An elective multibiometric authentication

Alexey Ruchay

Chelyabinsk state university, Chelyabinsk, Russia,
ruchai@pochta.ru

Abstract. This work aims to develop an elective multibiometric authentication. The novelty of this work is to develop the principles of distinction and multibiometric authentication, because at the moment there is no such development. Depending on various conditions and factors, including the availability of electronic means and convenience, resistance to attacks and exploits, disease or injury of users can be selected on the basis of biometric authentication of any such biometrics as rhythm password, voice, dynamic signatures and graphics password. The results of the software development based on the new approach are showed. The possible attacks on the developed system are analyzed, and the conclusions and recommendations on defenses from these attacks are submitted.

Keywords: biometrics, multibiometrics, multibiometric authentication, biometric technologies, managing permissions, image processing, signal processing, information security.

1 Introduction

There are the following problems in single–biometric systems [1]:

- Noise in sensed data (accumulation of dirt on sensor, deformed and noisy data, a cold has effects on the voice, wearing glasses alters iris recognition performance, variations in light or illumination in face sensed).
- Distinctiveness (intra-class variations and inter-class similarities).
- Non-universality (non-ability of biometric characteristic, the poor quality and consistency of the acquired biometric data, user-sensor interaction).
- Spoof attacks.

The developers and researchers of biometrics offer software implementation based on a single–biometric and single–sensor paradigm without additional tools and modules [2]. It creates problems in usage and operation [3]. However, current trends show a desire to take a different approach, creating a multibiometric authentication for different areas [4]. The main advantage of this approach is that the security of access can be enhanced [5].

Multibiometric system is a system using multiple biometric modalities and sensors, which can be integrated at various levels and can be used in different fusions [6]. Biometric characteristics are processed by different methods or fusions in multibiometric systems. The decision can be made on a fused decision rule to increase reliability. In addition other authentication methods can be used, for example, PIN–code, password, rhythm of password, tokens.

Multibiometric systems are known to be high security, protection against spoof attacks and reliability [4]. This biometric system may use multiple biometrics, multiple biometric samples, multiple decision rules, several normalization or some feature extraction techniques by achieve enhancement of reliability. However security and reliability of proposed multibiometric systems leads to additional processing requirements, user inconvenience and privacy issues. Therefore the development of multibiometric systems is supposed to find a reasonable compromise between reliability, security, computational costs and user convenience. This compromise should be found with some automatic or semiautomatic methods, and this decision should be limited to the dynamic management of security and reliability. However works are very little attention paid to theory, architecture, implementation, evaluation of reliability and performance multibiometric systems that provide dynamically changing the level of security by selecting different parameters in multibiometric system. In Section 2, different approaches to the creation of multibiometric systems are presented.

In this paper, an elective multibiometric authentication will mean multibiometric system where dynamically varying level of security provided by selecting its various parameters, including selecting a particular biometric characteristics. The proposed approach for the elective multibiometric authentication will be described in detail in Section 3.

For example, the managing permissions in an isolated room without extraneous can be used for authentication of voice, rhythm of password or graphic recognition. In another case the authentication can be performed based on the rhythm of password or signature. It can be selected rhythm of password, signature or graphic recognition for authentication to implement authentication in mobile or sensor devices. At the checkpoints it can be used signature authentication. Today's very urgent task is developing universal modules that implement managing permissions based on biometric authentication [7].

In addition, the managing permission control system based on biometric authentication has great practical importance and benefits:

- unique, inalienable and inalienability of biometric characteristics;
- difficulties in carrying out the attack on the selective biometric characteristics;
- independence from the operating system and encoding;
- selectivity in multibiometric authentication;
- possibility of authentication of person due to illness and disability.

The aim of this project was to develop, research and implementation of an elective multibiometric authentication.

In Section 4, security of multibiometric authentication are presented as the most important developing aspects.

2 An multibiometric authentication

Multibiometrics can be used to resolve various aspects of security management [4,5]. Its main aim is enhance the security of the biometric system.

Below you see different approaches to the creation of multibiometric systems [1]:

- multimodal (more than one biometric trait is used for user identification).
- multialgorithmic (multiple different approaches to feature extraction and matching algorithms are applied to a single biometric trait).
- multiinstance (multiple instances of a single biometric trait are captured).
- multisensor (information of the same biometric obtained from different sensors are combined for all).
- multisample (multiple samples of a same biometric trait are used for the enrollment and recognition).

