

Chapter 34

Identification and Authentication Potentials Based on Limited Biometric Data



Éva Kovács  and Tibor Kovács 

Abstract The success of biometric authentication and identification depends greatly on the amount of data taken at the time of template acquisition. The pandemic of 2020 and 2021 has highlighted the necessity to examine how feasible it is to determine the identity of a person based on a limited number of biometric features. This poses a serious technical challenge since most of the face is covered by a facemask, hands are gloved, characteristic body movement is hidden under protective gear, and detectors must not be touched. In hospitals, the solution to this problem is even more significant for both the staff and the patients as identifying a person with certainty must happen without the removal of personal protective gear. Determining the identity of a person based on limited biometric data is expected to raise interest from a criminalistics, military or a terrorist detection and identification perspective, too, where the masks, leaving the eye free, have hitherto prevented successful face recognition. The article examines potential solutions primarily from a theoretical angle.

Keywords Biometric identification · Authentication · Reduced amount of data · Pandemic · Terrorist detection and identification · Identification on the battlefield

34.1 Introduction – Identification vs. Authentication

It is a normal that the result of the examination aimed at determining the identity of a person on a mobile device on a mass scale is, very frequently, denoted as ‘identification’. However, often this is not the case.

É. Kovács (✉)
University of Public Service, Budapest, Hungary
e-mail: kovacs@uni-nke.hu

T. Kovács
Óbuda University, Budapest, Hungary
e-mail: kovacs.tibor@bgk.uni-obuda.hu

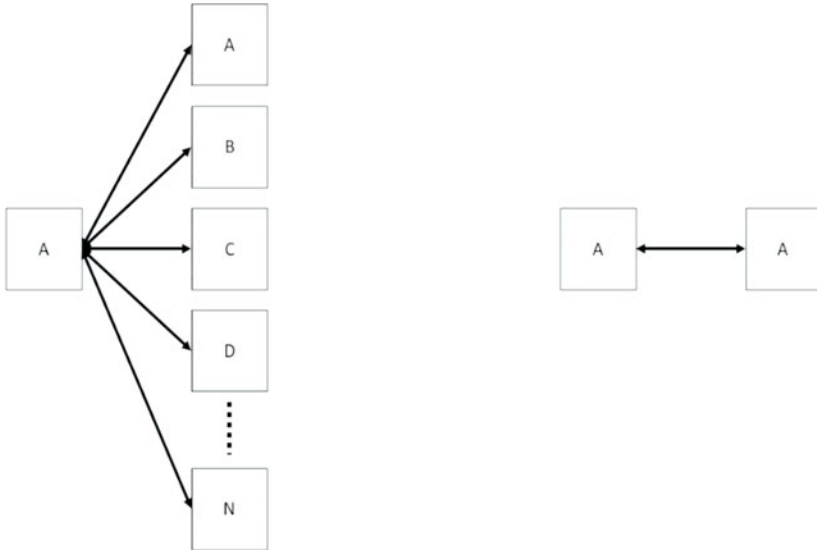


Fig. 34.1 The difference between biometric identification and authentication

During identification, the current template taken is compared to with a saved template, which is only one of the many in the database saved for the same purpose (templates in the database). One example is when a biometric pattern is located in the database of an access control system, together with ten, a hundred, a thousand or a million saved templates with the same purpose. Access will be permitted only after a comparison between the currently taken sample and the those in the database has been carried out and a matching equivalent has been found which will induce a gate to open. In such cases, the identity of the person requesting access may be accurately and reliably established. This is a 1:N type of comparison, where the current sample taken (1) is set against all items or user templates in the database (N).

During authentication, only one template is stored which is then later compared to the one taken at an earlier time. Such authentication algorithms are applied in personal identity cards and passports containing biometric data, fingerprint readers on mobile telephones and computers or even in the palm-vein identification-based access control system at Groupama Aréna. The examples above describe the verification process that a particular type of official document – personal identity card, passport – laptop, mobile telephone or football fan’s identity card belongs to the individual that is presenting it. This is called authentication, not identification, since it is apparent that in these instances the comparison carried out is of a the 1:1 type. The process verifies whether the currently taken template is identical with the one stored or not (see Fig. 34.1).

