УДК 658.71.08,519.87
DOI: 10.26467/2079-0619-2021-24-2-93-104

DEVELOPMENT OF BIOMETRIC SYSTEMS FOR PASSENGER IDENTIFICATION BASED ON NOISE-RESISTANT CODING MEANS

A.A. GLADKIKH[1], A.K. VOLKOV[1], T.G. ULASYUK[1]
[1]Ulyanovsk Institute of Civil Aviation Named after Air Chief Marshal B.P. Bugaev, Ulyanovsk, Russia

The paper deals with the issues of using the biometric technologies to establish identity of a passenger. The purpose of the article is to analyze the techniques of enhancing reliability of various biometric identification facilities by means of using error correction codes. The basic elements and the principle of the classical biometric system functioning are presented. On the basis of the International Civil Aviation Organization (ICAO) recommendations, the procedure features of pattern recognition are presented. The versions to adopt the biometric passenger authentication procedures are under consideration. The conclusion is drawn that with the centralized biometric databases the issues of confidentiality and information security exist. The problems are characterized by the possibility of biometric images compromise, which can potentially lead to the loss of their confidentiality and the impossibility of their further usage for personal identification. The passenger authentication procedure involving the simultaneous use of biometric parameters and contact-free SMART cards seems more reliable. SMART cards are used for distributed storage of biometric and other additional data, thus neutralizing the disadvantages of access to the centralized databases. It is shown that the subsequent step in the development of this domain is the application of biometric cryptography proposing "linking" encryption keys and passwords with the biometric parameters of the subject. Consideration is given to the principle of "fuzzy extractor" operation as one of the variants for the "biometrics-code" converter. Feasibility and necessity of upgrading the means of noise-resistant coding in the systems being studied are shown. The use of permutation decoding data algorithms capable of adequately corresponding to the particular problems of biometric identification is proposed. On the basis of the results of optical communication channels statistical modeling, the necessary and sufficient conditions for application of the permutation decoding tools for binary codes are determined. The problem to minimize memory amount for the permutation decoder cognitive map due to the permutation orbits allocation and usage of the generated loops combinations as pointers of reference plane is solved. The resulting algorithm for finding a unique orbit number and its corresponding reference plane by means of receiver formation of arbitrary parameters permutation from the set of permissible permutations is proposed.

Key words: passenger, biometrics, authentication, fuzzy extractor, permutation decoding, loop, orbit.

INTRODUCTION

Check and verification of the passenger's identity is one of the procedures of the inspection at an airport. This task is currently assigned to the qualified passport control specialists of the aviation security service, who carry out an inspection of travel documents and identification of passenger identity. In this case occurrence of a human factor can lead to embarkation of a person with wrongful intent. In order to board an aircraft illegally, these people resort to forgery of documents. Nevertheless, with the increase of modern passports security level, it is becoming increasingly difficult for law violators to realize similar actions. An alternative method to avoid forgery of documents, which can be revealed during a passport control, is the illegal use of another person’s passport that has a similar appearance to the potential violator. In this case, the detection of falsification depends on experience and training skills of the passport control officer.

In order to neutralize a negative impact of a human factor, a perspective tool is the application of biometric technologies while establishing identity of a passenger. The implementation of these technologies will make it possible to organize quick boarding exits, allowing passengers to scan their travel documents by themselves. After the check of boarding documents and positive authentication, the passenger will be able to board the aircraft through a special gate. Due to this pre-flight inspection organization, the staff of the inspection groups will focus on passengers with a high degree of risk. This will help reduce the requirement of ground personnel and ground handling, by additionally decreasing operating costs. In addition, self-boarding an aircraft can have a positive impact on customer satisfaction, as it cuts service time significantly. Quick boarding gates can also register various operational data that can help understand the passengers' behavior or satisfaction better.

The purpose of this article is to analyze various biometric personal identification facilities and to detect the ways of increasing efficiency of their operation by applying the updated error correction codes.

CONVENTIONAL BIOMETRIC SYSTEMS

The key components of a standard biometric system are: an input device (registration); a bio parameters extractor; a comparison device (matcher); and a template database [1]. Let us consider the operation principle of the classical biometric passenger identification system (fig. 1).

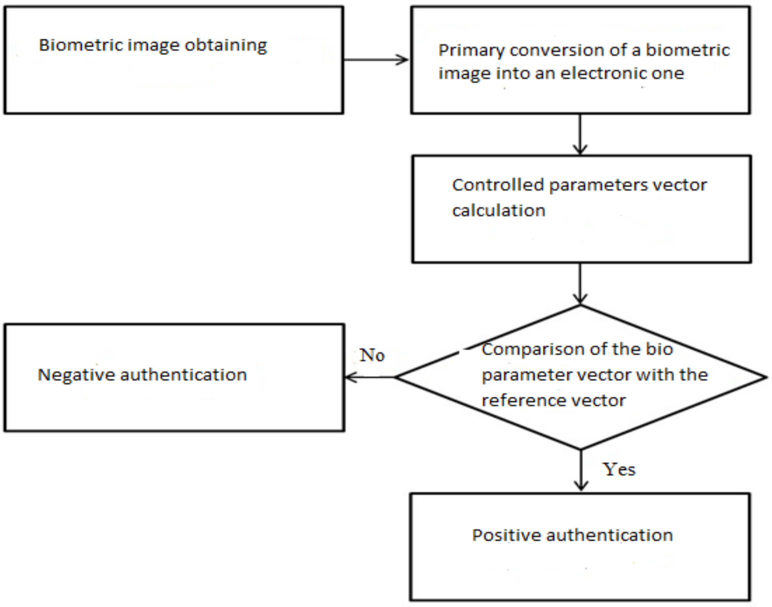

Biometric image obtaining
Primary conversion of a biometric image into an electronic one
Controlled parameters vector calculation
Comparison of the bio parameter vector with the reference vector
No
Negative authentication
Yes
Positive authentication

Fig. 1. Flowchart of the biometric authentication procedure

According to Figure 1, the biometric authentication procedure includes the following steps: taking a human biometric sample using an input device; converting the biometric sample into a machine representation using a property extractor; computed the magnitude of similarity between the newly entered biometric sample and the template stored in a centralized database. According to the results, the conclusion about positive or negative authentication is made.

