Biometric technologies in Cybersecurity

O Vysotska[1,3] **and A Davydenko**[2]

[1] Department of computerized information security systems, National Aviation University, 1 Liubomyra Huzara ave., Kyiv 03058, Ukraine
[2] Department of Mathematical and Econometric Modeling, Pukhov Institute for Modelling in Energy Engineering of NAS of Ukraine, 15 General Naumov Str., Kiev 03164, Ukraine

[3] E-mail: Lek_Vys@ukr.net

Abstract. In this research, biometric recognition technologies are considered. Protection systems, which use different biometric technologies for recognition, are analysed. Cybersecurity's tasks, which require using biometric systems for solving, are considered. Selection expediency of biometric recognition technologies is explained. To solve specific tasks in every specific organization parameters of such systems, which values should be taken to a view for protection system selection and configuration, are considered in details. Recommendations are given for system selecting to solve different cybersecurity's tasks. It is paid more attention to namely dynamic methods, such as users' keystroke pattern and handwriting. For these systems, there are identifying characteristics, which are analysed (can be analysed) at the recognition time; listed essential system steps and described flavours of such systems. The importance of the correct choice of the text, the characteristics of which will be analysed, and the need to perform primary processing of handwriting samples is indicated. Based on the results of the analysis, the paper argues the relevance of the task of developing new biometric recognition systems for cybersecurity and explains the feasibility of using such systems to protect information.

1. Introduction

There are manifold ways of information protection nowadays. All of them are based on using different methods. [1-10]. Of course, every method has its advantages and disadvantages. Using biometric technologies to protect information became quite popular these days [11, 12]. The use of these technologies in cybersecurity makes a lot of sense, so they are the object of analysis in this research. As part of the research, particular attention is given to technologies, which use dynamic biometric characteristics for analysing.

2. Problem definition

The main purpose of this research is to analyse existing biometric recognition systems; justify expediency of their use to solve different cybersecurity's tasks; scrutinize basic parameters, which help with system selection and configuration to solve specific tasks in every specific organization. Meanwhile, it is paid more attention to namely dynamic methods, such as users' keystroke pattern and handwriting. For these systems, a more detailed description of the principles of their operation will be given.

3. Problem solving

To solve this problem what biometric technologies are, their characteristics and the way they work will be first considered.

Biometric recognition systems are used to recognize one or several peculiarities of the human body structure, his/her motor skills, character, psychological and mental characteristics. Thus biometric recognition systems can be classified by biometric methods they use. Biometric recognition methods can be divided into two classes:

- static methods;
- dynamic methods.

Static methods are based on measuring physical (static) human's characteristics which have to be unique for every person or at least for most people. These characteristics do not change significantly over a long period and are not affected by any external factors, such as cosmetics, any weather phenomena, etc. Static characteristics include fingerprint; hand form; vein placement on the front of the palm; eye retina; eye iris; face shape; facial thermogram; DNA; other, less popular characteristics like a subungual layer of skin, finger volume, ear shape, body smell, thermogram of different parts of the body.

Dynamic recognition methods are based on behavioural (dynamic) characteristics namely based on peculiarities of subconscious movements in the course of reproduction of any action. Unlike physically distinct characteristics, in this case, the biometric system does not necessarily have to measure the same phenomenon every time: for example, a person may be asked to say, write, or walk in a certain way to reduce the risk of the intruder reproducing the characteristic. The dynamic characteristics include handwriting; keystroke pattern; "mouse" signature; voice; lip movement at code word reproduction; pace; others, less popular in an application, such as an acoustic signal from a human body, dynamics of a turn of a key in the door lock, psychological and mental characteristics (memory, attentiveness, the accuracy of estimations.

Depending on the planned tasks of the use of biometric system, the field of application and the requirements for the security level in a particular organization, the preference is given to the system based on one of these methods.

In cybersecurity biometric systems are typically used to solve one of the following problems [4-6]:

- User authentication system.
- User identification system.
- Employee's work monitoring.

The solution of the first two problems must be done once, when gaining an access to a system. The solution of the third problem is constantly (periodically) necessary, during a work. Monitoring is useful in any organization to capture the case if an authorized user leaves the computer unattended and the violator will make use of it. Besides, monitoring is needed in those organizations where the response and staff attentiveness is important, for example, for airport controllers. It is better to monitor unnoticed for the people being observed. Therefore, in this case, not all biometric methods are suitable, it is best to use keystroke pattern recognition systems (to control certain parameters when typing words or combinations of characters that are often repeated); by fingerprint, if the scanner is built into a standard mouse or keyboard; behind the iris with a nearby video camera.

