# A comparative study on the application of biometric technologies for authentication in online banking

**Silvia Parusheva**
Department of Informatics, Faculty of Computer Sciences
University of Economics-Varna, Bulgaria
parusheva@ue-varna.bg

## Abstract

In recent years online banking is gaining more and more acceptance thanks to the many advantages and conveniences it provides both for customers and financial institutions. One of the main challenges for the banks, however, is the reliable confirmation of the identity of their customers via the authentication procedure so as to prevent financial fraud. The traditional knowledge- and possession-based authentication methods have proved as not sufficiently strong. As one possible solution to overcome the abovementioned challenge are biometric-based authentication systems, which are generally considered to be more reliable.

The paper proposes a methodology for overall quantitative assessment of biometric features for choosing the most appropriate of them for inclusion in biometric authentication systems in online banking. The methodology includes evaluation in two stages - basic and advanced assessment of several biometric features like fingerprint, hand vein, hand geometry, iris, voice and others. The evaluation is based on selected characteristics of theirs which are used as criteria, respectively indicators for comparison. Examples include universality, performance, resistance to circumvention, acceptability, etc.

The results of the study at the first stage - basic assessment of eight biometric authenticators with seven criteria, showed that the four most suitable of them are DNA, fingerprint, iris and face. The subsequent advanced assessmentincludes additional criteria and proves DNA is to be removed because of the conflict with some important specifics of biometric authentications systems in online banking. The first three ranked authenticators show the following outcome - fingerprint has the highest final score, followed by iris and face. The received results would help financial institutions to choose the most suitable biometric authentication technology, respectively authenticator, and it would be required for them to take into account other important factors.

**Keywords**: *biometrics, authentication, online banking, quantitative assessment, multi-factor authentication*

## 1. Introduction

Thanks to the Information Technologies it is possible that a large part of the financial services are fulfilled electronically. Online banking services are becoming more popular and widespread, with more customers' acceptance.Theyare comfortableand cost effective both for financial institutions and customers, but they may be vulnerable because of problems with user authentication and the possibility of identity theft and financial fraud. The absence of face-to-face contact makes the process of identifying the real user really important and in the same time challenging. Therefore user authentication in online banking becomes very crucial.

In this context biometrical technologies increase their presence and impact in the banking information systems both in physical contact points - automated teller machines (ATMs) and in the electronic systems that one can use distantly (remote electronic banking like online banking, mobile banking, phone banking). Specifically, their possible application is for user authentication in online banking, i.e. biometric authentication systems, because they have the potential to solve many of the security problems [1].These systems are designed to diminish the bad effect of cyber-criminal activity – stealing log-in details and money fraud. This is how the strong need of more reliable confirmation of user identity when accessing online banking is addressed and it is displayed how it is a direct way of decreasing theft of private details.

## 2. Overview of the authentication methods and schemes. Advantages and disadvantages.

Authentication refers to the problem of confirming or denying a person's claimed identity (Am I who I claim I am?) and especially in online banking to a procedure which ensures that a bank user is who/whoever he or she claims to be [2].

### 2.1. Key findings about the authentication methods

The methods for authentication can be divided into three groups [3]:

- Something the user knows"or "Knowledge" - such as personal identification number (PIN), password, passphrase or answer of security question;
- „Something the user has" or "Ownership" such as smartcard or token;
- Something the user is"or "Inherence" – here the biometrical methods are used and there are two categories -based on aphysiological characteristics(fingerprints, iris,retina, face or hand geometry, DNA, palm, hand or finger vein etc.) or behavioral characteristics(voice, signature,keystroke sequence, gait).

The traditional and most used methods by now („Something the user knows") have proved to be prone to failure – they can be forgotten, shared or captured, also in an illegal way using different types of malware.

