO/IEC 19794-3	Information technology -- Biometric data interchange formats -- Part 3: Finger pattern spectral data
ISO/IEC 19794-4	Information technology -- Biometric data interchange formats -- Part 4: Finger image data
ISO/IEC 19794-5	Information technology -- Biometric data interchange formats -- Part 5: Face image data
ISO/IEC 19794-6	Information technology -- Biometric data interchange formats -- Part 6: Iris image data
ISO/IEC 19794-7	Information technology -- Biometric data interchange formats -- Part 7: Signature/sign time series data

Label	Name
ISO/IEC 19794-8	Information technology -- Biometric data interchange formats -- Part 8: Finger pattern skeletal data
ISO/IEC 19794-9	Information technology -- Biometric data interchange formats -- Part 9: Vascular image data
ISO/IEC 19795-1	Information technology -- Biometric performance testing and reporting -- Part 1: Principles and framework
ISO/IEC 19795-2	Information technology -- Biometric performance testing and reporting -- Part 2: Testing methodologies for technology and scenario evaluation
ISO/IEC 19795-4	Information technology -- Biometric performance testing and reporting -- Part 4: Interoperability performance testing
ISO/IEC 19795-7	Information technology -- Biometric performance testing and reporting -- Part 7: Testing of on-card biometric comparison algorithms
ISO/IEC TR 19795-3	Information technology -- Biometric performance testing and reporting -- Part 3: Modality-specific testing
ISO/IEC 19785-2	Information technology -- Common Biometric Exchange Formats Framework -- Part 2: Procedures for the operation of the Biometric Registration Authority
ISO/IEC 19785-4	Information technology -- Common Biometric Exchange Formats Framework -- Part 4: Security block format specifications
ISO/IEC 24761	Information technology -- Security techniques -- Authentication context for biometrics
ISO/IEC 24745	Information technology -- Security techniques -- Biometric information protection
P CEN/TS 16428	Biometrics Interoperability profiles - Best Practices for slap tenprint captures
ISO 19092	Financial services -- Biometrics -- Security framework

3.1 Advantages of biometric verification

During the life of the individuals some biometric characteristics does not change (e.g. DNA) or has very slow change in time (vein in your arm).

Biometric technologies have high percentage of reliability (depending on the method and implementation).

The applicants have the proof of identity always with them. The users do not need to worry about the loss or theft of the authentication tools or to worry about forgetting passwords.

High resistance to the theft of the original mark (included in the body of the user).

3.2 Disadvantages of biometric verification

Biometric technologies need to use additional hardware (e.g. biometric scanner). Compared to other authentication factors it has relatively higher complexity and could have difficulty for the technical and financial resources (system implementation, evaluation algorithms, sensors, creating a database of patterns) which depend on the chosen biometric method.

It is required that the users participate in the creation of authentication patters (creating biometrics pattern, etc.) compared to other authentication factors which can be sent by e-mail (password) or delivered (auth. tools).

It has various errors, the values of FAR and FRR.

Possibilities of counterfeiting the biometric systems which can be:

- On the side of the sensor: the static biometrics are weak against fake biometric features e.g. synthetic models (e.g. synthetized fake fingerprint, rubber facial mask reassembled from authorized users' characteristics). This option is not valid for dynamic biometrics.
- On the side of the processing / comparison: extractor modification, modification of templates, exchange in the pattern database, blocking the communication channel (man-in-the-middle attacks).

To eliminate these threats it is necessary to secure the database characteristics patterns and secure the communication channels of the verification devices and sensors.

3.3 Measurements of DBS (dynamic biometric signature)

DBS were recorded on the devices using the program signoSign2 (version 10.4.5) produced by Signotec. Each participant made 10 signatures on each device to a separate *.pdf file. From the 10 times signed pdf file the biometric data were exported, so the final matrix of signatures of each participant and all devices was formed: $P_{ij} = [x_1, \dots, x_{10}]_{ij}$; where *i* is a serial number of the device, *j* is a serial number of the participant, x_k (k = 1, … , 10) is the particular signature.