Multimodal biometric systems can operate in three different modes [1]:

- Serial Mode (cascade mode) — each modality is examined before the next modality is investigated.
- Parallel Mode — sensed/captured data from multiple modalities are used in concurrent way to perform recognition, then the results are combined to make final decision.
- Hierarchical Mode — individual classifiers are combined in a hierarchy or tree structure.

There are the following different levels of fusion in multibiometric system: decision, score, feature, and sample. Universal system should take into account all possible approaches to implementation multibiometrics by using fusion [8].

There are three strategies for multibiometric fusion [9]:

- User-specific normalization for multibiometric fusion. For example, depending on the quality of input samples, the proposed algorithm intelligently selects appropriate fusion algorithm for optimal performance [10].
- Robustness criterion to rank users according to their performance. It gives consistently good performance across different databases despite the lack of training samples. Fisher-ratio, F-ratio, and d-prime reported as examples of criteria in [9].
- Selective fusion strategy. Because not all biometric characteristics need to be operational for each transaction or the participating biometric systems can operate independently of each other, we should dynamically select appropriate fusion algorithm for effective performance.

In the work [11] a dynamic score level fusion scheme for a multialgorithmic recognition by incorporating quality as an input for fusion was investigated. Smartness has been very tactfully administered to the processing by employing different efficient algorithms for a given modality. Selection of the recognition algorithms is rooted on the attributes of the input. If one sensor is not functional, others contribute to the system making it fault-tolerant. Multiplicity has been employed to establish a unanimous decision. Information fusion at various levels has been introduced. Sensor level fusion, local decision level fusion at algorithmic level and global decision level fusion provide the right inference. A multitude of decisions are fused locally to decide the weightage for the particular modality. Algorithms are tagged with weights based on their recognition accuracy. Weights are assigned to sensors based on their identification accuracy. Adaptability is incorporated by modifying the weights based on the environmental conditions. All local decisions are then combined to result in a global decision about the person.

In the work [12] authors propose the design of a sequential fusion technique that uses the likelihood ratio test-statistic in conjunction with a support vector machine classifier to account for errors in the former; and the design of a dynamic selection algorithm that unifies the constituent classifiers and fusion schemes in order to optimize both verification accuracy and computational cost. Depending on the quality of the input biometric data, the proposed algorithm dynamically selects between various classifiers and fusion rules to recognize an individual [12]. The resulting algorithms are used to reduce the effect of covariate factors in face recognition by combining the match scores obtained from two face recognition algorithms.

In the paper [13] presents techniques for performing multibiometric fusion at the rank level. The proposed methods are suggested to enhance the performance of rank-level fusion schemes in the presence of weak classifiers or low quality input images. It's not required an additional training phase, making them suitable for a wide variety of databases. Also it should be included performing a comparative study on the effect of input image quality on score level, rank level and decision level fusion; using quality factor to select the best probe image for fusion; and conducting experiments using other databases consisting of different modalities.

Multibiometric systems must be highly flexible to take into account the different requirements and limitations of users. The system should solve the problem lack of biometric characteristics, as a result of poor quality or physical problems, with possibility to use other available biometric characteristics. In addition, it is important to comply with the requirement necessary security level. It requires developing a dynamic elective different rules and methods of multibiometric fusion.

One of the approaches described in article [14], which experimented with a few simple methods of fusion multibiometric.

The authors [15] proposed another interesting approach, that includes conducting continuous authentication. This approach requires a long physical presence of user and therefore it isn't suitable for some kinds of applications.

In article [16] proposed to use multiple security levels for multibiometric authentication with three biometric characteristics (face, lip movement, voice). When the required security level is low, it is sufficient to take a decision on the basis of two of the three biometric characteristics. On the other side, for applications with a high security level, this system requires the use of all three biometric characteristics. However, this system does not provide a way to change the dynamic security level. Instead, the administrator makes a decision witch strategies and methods of fusion has to be used.

Interesting architecture for dynamic security management of multibiometrics has been discussed in [17]. This work suggests a scenario of managing permission in the building with divided into different zones (this can be different floors or room numbers), and defined access rights for each user. Access solutions in a particular area may also depend on the solutions already adopted in the other zones. Furthermore, the amount of biometric characteristics required in each zone and different elective rules of fusion can be varied.

Another aspect of the development of elective multibiometric system is to provide the desired performance, as well as the performance of users' preferences, constraints, user convenience, and age–related changes [18]. Research challenges of these problems related to the dynamic fusion techniques.

Security level of multibiometric system must also be adjusted depending on the possible future attacks. This system requires the elective appropriate methods for the fusion.