Key representative of this method are the passwords that the users come up with themselves and use to login into online banking systems. However the passwords are ineffective as authenticators. The users make a number of mistakes applying them – some users have only one password, even if strong, for all websites and applications that they have account in. Others create passwords that are very similar and in most cases weaker than advised, hence they can be guessed. And still others create many different and strong passwords for the various sites and applications, but then they can be forgotten. The passwords are also susceptible to be captured by malicious technologies like phishing, pharming, Trojans, spyware, key logging, social engineering, Brute Force Attacks, dictionary attacks,SQL injection, etc. [4].That is why usernames and passwords aren't enough to protect customers' sensitive financial information.

An issue with the approach of authentication using possession such as smart cards, etc. is that the possessions could be lost, stolen, or misplaced and eventually duplicated. Furthermore, once in control of the authenticating possession, by definition, any other "unauthorized" person could abuse the privileges of the authorized user [2].

Unlike the abovementioned two groups of methods, biometric methods are based on a set of physiological or behavioral characteristics and their main advantage is that the consumer is embodying them, i.e. something the user is. They are characterized by a high degree of accuracy, reliability and convenience in comparison with the traditional authentication mechanisms. Physiological elements, in contrast to knowledge and possession elements are directly personally identifiable. Biometrics-based systems create more simplicity to the process of confirming the user's identity. They are also most difficult to compromise.Furthermore, biometrics provide affordability to widespread populations as they surmount difficulties like users' illiteracy, language barriers and others.

On the other hand biometric systems have some disadvantages and limitations, related with certain security issues like for example the possibility for data breaches and also compromising biometrics database (compromised passwords can be changed, but compromised biometric characteristics remain such forever). Another problem is the lack of universally-accepted technical and legal standard for the interoperability of systems and consumer biometric data protection [5]. Also the need of implementation of advanced detectors and scanners which can check the characteristic's vitality (e.g. smart finger print/vein reader, that has built-in anti-spoof and liveness detection and checks presence of blood flow).Other weaknesses are that biometric systems are vulnerable to errors and they can be "spoofed"(circumvention by animpostor) e.g.at the matching stage [6]. Furthermore, a difference between the perception and the reality of the sense of security provided by the system could exist.

Despite the abovementioned shortcomings, biometric systems have more advantages in comparison with the non-biometric ones [7].

### 2.2. Authentication schemes in online banking

In online banking systems there are mainly two schemes for user authentication used: single-factor authentication and multi-factor authentication which is usually two-factor authentication.

#### 2.2.1. Single-factor authentication (SFA)

SFA, as it can be easily judged by its name, is based on just one factor from the aforementioned groups. An authentication which relies only on one factor is highly vulnerable. Traditionally it relies on a username (user ID) and password, so-called bankingcredentials.As a typical SFA, password-based authentication has all the weaknesses mentioned above.

Studies show that exactly bank customers' credentials (user name and password) are object of theft bycrimeware more often than any other type of data [4].While possessing the user credentials in one-factor authentication cyber criminals realize identity theft and easily gain access to user accounts.

Steady position on issue of the unreliability of the single-factor authentication has the U.S. Federal Financial Institutions Examination Council (FFIEC), which perceives it as inadequate for high-risk transactions like movement of funds to other parties [3].

#### 2.2.2. Multi-factor authentication

Multi-factor authentication is based on the presentation of more than one (usually two) independent authentication factors (components). These factors could be something the user has in his/her possession (e.g. token device or smart card), something he/she knows (password, answer of security question) or some physical or behavioral characteristic of the user (e.g. fingerprint or voice).

A requirement for implementation of two-factor authentication to all EU payment service providers (PSPs) with a deadline of 1st of August, 2015 is set by the European Banking Authority (EBA) with released guidelines on securing online payments across the European Union. EBA is the EU body tasked with supervising and regulating the banking sector. It's guidelines require PSPs to ensure strong customer authentication to be used to verify the identity of all customers in online transactions. EBA defines "strong authentication" as "a procedure based on the use of two or more of the following elements categorized as knowledge, ownership and inherence" [8].

One of the most used combinations of two factors by banks is static password and one-time password (OTP)/one-time code. A one-time code can be generated by hardware token device or it can be sent by short message services (SMS) to the mobile user's phone or by e-mail. In this case if the user wishes to initiate a transaction for money transfer an SMS code is sent to the user's mobile phone and the user must enter this number at the bank's website for completing the transaction.