In accordance with the findings from the previous works (Smejkal, Kodl, 2014; Smejkal et al., 2016), the first signatures made by each person on the devices were not included in the evaluation. For the signature match rate automatic evaluation, a special algorithm was created which uses the original analytical software of the device manufacturer (Signotec - eSig-Analyze). The end result was a data matrix where the signature matches were evaluated among themselves in percent for every person each. Every person (40 people) had 8 times (number of the devices) 10 signatures which in one case had 36 signature alikeness comparisons. The overall 11520 signature alikeness comparison data were then used for calculations. The following values of selective means and unbiased estimates for variances of the degree of compliance of signatures were detected on the stated devices (Table 4):

Table 4: selective means and unbiased estimates for variances of the degree of compliance of signatures on the tested devices *(Source: authors' own research)*

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

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 the average percentage 79.33 % with the standard deviation of σ = 13.16 %. 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.

There was no statistically significant difference in the means and variances of the degree of compliance of signatures of a particular person on individual devices. The different scanning technology does not affect the degree of compliance and variability of signatures (see Table 3). In the opinion of the authors, the "user-friendliness" is a key factor in creating the signature. Another factor is then the individual characteristics of the signer. The variability of the signature, and hence the low degree of compliance among individual signatures, which is exceptionally manifested among the signers, is closely related to the stability of the signature. The greater the intra-personal variability is, the less stable the signer is (see Parziale et al., 2015).

4. Conclusion

In summary it can be concluded that every type of security method can undergo attacks. These threats can be reduced by using various authentication methods in combination with each other. On the other hand, the combination of too much authentication methods will lead to a rise in costs and an increased level of the user "harassment".

In the case of biometric system it is advisable to choose a biometry that is “easily” measurable and have stable properties in time. It is a wise choice for a user-friendly method no to disturb the users too much (which includes the necessary steps for authenticating and the time consuming part for this). To be able to authenticate all users all the users have to possess this biometry. Depending on the secured values (access to values, documents) a compromise should be considered between the secured values and the cost of effectiveness of the chosen authentication method.

Based on the conditions in the discussion part, the dynamic biometric signature (DBS) was selected as the main dynamic biometric authentication method which can be suitable for e.g. business and intercorporate communication. Signature is a natural, easily available, well-known tool for users to prove their identity. Earlier experiment showed that DBS is also well accepted by the users.

When authenticating a person, we generally employ the “1 to many” model, meaning that we compare the scanned record with all the records in the database of people. Some disadvantages of this are the higher risk of mistaken identification and high demands on computing power in the system. We remove this problem by using a prior identification step (entering identification data such as name, number, ID etc.), which can be done both in the case of authentication using a general record and also for authentication using a signature. To ensure higher safety (by means of lower global FAR value) and to lower the processing demands the verification should be based on 1-to-1 comparison (while verification the user’s biometric signature is compared to their specific signature). In the case of DBS the user is obvious due the signing process.

As it was discussed, each individual has an individual set of component movements. This enables verification of the signature to be based on the stability of the set of component movements during their implementation. A decisive indicator for a DBS is that this unique set significantly eliminates the possibility of its reconstruction by a counterfeiter. Regarding alleged changes in a signature due to aging and other influences, it is important to realise that two identical signatures do not exist – or rather, if they are identical, we can be sure that they are a so-called technical forgery, produced by copying from a specimen. Hence it is crucial to know how the level of agreement between the signature and its specimen should be set for automatic evaluation to ensure that handwriting experts only receive signatures in exceptional cases. One important attribute of the 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, and so there is no need to develop additional mechanisms to test whether the subject is present and alive or not – unlike with static biometric methods (checking the print of a finger, palm, iris etc.) It is also legally beneficial that we can rely on the (theoretically rebuttable) assumption that the person knew what he or she was signing.