Whether it is identification or authentication, first a template must be created which is then stored in a users’ database the size of $1 \dots N$. It is important to note that

the template is converted with such an algorithm that makes it impossible to restore the original pattern.

It is rational to establish the basic template in such a way that it contains the maximum number of characteristic features possible. After this, the owner or the operator of the system makes a decision about the extent and sophistication of similarity according to which access will be granted.

Let us take, for example, recording the template of a fingerprint containing 30 characteristic features. It is evident, that if we set the similarity threshold too high, to the maximum 30 for instance, then identification or authentication will frequently result in a ‘false rejection’ (FR), in other words, the individual entitled to enter will not be granted permission to do so. In the event that the threshold is set too low (for instance, 3 features out of 30 are set to be compared), the risk of ‘false acceptance’ (FA) increases, meaning that an unauthorized user will be accepted as a legitimate user and will be granted access. In either cases the system is has a severe risk of vulnerability, which is unacceptable. Determining the extent of sophistication and the setting of an accurate similarity threshold is a responsibility that requires reliable professional expertise.

34.2 The Most Frequent Biometric Identification and Authentication Procedures

In biometric systems establishing entitlement, the most frequently applied identification and authentication procedures are the following:

- Fingerprint identification. The finger is placed on the flat surface of a detector. Ridges constitute the overall pattern. In everyday life, the term ‘fingerprint’ is used generally almost exclusively. However, there is a difference between a fingerprint and a ‘finger-roll’, as shown in Fig. 34.2. A finger roll is collected by laying the fingertip on its side, then turning it to its other side without elevating the finger.

A fingerprint identification detector may be found as part of an access control system, on the back of our mobile telephones or on our laptops within easy reach. The features of ridges (endpoints, bifurcations, islands, etc. as the dark lines in Fig. 34.2). Constitute the potential elements to be recorded. Contact with the detector is direct. Optical solutions operating with polarized light are the only ones which make it possible for the users to leave on surgical gloves for example. Naturally, if the gloves are contaminated, the flat detector surface will also be affected and require decontamination.

Hand Geometry Identification The system records the characteristic features of our hand, such as the length, width and thickness of our fingers, the width of the palm at the fingers and wrist, resulting in about 20 bits of data. Collecting data for the size can be done by the measurement of length, or by determining the perimeter of

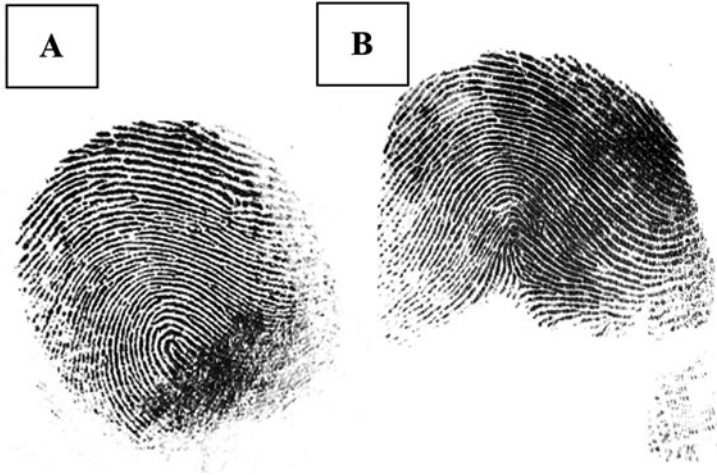
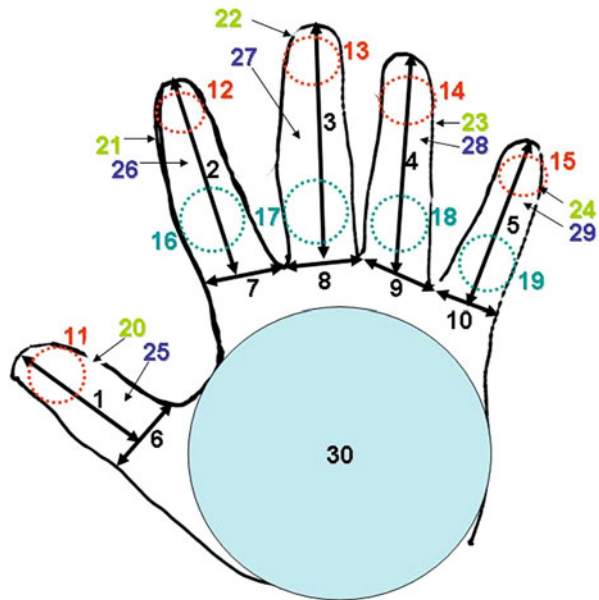