In the work [19] a new approach for the adaptive combination of multiple biometrics to dynamically ensure the desired level of security is presented. The proposed method uses a hybrid particle swarm optimization to achieve adaptive combination of multiple biometrics from their matching score performance. Experimental results suggest that the dynamic selection of fusion rules and their parameters using the proposed method can offer better performance than the decision level scheme. The work [19] is focused to estimate on the performance improvement. One of the key problems in adaptive multibiometric management pertains to the selection of biometric modalities.

Therefore this paper is focused to develop algorithms that can adaptively select best set of biometric modalities from the available set to ensure the desired level of security.

3 Proposed elective multibiometric authentication

In this paper, as opposed to all previous work it offers a combined approach to the development of elective multibiometric authentication system that uses all of the above criteria for selecting the method of fusion multibiometrics.

The criteria for the election of multibiometric authentication is described as a scheme in Figure 1, which shows the main stages of the elective multibiometric authentication based on rhythm of password, voice, dynamic signature and graphical recognition. This approach and design can be generalized to other biometric characteristics.

The most important building block for this scheme is a unit of semiautomatic settings, which performs the convert of all settings and parameters set by the administrator and the user at the stage of training. The parameters and settings of semi–automatic selection performs order of biometric characteristics,

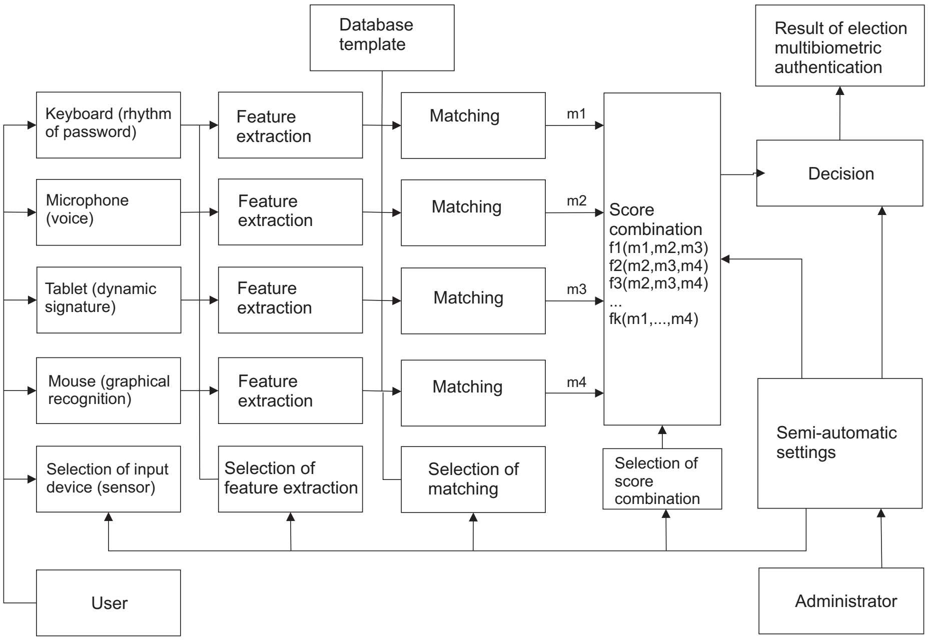
Database template
Result of election multibiometric authentication
Keyboard (rhythm of password)
Feature extraction
Matching
m1
Decision
Microphone (voice)
Feature extraction
Matching
m2
Score combination f1(m1,m2,m3) f2(m2,m3,m4) f3(m2,m3,m4) ... fk(m1,...,m4)
Tablet (dynamic signature)
Feature extraction
Matching
m3
Mouse (graphical recognition)
Feature extraction
Matching
m4
Semi-automatic settings
Selection of input device (sensor)
Selection of feature extraction
Selection of matching
Selection of score combination
User
Administrator

Fig. 1. Scheme of elective multibiometric authentication.

set of biometric characteristics, the input devices (sensor), the feature extraction methods, the matching methods, the method of the score combination and decision. The choice of semi–automatic selection of the methods is a fusion of predefined strict rules and criteria.

Here are the basic criteria and rules:

1. Availability of necessary input devices (sensors);
2. The security level (the number of required biometrics);
3. Elective priority of biometrics;
4. The result of previous authentication attempts;
5. Features of area (room, equipment);
6. Features of users and their preferences, age limits;
7. The request time for authentication;
8. The extent of the attacks and spoof attacks on the sensor;
9. The quality of biometric samples.

