Biometrics Selection and Their Influence over the Life Cycle of Electronic Identity Documents

DIMITAR GEORGIEV
School for PhD students
Technical University of Sofia
8 Kliment Ohridski Blvd., 1756 Sofia
BULGARIA
dimitargeogiev11@gmail.com http://ff.tu-sofia.bg/

TASHO TASHEV
Electrical Measurement Systems Dept.
Technical University of Sofia
8 Kliment Ohridski Blvd., 1756 Sofia
BULGARIA
ttashev@tu-sofia.bg http://elfe.tu-sofia.bg

IVO DRAGANOV
Radio Communications and Video Technologies Dept.
Technical University of Sofia
8 Kliment Ohridski Blvd., 1756 Sofia
BULGARIA
idraganov@tu-sofia.bg http://rcvt.tu-sofia.bg

Abstract: - In this paper is presented an extensive overview of the biometrics that are commonly used in the electronic identity documents or are considered perspective for future use for digital personal identification at large scale. All the presented features are compared based on their advantages and disadvantages concerning the practicality of feature extraction, identification accuracy, accessibility, needed effort and cost. They include face, finger print, iris, finger vein, voice, and lips. The level of trust, long term stability and template size are the other qualities taken into consideration during this study. The mutual influence of the application factors in relation to each characteristic type during exploitation is evaluated by analysis of the False Acceptance Rate and False Rejection Rate parameters of already developed systems. Advantageous suggestions are made for the future use of biometrics within the existing frameworks for personal identification.

Key-Words: - Biometrics, Identity Document, Face, Fingerprint, Iris, Finger Vein

1 Introduction

Biometric features are distinctive characteristics for every human which are measured from the body or represent specific behavioral properties observed over time. As such applied in engineering fields they are supposed to be unique for each person making possible one's identification with a satisfactory level of confidence.

Jain et al. [1] propose a model for the operation of contemporary biometric systems including four phases - data acquisition, evaluation and feature generation, scores estimation between input data and stored information in a database. The latter is recorded during the enrollment process. Using a suitable sensor, typically in the form of a reader, the actual biometric is transformed into digital values forming a template for later matching with unlabeled features that need to be identified. The process may be a part of verification, authentication or recognition in unconstrained environment.

Biometric features became an important part of citizen's identification for governmental purposes in the last decade [2]. Specifically, the images of a face, fingerprints and irises are incorporated in modern personal electronic documents, either for internal state identification (ID cards, residence permits, etc.) or for travel abroad – e-passports. The internationally interoperable infrastructure for identity verification opens new frontiers also in front of the electronic commerce, local governance, e-Health systems and others.

In this study an extensive overview is done of the most popular biometrics which are currently used or seem to have the potential to be embedded into the personal identification documents in the future. Their qualities are summarized in Section 2 of this paper in two groups concerning advantages and disadvantages mainly based on practicality. The measures used for estimation of the identification systems performance in terms of accuracy are given in Section 3. In Section 4 risk analysis of biometrics use for personal identification is made, and finally, in Section 5 a conclusion is presented.

2 Biometrics Selection for Digital Identification

Some of the most popular biometrics used for digital identification within the electronic Machine Readable Travel Documents (eMRTD) include face, signature, finger print, and iris. Also, perspective for future use are considered finger veins, lips and voice. Other biometric signals, such as the human scent, electroencephalogram (EEG), skin spectrum, knuckles and finger nails shape are still outside the reach of mass introduced identification systems. The advantages and disadvantages of the most popular features based on accuracy, the needed effort from the users during the enrollment and identification phases, intrusiveness, and cost are summarized below.

2.1 Face

The most popular technique for personal identification is face recognition. It relies on distinctive facial descriptors which may be constructed from a set of single points or the color and intensity properties of complete regions, sometimes also combining them together [3]. Thus, a particular person could be recognized in automated fashion from a digital image. The latter is opposed to a set of preliminary stored and labeled images in a database.

Advantages – there is no ne ed to collect any physical samples during identification or investigation, possibly from a cr ime scene or a location of an accident but rather rely only on a photo or video footage. The absence of a straight contact with the subject makes the acquisition process sanitary. No collaboration from the individual is needed and monitoring sometimes accompanied by tracking is easier to implement. Authentication and verification are done in contactless manner. Currently, detection of a particular face among multitude of other faces in public places is well-developed approach. As a result large scale identifications become possible in contrast to systems employing other biometrics.