Fig. 34.2 The appearance of a fingerprint (a) and a finger roll (b)

Fig. 34.3 Taking parameters for a hand geometry device (30 bits of data, for a solution without positioning guides) [1]



circles filling the palm, resulting in about 30 bits of data (see Fig. 34.3). Detection and template taking requires direct contact with the device if it applies positioning sticks on its flat detection surface. (See Fig. 34.4 – the hand must be placed on the flat detection surface with the fingers spread and pushed against the sticks.)

Face Recognition Most of our mobile and computer devices apply a geometric version of this method to perform authentications. Stable and characteristic features

Fig. 34.4 Guide-positioning hand geometry device (HandKey) [2]

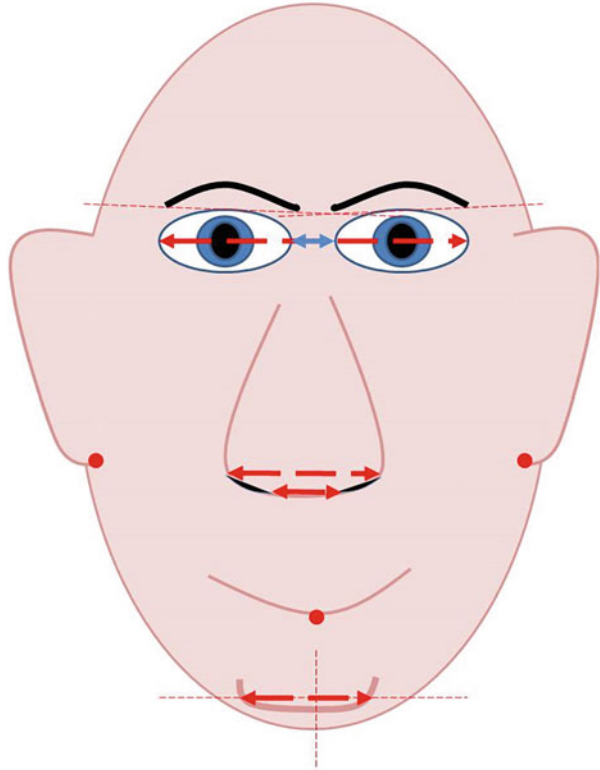


are the ones on a face where bones are covered with low-fat skin. Such points may be the inner and outer endpoints of the eyes, the tip of the chin or the lowest end of the earlobes (see Fig. 34.5).

In the long run, over years, the parameters pertaining to the nose undergo changes, since the size of our nose grows during our lifetime. The volume and fullness of our lips decrease, while the characteristics of the eyebrow may easily be altered intentionally within minutes. The technology used here obviously does not necessitate contact with the detector (contactless technology), while cooperation with the camera is unavoidable. In order for a successful detection, the user must look directly into the lens.