DBS has the advantage compared to other dynamic authentication that the signature can be used immediately in authentication. For this authentication method no special premises or longer period of time is required (compered to e.g. walking dynamics). Signing is a stable, non-interrupted process due to the signature process done at once.

Legislation: the ISO/IEC 19794-7 standard (Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data standard) specify the scanned channels which are recorded in the DBS. According to ISO/IEC 19794-7 standard the following channels are recorded (in effect the parameters DBS) in Table 5:

Scanning dynamic parameters when creating a signature is done through a special signature tablet. During the retrieval of signature data the tablet acquires biometric data (usually x and y coordinates, pressure, time). These biometric data are also used to calculate other parameters defined by ISO/IEC 19794-11 Information technology. Biometric data interchange formats. Part 11: Signature/sign processed dynamic data.

Table 5: DBS channels *(Source: ISO/IEC 19794-7 standard, 2014)*

Channel name	Interpretation
X	x coordinate (horizontal pen position)
Y	y coordinate (vertical pen position)
Z	z coordinate (height of pen above the writing plane)
VX	velocity in x direction
VY	velocity in y direction
AX	acceleration in x direction
AY	acceleration in y direction
T	time
DT	time difference
F	pen tip force (pressure)
S	tip switch state (touching/not touching the writing plane)
TX	tilt along the x axis
TY	tilt along the y axis
Az	azimuth angle of the pen (yaw)
El	elevation angle of the pen (pitch)
R	rotation (rotation about the pen axis)

To use DBS on electronic identification and trust services for electronic transactions in the internal market, the given country regulation has to be used and for the internal intercorporate communication the security policy of the organization has to be used. DBS can assure protection against signature frauds, environmental friendliness (saving paper), and direct insertion into electronic information systems where it ensures the integrity of the signed document. In this case the regulation in EU No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (repealing Directive 1999/93/EC) has to be followed. The dynamic biometric signature is in accordance with the eIDAS Regulation (Regulation (EU) No 910/2014 of the European Parliament and of the Council), which became valid on 17 September 2014 and focuses on the secure identification of people in electronic communication, respectively the provision of remote services. 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 and also bringing significant organisational and technical problems during the deployment of a guaranteed or qualified electronic signature (Advanced Electronic Signature, Qualified Electronic Signature) under the eIDAS Regulation. Its advantage over a cryptographic electronic signature is the existence of this "handwritten" quality.

In case of DBS technology of the used channels (defined by ISO/IEC 19794-7 standard), the used acquiring technology, the evaluating algorithm, and the performance may vary among the technology manufacturers. The FAR and FRR are also dynamical and related to the users' intra-personal variability, the length of his or her signature itself, etc. One of the main new findings was that no statistically significant difference in the means and variances of the degree of compliance of signatures of a particular person on individual devices.

Costs related by implementing an authentication system (purchasing, service, user training, etc.) depend on the types of authentication technology used (accuracy, options, multifactor authentication, etc. of the system), the size of the company, number of employees, etc. The communication and the sensitivity of secured data also is important. It makes no sense to implement strong authentication to secure data that in case they would be lost or abused would have caused less damage than the costs of implement of the chosen authentication system. In this case other risk reduction or risk retention should be used.

Acknowledgements

This paper was supported from the Internal Grant Agency at Brno University of Technology by grant: FP-J-17-4137 Expert methods and ICT support for risk management in enterprises.

The research could be done thanks to the Moravian University College Olomouc, its academic staff, and students for active participation and also thanks to the company Contrisys spol. s r. o. for the lease of equipment and technical support.