At the heart of the classifier construction, which realizes the comparison of the bio parameters current vector with the reference vector, there are three concepts of decision-making based on pattern recognition methods [2]:

- a distance estimation based concept. The estimation of the proximity of classes (patterns) relative to another class in a given sign space is based on a certain measure of proximity (metric). If there is no correlation between the signs, the measure of Euclid, Pearson, etc. is used. If there is correlation – the distance of Mahalanobis is used.
- a probabilistic approach based concept. This approach assumes the laws and values distribution parameters of the analyzed biometric signs determination. Most often, the classifier is based on Bayesian decision rules.
- a concept based on the boundaries of decision-making. The approach involves minimizing of the criterion value that evaluates the error between the input pattern and the reference one. The operation of classifier is based on the usage of Fisher linear discriminator, neural networks (the multilayer perceptron in particular), etc.

Currently, there are both dynamic and static biometric parameters that are used in identification systems. Dynamic characteristics include a person's voice, signature, and keyboard handwriting, while static characteristics include fingerprints, face, hand geometry, and iris. According to the results of the ICAO[1] specialized working group the proposals to use the passenger faces as a key biometric identifier were developed. One of the main reasons is the possibility of implementing the global compatibility of passport verification systems. It is facilitated by a number of factors, such as people's social acceptance of the ordinary fact that the face is used as a personality identifier, in particular. According to the ICAO recommendation, it was suggested to consider the fingerprint and the iris as additional identifiers.

In general, the procedure of passenger identification by face comprises 4 major stages: entering a biometric sample, detecting the face in the photo, calculating the distances between the key points of the face, and direct identification. Developments in the field of pattern recognition have led to the formation of 2 classes of biometric systems that can analyze 2D and 3D images. Digital passenger identification systems use two-dimensional flat patterns analyzers. The points and distance between the centers of eyes, between the eye line and the nose tip corresponding to the largest nose width, between the eyebrows arches and the lower chin point, between the lower earlobes points, between the nose tip and the lower lips point are analyzed in the portrait of the face [3].

ICAO considers the following techniques for the biometric passenger authentication procedures:

1) Two-way verification, which involves assessment of the matching degree between the presented biometric sample (the image of the passenger's face) and the template stored in the travel document or in the central database.

2) Three-way verification, which involves assessment of the matching degree between all three parties: the presented biometric sample; the template stored in the travel document, and in the central database.

A significant disadvantage of the organization of passenger biometric identification systems based on a single server with the pattern database is the possibility of compromising these patterns, which can potentially lead to loss of their confidentiality. There is a probability of biometric patterns abuse for a purpose unknown to a passenger. Illegal sale of biometric databases to third parties or the rights to use them can be referred to the stated above facts. In case at least the template of one passenger is compromised a probability exists that the entire database may become invalidated. In addition, in contrast to long passwords, which can be recovered if they are lost or stolen, biometric parameters (for example, the passenger's face or fingerprints) are unique and their compromising makes it impossible their further use for personal identification.

Thus, the approach to biometric authentication organization of passengers based on the biometric data centralized storage does not allow us to ensure entirely passengers anonymity. This is due to the fact that the standard biometrics technologies require storage of an open biometric pattern, the extraction of which is equivalent to compromising anonymity of a person. The task of additional security measures for biometric templates implementation or changing the biometric identification procedure organization itself has emerged.

The organization of the passenger authentication procedure with the simultaneous use of biometric parameters and contactless SMART cards (without access to a central database) will allow you to realize additional advantages in the field of information confidentiality. SMART cards are used for distributed storage of biometric and other additional data, thereby neutralizing the disadvantages of the centralized databases. The recorded supplementary information can provide an additional support to a matching device. For example, in the event of the recognition system, expected changes to the face pattern can also be additionally recorded. In case of a fingerprint recognition system, their additional properties combined with the matching threshold value can be recorded. Bank plastic cards, RFID devices, biometric passports, etc. can be used as SMART cards.

[1] DOC 9303 Machine-readable Travel Documents. Part 1. Machine-readable Passports with Biometric Identification Tools. Volume 2 Specifications for Electronic Passports with Biometric Identification Tools Sixth Edition, 2006, 40 p.

Let us consider the operational principle of the similar authentication system comprising a SMART card, a reading terminal, and a communication channel between them [4]. Depending on where the biometric data matching stage is implemented there are two possible approaches to functioning of the similar systems: 1) on the side of the reading terminal; 2) on the side of the SMART card.

1) At the registration stage, the biometric standard, which was previously protected by a noise-resistant code on the terminal side, is recorded on the SMART card. For authentication, the passenger submits the reader terminal both a real biometric parameter and a SMART card. The terminal decodes the encoded reference biometric vector stored on the SMART card by means of transmitting over the communication channel, while simultaneously extracting the vector of bio parameters from the submitted biometric sample of a passenger, and then checks matching.