Iris-Recognition (Based on Iris Patterns of the Eye) This identification technology is considered the most reliable at present, since the probability that two patterns would be equivalent is 1:1078, while the population of the Earth is of a scale of 10^{10} . Iris patterns are outstandingly stable, as they are formed by the eighth month of embryonic development and do not undergo any alteration afterwards. The

Fig. 34.5 The most characteristic points and lines of the geometric face recognition method (marked in red) [3]



examination means that the camera takes all the characteristic features of the iris (radial and ciliary body patterns, etc.) which is converted to a three-dimensional map image and which then becomes encoded by a computer program. The probability of a 75% correlation of two codes is 1:1012 [4]. Reading may be done in an active or passive manner. In case of an active reading the user is required to strongly cooperate with the device which audibly and/or visually gives instructions (e.g. turn your head right), which is all done within a short distance, 15–20 cm of the reader. In a passive method, the instrument scans for the eye on the face and focuses on the iris. The distance from the device should not be greater than 1–1.5 m. In both versions, detection remains contactless, however, it is an inconvenient form from the user's perspective. The application of this method prevails primarily in highly enhanced security premises, such as entry to control rooms of nuclear power stations.

Palm and Finger Vein Recognition During palm-vein recognition, the hand (palm and fingers) is lit with infrared light of wavelength 740–950 nm. If a wavelength of 750 nm is chosen for detection, the absorption of low-oxygen blood vessels is significantly greater than that of arteries (see Fig. 34.6). However, other wavelength ranges may also be used for detection (see Fig. 34.7).

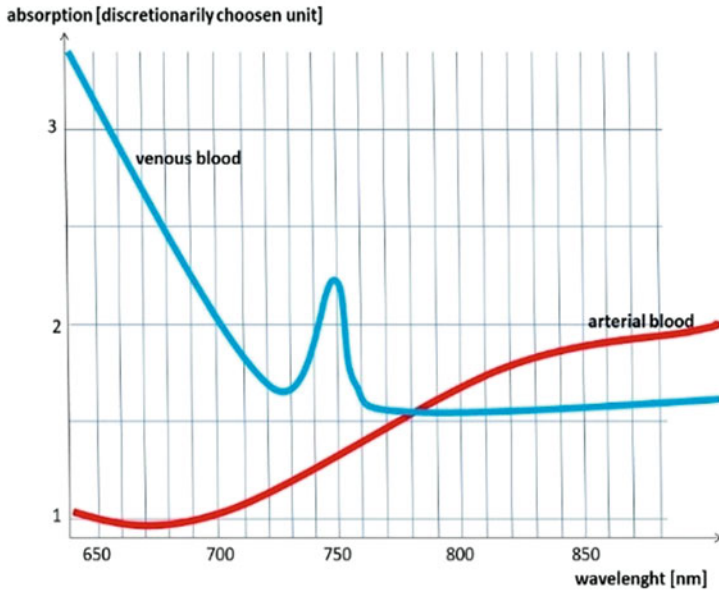


Fig. 34.6 Caption [5]

Fig. 34.7 Caption [6]



There is a contactless solution for such identification, although it is worth noting that the distance of the palm and fingers from the detector is a critical factor. The application of the technology in Hungary has become familiar because of its use at a football club. In accordance with the management’s decision, only those who hold a fan’s identity card, which is similar to a plastic debit card, may be eligible to purchase a ticket for a football match. A fan’s encoded palm-vein pattern of is

recorded on the card, thus supplementing his personal details with a biometric feature. The actual palm vein pattern is read and encoded upon entry to the stadium, which the system compares to the one previously recorded on the card. Only total equivalence of the two recorded patterns will enable the visitor to enter the sporting event. This biometric identification technology is becoming more and more widespread in facilities for medical, retail purposes to support authentication and access control solutions.

34.3 The Vulnerability of Biometric Data

After encoding, original biometric data and patterns may not be retrieved from a sequence of digital signs in a users' database. However, individual biometric identification technologies may have several vulnerabilities. Next, these vulnerabilities will be listed and explained.