Disadvantages – various lighting conditions (Fig. 1), emotional expressions and spatial positioning of the head make face recognition hard to perform in real-world environment. In a number of countries the photo included in the issued passports is mandatory to be taken at neutral emotional state. The field of view of the camera covers faces, especially when in movement, at different angles, so corrections need to be used at the stage of features generation. Wearing sunglasses, long hair, scarfs and other occluding objects or falling within shades are other factors leading to lower recognition rate. The cost is higher in comparison to other identification methods demanding more complex hardware and software to be installed and maintained. Filming at low resolutions also prove to make face recognition more inaccurate.

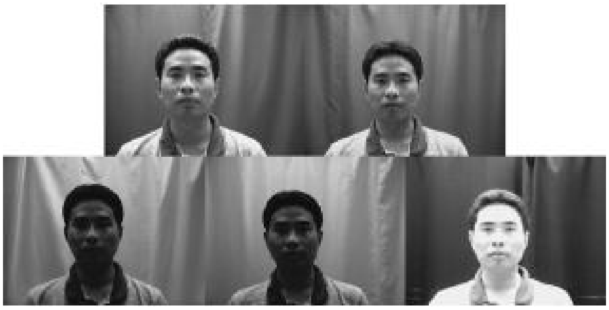

Fig. 1. Facial images for recognition of a person taken at various lighting conditions and over varicolored backgrounds, [4]

2.2 Fingerprint

Fingerprints are formed from ridges and valleys over the skin of the lower part of fingers [5]. They are considered unique for every person. Distinction among fingerprint is achieved by comparison of given patterns of ridges along with minutiae points. Automation of the matching when performing a search within database of previously stored samples is achieved by obtaining a cer tain amount of correspondent points and patterns.

Advantages – highly accurate when fingerprints are properly taken the systems of this type are also fast and reliable. They consume less power with respect to other systems and are constructively simpler with easier maintenance. The cost therefore for their introduction is smaller. High levels of security are typical for this type of identification since scanners register feature points with extremely small probability to be counterfeited. No additional information is needed from the subject, such as a PIN, and this makes it the highly preferred biometric feature. Moreover, fingerprints retain their properties over time [5]. Skin injuries prevent only 2 % of the population to use their fingerprints.

Disadvantages – accuracy performance could be affected by skin scratches. Also, because of the limited size of the area being scanned such a reduction from increased error may be observed (Fig. 2). There are reported cases of engaging artificially constructed fingers or using a finger of another subject in order to mislead security systems. Repeating placements of the finger are sometimes demanded in order to properly register with the control unit. More rarely, chemicals could also change the patterns of fingerprints when used for prolonged time in a working environment for example.

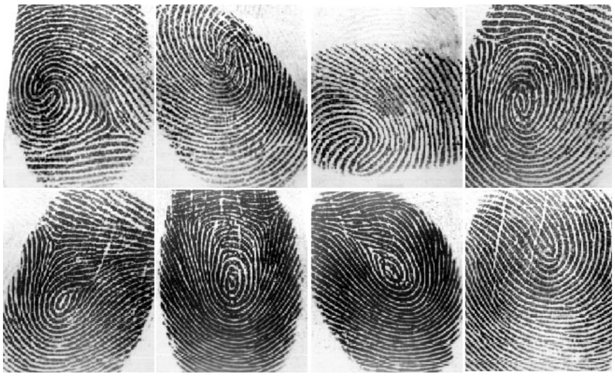

Fig. 2. Finger print samples taken at different spatial orientations, [6]

Fingerprints themselves are not limited from distribution since all people touch objects with their fingers on a daily basis. The possibility of stealing a fingerprint is open and should be considered when operating a security systems of a higher level.

2.3 IRIS

As one of the most reliable biometric features in terms of security is considered the iris recognition. Authentication is its primary application. Typically the iris is being captured with a common digital camera. The recognition is done by opposing that image with a known templates from a database. False acceptance rate (FAR) and false rejection rate (FRR) are known to be low making the overall accuracy of such systems very high rendering the popularity of the technology also high.

Advantages - the pattern of the iris is formed up to the tenth month during the growth of a human and is known to preserve its uniqueness during the entire life. The ease of the recognition process along with its high accuracy place this method as desired among manufacturers of systems assuring tight security. The computational complexity of the recognition algorithm involved takes no more than two seconds. Iris's pattern consist of delicate texture with fine details which differs even between genetically similar people [7]. The capturing process may be accomplished from a few centimeters up to a few meters of distance. Nevertheless, minimal FAR is reported among other techniques while it is completely non-intrusive approach. Contact lenses and glasses introduce no distortions to the processed pattern. The processing speed lends itself to scalability.