2) At the registration stage, the open biometric standard is transmitted to the SMART card, which protects it with the noise-resistant code and then saves it in the memory. At the authentication stage, the terminal extracts the vector of bio parameters from the submitted biometric sample of a passenger and transmits it to the SMART card matcher via the communication channel. Simultaneously, the matcher obtains a biometric standard decoded from the card memory. Then the terminal reads the solution computed by the matching device on the SMART card.

In the both considered examples the decision about positive or negative authentication occurs without contacting the database server. If the passenger loses this card, the access is blocked until a new card is received. Even if intruders take possession of the card in order to use it and deceive the authentication system, it will be necessary to present a biometric sample (real or simulated).

Let us analyze the drawback of the first functioning scheme of the analyzed authentication system. It is reasonable to assume that the reading terminals have the necessary computing resources to implement effective noise-resistant encoding and decoding of biometric data [4]. Therefore, a reliable communication channel is a key element of the identification system. The following situation can be considered as a key drawback of the given scheme. Suppose that an error occurred in the code during the data transmission and the reading terminal was able to correct it. Subsequently, the data in the SMART card will be rerecorded onto the original one. Otherwise, an imaginary irrecoverable loss of data in the card memory will be fixed while it is actually preserved.

The advantage of the second operation scheme is an increased level of security against compromise and various attacks due to the fact that the matcher operates directly on the card and the recorded biometric standard is not transmitted beyond its limits. Moreover, a certain disadvantage concerns the small amount of memory and performance of SMART cards integrated circuit. Modern cards can have approximately 4–16 Kb of random access memory (RAM) and 16 to 256 Kb of permanent storage memory. According to ICAO[2], the minimum memory capacity of an integrated circuit must be at least 32 Kb. This allows you to store a standard photo of a face with 15–20 Kb of size. For this purpose the memory capacity of the circuit can be increased up to 112 Kb. Therefore, the applied noise-resistant code, comprising its redundant part, should not be too large. This volume should correspond to the hardware capabilities of the card. Coupled with the limit for the code redundant information amount, the restriction concerning the card performance requires application of effective noise-resistant coding algorithms to carry out data processing procedures within acceptable time.

BIOMETRIC CRYPTOGRAPHIC SYSTEMS

Further development of the biometric passenger identification systems is directly linked to a new direction in the field of data security – biometric cryptography. Within the framework of this technology, encryption keys or passwords with the biometric parameters of the subject are combined

[2] DOC 9303 Machine-readable Travel Documents. Part 1. Machine-readable Passports with Biometric Identification Tools. Volume 2 Specifications for Electronic Passports with Biometric Identification Tools Sixth Edition, 2006, 147 p.

on the basis of the "biometrics-code" converters (BCC) usage. These converters, in contrast to the above studied classical biometrics, allow you to convert the original biometric data into a bit (key) sequence, which is then used for subject authentication. In this respect, it is impossible to restore the original biometric pattern from supporting information.

Two basic types of biometric code converters have been distinguished so far: "fuzzy extractors" and neural network biometric code converters. The first version of the biometric code converter is going to be discussed in this paper.

"Fuzzy extractors" are a technique of extracting random, evenly distributed bits sequences from fuzzy (noisy) biometric data, to which error-correcting codes are subsequently applied to correct the unstable bits of the generated key-password [5–9]. The "fuzzy extractor" enables you to receive only one key, which length is assigned as a parameter. Let us study the "fuzzy extractor" model. As an example, Figure 2 demonstrates the key generation scheme using the eye iris.

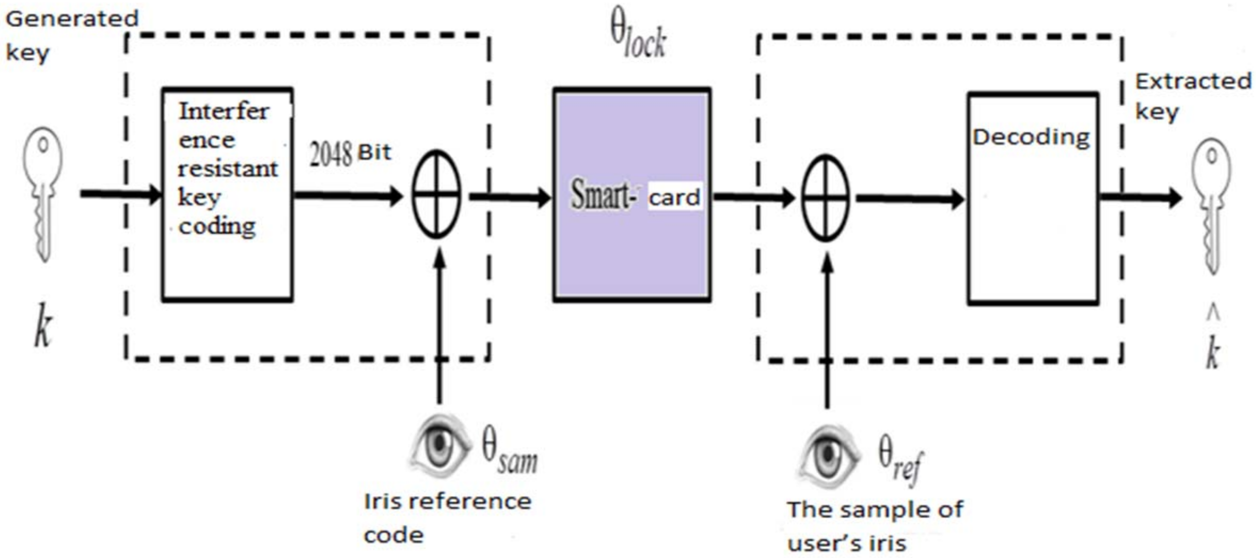


Fig. 2. Biometric key generation scheme by a "fuzzy extractor"