Fifteen years ago, experts used to think that the general solution for the problem of secure biometric identification would be provided by fingerprint recognition based on its universal nature and acceptance. In line with this concept, fingerprints made their way into certain personal identification documents, passports, document attachments and various authentication solutions. It has become clear by now that the vulnerability of the pattern is significant. It is a generally accepted fact that 5%, or 1 in every 20 people do not have an electronically recordable fingerprint. Additionally, the most frequently taken fingerprint template is the ones linked to the most frequently used digits (thumb, index finger, middle finger) thus suffering the most physical injuries. Regarding the nature of injury, it may be one-dimensional due to a cut or two-dimensional due to the effect of caustic, washing or abrasive material used in the building industry. Because of dehydration, the original fingerprint pattern may be missing temporarily even from a larger surface of the finger (see Fig. 34.8). After determining the root cause of various injuries, the finger regenerates and a few days later ridges reappear and characteristic features may again be processed.

The fingerprint can be copied: the patterns can be taken from a surface on which it was left (glass, door handle, polished flat surface, etc.). In a pandemic situation, the application potentials are limited, regarding due to the contact nature of the technology. There is a technical solution which enables a template to be read with surgical gloves on. Such technologies use polarized light. However, not even polarized light is able to penetrate chemical protection or any other thicker gloves.

The hand geometry pattern is relatively unaffected by such vulnerabilities. In order for the hand and finger parameters to change suddenly, a severe physical or biological impact must contribute to the change. Such a sudden distortion might be an occasion when fingers swell due to an insect bite. Identification is made problematic or even impossible by diseases causing the deformation of the hand, wearing a bandage or a larger ring.



Fig. 34.8 The effect of a caustic substance (the upper part of the left fingerprint), the effect of dehydration on the fingerprint pattern (central and right image) [7]

Developers of biometric devices put a great emphasis on improving the efficiency of face recognition. Practical experiences show that, with a large number of users, comparing a current template to the ones in the database remains a challenge.

One of the bases of the introduction of the social credit system in the Chinese Republic is that the movement and activities of a ‘good citizen’ may be observed and assessed [8]. This is substantially aided by personal identification and face recognition systems enhanced with artificial intelligence. A ‘good citizen’, whose behaviour is law-abiding and norm-following, receives credits as a reward. Based on the credits, citizens enjoy many benefits, such as gaining admission to higher education institutions for their children.

The most disturbing disruptive elements during 2D face recognition are:

- illumination,
- the viewpoint of the camera,
- the turn of the head,
- facial expression,
- aging,
- make-up,
- glasses [9].

Several applications exist to solve the problem of authentication, for instance when a low quality image is recorded on a personal identification card and is compared to the one taken at the time of identification.

The disruptive elements of 2D face recognition are eliminated with greater efficiency by 3D, which can only be applied from a close proximity and generally requires the complete cooperation of the user with the system. In practice it involves that the person being identified must stand within 0.5–1 m from of the camera. A greater distance would make a successful identification doubtful. The success of face recognition is significantly limited by the wearing of a mask, a hat or cap uncovering

Fig. 34.9 With surgical gloves on the hand, detecting blood veins is impossible (latex rubber gloves, 0.14 mm) [11]



the eyes or a scarf or an injury on the face. In these cases, of the minutia points on the face mentioned before previously, only the ones related to the eye can be used. Naturally, these are contactless technologies.

During iris recognition, a CCD camera, operating in the infrared range, takes a photo of the patterns of the iris within the eye. A great advantage of the technology is that, during identification, the recognition device and the individual do not come into physical contact. Regarding the faults problems of identification, we can state that the most frequent problems are caused by the eyelid covering the iris, or by the illumination itself, being reflected onto the iris [10].

The pattern of the blood vessels in the hand or in the fingers is unique, and a further advantage is that it applies to an inner biological feature, which is obviously less likely to suffer an injury. Producing a fake template would be a far more complex task, since the entire blood vein pattern is invisible for to the human eye. This method can exclude the disruptive factors of illumination, temperature and sunlight with greater efficiency. However, wearing surgical gloves and certain types of contaminants, including the ones gained on the battlefield, (oil, cream, dust, etc.) on the hand may make template acquisition harder or even impossible (see Fig. 34.9).