Disadvantages – iris printed as high quality image could lead to false acceptance. The opposite case is when a person with diabetes is rejected from clearance due to the change of the iris's pattern. The quality of the generated picture from the system must always be with appropriate quality. Otherwise FRR would rise. Admittance from more than several meters becomes problematic and needs additional hardware support. Regardless of the operational distance precise calibration is needed taking into account the variation of height among all users. Change into the illumination can affect the accuracy of the recognition (Fig. 3). The cost of these systems is higher than other, more traditional, systems.

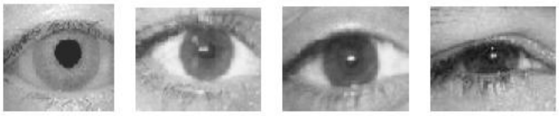

Fig. 3. Various iris images needing preprocessing prior to identification, [8]

2.4 Finger veins

The blood vessels within a human's finger possess unique pattern which is used for finger vein authentication and became popular biometric technology in the last decade. Specialists from the filed find it more secure when granting access to information or other resources [9]. Finger veins distribute blood to the human heart and the hemoglobin with lower oxygen concentration has the ability to absorb infrared light. Thus, the vein patterns become visible when capturing the light stream passing though the finger or being reflected from it in some variants of these systems. A digital image contains veins' shapes as darker outlines as a result (Fig. 4). Further, the shapes are represented as numeric data. One of the methods for the purpose rely on repeated line tracking [10] while other – on the curvature of the veins [11]. There are also other methods applied in practice [9]. During the enrollment process all images of finger veins are transformed into template feature values as a part of a database which are later used in the matching with the data from the user seeking access or being checked.

Advantages – the FAR is low for this particular biometric feature due to its uniqueness even between identical twins. The finger veins images are relatively small in size – in the order of 100x200 pixels. Other their property is that they are low contrast which does not affect the recognition accuracy. Technological expenses are considered low. It's a non-intrusive method although a physical contact with the reader is necessary. Since blood vessels are contained into the human body no actual access to their pattern could be accomplished by simply using some residual traces. Thus the probability for counterfeiting is reduced. Authentication is in the order of half a second which actually does not pose any inconvenience to the subject in timely manner while the level of accuracy is high. The quality of the skin in terms of thickness and injuries does not affect the authentication process. Aging has no impact on the recognition accuracy as well because of the stable pattern of veins without any need of updates through the years. There are no significant observations of veins' structure modification related to weather change or health status.

Disadvantages – batch processing is not applicable. Serious injuries leading to the loss of a finger makes authentication impossible and registering the veins' pattern of another finger becomes necessary. The technology is still expensive, partly because of the related patent fees. End-user sensors are larger than those for the fingerprint recognition because there is a camera embedded into them. Future versions of sensors and supporting hardware and software for mass production, especially in the government sector, are expected to be deployed in the near future.

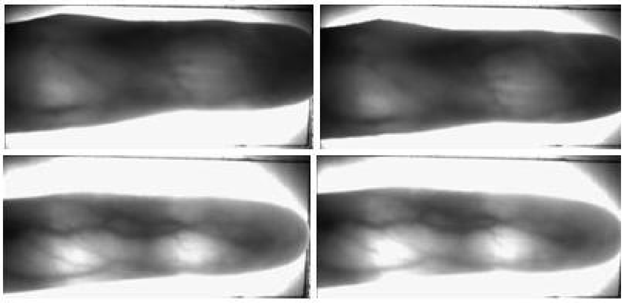

Fig. 4. Finger veins images at diverse penetration levels of infrared light, [12]

2.5. Voice identification

Voice identification [13] is another biometrical approach where distinctive sounds some of which may represent whole words pronounced by a human are at first captured by the use of a microphone. Then the resulting electrical signal in digitized form is submitted to identification software module. It is extremely natural type of characteristic since its daily use for common communication.

Advantages - a direct input is possible without the need of a learning phase with a typical for each subject pace of speaking which pose no discomfort during the identification stage. The actual speed of pronouncing different phrases may vary but still it is a part of the distinctive properties of the particular voice. Having this situation the speech continues to be correct in spelling and grammar. There is no devices that need to be attached to the human body so the level of inconvenience is low. In the same time there is guaranteed equality between people with motor disabilities and persons without such. Any specialized preparation is obsolete which makes the process quite fluent as well. Even the level of literacy is not an obstacle between low educated persons and this type of identification systems. It makes it especially perspective for introduction in developing countries. Voice identification offers also diverse means to complement the establishing of a personality with other types of biometric features without the requirement of strictly fixed template that was preliminary recorder. In other words, any speech content is applicable within such a system including the case if it is spoken in random moment of time or order possibly with a partially pronounced phrases. The reason for that lays over the selection of recognition features based on statistical parameters from the very vocal sounds generalized in order to be invariant. In that sense the required interval on a timely basis for identification could be shorter.