However implementation of two-factor authentication, based on the combination of static passwords and one-time-codes is not always sufficiently reliable. Related works indicate that there are cases of illegal tracking of one-time codes sent via SMS and then using them for fraud money transfers [9, 10]. SMS-based authentication has been compromised through mobile malware, mainly intended for Android phones [10].Therefore тwo-factor authentication on its own is not good enough of a security tool. There are other authentication threats and risks that need to be taken into account like for example man-in-the-middle attacks which involve cyber attackers trying to gain control of data communication between customer and bank servers, in order to be able to look at and manipulate the data as need serves them.

Established breaches of two-factor authentication schemes with factors involved from "Knowledge" and "Ownership" lead to the conclusion that the need for more reliable schemes, for example including a factor of the group with biometric methods is present, i.e. using a biometric authentication system. In this context, the question of comparison and evaluation of a number of possible biometric characteristics arises and also how to select the most appropriate of them for an authentication system.

## 3. Overall assessment of biometric features based on their properties

In general in biometric systems a number of biometric features can be used: fingerprint, palm print, iris, retina, hand geometry, finger or hand vein, face, DNA, signature, gang, voice and others [11].

### 3.1. Biometric features' basic assessment of their properties

The wide potential range of biometric features can be subjected to comparison with the help of their properties that can be used as criteria,respectively indicators for comparison. In most studies authors use the following seven properties tocharacterize the biometrics features [7, 12, 13, 14, 2, 15]:

- **Universality**– the property is included in each person.
- **Uniqueness**- the property should be sufficiently different for two people.
- **Permanence**–the property should remain unchanged during the life of the individual.

- **Collectability**– indicates the extent of easiness with which biometric property can be measured.
- **Performance**– indicates the achievable accuracy, speed and robustness of the biometric property [14]. The most common performance metrics are the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). The FAR measures the extent to which a given biometric system will match on an incorrect input (an impostor will be accepted as a valid match) and the FRR measures the extent to which a given biometric system will fail to match a correct input (a legitimate user is rejected) [6].