34.4 Criteria to Determine Applicable Biometric Methods

With limited biometric parameters, a specifically compiled list of criteria must be compiled. It must include those aspects based on whichever methods of identification and authentication might be selected and applied. Let us collect and review the elements in this list individually, then examine the methods from the viewpoint of applicability.

1. **Universality.** Potential biometric patterns derive from the geometric or behavioural features of the human body. Here, all of the examined methods (fingerprint, hand geometry, face, iris and palm vein recognition) fulfil this requirement, even though 5% of people do not possess a recordable fingerprint.
2. **Uniqueness.** The uniqueness of the biometric template ensures that the users are distinguishable. The more definite the divergence among individual biometric templates is, the wider the database for identification may be made. If the divergence is small, we have to deal with a high proportion of falsely rejected readings (FRR – False Rejection Rate), or falsely accepted readings (FAR – False Acceptance Rate). These rates are typical of all identification methods.
3. **Reliability.** One of the most important criteria of any particular method is its ability to identify a biometric template with the highest possible reliability. In other words, after the examination of two identical templates, the current one should be pronounced equal identical to the previously recorded one with a high precision. All five identification potentials fulfil this requirement.
4. **Template-stability.** Biometric features may change over time. In a period of several years, the face is subject to change, or the voice changes over shorter periods of time. The fingerprint, face and iris remains stable in this respect. Possible modifications may mostly be tracked if the most recently read templates overwrites the older one and is stored until the next attempted match.
5. **Cooperation requirement.** It is a significant aspect to consider to what extent a biometric identification or authentication device demands the cooperation of the user. With iris recognition for instance, a strong cooperation is essential with the biometric device, while with face recognition, taking a biometric template may even be conducted without the awareness of the individual.
6. **Acceptance.** Certain methods and instruments may induce resistance or even fear in the user. Acceptance will indicate to what extent the user is willing to cooperate with the identification device. Iris recognition, for instance, may prompt rejection from the user, as, during detection, infrared light is directed at the eye.
7. **Internal biometric feature measurement.** Inner biometric characteristics are less prone to injury, and are difficult or even impossible to copy or forge. On the body surface, biometric characteristic may become unreadable due to external physical or chemical impacts.
8. **Living sample recognition.** During identification and authentication, with the contribution of the technology, it must be ascertained whether the template to be examined is a real living sample or a fake copy. In practice, the so-called living sample recognition technical procedure measures the temperature, pulse or the change of air humidity around the pattern placed on the surface. All identification technologies listed possess such solutions.
9. **Contactless technology.** Biometric instruments, which have to be touched, may often induce rejection in users and can pose considerable hardship during a pandemic, when facemasks, gloves and individual protective gear are in general use. Therefore, it is beneficial if a particular method which is capable of identification does not require the user to touch the device. (For instance, we


No.	aspect	biometric identification method									
		finger		hand		face		iris		vein	
		M	+	M	+	M	+	M	+	M	+
5.	Cooperation requirement.	a	a	b	b					c	c
6.	Acceptance.										
7.	Measuring internal biometric feature.	d	d	d	d	d	d				
9.	Contactless technology.										
10.	Verification time.										
11.	Biometric data amount reduction.		e								
	Applicability (summary).			f		h	h				


Legend:

M: application partially covering the face

+: application partially covering the face and in surgical gloves

 optimal

 not optimal, but not excluded

 not acceptable

a: the surface of the detector must be decontaminated after each user

b: in case of the technology without the guide, otherwise „a”

c: in contactless technologies, otherwise „a”

d: external biometric feature is measured

e: in case of illumination with polarized light, detection and identification may be attempted

f: in case of no-guide positioning technology

h: may not be applied for identification, may be applied for authentication

Fig. 34.10 The applicability of biometric identification methods based on limited data. (The table was compiled by the authors based on the references in the text)

do not count on terrorists’ cooperation with the device; or due to injury suffered on the battlefield, a victim’s cooperation in identification is impossible).