Speaking in several languages does not affect the operability of the system.

Disadvantages – the sensor should be at proper distance from the subject since there is significant reduction of the accuracy with its growth. Noise and other background sounds may also considerably reduce the overall performance of voice identification. There is possibility for forgeries if prerecorded vocal sounds are played out but such a situation concerns only systems without authorized personnel being present. When officers from connected service perform identity verification whether at a checkpoint or in mobile conditions this scenario is practically impossible. The expense for implementing the vocal identification is higher than that for other types of biometrics.

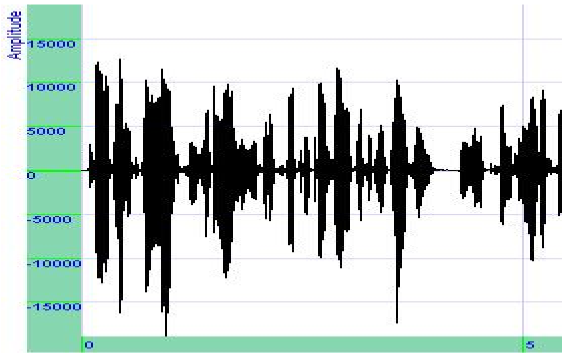

Fig. 5. Voice sound wave input for identification, SPDEMO used [14]

2.6. Lip identification

Human lips identification is another perspective approach which is under intensive development in the recent years [15]. Originally intended for use within forensic activities related to various crimes it may appear to be also effective for personal identification of general type. The spatial properties and color distribution over the lips' area are the source of unique descriptors which some authors find more efficient than other biometric features [15]. A series of difficulties from the complete identification process are thought to be overcome given a wide range of input conditions from practical point of view.

Advantages – lips as part of the face are typically visible. Taking a lips image from a distance defines this biometric feature as contactless type. Their structure is discriminative among different persons and persistent over time. During criminal investigations lips prints are used as c lues and forensic specialist are familiar with the techniques for their properties. All these qualities make them proper for combined exploitation with the face and voice. Less amount of data is stored for the templates in comparison to other features. Additional cooperation from the subject is not obligatory.

Disadvantages – wider smiles may interfere with correct recognition if the templates for the identified person include only neutral appearances. Multimodal implementations including the lips are considered more expensive rather than the unimodal variants. The presence of teeth in the images makes recognition more difficult.

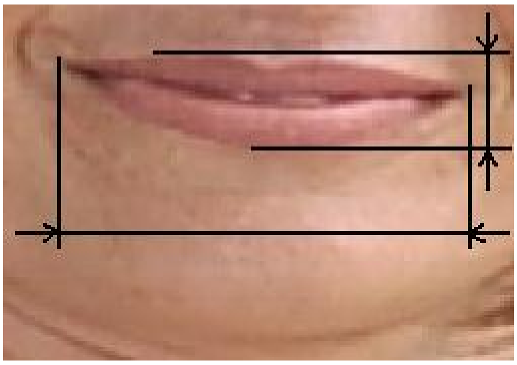

Fig.6 Lips recognition metrics

2.7. Biometrics overall comparison

Fig. 7 gives the parallel among the biometric features discussed above. They are compared by 5 main attributes the complete systems that are employing them have [16]:

- Security level;
- Long term stability;
- Size of template;
- Cost;
- Accuracy.

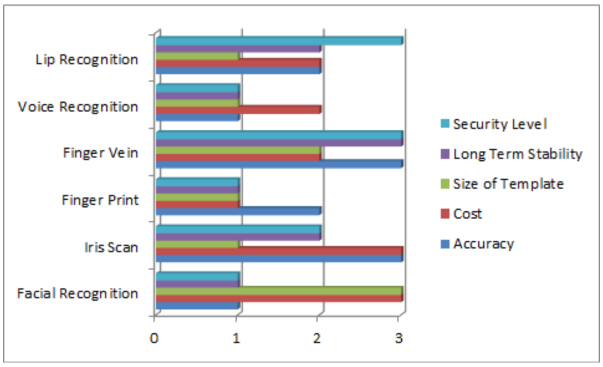

Fig.7 Biometrics qualities comparison

On the scale from 1 to 3 where the following correspondence holds: 1 – low, 2 – medium, and 3 – high, the most secure biometrics are the lips and finger veins while the fingerprints, voice and the face are at the bottom of the leaderboard. Finger veins are most stable over time but in the midrange as for the size of the template. Faces need largest amount of memory to be preserved since the lips, fingerprints, voice, and the iris are very sparing. The most expensive biometric systems incorporate the iris and the face. The cheapest appear to be fingerprint recognition systems.