The primary task is to form the sequence k. The sequence must have a random even distribution. Afterwards key noise coding is performed, as a result we obtain the "pseudo-code" of the eye iris θ_{ps}. It is similar to the real iris code, because it has the same length of 2048 bits. A two-layer error correction method is used to correct unstable bits of biometric data. The outer layer uses Hadamard code to fix random errors at the binary level. To fix errors at the internal level (burst bit errors), Reed-Solomon code (RS) is used. Further, the "pseudo-code" is blocked using XOR operation with the reference code of the iris θ_{ref} obtained during the user registration [7]:

$$\theta_{lock} = \theta_{ps} \oplus \theta_{ref}.$$

The results of integration are stored on the physical token *T*. The results of hashing the key, *H(k),* are also added to θ_{lock}. Subsequently, the key *k* must be safely erased. The coding formula can be described in the following way [7]:

$$\left\langle k, \theta_{ref} \right\rangle \Rightarrow T : \{\theta_{lock}, H(k)\}.$$

At the decoding stage, in order to unlock the key, the user is provided with his or her iris θ_{sam}. After conducting XOR operation with lock data θ_{lock} they are sequentially decoded using PC and Hadamard codes to extract biometric key $\hat{k}$. If the hash key value matches the stored one, i.e. $H(\hat{k}) = H(k)$, in this case the obtained key is recognized as correct. In any other case, the key is considered to be false and will be rejected. The decoding process formula is described as follows:

$$\langle \theta_{sam}, T \rangle \Rightarrow \hat{k}.$$

As it can be seen, the advantage of "fuzzy extractors" over traditional biometrics is the absence of necessity to store directly the biometric standard of the subject. On any physical token, it is only necessary to store an open line, which makes it impossible to restore the subject model.

The effectiveness of "fuzzy extractors" primarily depends on the methods of noise-resistant coding, the disadvantages of which in this type of biometric code converter include [10]:

1. The classical applicable codes such as (Hamming, Hadamard, Bose-Chowdhury-Hawkwingham) introduce redundancy. The greater the correcting code power is, the greater redundancy is and the shorter the generated password key length is.

2. Classical codes are not able to correct a great amount of errors.

Thus, one of the most important ways to improve biometric cryptography systems based on the "fuzzy extractor" is to choose an effective algorithm for noise-resistant coding.

PERMUTATION DECODING IN BIOMETRIC SYSTEMS APPLICATION PROSPECTS

As a result of the analysis, it is shown that the means of noise-resistant coding in the considered systems need to be improved. The following authors in their works [11, 12] propose to use the method of permutation decoding (PD) with elements of cognitive data processing in order to enhance reliability of biometric systems functioning. This approach is based on the use of the cognitive (CD) decoder map whose application allows you to replace the computational process by searching for the finished result in the card with a small amount of additional actions [12]. In addition, there is an opportunity to minimize further decoder cognitive map (CD) amount of memory. Its underlying idea is revealed in this part of the article.

Essential and Sufficient Conditions for Permutation Decoding Implementation

The use of permutation decoding (PD) enables you to execute the procedure of "training" the decoder with the purpose of speeding up the data processing. This is accomplished due to the deterministic component $Dn(t)$, which is the part of the permutation decoding (PD) process. The fact of decoder "training" consists of the ability to identify specific permutations and, without making complex computations, to produce a finished result. The card memory capacity depends on the code dimension and since it is assumed to use non-binary code structures, the problem of such memory rational organization emerges. The decoder cognitive map takes into account the possible code vectors symbols permutations, which directly depend on ratings distribution of character reliability. The result is an equivalent code (EC) formation.

This is provided by the procedure of soft binary or non-binary characters processing and selecting the most reliable characters from the tuple of accepted ones. Thus, a necessary condition for implementation of the data decoding process acceleration is the availability of a cognitive decoder map. Soft values of characters are obtained according to the expression (1):

$$\lambda_i(z) = \left\lfloor \left| \frac{\lambda_{\max}}{\mu\sqrt{E_b}} \times z_i \right| \right\rfloor, \ at \ 0 \le z_i \le \mu\sqrt{E_b}, \tag{1}$$

Where $\lambda_{\max}$ – is the maximum value of the soft solution (assigned by a designer); μ – is the erasure interval value (usually $0 \le \mu < 1$); E_b – is one Bit signal energy; z_i – is the objective fixed value of the signal.

It is significant that in quotation 1 the parameters characterizing the communication channel property, for example in noise variance, are not presented. It is advisable to use the method of comparing histograms for non-binary codes.

Results of Statistic Modeling for the Soft Decision Formation System

Let us evaluate the permutation decoding implementation possibilities for some codes. Let the code be the maximum decodable code for which $d_{\min} = n - k + 1$. The equivalent code asymptotic estimation for such type of codes can be determined by the equation $D_{\max}(k) = 10\lg(k - \frac{k^2}{n} + \frac{k}{n})$ [11]. The mentioned function extremum evaluation results in the equation $2k = n + 1$. This means that permutation decoding is effective when the length of k parameter is half n code vector. The test results are shown in Figure 3.