10. **Verification time.** The time period required to verify the eligibility of a user may depend on the technology itself. The user’s inconvenience and resistance towards the particular technology is increased if the verification time lasts longer than 1 or 2 s.

11. **Reduction in the amount of biometric data.** Assuming that the individual to be identified is wearing a scarf partially covering the face or disposable three-ply facemask and additionally a disposable latex rubber gloves (0.14 mm thickness), we must establish whether the identification method receives sufficient data.

Excluding the aspects true for all technologies (1–4 and 8), we can set up a matrix demonstrated in Fig. 34.10, which eventually answers the question of applicability with regard to a particular technology, with the user wearing protective equipment.

Analyzing the results of the table above, we can conclude the following regarding these individual identification technologies:

Fingerprint Recognition The method does not require special cooperation and is regarded as an accepted technology. Upon touching the detector, the external biometric feature measurement is conducted. The identification time lasts a few seconds. It may only be applied if the device operates with polarized light

technology, and needs decontamination after each user. In summary, its application is too complicated and thus can be excluded.

Hand Geometry Identification It does not necessitate special cooperation and is an accepted method. It involves external biometric parameters. The technology, without the positioning guide, is a contactless method, with a favourable verification time. The reduction of the amount in biometric data has no significant effect on it. It has a potential for application.

Face Recognition It does not require special cooperation from the user, and it is an accepted technology. Both external and internal features are measured in a contactless manner. When partially covering the face, the amount of biometric data is reduced critically. It may only be applicable for a limited number of users (10–15), otherwise it may not be applied for identification. Its potential application for authentication must be further examined.

Iris-Recognition The disadvantage of the method is that it has a strong cooperation demand, is a less accepted technology and the identification time may grow significantly. On the other hand, detection is conducted based on an internal biometric characteristic and is a contactless technology. It has a potential for application.

Palm or Finger Vein Identification It does not require a high degree of cooperation from the user, however, its acceptance is low at present. It measures an internal biometric feature, without direct contact with the device in a short time. It may not be applicable in gloves; thus this method may be excluded.

34.5 Conclusion

Solving the problem of personal identification and authentication based on limited data is in best interest of both the professional staff and patients in modern hospitals. It is also essential in the fields of the military, criminalistics and terrorist identification. The task must be solved successfully and flawlessly even when a particular user is wearing camouflaging or protective gear, such as a facemask or gloves. In this present article we have searched for answers to this problem and we have determined which biometric methods, of those presently existing, are able to perform successfully under special conditions and circumstances. In our research, we have concluded that hand geometry and iris recognition acceptably fulfilled the requirements of the list of criteria we presented. We have also suggested that it is practical to examine how appropriate the application of face recognition for authentication purposes might be in the near future.

References

1. Kovács, T.: Biometric identification, Digital university lecture notes, Óbuda University, (2015). pp. 2–7. (In Hungarian)
2. Ibidem 1. pp. 3–6
3. Ibidem 1. pp. 2–15
4. Rathgeb, C., Uhl, A., Wild, P.: Iris biometrics: from segmentation to template security. Springer, New York (2012)
5. Ibidem 1. pp. 2–13
6. Ószi, A.: The place and role of biometrics identification in e-commerce. PhD thesis, Doctoral School on Safety and Security Science, Óbuda University (2019). p. 80. (In Hungarian)
7. Ibidem 6. p. 62., p. 64
8. Planning Outline for the Construction of a Social Credit System (2014–2020) State Council (2014)
9. Ibidem 6. pp. 42–43
10. Földesi, K.: The applicability of biometric identification procedures in police operations. PhD thesis, Doctoral School on Safety and Security Science, Óbuda University (2017). pp. 85–89. (In Hungarian)
11. Ibidem 6. p. 81