3 Biometrics Influence over the Accuracy of Personal Identification

The accuracy of personal identification is closely related to two parameters – the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) [17]. FAR is defined as the rate at which authorization is given to subjects without proper rights. In the opposite, FRR represents the rate at which genuine by identity persons are rejected from access (Fig. 8). These two parameters are always in contradiction – the bigger is getting the one, the smaller is the other and vice versa. The optimal value for the acceptance rate $a_{opt} = A$ (represented by the axis abscissa in Fig. 7) lays at the level defined by the *Acceptance threshold* – the crossing point of the curves for *Positive Responses* and *Negative Responses* during identification. Over the ordinate axis are the values of the *Point Density Function* (PDF) which gives the differential probability of each of these events occurring.

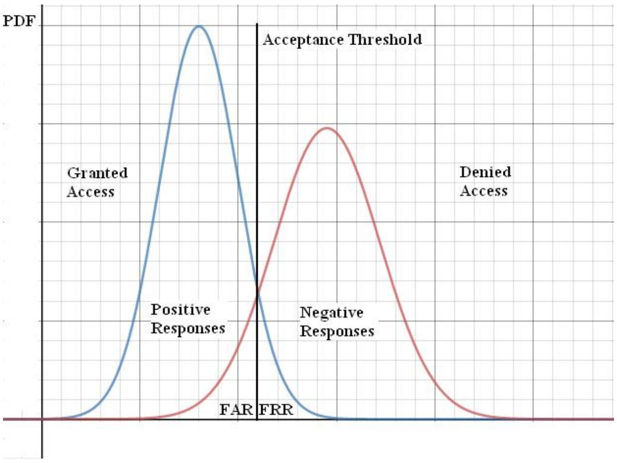

Fig. 8. Correct and incorrect (forgeries) distribution areas

Porwik [18] uses also a co uple of other parameters – the *False Match Rate* (FMR):

$$FMR(A) = \int_{a=-\infty}^{A} p_n(a)da, \quad (1)$$

and the *False Non-Matched Rate* (FNMR):

$$FNMR(A) = \int_{A}^{a=+\infty} p_m(a)da, \quad (2)$$

where $p_n(a)$ and $p_m(a)$ are the distributions of the matched and non-matched cases respectively.

E-passports from the first generation store digital image of the owner’s face [19]. Typically a neutral facial expression is photographed in enrolment offices with resolution of the digital image of 7 Mpx [20]. The reported FAR is 0.1% and in the same time FRR varies between 0.5% and 1.7% [20]. Lighting conditions appeared to be crucial for preserving the erroneous recognition as low as possible. Even illumination with smooth and constant in color background behind the citizen’s face are a must to comply with the above requirement. In some Member States of the European Union a second photo is also captured with the person smiling.

In the second generation also a fingerprint is stored in the embedded integrated circuit [21]. Multitude types of minutiae are discoverable on the finger skin but for the purposes of identification only bifurcations and endpoints take place. They form the so called minutiae analysis. There are also other recognition methods but proven with time to be less effective. Variety of verification tests are implemented over fingerprint recognition systems like the Fingerprint Vendor Technology Evaluation (FpVTE) [22] and the Fingerprint Verification Competition (FVC) [23]. The accuracy of these systems along with the factors affecting it are thoroughly analysed during these events. Some special occasions are included in the tests such as dry, moist, and scratched finger imprints extending standard databases to a l evel for more demanding recognition process.

Some typical values achieved by the most efficient systems are FRR = 0.6% at FAR = 0.01% for a single fingerprint. FRR falls down to 0.1% at FAR = 0.01% for four fingerprints [20].

Face recognition systems are also subject to wide scale testing. Example for such initiative is the Face Recognition Vendor Tests (FRVT) [24]. Newly developed prototypes of facial identification frameworks are compared during it and useful guidelines are obtained for future enhancements.

4 Risk analysis of biometrics use for personal identification

Frontex presented report [25] on the operational and technical security of the European electronic passports. A part of it treats the possible risks involved from the embedding of biometric features for personal identification. Attention is paid to all phases of the e-passport life cycle (Fig. 9). The foundation for it is the development and manufacturing process (not shown in the figure).