**Table 1. Comparison of various biometric authenticators using seven categories of evaluation**

| Biometric authenticator | Reference | Universality | Uniqueness | Permanence | Collectability | Performance | Acceptability | Resistance to circumvention | Total |
|---|---|---|---|---|---|---|---|---|---|
| **Fingerprint** | [7] | 2 | 3 | 3 | 2 | 3 | 2 | 1 | 16 |
| | [12] | 2 | 3 | 3 | 2 | 3 | 2 | 1 | 16 |
| | [13] | 2 | 3 | 3 | 2 | 3 | 2 | 2 | 17 |
| | [14] | 2 | 3 | 3 | 2 | 3 | 2 | 1 | 16 |
| | [2] | 2 | 3 | 3 | 2 | 3 | 2 | 1 | 16 |
| **Face** | [7] | 3 | 1 | 2 | 3 | 1 | 1 | 1 | 12 |
| | [12] | 3 | 1 | 2 | 3 | 1 | 3 | 3 | 16 |
| | [13] | 3 | 1 | 2 | 3 | 1 | 3 | 3 | 16 |
| | [14] | 3 | 1 | 2 | 3 | 1 | 3 | 3 | 16 |
| | [2] | 3 | 1 | 2 | 3 | 1 | 3 | 3 | 16 |
| **Iris** | [7] | 3 | 3 | 3 | 2 | 3 | 1 | 1 | 16 |
| | [12] | 3 | 3 | 3 | 2 | 3 | 1 | 1 | 16 |
| | [13] | 3 | 3 | 3 | 2 | 3 | 1 | 1 | 16 |
| | [14] | 3 | 3 | 3 | 2 | 3 | 1 | 1 | 16 |
| | [2] | 3 | 3 | 3 | 2 | 3 | 1 | 1 | 16 |
| **Signature** | [7] | 1 | 1 | 1 | 3 | 1 | 3 | 3 | 13 |
| | [12] | 1 | 1 | 1 | 3 | 1 | 3 | 3 | 13 |
| | [13] | 1 | 1 | 1 | 3 | 1 | 3 | 3 | 13 |
| | [14] | 1 | 1 | 1 | 3 | 1 | 3 | 3 | 13 |
| | [2] | 1 | 1 | 1 | 3 | 1 | 3 | 3 | 13 |
| **Voice** | [7] | 2 | 1 | 1 | 2 | 1 | 3 | 3 | 13 |
| | [12] | 2 | 1 | 1 | 2 | 1 | 3 | 3 | 13 |
| | [13] | 2 | 1 | 1 | 2 | 1 | 3 | 3 | 13 |
| | [14] | 2 | 1 | 1 | 2 | 1 | 3 | 3 | 13 |
| | [2] | 2 | 1 | 1 | 2 | 1 | 3 | 3 | 13 |
| **Hand Vein** | [7] | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 13 |
| | [12] | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 13 |
| | [13] | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 13 |
| | [14] | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 13 |
| | [2] | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 13 |
| **Hand Geometry** | [15] | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 15 |
| | [12] | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 15 |
| | [13] | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 15 |
| | [14] | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 15 |
| | [2] | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 15 |
| **DNA** | [7] | 3 | 3 | 3 | 1 | 3 | 1 | 3 | 17 |
| | [12] | 3 | 3 | 3 | 1 | 3 | 1 | 3 | 17 |
| | [13] | 3 | 3 | 3 | 1 | 3 | 1 | 3 | 17 |
| | [14] | 3 | 3 | 3 | 1 | 3 | 1 | 3 | 17 |
| | [2] | 3 | 3 | 3 | 1 | 3 | 1 | 3 | 17 |

- **Acceptability** - indicates the degree of willingness of the people to use a biometric system and to present their biometric property for identification/authentication purposes.
- **Circumvention** - relates to the ease with which the biometric system can be circumvented or fooled by deceptive methods.

It is considered that the biometric identifiers should have all the properties listed. In the absence of one or more of the following properties of a biometric identifier, it can’t be used in a biometric system [7].

Different authors evaluate different biometric identifiers using these seven criteriawhich are characterized by three possible levels - low, medium and high [7, 12, 13, 14, 2,15]. In our study we have chosen the following biometrics featureswhich are most applicable: fingerprint, face, iris, signature, voice, hand vein, hand geometry, DNA.

The aim of the study is to make an overall quantitative assessment of those indicators that may help with the choice of the most adequate to include in an authentication system. Therefore, we apply 3-point scale assessment, where number 1 corresponds to a low level, 2 to a medium and 3 to a high. In all indicators, except for the last (circumvention), the most favorable value is 3, i.e. high level.For the purposes of research the formulation of the last indicator is changed from "Circumvention" to "Resistance to circumvention", and with this change number 3 will indicate its most favorable value, i.e. the corresponding biometric authenticator is the most resistant to circumvention. In this way consistency of the evaluation of the seven indicators is accomplished and therefore the best authenticator will be the one with the highest total value of all parameters, i.e. the authenticator with the highest total value of all seven indicators will be referred as optimal for biometric authentication system.

Table 1 provides a comparison between the biometric authenticators based on those indicators. The last column summarizes the values of all items. For each identifier values of these five references are included [7, 12, 13, 14, 2, 15].

Based on the aggregate values of the indicators of the five sources (the data in the last column of the table) arithmetic mean value for each biological authenticator is calculated and all of them are shown in Table 2. The data in it displays the following: the highest average among the seven indicators is DNA with a grade of 17.0, second is fingerprint with 16.2, third is iris with 16.0 and further fourth is face with 15.2.