After setting all parameters, unit semi–automatic settings may select a desired decision in the block score combination $f_1(m1, m2, m3), ..., f_k(m1, ..., m4)$ and a decision threshold, where $m1, m2, m3, m4$ — result matching each biometric characteristics individually.

However, this elective multibiometric system doesn't automatically select the parameters to guarantee a certain security level; this work is to further research and development.

In our proposed elective multibiometric authentication there are 4 biometric characteristics (voice, dynamic signature, rhythm of password, graphical recognition). All possible subset $\{1, 2, 3, 4\}$ can be: $\{\cdot\}, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}$.

Each of 16 subsets describes one of the choices of biometric characteristics in elective multibiometric authentication. We describe the algorithm of select combination of biometric characteristics, depending on the level of security through the following model.

Let the set used biometric characteristics defined as $\{p_1, p_2, p_3, p_4\}$, where p_i — the index of using biometric characteristics i. We assume that the criteria influencing for p_i are independent. Then

$$p_i = \prod_{j=1}^{k} p_i^j,$$

where p_i^j — assessment of factor of using biometric characteristics i using the criteria j.

Here are the criteria j for each biometric characteristics i in the proposed elective multibiometric authentication:

- $p^1 = \{0, 1\}$ — factor of availability of necessary input sensors. $p^1 = 1$ when input sensor is available, and $p^1 = 0$ when input sensor is not available.
- $p^2 = [1, 10]$ — factor of necessary security level. Administrator sets this factor for each biometric characteristics i. For example, $p^2 = 10$ for implicit voice authentication, for other biometric characteristic (dynamic signature, rhythm of password, graphical recognition) $p^2 = 3, 9, 6$ respectively.
- $p^3 = [1, 10]$ — factor of using attacks on sensor. Administrator sets this probability for each biometric characteristics i. For example, $p^3 = 3$ for voices because of high risk of spoof attacks, for other biometric characteristic (dynamic signature, rhythm of password, graphical recognition) $p^3 = 9, 7, 6$ respectively.
- $p^4 = [0, 1]$ — factor of quality of biometric samples. Depending on the quality of input samples, the proposed algorithm dynamically selects appropriate fusion algorithm for optimal performance [10,11,13].
- $p^5 = [3, 10]$ — factor of result of previous authentication attempts. This factor dynamically estimate. For example, $p^5 = d$ if the last d attempts had failed to authenticate.
- $p^6 = [1, 10]$ — factor of security level of area (room, equipment). Administrator sets this factor for each biometric characteristics i.
- $p^7 = [0, 1]$ — factor of user preferences. Administrator sets this factor for each user. For example, because of age limits or lack biometric characteristic then $p^7 = 0$, otherwise $p^7 = 1$.
- $p^8 = [0, 10]$ — factor of request time for authentication. For example, $p^8 = 3$ for voices because of long process, for other biometric characteristic (dynamic signature, rhythm of password, graphical recognition) $p^8 = 9, 7, 6$ respectively.

An algorithm for selecting a subset of elements for elective multibiometric authentication:

1. Consider $\{p_1, p_2, p_3, p_4\}$, all values by evaluating all criteria p^j.
2. Compare p_i with a threshold $\alpha > 0$. If $p_i < \alpha$ then exclude p_i. Administrator sets this threshold α.
3. Once the values have been calculated $\{p_1, p_2, p_3, p_4\}$, we sort p_i desc.
4. Choose the t first p_i, which correspond to the high indices selected biometric characteristic. Administrator sets this parameter t.

In our proposed elective multibiometric authentication, depending on various conditions and factors, including the availability of electronic means and convenience, resistance to attacks and exploits, disease or injury of users can be selected on the basis of biometric authentication of any such biometrics as rhythm password, voice, dynamic signatures and graphics password.

4 Security of elective multibiometric authentication system

Implementation of biometric systems has problems in the security, so let's consider the most important developing aspects of elective multibiometric authentication [20,21,22].

