Noiseless coding algorithm based on cognitive processing of biometric data in system of digital identification of passengers

A A Gladkikh¹, Alexander K Volkov², Andrei K Volkov² and R Z Ibragimov³

¹Ulyanovsk State Technical University, 32, Severnyj venec, Ulyanovsk, 432027, Russia
²Ulyanovsk Civil Aviation Institute, 8/8, Mozhaisky Street, Ulyanovsk, 432071, Russia
³Siberian State University of Telecommunications and Informatics, 86, Kirov Street, Novosibirsk, 630102, Russia

E-mail: volkovalex8@rambler.ru

Abstract. The new approach to increasing the reliability and validity of the transmission of biometric information in the digital passenger identification system based on the use of noiseless coding algorithms with elements of cognitive data processing is presented in the article. Reed-Solomon non-binary codes as best suited for protecting digitized images are given to use in the proposed permutation decoding method data protection against errors. When integrating the cognitive map into the model of the permutation decoder, it is possible to implement the learning function. The training consists in that the decoder records the results of the transformations of the generating matrices of equivalent codes into the memory of a cognitive map using a ready solution under the conditions of permutations repetition. Thereby, a reduction in the volume of arithmetic calculations is achieved with use of only fast matrix transformations. The proposed method has a number of properties allowing one to reduce the memory cognitive maps volume. The simulation results have shown that the implementation of the proposed method makes it possible to gain speeding up the calculations by reducing the number of operations.

1. Introduction

Improving network technologies and programme-technical tools for image processing has allowed, at the present stage of their development, actively introducing into the practice of aviation security a method of authenticating a person accordingly to his or her biometric characteristics. Biometric systems of identification consist of a biometric scanner (a physical device allowing us to measure one or another biometric characteristic) and an algorithm for comparing the measured characteristic with a pre-registered (biometric template). The most prevalent technology called "Smart Pat", proposed by SITA, fixes the geometric characteristics of the subject at the entrance to the airport with help of special equipment. After realization of the passenger identification procedure a digital travel document is created. The implementation of the concept of passenger digital identification will make it possible for airports to significantly increase the capacity of the passenger traffic control system and optimize the number of aviation security officials and workers. But at the same time the key problem of the implemented concept is the constant variability of the biometric characteristics of passengers, which can lead to errors in identification, independent of the unintended actions of the owners or deliberate ones made by the potential criminal. An obvious disadvantage of the scanning method of passenger traffic subjects consist in a large database, which due to economic reasons cannot be placed in data storages of
particular numerous aviation enterprise and for this reason it is located in the system of central servers. In this case, the scanned data having digital form are transmitted at high speed from the particular airports to the system of such servers, where comparison of the received information with the server data is realized and then the result of the check is formed. The result of the test is given to the control point. The probability of database tuple distortion in the described system should be sufficiently low. This can only be provided by means of noiseless coding. The requirements for high processing speed in such systems do not allow using long redundant codes [1]. Some results of using noiseless coding algorithms in biometric identification systems are presented in works [2-5]. At the same time, in previous studies there were no scientifically based approaches to the organization of noiseless coding in data exchange systems with using cognitive principles. These provisions do allow us to justify the relevance of the selected topic.

2. Materials and methods

The proposed concept of cognitive biometric data processing in a permutation decoding system (PD) consists in the fact that some of the reliable symbols of the length code word $n$ are relocated to the place $k$ of information digits, where $n < k$ and these bits are encoded with an equivalent code [6]. This procedure is carried out in the receiver. Since the data of such code are not transmitted through telecommunication systems with a high level of interference, the probability of erroneous decoding of the equivalent code turns out to be at the level of internal failures of the receiver’s computing system. The main obstacle in the way of the implementation of this method is concluded in the complicated procedure of obtaining the generating matrices of equivalent codes, which should be achieved for each unique symbol permutation, each code vector [6]. The number of permutations for a length code $n$ is estimated as $n!$.

In the proposed method PD of data protection against errors, it can be proposed to use Reed-Solomon non-binary codes (RS) as best suited ones for protecting digitized images. The essence of the cognitive approach is simple: if the decoder has calculated at least once a certain generating matrix of the equivalent code, then it is recorded into the cognitive map (QM) of the decoder, and by repeating such permutation, the finished result is extracted from the map. This method allows avoiding complex repetitive calculations and we can solve the problem of maintaining high speed data processing by the server. Using the PC code $(7,3,5)$ as an example, it can be illustrated that the proposed method has a number of properties allowing one to reduce the QM memory size, which is very important for codes having a big length, for example, for Galois fields of the eighth expansion degree.

3. The results of integrating a cognitive map into a permutation decoder

Let us use the non-binary RS code with parameters $(7,3,5)$ in the data exchange system. The generating matrix $G$ of this code has a systematic form and the columns of the matrix are numbered in the usual way from left to right:

$$G = \begin{bmatrix}
\alpha^0 & 0 & 0 & \alpha^4 & \alpha^0 & \alpha^4 & \alpha^5 \\
0 & \alpha^0 & 0 & \alpha^2 & \alpha^0 & \alpha^6 & \alpha^6 \\
0 & 0 & \alpha^0 & \alpha^3 & \alpha^1 & \alpha^3
\end{bmatrix} \tag{1},$$

here and throughout $\alpha$ – a primitive field element $GF(2^3)$.