**Table 2. Rankings of the eight authenticators based on seven properties**

| № | Biometric | Average total of the seven indicators from the five different sources |
|---|---|---|
| 1 | DNA | 17.0 |
| 2 | Fingerprint | 16.2 |
| 3 | Iris | 16.0 |
| 4 | Face | 15.2 |
| 5 | Hand geometry | 15.0 |
| 6 | Signature | 13.0 |
| 7 | Voice | 13.0 |
| 8 | Vein | 13.0 |

## 3.2. Overview of the first four ranked authenticators

### 3.2.1. DNA

DNA is a unique code for one's individuality and it is called the ultimate identifier. Every cell in a human body contains it and it can be recognized digitally. It is, however, currently used mostly in the context of criminological applications for identification because it is expensive and slow, but also not widely available as it needs skilled labor to intervene [2]. Another setback of it is that it does not allow a real-time identification. A fact worth mentioning as well is that it is impossible to differentiate the DNA patterns of identical twins.

### 3.2.2. Fingerprint

The fingerprint is such a pattern of ridges and valleys on the surface of the finger that are unique for every person, even in twins. The ridges themselves have a non-continuous flow, where the discontinuity brings about feature points called minutiae and the pattern can be of arches, whorls and loops, which are the basis of fingerprint recognition [14]. Fingerprints are the oldest and probably best known biometric identifiers and because of the long and widespread experience with fingerprint technology. Fingerprints scanners are included in many consumer electronic devices like laptops, smart phones, etc. (e.g. Apple’s fingerprint scanning technology TouchID available on the iPhone 5S, the iPhone 6 and iPhone 6 Plus) [6].

There are two main technical approaches for fingerprint recognition: minutia matching and pattern matching, of which minutia matching approach is most used in the fingerprint recognition systems [14].

Presently, a good advantage of fingerprint recognition is its sufficient accuracy. It is also considered as low cost and easy to use. However, there may be some issues with fingerprint recognition. The recognition sensors are not able to capture acceptable quality fingerprint images for people with very wet or very dry skin. Also, sensors need to be maintained properly in order to get the consistent performance required. The Spring 2002 international developer survey conducted by Evans Data has presented the conclusion that fingerprints have the most potential in terms of user authentication [14].

### 3.2.3. Iris

Iris is another biological piece of every person and its recognition offers one of the most secure authentication technologies, because according tomanufacturers’ claims, so far there has never been a false non-match [6].The iris is also one of the most accurate technologies when it comes to false acceptance rate - the levels are very low. It is considered as the most recognizably distinctive feature in the human body that is enduring and unchangeable all throughout the life of an individual. An iris image is typically obtained in a non-contact way using a regular digital camera and therefore this technique could be used in an online banking authentication system.

As a disadvantage it could be claimed that it produces a sense of discomfort as some users are not sure where to focus when providing a sample. In addition, it is a fact that not every person can enroll satisfactorily, missing one of the two compulsory operating stages of a biometric system [6].

### 3.2.4. Face

Face recognition is probably the most common biometric characteristic which is used by people for personal recognition every day. It is a method that is non-intrusive and has a high level of user acceptance because of that. The face recognition can be based on two primary approaches: a global one and a feature-based one [14]. The global one is using the image of the face and processing it without concentrating on single features and is used in statistical analysis with well-known examples such as eigenface technique. A proper preparation is required to perform this method with accurate results since it can be sensitive to just a slight movement during imaging. The feature-based one is, as its name hints, focusing on specifics - eyes, nose, brows, etc. where there are the so-called fiducial points and the geometrical relationship between those points is unique in every person. Again, automatic detection is subjected to flaws – movement and position variations of the face.

To sum up, face recognition is easy to use, rather inexpensive and very common. It is performing well when harmful factors are well taken care of – no glasses, proper lighting conditions, even aging could prove to cause inefficiency. Also when recognizing twins, this method has proved to give insufficient results.

### 3.3. Biometric features' advanced assessment of additional properties

To indicate the most appropriate authenticator/feature for biometric authentication systems certain characteristics of this technology in online bankingmust be taken into account when remote online communication with users is realized.An important specification is that banks should ensure appropriate authentication technology to large number of users and therefore should be reported need for real time large-scale implementation.