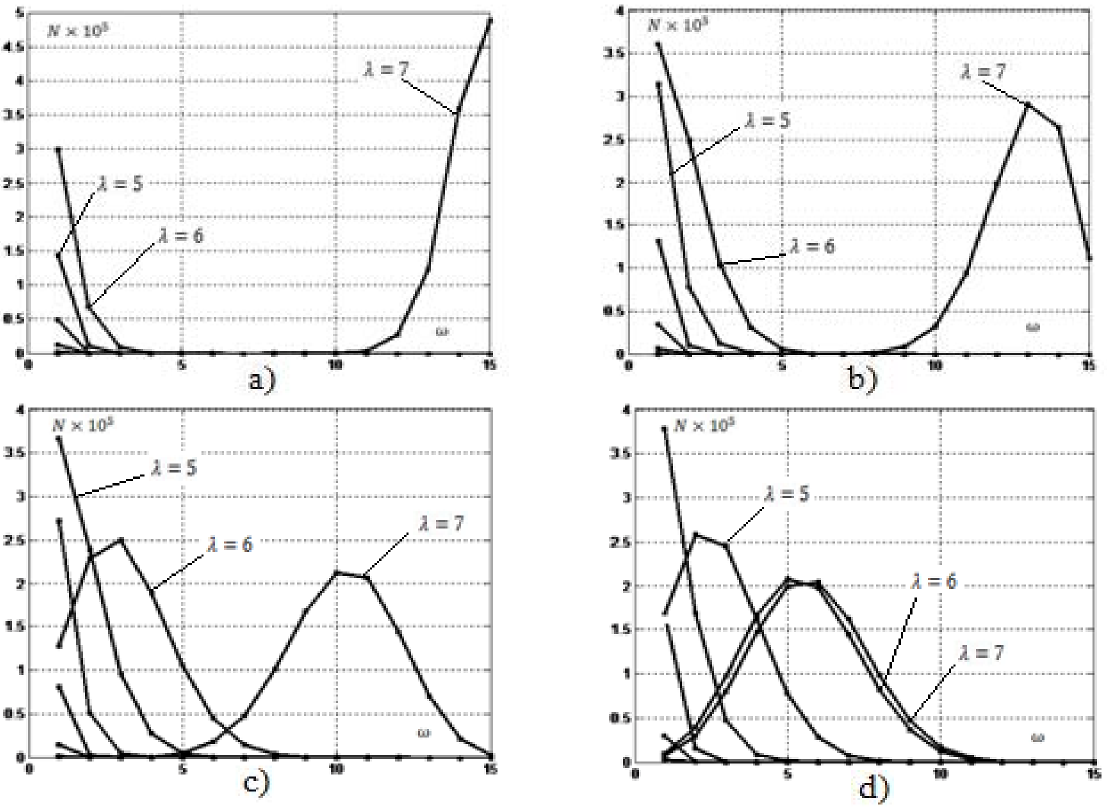
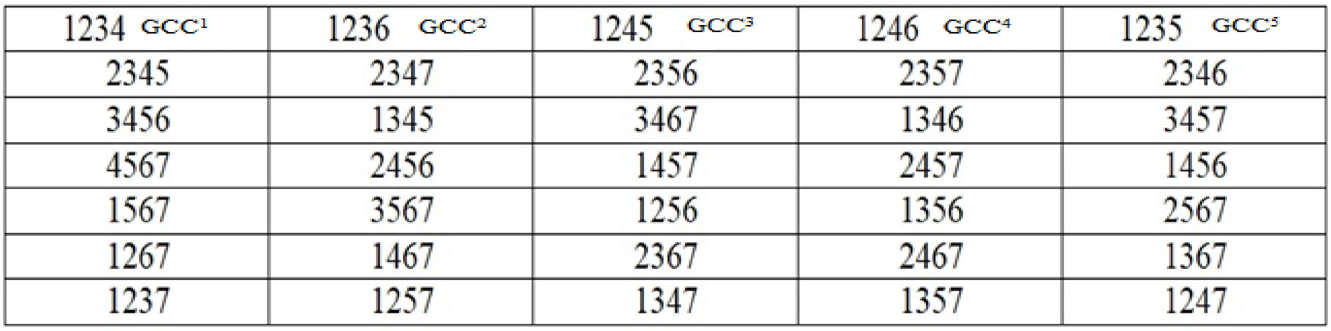


Fig. 3. Occurrence frequency of the soft solutions index in n = 15 code vector of length, where a) $\rho = 0.6$; b) $\rho = 0.7$; c) $\rho = 0.8$; d) $\rho = 0.9$

The fundamentally erasing communication channel can be replaced by a polar coding system and the utilization of the fuzzy set apparatus, but the evaluation of such a solution requires additional research.

Cyclic Properties of Permutations and their Orbits

When organizing the permutation decoding procedure, the decoder according to a certain criterion, must select *k* reliable characters from *n* accepted, and in general, we can create similar C_k^n combinations. It is important to note that in the created number of combinations, you can notice certain patterns that are cyclical in nature. In combinatorial calculus, such structures are called orbits. For each orbit, one can indicate the smallest number that underlies the combination cyclic shift of *k* non-recurrent elements (numbers). Let us call this number the generative combination of the cycle. Adding a number to the generative combination of the cycle, you can indicate the number of the orbits in the general system of permutations, that in the future are advisable to associate with a specific generative matrix of the equivalent code (EC), which is the basis of the permutation decoding system. Since permutations represent a group, it seems convenient to associate this group with group codes that are formed over binary Galois fields or their extensions. Consequently, being developed material of the permutation decoding system is applicable for both binary codes and non-binary redundant codes. Suppose the binary group gives Hamming code (7, 4, 3). Let us number the code combination elements of the code from 1 to $n = 7$ and call these similar numbers by the position numerators. In this case, for the code under consideration, it is permissible to form 35 permutations, which can be conveniently divided into orbits with their generative combinations of the cycles (GCC), as it is shown in Figure 4.