In addition, system recognition selection should be also conducted by other criteria. Biometric authentication systems can be evaluated by the following criteria (one or more) [4-6]:

1. Type I error probability – probability of system access denying for legitimate user (allow entering for "right" user).
2. Type II error probability – probability of spoofing the system by intruder (allow entering for "wrong" user).

3. The probability of concurrently occurring both type I and type II errors – the probability that the system will take one legal user for another, also a legal user (but with different access rights).

4. The error level of the biometric system, at which the type I error is equal to the type II error – the equality point of probabilities (complex quality indicator).

5. Authentication speed.

6. Minimum quantity of training patterns.

7. Minimum volume of training patterns of the database.

8. System strength of changes in the environment.

9. Possibility of remoted authentification.

10. The system cost, which significantly depends on the need to use any equipment.

Depending on the field of application, the significance of these criteria differ due to the tasks for which the system is used and the needs to the level of security in a particular organization. That is, in one case, the main thing is not to let the intruder get into the system, and in another – to provide the ability to use the system remotely in the global network.

Regardless of the chosen method, the operation of any biometric recognition system consists of the following two stages [4-6]:

- *Initial registration*. At this step, a database of training patterns of the relevant biometric characteristics of the required amount (depending on the selected biometric technology) for each user is created. If after a while the biometric characteristics of the person have significantly changed or, for some reason, inaccurate (erroneous) patterns were collected at the initial registration, and as a result, there are frequent refusals to the legal user, then the step of initial registration should be repeated.
- *Recognition* (authentication, monitoring, identification). At this step, if authentication or monitoring is performed, then the user firstly enters his/her name (login) and then, if the database contains training patterns for this user, a biometric characteristics pattern of the person is created and compared with training patterns of the verified user. The result of the comparison is the probability that the compared patterns belong to one person. Then, using any mathematical criterion, a decision is made about the identity of the patterns, thus deciding whether this user is really whom he claims to be. If the user identification is performed, then the user name is not entered and, accordingly, the presence of information about him in the database is not checked, and immediately a sample of biometric characteristics of the person is created and compared with all training patterns of all users. Then the list from some most similar patterns as a result of the comparison is formed (for which the greatest values of probability of similarity at comparison are received). Then, using any mathematical criterion, a decision is made depending on the identity of the patterns and thus determine whose data is in the database, and most likely who is the owner of the presented biometric sample.

One of the main parameters by which biometric systems are distinguished is the characteristics plainness used for recognition. According to this, biometric systems can be divided into:

- systems, which use *open characteristics*;
- systems, which use *secret characteristic*.

Biometric systems that use open characteristics for recognition are those systems that use any human available characteristics for observation by outsiders.

Biometric systems that use secret characteristics for recognition are those systems that use any human characteristics that are not available for observation by outsiders.

All systems, which use statistic recognition methods are the systems with open characteristics. But dynamic methods can use both open characteristics and secret ones. For example, if it is specified which word needs to be entered during recognizing by keystroke pattern, then it is a system with open biometric characteristics, and if the user has to enter a password known only to him, then this system is a system with secret biometric characteristics. Systems that use secret biometric indicators are more effective protection systems, so further, in this paper, protection systems will be considered based on the analysis of dynamic biometric characteristics of the person, such as keystroke pattern and handwriting. To read the characteristics of keystroke pattern, you need a regular keyboard, and to read handwriting you need to have a graphics tablet or other device with a touch screen, which is used to dynamically transmit the handwriting characteristics to the user. That is, we can say that these methods do not require any significant financial costs.