As authenticator in real-time systems DNA is inappropriate because of its difficulty to be collectable and also its low users' acceptability and therefore DNA is eliminated.

After eliminating DNA, a more advanced estimate of the next three authenticators derived in Table 2, namely fingerprint, iris and facecould be made as in the evaluation five additional criteria cost, accuracy, ease of use, security, and liability are included. Their assessment is performed again with a 3-point scale to assess: 1 (low), 2 (medium) and 3 (high); for each criterion evaluations from studies from two references are included [16, 17, 18, 13, 19]. The results are summarized in Table 3.

**Table 3. Comparison of biometric authenticators in another five categories of evaluation**

| Biometric authenticator | | Fingerprint | Iris | Face |
|---|---|---|---|---|
| **Average from previous 7 criteria** | | **16.2** | **16.0** | **15.2** |
| **Accuracy** | [16] | 3 | 3 | 2 |
| | [17] | 2 | 3 | 1 |
| | **Average** | **2.5** | **3** | **1.5** |
| **Ease of use** | [16] | 3 | 3 | 3 |
| | [18] | 3 | 2 | 2 |
| | **Average** | **3** | **2.5** | **2.5** |
| **Security** | [13] | 3 | 3 | 2 |
| | [17] | 1 | 2 | 1 |
| | **Average** | **2** | **2.5** | **1.5** |
| **Liability** | [13] | 3 | 3 | 2 |
| | [19] | 3 | 3 | 2 |
| | **Average** | **3** | **3** | **2** |
| **Cost*** | [16] | -1 | -3 | -2 |
| | [17] | -1 | -3 | -3 |
| | **Average** | **-1** | **-3** | **-2.5** |
| **Total** | | **25.7** | **24.0** | **20.2** |

*In criterion cost the estimates are negative values in order to reflect the negative impact of this indicator, i.e. when the price of authenticator is high, it is included in the table with -3.

From the grades of the two sources there are averages calculated for each indicator. Then they are added up to the aggregate values from the basic assessment (the first row with numbers in the table) so that in the end there are final grades for each biometric authenticator in the bottom row. (e.g. for fingerprint: 16.2+2.5+3+2+3+(-1)=25.7).

The analysis of the resultsallows to draw the following conclusions: the advanced assessment including five additional criteria does not change the interim ranking of authenticators and final quantitative assessments confirm the leading position as most-appropriate authenticator of fingerprint (with a final score of 25.7), followed by iris (24.0 ), and face (20.2).

For distance matching of large numbers of people in biometric authentication system specific devices like a fingerprint scanner and a digital camera for iris and face recognition are required. Essential prerequisite is that the majority of laptops, computers, smart phones, tablets, phablets, etc. are equipped with webcams, microphones, and some electronic devices even with fingerprint scanners. This fact simplifies banks' projects for implementation of biometric systems, which are based on fingerprint, iris or face recognition.

Because of the strict requirement for "strong authentication", especially in EU, a two-factor authentication is recommended, in which one of this three biometric identifiers can be combined with password. In this case when customers attempt to fulfil an active transaction like a money transfer, the bank will require them to present a biometric feature (authenticator) together with a password.

## 4. Conclusion& Future work

This paper presents a methodology for overall quantitative assessment and metrification of biometric features for choosing the most appropriate of them, suitable for inclusion in biometric authentication systems in online banking.It includes evaluation in two stages- basic and advanced assessment. Their practical implementation allows the following findings to be presented:

- After the basic metrification of eight biometric authenticators with seven criteria the four most suitable of them are derived - DNA, fingerprint, iris and face.
- The advancedmetrificationand analysis of the abovementioned first four ranked authenticators reveals the need of eliminating DNA as it is proven to be mismatching the properties of biometric authentications systems in online banking. From the three left, fingerprint has the largest final score, followed by iris and face. Therefore those three authenticators are most suitable for inclusion in biometric authentication systems in online banking, and choosing one of them would be suitable in the required at least two-factor authentication system.