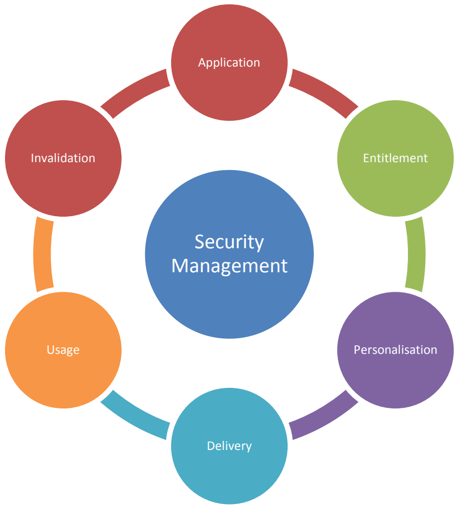

Fig.9. The e-passport life cycle

One of the aspects of the study concern the capturing of the biometrics features.

Providing own image by the passport bearer is a requirement claimed by the authorities in 40% of the cases. At 15% of the filing desks, people are photographed on the spot and the rest of the respondents point to the need to take facial images in licensed photographic studios.

The automated biometric verification of the person is carried out in a limited number of border crossing points, usually in specialized cabins, mobile stations with readers and fully automated control systems. When reading the chip by an authorized control officer, the stored files with faces are visualized as an additional security measure. One of the prescribed measures to improve security against fraud related to the use of foreign documents by visual similarity is to increase the quality of the captured images.

Interviewees question the effectiveness of the fingerprint verification technique from both points of view – the cost involved for introduction of the technology and the accuracy achieved at the verification stage. Border control in most of the Member States still does not use it on a regular basis. Typically, it is applied as a se condary measure – at second check line in at least 2 EU countries quite frequently and in another one it is considered equal by importance with the facial recognition. The quality of the fingerprint images is under question by the researchers. Verification time is also a concern and together with the other previously mentioned disadvantages lead to the ultimate decision by the governing bodies of some countries not to use it as a f ront stage measure. Being used at first line border control in only one state the fingerprint verification is actually applied for around 10% of the travellers. Two other countries use it at second line border control. Verification of fingerprints there takes place for 50% of the citizens in the one and in only 5 % for the other.

Automated border control (ABC) systems are fully implemented in 5 Member States while other 4 did not take initial steps towards introducing them. Manned booths initially were introduced in 4 countries and mobile readers – by 5 governments. Officers in 8 countries are obliged to visually check the facial images in each case. In 3 of the other states this is a n on-due. It is not clear from the respondents' representatives of the participating countries whether other types of biometric features are used, orwhether or not they apply additional documents or information media (tokens).

Facial image identification is used as additional control element in 8 Member States but in not all of them the image is read automatically. Four of the countries within the EU don not incorporate that verification at all. The procedures following a rejection from facial verification are strictly defined by only half of all the jurisdictions. As a guarantee against deception based on visual similarity 40% of the interviewed participants point out the necessity of higher quality facial images. This problem leads also to the increase of the false rejection rate at valid entrance attempts. There are some more rarely occurring cases when the image recorded in the chip belongs to another person due to personalization errors.

Five Member States intend to introduce fingerprint verification in parallel to other four in which no such intentions are currently aroused. Still, one country is in a process of considering this possibility. In virtually all cases, this type of a check will be applied at second line border control. All the undergoing initiatives towards the selected direction are scheduled to be completed by the end of 2017.

Some of the obstacles in front of the mass introduction of fingerprint verification in a national scale are:

- Public disapproval inducted by prejudices related to application of the technology in criminal investigations;
- The growing degree of adoption of facial recognition becoming more accurate over time;
- Low level of fingerprints in certain cases;
- Slower verification time;
- The need of PKI (Public Key Infrastructure) demanding intricate key management, certificate processing and supporting frameworks which seems expensive for some governments to implement.

The benefits of using fingerprints, the most important of which is the evasion of facial resemblance frauds, are acknowledged by 10 of the explored countries. Three of the others find this security measure's cost effectiveness as too low. Minor number of states have built-up PKI and in the same time are using certificates signed by organizations from other countries. While the latter could not be pinpointed as definite disadvantage there are countries which continue to reject fingerprint verification from admission.

Poor quality of the applied biometrics pose significant concern regarding the evaluated risk (Table 1).

Table 1. Opinion scores for the risk involvement from the poor quality of e-passport biometric images [25], in %

	Fingerprint	Face
Very likely	10.6	6.4
Likely	36.2	42.6
Not likely	17.0	14.9

The risk rating methodology is based on the introduction of 2-dimensional level evaluation ranging from 1 to 25. On one side an incident impact influence is considered on the scale from very low (1) to very high (5) and from the other – the likelihood of its occurrence – from very unlikely (1) to very likely (5) (Fig. 10). Five possible actions are targeted against the risks: reduction (removal), avoiding, transfer or acceptance.