1234 GCC^{1}	1236 GCC^{2}	1245 GCC^{3}	1246 GCC^{4}	1235 GCC^{5}
2345	2347	2356	2357	2346
3456	1345	3467	1346	3457
4567	2456	1457	2457	1456
1567	3567	1256	1356	2567
1267	1467	2367	2467	1367
1237	1257	1347	1357	1247

Fig. 4. The permutations orbits for (7, 4, 3) code

It is evident that the right-hand movement in the cycle that we will call direct is used in Figure 4. In case the left movement in the cycle is used, we will call it reverse. The weight of any permutation equals to the sum of the numbers it includes. At that point the fact, that several properties of an arbitrary generative combination of the cycle are crucial in terms of minimizing the memory size of the decoder cognitive map, become obvious.

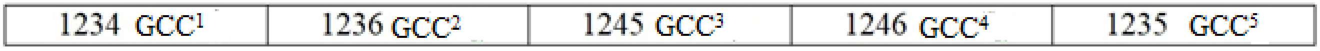
Property 1. Any generative combination of the cycle (GCC) has a low weight value (the sum of numbers permutation) as regard to the weights of all other elements of the orbit that it forms. This property is explained by the fact that it is the generative combination of the cycle (GCC) numerators that occupy the left positions in the series of the cycle numbers from 1 to *k*, and the forward movement along the orbit at least one step up to *n* value only increases the permutation weight.

Property 2. In the event of a complete cycle, the total permutations number of any orbit starting with number 1 always equals to k value. This is easily proved by the full-cycle orbits elements combination.

Property 3. The rule of the permutation weight minimizing by sign 1 in the left category permits to implement an accelerated search of the generative combination of cycle (GCC) and therefore to give the exact orbit number. Let us assume from Table 1 that the decoder in the decoder cognitive map only knows the top line contents, and let an arbitrary permutation be given in lexicographic format (LF). Applying the reverse cycle rule and minimizing the permutation, it is always possible to find the permutation with the minimum weight.

Example 3.1. Let us assume that permutation of form7641 for code (7, 4, 3) is obtained. Its lexicographic format (LF) has the value of 1467, and since the combination is headed by number 1, due to the reverse cycle. Then we go to permutation 4678 to minimize it, resulting in the form 4678 – 3333 = 1345. The weight of original permutation (the sum of all numbers) is 18. The weight of the resulting permutation is 13. Remember: 18 > 13. The transformation cycle continues. Permutation 1345 transforms into 3458 due to the reverse cycle. Next, 3458 – 2222 = 1236, permutation weight of is 12. Remember: 13 > 12, the sense of inequality does not change. Further, we calculate: 2368 – 1111 = 1247. Permutation weight is 14. Remember: 12 < 14 and state that the inequality sense has changed. Therefore, according to property 1, the generative combination of the cycle (GCC) for the obtained permutation equals to generative combination of the cycle GCC ^{2} = 1236.

Application of the properties mentioned above, enables us to reduce the capacity of decoder cognitive map by n-times and the table in Figure 4 gets the pattern shown in Figure 5.



1234 GCC^1	1236 GCC^2	1245 GCC^3	1246 GCC^4	1235 GCC^5

Fig. 5. Abbreviated version of the decoder cognitive card for code (7, 4, 3)

Joining the concrete generative combination of the cycle with the corresponding generative matrix and converting it by circular shifts it is easy to get the generative matrix of the equivalent code for arbitrary permutation.

CONCLUSION

The article deals with the issues of biometrical technologies application for passengers' personal identification. The existing types of biometrical systems were analyzed and their disadvantages were revealed. It is proved that the major problem for the biometrical systems with centralized base of biometrical data is the issue of confidentiality regarding compromise of biometric patterns. That can potentially cause loss of biometric characteristics confidentiality and failure to use it for personal identification in future. The paper considers the possibility of application of the biometric cryptography systems, in particular "fuzzy extractors" for passenger authentication.

Further prospects for usage of the upgraded permutation decoding method in biometric systems are presented. Permutation decoding is the variety of soft-decision decoding for block noise-resistant codes. It has the apparent advantages of the equivalent code with reference to the hard methods of data decoding. Permutation decoding is based on the receiver computation for each accepted combination and transmitted via noisy channel of the equivalent code vector. The complexity of the computational process for the classical algorithms implementation is unacceptably high. From the practical point of view, the situation is changing dramatically for the better with the introduction of cognitive methods for data processing, when a complex computational process is replaced by the amount of decoder cognitive map memory. The article studies the possibilities of techniques for subsequent reduction of the decoder cognitive map memory.

REFERENCES

1. **Bolle, R.M., Connell, J.H., Pankanti, Sh., Ratha, N.K. and Senior, A.W.** (2004). *Guide to Biometrics.* Springer-Verlag, New York, 364 p. DOI: 10.1007/978-1-4757-4036-3

2. **Sinha, P., Balas, B., Ostrovsky, Y. and Russell, R.** (2006). *Face recognition by humans: nineteen results all computer vision researchers should know about.* Proceedings of the IEEE, vol. 94, no. 11, pp. 1948–1962. DOI: 10.1109/JPROC.2006.884093

3. **Jain, A.K., Duin, P.W. and Mao, J.** (2000). *Statistical pattern recognition: a review.* IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 1, pp. 4–37. DOI: 10.1109/34.824819

4. **Kryukov, D.A.** (2012). *Action models of personal identification systems with antinoise coding procedures.* Scientific edition of Bauman MSTU Science & Education, no. 10. DOI: 10.7463/1012.0486630 (accessed 23.01.2021).