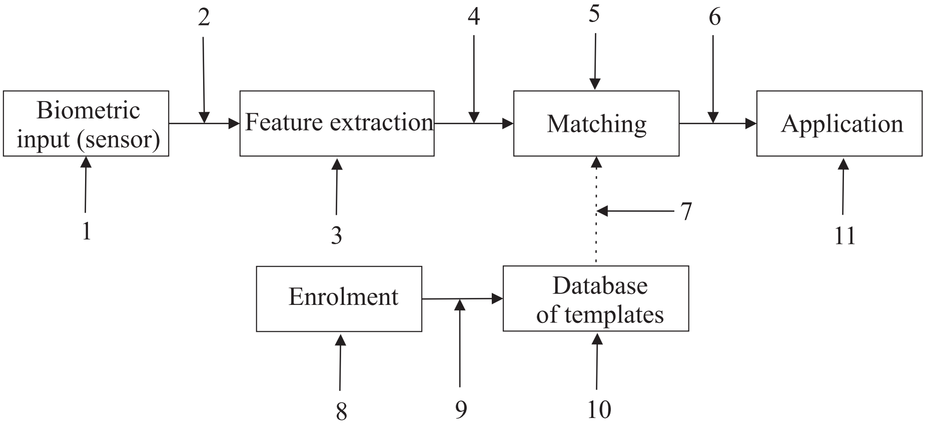

Fig. 2. The general scheme of biometric authentication with the designated attack.

The article gives an overview of current attacks and protection measures [23,24]. Here are all the typical attacks, threats related to the elements of the authentication system (see Fig. 5):

1. An attack on the biometric input (sensor);

2. An attack on the communication channel between sensor and biometric systems;
3. An attack on the feature extraction;
4. An attack on the communication channel of feature extraction;
5. An attack on the matching;
6. An attack on the score;
7. An attack on the link with the database of templates;
8. An attack on the enrolment;
9. An attack on the channel between the enrolment and database of templates;
10. An attack on the templates;
11. An attack on the application.

All of the above attacks, excepts an attack on the input device, are common to all biometric systems. Protection against these attacks is to use digital encoding, timestamp, encrypt the data channel, the special methods to prevent the introduction of malicious code, antivirus methods and other methods to protect the information [25].

Most interesting attack is an attack on the input sensor in a multibiometric system, since this attack poses a real threat [26,27,28,29]. This attack is directed to an biometric input (sensor), and occurs when an attacker provides illegitimate biometric sensor. This attack can be divided into three types:

- forced attack is providing biometric characteristics on illegitimate grounds, such as the use of violence;
- simulation attack is simulating biometric characteristics by synthesized biometric data;
- replay attack is replaying previously recorded biometric data.

Many of problems and attacks can be prevented by using digital coding, timestamp and encrypt data channel. In other words, there are special cryptographic protocols to help prevent various attacks [30].

Also you can use the following methods to prevent attacks:

- Use the methods of detecting the liveness of biometric characteristics;
- Apply the different approaches of organization of database templates and the structure of template to improve security systems;
- Use multifactor authentication to improve the reliability of biometric systems;
- Use special methods of reducing biometrics and «encryption personality» to resolve the problem of confidentiality and protection of biometric data.

The analysis of all threats of the elective multibiometric authentication system allows making the conclusion: the using of multibiometric and the principle of selectivity increase the reliability and security, since the attacker must take into account all the parameters and characteristics of the implementation of security system and the criteria for selecting all parameters.

Quantitative estimates of reliability and security of multibiometric authentication doesn't restrict to test a large base of multibiometric samples, and the results obtained by generalized theoretical estimates of reliability can be found in [5].

5 Conclusion

As a result of this work it has be developed the elective multibiometric authentication system. In this paper, as opposed to all previous work it was offered a combined approach to the development of elective multibiometric authentication. In this approach uses different criteria for the choice of semi–automatic method of fusion and other parameters of multibiometric authentication system.

In addition, an analysis of possible attacks, recommendations of protects and conclusions were carried out.

However, there are some trends in future developments of the system: providing greater versatility, using other biometric features, increasing performance and reliability, implementation of dynamic selection of parameters, in particular, the method of fusion multibiometric data for a guaranteed level of security.

Acknowledgements. This research was supported by grant RFBR 14-07-31049-mol-a.