Theoretically, any protection system can be overcome by searching all possible values of all analysed parameters, the question only in the time spent and the amount of spent hardware resources. The number of possible combinations in the search is calculated by the formula: $Komb = (\prod_{i=1}^{k_{pr}} kol_{znpr_i})^{kol_s}$, where $Komb$ is number of possible combinations of all analysed parameters, kol_s is the number of characters entered in any way (depending on the method), k_{pr} is the number of characters analysed entering each character, kol_{znpr_i} is the number of possible values of the i-th feature under analysis when entering each character. We are talking about symbols because in dynamic methods (discussed in more detail in this paper), as a rule, one way to enter characters (pronounced, written, typed on the keyboard), and then analyse any parameters measured when entering each symbol. When using secret biometric characteristics, i.e. if outsiders do not know which signs are placed, the number of possible combinations in the search increases significantly. This value is calculated by the formula: $Komb = (kol_{zns} \prod_{i=1}^{k_{pr}} kol_{znpr_i})^{kol_s}$, where kol_{zns} is the number of possible values of the entered character. The increase of efficiency using secret biometric images, which is possible only for dynamic methods, is obvious.

From the formula, you can see the probability of correct recognition is significantly affected by the number of characters whose input characteristics are analysed, and the number of these characteristics. It should also be noted, that the quality of recognition is significantly affected by which word input characteristics are analysed. That is, there are more informative characteristics and less informative [5-6].

There are characteristics, which can be analysed to recognize users by their *handwriting*_(all or several) [5-6]:

- *X*-points coordinates of the image;
- *Y*-points coordinates of the image;
- image points type;
- user pressure on the touch screen at the point creation time;
- angle change of the writing direction at the point creation time;
- time from the beginning of the symbol writing to the creation of a certain point;
- speed of moving a pen from previous point to particular point;
- square of the symbol image;
- point quantity of symbols, which are analysed at the recognition time;
- slope angle of the symbol;
- point frequency of the symbol fixated by a system;
- quantity of point iteration in symbol image (consecutive points with the same coordinates);
- others.

When recognizing users by their handwriting it makes sense to divide the process to two steps:

- password recognition;
- recognition of the password style.

In this case the time can be saved. This means that the second step should be executed if only there is a positive result on the first step.

To recognize users by their *keystroke pattern* following characteristics can be analysed (all or several) [4]:

- The time between pressings of two contiguous word symbols.
- The time between releasing the keys of two contiguous word symbols.

• The time between releasing the key of the first symbol of the letter and pressing the key of the second symbols of the letter.

• The time between pressing and releasing word characters.

• Symbol error percentage.

• Percentage of wrong symbol input in place of a certain word symbol/ Symbol error percentage of a certain word symbol.

• Symbol error percentage of a certain word symbol instead of any other word symbol.

• A list of characters, instead of which other characters are most often mistakenly entered.

• A list of characters that are most often entered instead of other characters.

• Error type, which means the reason of certain errors, is inattention to the keyboard or typical grammatical mistakes.

A greater number of the characteristics changes is analysed according to the task, where there is a need of recognition, and to the necessary security level, where there is a certain system used [4-6].

In addition, it is quite important to choose the characteristics of the input of parsed text. To choose this text the field of activity, in which this biometric recognition system is used, should be taken into account, i.e. you need to choose words that are often used in the work of employees of this organization. Then the style of their input will be the most distinctive. It is especially important to use the information that employees often repeat when authentication is performed to covert monitoring, as this password word.

Also, to select a specific biometric recognition system by keystroke pattern, four main types of this technology should be considered:

1. According to the dynamics of typing a constant key phrase.
2. According to the dynamics of typing a free text – a phrase that is constantly changing.
3. According to the dynamics of typing the set of one randomly selected word from a pre-selected set of words, thus all the obtained characteristics can be analysed, but they must be compared with the corresponding characteristics of the same word only.
4. According to the dynamics of typing the same randomly selected word from a pre-selected set of words, but all these words must have the same fragment and the characteristics can be compared with the corresponding features of this only this fragment from any word of this set.

Technologies of the type I do not provide a high enough level of security. The implementation of type II of technology requires a significant amount of resources. Nevertheless, this type of technology is optimal and most appropriate for solving the problem of monitoring, and especially covert monitoring. To solve the problem of identification or authentication the recognition technologies types III and IV are often used.

In addition, in the case of keystroke pattern recognition and handwriting recognition, all patterns (recognizable) require primary processing. In the case of keystroke pattern, this process is used to remove error patterns from the database of training patterns, namely patterns with gross deviations of the value of at least one characteristic from the arithmetic mean of the same feature in all other training patterns of this user's handwriting. In the case of handwriting, the process is, firstly, to remove errors that occur due to user inattention; secondly, to correct errors caused by the graphics tablets specifics or similar devices. The step of primary patterns processing is a necessary step of the running of any biometric recognition system.