5. **Juels, A. and Wattenberg, M.** (1999). *A fuzzy commitment scheme*. Proceedings of the 6th ACM conference on Computer and communications security, pp. 28–36. DOI: 10.1145/319709.319714

6. **Dodis, Y., Reyzin, L. and Smith, A.** (2004). *Fuzzy extractors: how to generate strong keys from biometrics and other noisy data*. Advances in Cryptology – EUROCRYPT 2004: Lecture Notes in Computer Science. In Cachin C., Camenisch J.L. (eds.)., vol. 3027, pp. 523–540. DOI: 10.1007/978-3-540-24676-3_31 (accessed 28.01.2021).

7. **Hao, F., Anderson, R. and Daugman, J.** (2006). *Combining crypto with biometrics effectively*. IEEE Transactions on Computers, vol. 9, no. 55, pp. 1081–1088. DOI: 10.1109/TC.2006.138

8. **Al-Saggaf, A.A.** (2018). *Secure method for combining cryptography with iris biometrics*. Journal of Universal Computer Science, vol. 24, no. 4, pp. 341–356.

9. **Peng, L., Xin, Y., Hua, Q., Kai, C., Eryun, L. and Jie, T.** (2012). *An effective biometric cryptosystem combining fingerprints with error correction codes*. Expert Systems with Applications, vol. 39, pp. 6562–6574. DOI: 10.1016/j.eswa.2011.12.048 (accessed 23.01.2021).

10. **Akhmetov, B.B., Ivanov, A.I., Funtikov, V.A., Bezyaev, A.V. and Malygina, E.A.** (2014). *Tekhnologiya ispolzovaniya bolshikh neyronnykh setey dlya preobrazovaniya nechetkikh biometricheskikh dannykh v kod klyucha dostupa: Monografiya* [Technology of using large neural networks for converting fuzzy biometric data into access key code: Monograph]. Almaty: TOO "Izdatelstvo LEM", 144 p. (in Russian)

11. **Gladkikh, A.A., Volkov, An.K., Volkov, Al.K. and Ibragimov, R.Z.** (2019). *Noiseless coding algorithm based on cognitive processing of biometric data in system of digital identification of passengers*. Journal of Physics: Conference Series (ITBI 2019), vol. 1333, issue 3, pp. 1–5. DOI: 10.1088/1742-6596/1333/3/032022

12. **Gladkikh, A.A., Volkov, Al.K., Volkov, An.K., Il'in, V.M. and Kozlov, D.A.** (2019). *Cognitive decoding of redundant block codes in the system of processing and protection of biometric data of air passengers*. IOP Conference Series: Materials Science and Engineering (MIST: Aerospace-2019), vol. 734, pp. 1–6. DOI: 10.1088/1757-899X/734/1/012163

INFORMATION ABOUT THE AUTHORS

Anatoliy A. Gladkikh, Doctor of Technical Sciences, Professor, Ulyanovsk Institute of Civil Aviation Named after Air Chief Marshal B.P.Bugaev, a_gladkikh@mail.ru.

Alexander K. Volkov, Candidate of Technical Sciences, Associate Professor, Ulyanovsk Institute of Civil Aviation Named after Air Chief Marshal B.P.Bugaev, volkovalex8@rambler.ru.

Tatiana G. Ulasyuk, Post-graduate Student, Senior Lecturer, Ulyanovsk Institute of Civil Aviation Named after Air Chief Marshal B.P.Bugaev, tgu-7@yandex.ru.

РАЗВИТИЕ БИОМЕТРИЧЕСКИХ СИСТЕМ ИДЕНТИФИКАЦИИ ПАССАЖИРОВ НА ОСНОВЕ СРЕДСТВ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

А.А. Гладких[1], Ал.К. Волков[1], Т.Г. Уласюк[1]
*[1] Ульяновский институт гражданской авиации
имени Главного маршала авиации Б.П. Бугаева,
г. Ульяновск, Россия*

В работе рассматриваются вопросы применения биометрических технологий для идентификации личности пассажиров. Целью работы является проведение анализа возможностей повышения надежности функционирования различных биометрических устройств идентификации путем использования кодов коррекции ошибок. Представлены основные элементы и принцип функционирования классической биометрической системы. На основании рекомендаций Международной организации гражданской авиации (ИКАО) представлены особенности процедуры распознавания пассажиров по изображениям лица. Рассмотрены варианты реализации биометрических процедур аутентификации пассажиров, и сделан вывод, что при централизованных баз биометрических данных существуют проблемы конфиденциальности и защиты информации. Проблемы характеризуются возможностью компрометации биометрических образов, что потенциально может привести к утрате их конфиденциальности и невозможности дальнейшего использования для идентификации личности. Более надежной представляется организация процедуры аутентификации пассажиров с одновременным применением биометрических параметров и бесконтактных SMART-карт. SMART-карты используются для распределенного хранения биометрических и других дополнительных данных, тем самым нивелируя недостатки доступа к централизованным базам данных. Показано, что следующим шагом в развитии данной области является применение биометрической криптографии, предполагающей «связывание» ключей шифрования и паролей с биометрическими параметрами субъекта. Рассмотрен принцип работы «нечеткого экстрактора» как одного из вариантов преобразователя «биометрия-код». Показана целесообразность и необходимость совершенствования в рассматриваемых системах средств помехоустойчивого кодирования. Предлагается использование алгоритмов перестановочного декодирования данных, способных адекватно соответствовать именно задачам биометрической идентификации. На основе результатов статистического моделирования оптических каналов связи определяются необходимые и достаточные условия применения средств перестановочного декодирования для двоичных кодов, решается задача минимизации объема памяти когнитивной карты перестановочного декодера за счет выделения орбит перестановок и использования образующих комбинаций циклов в качестве указателей эталонных матриц. Предлагается результативный алгоритм поиска уникального номера орбиты и соответствующей ему эталонной матрицы при формировании приемником произвольной перестановки символов из множества допустимых перестановок.