Let the reliable symbols in some adopted code vector of the RS code be the symbols having numbers $(2 4 5)$, and less reliable symbols in the decreasing order of likelihood ratio values are placed in following sequence $(6 7 1 3)$. Then from expression (1), it follows that:

$$G_{per} = \begin{bmatrix}
0 & \alpha^4 & \alpha^0 & \alpha^4 & \alpha^5 & \alpha^0 & 0 \\
\alpha^0 & \alpha^2 & \alpha^0 & \alpha^6 & \alpha^6 & 0 & 0 \\
0 & \alpha^3 & \alpha^0 & \alpha^1 & \alpha^3 & 0 & \alpha^0
\end{bmatrix}. \tag{2}$$
The task consists in transforming the matrix (2) into a systematic form. Basically for this, classical methods of matrix computations known as linear transformations can be used. Let us denote a similar procedure through the expression of the form $G_{\text{per}} \Rightarrow G_{\text{sys}}^{\text{per}}$. Then:

$$G_{\text{per}} \Rightarrow G_{\text{sys}}^{\text{per}} = \begin{bmatrix} a^0 & 0 & 0 & a^6 & a^2 & a^6 & a^2 \\ 0 & a^0 & 0 & a^3 & a^3 & a^1 & a^1 \\ 0 & 0 & a^0 & a^5 & a^4 & a^1 & a^5 \end{bmatrix}. \quad (3)$$

The combination of reliable symbols of a code combination of the form (2 4 5) can be repeated with a high probability during operating data processing. It is advisable to keep the obtained result in memory and use it with possible permutations having numbers (2 4 5) in order to save the decoder's computational resource in the future. The matrix presented in Figure 1 with a strictly increasing sequence of line numbers is called canonical one, and the matrix itself is a reference matrix:

$$\begin{bmatrix} a^6 & a^2 & a^6 & a^2 & 2 \\ a^3 & a^3 & a^1 & a^1 & 4 \\ a^5 & a^4 & a^4 & a^5 & 5 \end{bmatrix}$$

Figure 1. The structure of the reference matrix having a canonical form accordingly to the system of reliable symbols.

Following the principles of cognitive data processing, the decoder that has received, for example, a tuple of likelihood ratio values in the form (5 2 4) for the first $k$ reliable symbols of the adopted combination and the remaining $(n - k)$ less reliable symbols in the form (3 7 1 6) can form a matrix $G_{\text{per}}$ taking into account the structure of the reference matrix, as it is shown below:

$$G_{\text{per}} \Rightarrow G_{\text{sys}}^{\text{per}} = \begin{bmatrix} a^0 & 0 & 0 & a^5 & a^4 & a^4 & a^6 & a^6 \\ 0 & a^0 & 0 & a^2 & a^2 & a^6 & a^6 \\ 0 & 0 & a^0 & a^1 & a^3 & a^1 & a^3 \end{bmatrix}. \quad (4)$$

It has been found in the course of the research that by storing the position numbers in the permutations of $k$ reliable and $(n - k)$ unreliable characters, we should rearrange the rows of the matrix (4), in the first step, and the columns of this new matrix – in the second one.

Permutation decoding of such codes leads to decreasing in the computational complexity of the decoder due to the formation of constant structures in the computational process of decoding that are common to the entire functional cycle of the device. The use of cognitive procedures gives an additional benefit in the procedure for minimizing computational complexity. The carried out studies have found that the cyclical property of code combinations allows reducing the requirements for the decoder's memory volume in $n$ times. For example, for the RS (7,3,5) code, instead of 35 reference matrices, only 5 are to be used. Let the sorting of reliable symbols lead to a sequence (6 2 7) and some sequence of unreliable ones of the form (3 5 1 4). The canonical form of the first sequence gives (2 6 7). It becomes clear that the reference matrix should be processed with row numbers (6 7 2) and column numbers (1 3 4 5) on purpose with their subsequent permutation:

$$G_{672}^{\text{sys}} = \begin{bmatrix} \alpha^1 & \alpha^3 & \alpha^1 & \alpha^0 & 6 \\ \alpha^3 & \alpha^1 & \alpha^1 & \alpha^0 & 6 \\ \alpha^1 & \alpha^3 & \alpha^1 & \alpha^0 & 6 \\ 0 & a^0 & 0 & a^2 & a^2 & a^6 & a^6 \\ 0 & 0 & a^0 & a^1 & a^3 & a^1 & a^3 \end{bmatrix} \Rightarrow \begin{bmatrix} \alpha^6 & \alpha^2 & \alpha^2 & \alpha^0 & 7 \\ a^4 & a^4 & a^5 & a^0 & 2 \\ a^4 & a^4 & a^5 & a^0 & 2 \\ a^4 & a^4 & a^5 & a^0 & 2 \\ 1 & 3 & 4 & 5 \end{bmatrix} \Rightarrow \begin{bmatrix} \alpha^6 & \alpha^2 & \alpha^2 & \alpha^0 & 7 \\ a^2 & a^2 & a^0 & 7 \\ a^2 & a^2 & a^0 & 7 \\ a^2 & a^2 & a^0 & 7 \\ 3 & 5 & 5 & 1 \end{bmatrix}.$$
Table 1. The number of arithmetic operations in the procedure of classical calculation of the matrix of equivalent code