References

Arthur, Charles, 2014: Naked celebrity hack: security experts focus on iCloud backup theory. *The Guardian* [Online]. september 1, 2014. Retrieved (26-01-2017): https://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence

Banerjee, S.P. & Woodard, D.L., 2012: Biometric authentication and identification using keystroke dynamics: A survey. *Journal of Pattern Recognition Research*, 7(1), pp.116-139

Diaz, M., Ferrer, M. A., Pirlo, G., Giannico, G., Henriquez, P., & Impedovo, D., 2015: Off-line signature stability by optical flow: Feasibility study of predicting the verifier performance. In *Security Technology (ICCST), 2015 International Carnahan Conference on* (pp. 341-345). IEEE. ISBN 978-9-860-46303-3

Francis, F., Aparna, M.S. & Vincent, A., 2015: Biometric Online Signature Verification*. IOSR Journal of Electronics and Communication Engineering*, pp. 82-89

FUJITSU, 2014: PalmSecure datasheet. [online]. [cit. 2017-03-26], Retrieved from: http://www.fujitsu.com/downloads/COMP/ffna/palm-vein/palmsecure_datasheet.pdf

Galbally, J. Diaz-Cabrera, M., Ferrer, M. A., Gomez-Barrero, M., Morales, A., & Fierrez, J., 2015: On-line signature recognition through the combination of real dynamic data and synthetically generated static data. *Pattern Recognition*, Volume 48, Issue 9, 1 September 2015, Pages 2921-2934. ISSN: 00313203

Han, Wei, Chan, Cheong-Fat, Choy, Chiu-Sing and Pun, Kong-Pang, 2006: An efficient MFCC extraction method in speech recognition. *IEEE International Symposium on Circuits and Systems*, Island of Kos, 2006, pp. 4 pp.-.doi: 10.1109/ISCAS.2006.1692543

He, D. and Wang, D., 2015: Robust biometrics-based authentication scheme for multiserver environment. *IEEE Systems Journal*, 9(3), pp.816-823

Hortai, F., 2015-a: Dynamický biometrický podpis ako efektívny nástroj pre autentizáciu. In QUAERE 2015. Hradec Králové: MAGNANIMITAS, 2015. s. 1344-1352. ISBN: 978-80-87952-10- 8

Hortai, F., 2015-b: Low- cost data mining application via unused smartphone devices using computer vision and relevant data security issues. In *18 Annual International Conference Enterprise and Competitive Environment Conference Proceedings*. First edition. Brno: Mendel University in Brno, 2015. p. 304-313. ISBN: 978-80-7509-342- 4

Hortai, F., :2017: Options and Benefits of authentication system via Dynamic Biometric Signature. In *International Day of Science 2017 - Economics, Managemnet, Innovation*. Olomouc: Moravian University College Olomouc, 2017. p. 75-83. ISBN: 978-80-7455-060- 7

Huang, X., Xiang, Y., Chonka, A., Zhou, J. and Deng, R.H., 2011: A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, 22(8), pp.1390-1397

ISO/IEC 19794-7 standard, 2014: *Information technology -- Biometric data interchange formats -- Part 7: Signature/sign time series data.* URL at*:* https://www.iso.org/standard/55938.html [Accessed 30 January 2015]

Jain, Anil and Arun Ross, 2015: Bridging the gap: from biometrics to forensics. *Philosophical transactions - Royal Society*, 370(1674), 20140254 [cit. 2017-03-31].. ISSN 09628436. DOI: 10.1098/rstb.2014.0254.

Kodl J. Jr., 2010: Mechanisms of Human Arm Motion Planning in the Presence of Multiple Solutions. Imperial College, London

Koch, M., & Chvátalová, Z., 2017: Information Systems Efficiency Model. *Journal of Systems Integration*, *8*(3), 3-9

Lenzini, G. Bargh, M. S. and Hulsebosch, B., 2008: Trust-enhanced Security in Location-based Adaptive Authentication. Electronic Notes in: *Theoretical Computer Science*. Volume 197, Issue 2, Pages 105–119. Proceedings of the 3rd International Workshop on Security and Trust Management

Lopez-Garcia, M. et al., 2014: Embedded system for biometric online signature verification. *IEEE Transactions on Industrial Informatics.* Publisher: IEEE Computer Society. ISSN: 15513203

Mates, P. & Smejkal, V., 2012: *E-government v České republice: právní a technologické aspekty*, 2nd edition, Praha: Leges. ISBN 978-80-87576-36-6