References

1. Gad, R., El-Fishawy, N., El-Sayed, A., Zorkany, M.: Multi-Biometric Systems: A State of the Art Survey and Research Directions. International Journal of Advanced Computer Science and Applications 6(6), 128–138 (2015)
2. Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., Senior, A. W.: Guide to biometrics. Springer-Verlag, New-York (2003)
3. Dunstone, T., Yager, N.: Biometric system and data analysis: design, evaluation, and data mining. Springer, Boston, Ma (2009)
4. Ross, A. A., Nandakumar, K., Jain A. K.: Handbook of multibiometrics. Springer, New York (2006)
5. Bhanu, B., Govindaraju, V.: Multibiometrics for Human Identification. Cambridge University Press, Cambridge (2011)
6. Sesin, E. M., Belov, V. M.: Personal identification system based on integration organization of several biometric characteristics of the person. Proceedings of Tomsk State University of Control Systems and Radioelectronics 2(25), 2, 175–179 (2012)
7. Ruchay, A. N.: Development of a universal set of modules for managing permissions windows xp on based biometric authentication. Security of information technology 2, 74–78 (2013)
8. Vokhmintsev, A., Makovetskii, A., Kober, V., Sochenkov, I., Kuznetsov, V.: A fusion algorithm for building three-dimensional maps. SPIE Proceedings (9599), 1–7 (2015)
9. Poh, N., Ross, A., Lee, W., Kittler, J.: A user-specific and selective multimodal biometric fusion strategy by ranking subjects. Pattern Recognition 46, 3341-–3357 (2013)
10. Vatsa, M., Singh, R., Noore, A.: Context Switching Algorithm for Selective Multibiometric Fusion. Pattern Recognition and Machine Intelligence (5909), Springer, 452–457 (2009)
11. Fathima, A., Vasuhi, S., Treesa, T., Babu, N.T., Vaidehi, V.: Person Authentication System with Quality Analysis of Multimodal Biometrics. WSEAS transactions on information science and applications

12. Vatsa, M., Singh, R., Noore, A., Ross, A.: On the Dynamic Selection of Biometric Fusion Algorithms. IEEE transactions on information forensics and security 5(3), 470–479 (2010)
13. Abaza, A., Ross, A.: Quality Based Rank-Level Fusion in Multibiometric Systems. Proc. of 3rd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS) (2009)
14. Kittler, J., Hatef, M., Duin, R. P. W., Matas, J.: On combining classifiers. IEEE Trans. Patt. Anal. Machine Intell. 20, 226–239 (1998)
15. Sim, T., Zhang, S., Janakiraman, R., Kumar, S.: Continuous verification using multimodal biometrics. IEEE Trans. Patt. Anal. Machine Intell. 29(4), 687–700 (2007)
16. Frischholz, R. W., Deickmann, U.: BioID: a multimodal biometric identification system. IEEE Comput. 33(2) (2000)
17. Bradlow, E. T., Everson, P. J.: Bayesian inference for the beta-binomial distribution via polynomial expansions. J. Comput. Graphical Statistics 11(1), 200–207 (2002)
18. Poh, N., Wong, R., Kittler, J., Roli, F.: Challenges and research directions for adaptive biometric recognition systems. Proc. ICB, Alghero, Italy. (2009)
19. Kumar, A., Kanhangad, V. Zhang, D.: A new framework for adaptive multimodal biometrics management. IEEE Transactions on Information Forensics and Security. (5), 92–102 (2010)
20. Ruchay, A. N.: Prototype centralized system of election multifactor biometric authentication. Security of information technology 1, 118–120 (2013)
21. Ruchay, A. N., Gorshenin, V. V., Matkin I. A.: Development of prototype centralized system of elective multifactor biometric authentication. Intelligent information processing: theses of the 10th international conference, Greece, Crete 2014. 231 (2014)
22. Wayman, J.: Technical testing and evaluation of biometric devices. Biometrics — personal identication in networked society. Kluwer Academic Publisher. 345–368 (2002)
23. Ruchay, A. N.: The model of attacks and protection of the speaker recognition biometric system. Proceedings of Tomsk State University of Control Systems and Radioelectronics 1(23), 96–100 (2011)
24. Roberts, C.: Biometric attack vectors and defences. Computers and Security 26(1), 14–25 (2007)
25. Ruchay, A. N.: Dependent speaker verification. LAP LAMBERT Academic Publishing, Saarbrucken (2012)
26. Ratha, N. K., Connell, J. H., Bolle, R. M.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40(3), 614–634 (2001)
27. Yanushkevich, S., Shmerko, V., Stoica, A., Popel, D.: Inverse Problems of Biometrics. CRC Press, Taylor and Francis Group (2005)
28. Yanushkevich, S., Wang, P., Gavrilova, M., Srihari, S.: Image pattern recognition: synthesis and analysis in biometrics. Series in Machine Perception and Artifical Intelligence 67 (2007)
29. Uludag, U., Jain, A.: Attacks on biometric systems: a case study in fingerprints Proc. SPIE. 5306, 622–633 (2004)
30. Schneier, B.: The uses and abuses of biometrics. Communications of the ACM 42(8) (1999)