| Codes            | The classic approach | The number of operations by using the method proposed |
|------------------|----------------------|------------------------------------------------------|
|                  | $PC(7,3,5)$          | $PC(15,5,11)$                                       | $PC(15,9,7)$                                           | $PC(15,13,3)$                                          |
|                  | 336                  | 2410                                                | 2912994                                               | 68584334026                                           |
|                  | $6720*10^{-9}$ s     | $48200*10^{-9}$ s                                  | $58259880*10^{-9}$ s                                 | $1371686680520*10^{-9}$ s                             |
|                  | (3+4)                | (5+10)                                              | (9+6)                                                 | (13+2)                                                |
|                  | 7                    | 15                                                  | 15                                                    | 15                                                    |
|                  | $140*10^{-9}$ s      | $300*10^{-9}$ s                                    | $300*10^{-9}$ s                                       | $300*10^{-9}$ s                                       |
|                  | 48-time benefit      | 1.6*10^2-time benefit                              | 1.9*10^6-time benefit                                 | 4.6*10^9-time benefit                                 |

Implementation of the principles of cognitive data processing in a non-binary code decoder makes it possible to reduce the complexity of the implementation of the decoding procedure by using a system of fast matrix transformations (FMT) that do not require arithmetic operations.

According to Table 1, when the proposed method is used, a significant benefit in accelerating the calculations is achieved with eliminating arithmetic operations in the search procedure for the equivalent code in the classical scenario and replacing it when the decoder operates with a trivial sorting of the lines and columns of the reference matrix, extracted from the QM memory, according to the permutations of reliable and unreliable code vector symbols.

Table 2 shows the possibility of storing the data of the reference matrices of the cognitive map in the RAM of typical programmable logic integrated schemes (PLIS). This can allow us to maintain high rates of data processing by the receiver, since there is no need for spending time to access the external memory of the receiver process.

Table 2. The possibility of implementing a cognitive decoder map relative to the internal memory of the "Altera" PLIS

| Codes            | System of full set of matrices | System (FMT) System of reference matrices | System based on the cyclical properties of reference matrices |
|------------------|--------------------------------|------------------------------------------|-------------------------------------------------------------|
| $PC(7,3,5)$      | $V_{kk} << 1% (9*10^{-4})$    | $V_{kk} << 1% (1.5*10^{-4})$             | $V_{kk} << 1% (2.1*10^{-5})$                                |
|                  | Mbite                         | Mbite                                    | Mbite                                                       |
| $PC(15,11,5)$    | 5715950 %                     | 1.5 %                                    | 0.1 %                                                       |
| $PC(15,7,9)$     | 43300 %                       | 8.6 %                                    | 0.5 %                                                       |
4. Conclusion
The improvement of the reliability of functioning digital passenger identification systems can only be achieved by means of noiseless coding. The scientific novelty of this research lies in the fact that an important contribution to the expansion of ideas about the applicability of cognitive principles in the system of exchanging biometric data at the level of processing of error-correcting codes has been made. Along with the scientific and theoretical value of the work, the scientific and applied nature is associated with the development of a permutation decoding algorithm for the redundant code on the basis of cognitive biometric data processing. In the proposed method of permutation decoding for data protection against errors, it has been suggested to use RS non-binary codes as the most suitable for protecting digitized images of passengers' faces. On help with integrating the cognitive map into the permutation decoder model, it is possible to apply the learning function. The learning consists in that the decoder records the results of the transformations of the generating matrices of equivalent codes into the memory of a cognitive map using ready solution under the conditions of permutations repetition. The proposed method has a number of properties that allow reducing the memory volume of cognitive maps.

References
[1] Gladkikh A A, Mishin D V and Chilikhin N Y 2018 Improving efficiency of fiber optic communication systems with the use of lexicographic decoding of polar codes Proceedings of SPIE. Optical Technologies for Telecommunications (Bellingham: SPIE) Volume 10744. pp 1-15.
[2] Hao F, Anderson R and Daugman J 2006 IEEE Trans. Comput. 55(9) 1081–88
[3] Alawi A Al-Saggaf 2018 J.UCS 24(4) 341–356
[4] Peng L, Xin Y, Hua Q, Kai C, Eryun L and Jie T 2012 Expert Syst. Appl. 39 6562–74
[5] Haitham W, Abdel-Moneim W and Aliaa A A Y 2013 ESJ 9(30) 242–256
[6] Carrasco R A and Johnston M 2009 Non-binary error control coding for wireless communication and data storage (Chichester: John Wiley & Sons, Ltd) p 322