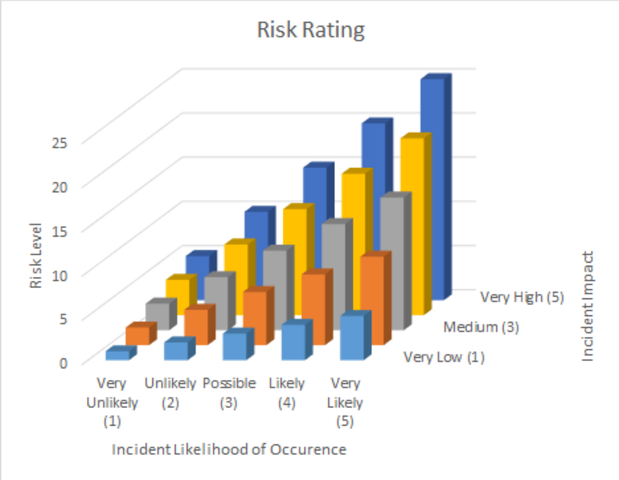

Fig. 10. Evaluation of the incident risks

Frontex analysis [25] of the application of biometrics across Europe, specifically introduced for border control, could be summarized to the following items:

- Passive authentication is not checked, partially or fully, due to the lack of verification of signature by the inspection system.
- Identity cards partially can substitute the e-passports in the identification process but hardly unification could be achieved some have no chips, other used only contact ones.
- The level of integrity protection of certificates containing public keys is not satisfactory.
- The contained chip may be broken intentionally.
- Extended Access Control uses keys which need better protection from unauthorized access.
- New security standards with centralized nature are needed.
- The support of the information systems is limited only to Active Authentication or Chip Authentication.
- Common legal requirements are necessary within the EU on border control.
- The development process of the information systems for border control needs tighter security.
- Fingerprints stored in the currently operational chips do not have satisfactory quality.

- Governmental interconnection for exchange and signing certificate requests needs to be introduced at a global scale.
- Second line inspection is not supporting at wide fingerprint verification.
- There are no strict requirements for: reading the chip; performing automated biometric verification; for checking the fingerprints; common operations by border officers when exploiting either fixed or mobile inspection systems at first line; complete specifications of ABC systems including the supervision of border guards, as well as for the second line systems; procedures describing the interaction between the first and second line systems when the initial produces denial.
- Control officers need specific training on handling electronic personal documents.
- PKIs for the purposes of verification need to be established in certain countries and linked to the Inspection systems.
- There is a need for standard procedures including decisive actions when security mechanism and reading a chip fail.

High-level risks in the order of 20 to 25 appear for numerous aspects from the operation of the ABC systems. They can be divided into 3 categories: inability to complete fingerprint verification because of interruptions in the Extended Access Control using the existent PKI and certificate interchange as well as for the low quality of fingerprints; system suspension due to active authentication, chip authentication or passive authentication intermissions; security breaches in the inspection system as a co nsequence of undiscovered vulnerabilities.

In order to overcome or at least decrease the level of risk involved with all the issues described above experts from the sector propose the following solutions [25]:

- Increasing the necessary level in proper standards for fingerprint images quality.
- Further expansion the scale of using of fingerprints for the purposes of identification;
- Intensification of service data exchange among stakeholders including issuance and control authorities on ne wly discovered weaknesses in the inspection systems.
- Improvement of the quality of facial images considering unification of lighting conditions, backgrounds, etc.
- Introduction of ID cards in the process of automated border and inland control at fixed and mobile checkpoints.
- Ongoing training of control officers (guards) on successful e-passport identification ;
- Continuous collection of ABC systems exploitation statistical data;.
- Introduction of mutually approved guidelines for e-passports issuance;
- Document signing certificates should be embedded within e-documents on a considerably larger scale.
- Incorporation of chip authentication in all EU e-passports, and possibly in ID cards at a later stage.

5 Conclusion

In this paper an extensive overview of the most popular biometric features is done in regards with personal identification at governmental level and their aptness for inclusion in identity and travel documents. Currently, face, fingerprints, and iris are used for the purpose. Based on the presented analysis concerning the advantages and disadvantages from practical point of view finger veins seem to be also very promising for future incorporation within the chips of these documents. Still, the technology is not mature enough to be directly placed. Their adoption is expected by intergovernmental harmonization bodies and by the governments themselves on a worldwide scale in the near future.

Acknowledgement

Portions of the research in this paper use the CASIA-FingerprintV5 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA) and the Hong Kong Polytechnic University Finger Image Database (Version 1).

References:

[1] Jain, Anil K, Ross, Arun; Prabhakar, Salil, An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, Vol. 14, No. 1, 2004, pp. 4-20.