Ключевые слова: пассажир, биометрия, аутентификация, нечеткий экстрактор, перестановочное декодирование, цикл, орбита.

СПИСОК ЛИТЕРАТУРЫ

1. **Болл Р.М.** Руководство по биометрии / Р.М. Болл, Д.Х. Коннел, Ш. Панканти, Н.К. Ратха, Э.У. Сеньор. М.: Техносфера, 2007. 368 с.

2. **Sinha P.** Face recognition by humans: nineteen results all computer vision researchers should know about / P. Sinha, B. Balas, Y. Ostrovsky, R. Russell // Proceedings of the IEEE. 2006. Vol. 94, no. 11. Pp. 1948–1962. DOI: 10.1109/JPROC.2006.884093

3. **Jain A.K., Duin P.W., Mao J.** Statistical pattern recognition: a review // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2000. Vol. 22, no 1. Pp. 4–37. DOI: 10.1109/34.824819

4. **Крюков Д.А.** Модели функционирования персональных систем идентификации с процедурами помехоустойчивого кодирования и декодирования хранимых данных [Электронный ресурс] // Электронное научно-техническое издание «Наука и образование: научное издание МГТУ им. Н.Э. Баумана». 2012. № 10. DOI: 10.7463/1012.0486630 (дата обращения: 23.01.2021).

5. **Juels A., Wattenberg M.** A fuzzy commitment scheme // Proceedings of the 6th ACM conference on Computer and communications security, 1999. Pp. 28–36. DOI: 10.1145/319709.319714

6. **Dodis Y., Reyzin L., Smith A.** Fuzzy extractors: how to generate strong keys from biometrics and other noisy data [Электронный ресурс] // Advances in Cryptology – EUROCRYPT 2004: Lecture Notes in Computer Science / Под ред. C. Cachin, J.L. Camenisch. 2004. Vol. 3027. Pp. 523–540. DOI: 10.1007/978-3-540-24676-3_31 (дата обращения: 28.01.2021).

7. **Hao F., Anderson R., Daugman J.** Combining crypto with biometrics effectively // IEEE Transactions on Computers. 2006. Vol. 55, no. 9. Pp. 1081–1088. DOI: 10.1109/TC.2006.138

8. **Al-Saggaf A.A.** Secure method for combining cryptography with iris biometrics // Journal of Universal Computer Science. 2018. Vol. 24, no. 4. Pp. 341–356.

9. **Peng L.** (2012). An effective biometric cryptosystem combining fingerprints with error correction codes / Y. Xin, Q. Hua, C. Kai, L. Eryun, T. Jie [Электронный ресурс] // Expert Systems with Applications. 2012. Vol. 39. Pp. 6562–6574. DOI: 10.1016/j.eswa.2011.12.048 (дата обращения: 23.01.2021).

10. **Ахметов Б.Б.** Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа: монография / Б.Б. Ахметов, А.И. Иванов, В.А. Фунтиков, А.В. Безяев, Е.А. Малыгина. Алматы: ТОО «Издательство LEM», 2014. 144 с.

11. **Gladkikh A.A.** Noiseless coding algorithm based on cognitive processing of biometric data in system of digital identification of passengers / A.A. Gladkikh, An.K. Volkov, Al.K. Volkov, R.Z. Ibragimov // Journal of Physics: Conference Series (ITBI 2019). 2019. Vol. 1333, iss. 3. Pp. 1–5. DOI: 10.1088/1742-6596/1333/3/032022

12. **Gladkikh A.A.** Cognitive decoding of redundant block codes in the system of processing and protection of biometric data of air passengers / A.A. Gladkikh, Al.K. Volkov, An.K. Volkov, V.M. Il'in, D.A. Kozlov // IOP Conference Series: Materials Science and Engineering (MIST: Aerospace – 2019), 2019. Vol. 734. Pp. 1–6. DOI: 10.1088/1757-899X/734/1/012163

СВЕДЕНИЯ ОБ АВТОРАХ

Гладких Анатолий Афанасьевич, доктор технических наук, профессор, профессор Ульяновского института гражданской авиации имени Главного маршала авиации Б.П. Бугаева, a_gladkikh@mail.ru.

Волков Александр Константинович, кандидат технических наук, доцент Ульяновского института гражданской авиации имени Главного маршала авиации Б.П. Бугаева, volkovalex8@rambler.ru.

Уласюк Татьяна Георгиевна, аспирант, старший преподаватель Ульяновского института гражданской авиации имени Главного маршала авиации Б.П. Бугаева, oabuvauga@mail.ru.

Поступила в редакцию 18.01.2021 Received 18.01.2021
Принята в печать 25.03.2021 Accepted for publication 25.03.2021