Pal, S., Pal, U. & Blumenstein, M., 2014: Signature-based Biometric Authentication. in *Computational Intelligence in Digital Forensics: Forensic Investigation and Applications*, (Eds. Editors: Azah Kamilah Muda, Yun-Huoy Choo, Ajith Abraham, Sargur N. Srihari), pp.285-314

Parziale, A., Fuschetto, S. G. & Marcelli, A., 2013: Exploiting stability regions for online signature verification. In *International Conference on Image Analysis and Processing* (pp. 112-121). Springer, Berlin, Heidelberg

Porada, V. and Smejkal, V., 2017: Forensic identification and its possibilities in the process of detection, investigation and proving of cyber offences. In *International Day of Science 2017 - Economics, Managemnet, Innovation*. Olomouc: Moravian University College Olomouc, 2017. ISBN: 978-80-7455-060- 7

Rak, R. Matyáš, V. Říha, Z., 2008: Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: GRADA. ISBN 978-80-247-2365-5

Singh, Avinash Kumar; Joshi, Piyush; Nandi, Gora Chand, 2014: Face recognition with liveness detection using eye and mouth movement. In: *Signal Propagation and Computer Technology (ICSPCT), 2014 International Conference on. IEEE*, 2014. p. 592-597

Smejkal, V., 2015, Kybernetická kriminalita, Plzeň: Aleš Čeněk. 636 p. ISBN: 978-80-7380-501- 2

Smejkal, V. Kodl, J., 2011: Strong authentication using dynamic biometric signature. Published in: 2011 *Carnahan Conference on Security Technology. IEEE*, s. 1-5. ISBN 978-1-4577-0903-6, ISSN 1071-6572

Smejkal, V. Kodl, J., Kodl, J. Jr., 2013: Implementing trustworthy dynamic biometric signature according to the electronic signature regulations. In: *47th International Carnahan Conference on Security Technology*, ICCST 2013; Medellin; Colombia. ISSN: 10716572 ISBN: 978-147990889-9

Smejkal, V., Kodl, J., 2008: Development trends of electronic authentication. *Proceedings of the 42nd Annual Conference IEEE International Carnahan Conference on Security Technology*, Diplomat Hotel Prague, Czech Republic, October 13 - 16, 2008, p. 1 – 6

Smejkal, V.; Kodl, J.; Sieger, L., 2016: The Influence of Stress on Biometric Signature Stability. In *Proceedings of 50th Annual 2016 IEEE International Carnahan Conference on Security Technology*. Orlando, Florida: Institute of Electrical and Electronics Engineers, 2016. s. 37-41. ISBN: 978-1-5090-1070- 7

Smejkal, V. and Kodl, J., 2016: Authentication and Encryption in Ensuring the Security of Information Systems. In: Lisník, A., Pavlíček, A. (ed.) Current Trends and Challenges in Economics and *Management. Conference proceedings of the international conference* "The message of John Paul II", 21.-22. 4. 2016, Poprad: VERBUM – 2017, p. 251-262. ISBN 978-80-561-0440-8

Smejkal, V. and Kodl, J., 2014: Assessment of the authenticity of Dynamic Biometric Signature. The results of experiments, *Proceedings of 48th Annual 2014 IEEE International Carnahan Conference on Security Technology (ICCST)*, 13-16 October 2014, Roma, Italia, s. 45–49, ISBN: 978-1-4799-3530-7

Straus, J and Jonák, J., 2008: Využití záznamů z bezpečnostních kamer ve forenzní praxi. *Akadémia Policajného zboru SR*, Vydanie: V Tribunu EU vyd. 1. Vydavateľ: Brno: Tribun EU

Trevisan, M.A., Eguia, M.C. and Mindlin, G.B., 2005: Topological voiceprints for speaker identification. *Physica D: Nonlinear Phenomena*, 200(1), pp.75-80

JEL Classification: K20, L63