[2] Unar, J. A, Seng, Woo Chaw, Abbasi, Almas, A review of biometric technology along with

trends and prospects, *Pattern recognition*, Vol. 47, No. 8, 2014, pp. 2673-2688.

[3] Zhao, Wenyi, et al., Face recognition: A literature survey, *ACM computing surveys (CSUR)*, Vol. 35, No. 4, 2003, pp. 399-458.

[4] Gao, Wen, et al., The CAS-PEAL large-scale Chinese face database and baseline evaluations, *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, Vol. 38, No. 1, 2008, pp. 149-161.

[5] Maltoni, Davide, et al., *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[6] CASIA-FingerprintV5, http://biometrics.idealtest.org/ , visited on October 3rd, 2017.

[7] Sheela, S. V., Vijaya, P. A., Iris recognition methods-survey, *International Journal of Computer Applications*, Vol. 3, No. 5, 2010, pp. 19-25.

[8] Proença, Hugo, Alexandre, Luís A., UBIRIS: A noisy iris image database, In Proc.: *International Conference on Image Analysis and Processing*. Springer, Berlin, Heidelberg, 2005, pp. 970-977.

[9] Mulyono, David, Jinn, Horng Shi, A study of finger vein biometric for personal identification. In Proc.: *IEEE International Symposium on Biometrics and Security Technologies (ISBAST 2008), 2008,* pp. 1-8.

[10] Miura, Naoto, Nagasaka, Akio, Miyatake, Takafumi, Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification, *Machine Vision and Applications*, Vol. 15, No. 4, 2004, pp. 194-203.

[11] Miura, Naoto, Nagasaka, Akio, Miyatake, Takafumi, Extraction of finger-vein patterns using maximum curvature points in image profiles. *IEICE TRANSACTIONS on Information and Systems*, Vol. 90, No. 8, 2007, pp. 1185-1194.

[12] Kumar, Ajay, Zhou, Yingbo, Human identification using finger images. *IEEE Transactions on image processing*, Vol. 21, No. 4, 2012, pp. 2228-2244.

[13] Delac, Kresimir, Grgic, Mislav, A survey of biometric recognition methods. In: *Proceedings of the 46th International Symposium IEEE Elmar Electronics in Marine*, 2004, pp. 184-193.

[14] Moshe, Yair, Peleg, Nimrod, Cohen, Nadav, SPDEMO - a novel software tool for teaching multimedia signal processing. In: *2nd International IEEE Conference on Information Technology: Research and Education ITRE 2004,* 2004, pp. 116-120.

[15] Dineshshankar, Janardhanam, et al., Lip prints: Role in forensic odontology. *Journal of pharmacy & bioallied sciences*, Vol. 5, Suppl. 1, 2013, pp. 95-97.

[16] Liu, Simon, Silverman, Mark, A practical guide to biometric security technology. *IT Professional*, Vol. 3, No. 1, 2001, pp. 27-32.

[17] Malik, Jyoti, et al., Reference threshold calculation for biometric authentication, *International Journal of Image, Graphics and Signal Processing*, Vol. 6, No. 2, 2014, pp. 46.

[18] Porwik, Piotr, The Biometric Passport: The Technical Requirements and Possibilities of Using. In: *IEEE International Conference on Biometrics and Kansei Engineering ICBAKE2009,* 2009, pp. 65-69.

[19] Hoepman, Jaap-Henk, et al., Crossing borders: Security and privacy issues of the european e-passport. *Advances in information and computer security*, 2006, pp. 152-167.

[20] Schimke, Sascha, et al., Security analysis for biometric data in ID documents, *Security, Steganography, and Watermarking of Multimedia Contents*, 2005, pp. 7.

[21] Juels, Ari, Molnar, David, Wagner, David, Security and Privacy Issues in E-passports, In: *First IEEE International Conference on Security and Privacy for Emerging Areas in Communications Networks SecureComm 2005,* 2005, pp. 74-88.

[22] Watson, Craig I., et al., Fingerprint vendor technology evaluation. *NIST Interagency/Internal Report (NISTIR)-8034*, 2015.

[23] Cappelli, Raffaele, et al., Fingerprint verification competition 2006. *Biometric Technology Today*, Vol. 15, No. 7, 2007, pp. 7-9.

[24] Grother, Patrick, Ngan, Mei, Face Recognition Vendor Test (FRVT). *Performance of Face Identification Algorithms, NIST Interagency Report*, Vol. 8009, 2014, pp. 84.

[25] FRONTEX, Operational and Technical security of Electronic Passports, Warsaw, Poland, July 2011, http://frontex.europa.eu/assets/Publications/Research/Operational_and_Technical_Security_of_Electronic_Pasports.pdf , visited on October 3rd, 2017.