The future work will focus on studying and analyzing of important factors and specifics – other than the above mentioned, which financial institutions have to consider when they choose the appropriate biometric technology, most adequate to include in an authentication system in online banking. Another field for future research would be the problems, associated with security threats in biometric systems.

## References

[1] W. Khalifa, M. I. Roushdy, and A.-Babeeh M. Salem"A Rough Set Approach for User Identification Based on EEG Signals", Egyptian Computer Science Journal (ECS), Vol.38, No. 3, ISSN 1110-2586, September 2014, pp. 43-50.

[2] A. K. Jain, R. Bolle, and S. Pankanti "Introduction to biometrics", in: "Biometrics. Personal Identification in Networked Society", Kluwer Academic Publishers, 2002, pp. 1-17.

[3] Federal Financial Institutions Examination Council "Authentication in an Internet Banking Environment", October 2005, pp. 1-14.

[4] Verizon 2014 "Data Breach Investigations Report", 2014, pp. 20-34.

[5] R. Tassabehji "The rise of biometric banking as fight against fraud is stepped up", http://theconversation.com/the-rise-of-biometric-banking-as-fight-against-fraud-is-stepped-up-31433, (Accessed on 02.07.2015).

[6] Maghiros, I.; Punie, Y.; Delaitre, S.; Lignos, E.; Rodríguez, C.; Ulbrich, M.; Cabrera, M.; Clements, B.; Beslay, L.; Van Bavel, R. "Biometrics at the Frontiers: Assessing the impact on Society", 3/2005, pp.37-44.

[7] A. Elçi, J. Pieprzyk, Al. G. Chefranov, M. A. Orgun, H. Wang, R. Shankaran „Theory and Practice of Cryptography Solutions for Secure Information Systems", IGI Global, 2013, pp. 373-376.

[8]. European Banking Authority (EBA) "Final guidelines on the security of internet payments", 19 December 2014, p. 11.

[9] D. Danchev "Modern banker malware undermines two-factor authentication", http://www.zdnet.com/article/modern-banker-malware-undermines-two-factor-authentication/, (Accessed on 31.07.2015).

[10] K. Baylor, NSS Labs „View From The Precipice Mobile Financial Malware", 2013, pp. 4-7.

[11] Sh. Al-seddek, H. Soliman, M. Morsy, Sh. Kishk "A Palmprint-Based Identification System using Radon Transform", Egyptian Computer Science Journal (ECS), Vol.38, No. 3, ISSN 1110-2586, September 2014, pp. 75-85.

[12] P. Stavroulakis, M. Stamp „Handbook of Information and Communication Security", Springer Science&Business Media, 2010, p. 139.

[13] K. Sharma, A. J. Singh "Biometric Security in the E-world", in: "Cyber Crime: Concepts, Methodologies, Tools and Applications: Concepts, Methodologies, Tools and Applications", IGI Global, 2011, pp. 507-514.

[14] Y. W. Yun „The '123' of Biometric Technology", 2003.pp. 83-96, http://www.cp.su.ac.th/~rawitat/teaching/forensicit06/coursefiles/files/biometric.pdf, (Accessed on 29.07.2015).

[15] N. Paveši, S. Ribari, D. Ribari "Personal authentication using hand-geometry and palm print features – the state of the art", http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.93.8771&rep=rep1&type=pdf (Accessed on 25.07.2015).

[16] L. Martin "Biometrics", in: J. R. Vacca "Computer and Information Security Handbook, 2009, pp. 644-660.

[17] R. Saini, N. Rana "Comparison of various biometric methods", International Journal of Advances in Science and Technology, Vol 2, Issue I, March 2014, pp. 24-30.

[18] K. P. Tripathi "A Comparative study of Biometric technologies with reference to Human computer Interface", International Journal of Computer Applications, Vol. 14 , No. 5 January 2011, pp.10-15.

[19] P. Gregory, M. A. Simon "Biometrics For Dummies", Wiley Publishing, Inc., 2008, pp. 256-257.