All considered factors should be taken into account to choose the right configuration of each specific biometric recognition system in each specific organization.

Conclusion

In this research manifold biometric authentication systems, which use different biometric technologies for recognition, were analysed. Justified expediency of the use of biometric recognition systems to solve different cybersecurity’s tasks. Scrutinized basic parameters, which help with the selection of the security system. To solve different cybersecurity’s tasks recommendations for the selection of the system are given. Meanwhile, it is paid more attention to namely the dynamic methods. For these systems, there are identifying characteristics, which are analysed (can be analysed) at the recognition time; listed essential system steps and described flavours of such systems. Based on the analysis, it can be noted that the development of new biometric security systems is an urgent task in the field of cybersecurity, and the use of such systems is appropriate.

References

[1] Abdeljalil Gattal and Youcef Chibani 2012 Segmentation and Recognition Strategy of Handwritten Connected Digits Based on the Oriented Sliding Window *International Conference on Frontiers in Handwriting Recognition* pp 297-301 DOI: 10.1109/ICFHR.2012.265

[2] Ali Benafia, Smaine Mazouzi and Benafia Sara 2017 Handwritten Character Recognition on Focused on the Segmentation of Character Prototypes in Small Strips *International Journal of Intelligent Systems and Applications(IJISA)* Vol 9 No 12 pp 29-45 DOI: 10.5815/ijisa.2017.12.04

[3] Muthana H Hamd and Samah K Ahmed 2018 Biometric System Design for Iris Recognition Using Intelligent Algorithms *International Journal of Modern Education and Computer Science(IJMECS)*, Vol 10 No 3 pp 9-16 DOI: 10.5815/ijmecs.2018.03.02

[4] Vysotska O and Davydenko A 2019 Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor Authentication *Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing,* vol 938 pp 356-368 DOI: https://doi.org/10.1007/978-3-030-16621-2_33

[5] Korchenko O, Davydenko A and Vysotskaya O 2019 Method of authentication of information systems users by their handwriting with multi-step correction of primary data. *Information security*, vol 21 №1 pp 40-51 DOI: https://doi.org/10.18372/2410-7840.21.13546

[6] Vysotska Olena and Davydenko Anatolii 2018 Authentication of information systems users, based on the analysis of their handwriting *Scientific and Practical Cyber Security Journal (SPCSJ)*, №2(4) pp 51-63 [Electronic resource]. Online: https://journal.scsa.ge/wp-content/uploads/2018/12/2.4_04_dec_18.pdf

[7] Leila Zoubida and Réda Adjoudj 2017 Integrating Face and the Both Irises for Personal Authentication *International Journal of Intelligent Systems and Applications (IJISA)* Vol 9 No 3 pp 8-17 DOI: 10.5815/ijisa.2017.03.02

[8] Shanmukhappa A Angadi and Sanjeevakumar M Hatture 2016 Biometric Person Identification System: A Multimodal Approach Employing Spectral Graph Characteristics of Hand Geometry and Palmprint *International Journal of Intelligent Systems and Applications (IJISA)* Vol 8 No 3 pp 48-58 DOI: 10.5815/ijisa.2016.03.06

[9] Kazmirchuk S, Ilyenko A and Ilyenko S 2019 Digital Signature Authentication Scheme with Message Recovery Based on the Use of Elliptic Curves *In: Hu Z, Petoukhov S, Dychka I, He M (eds) Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing*, vol 938 pp 279-288 Springer, Cham DOI: https://doi.org/10.1007/978-3-030-16621-2_26

[10] Ilyenko AV 2018 Modern ways of improving the procedure for the formation and verification of digital signature *Science-Based Technologies* 1(37) pp 61-66 https://doi.org/10.18372/2310-5461.37.12370

[11] Arthur Galeev 2018 Almost all companies in the U.S. and Europe will use biometrics in two years 30.03.2018 http://safe.cnews.ru/news/top/2018-03-26_pochti_vse_kompanii_v_ssha_i_evrope_budut_ispolzovat

[12] World market of the biometric systems, 2015-2022, 19.01.2017. http://json.tv/ict_telecom_analytics_view/mirovoy-rynok-biometricheskih-sistem-2015-2022-gg-20170119025618