

УДК 621.398

COMPARISON OF METHODS OF BIOMETRIC AUTHENTICATION ON THE TOTAL OF QUALITY INDICATORS

DOI 10.36994/2788-5518-2021-01-01-05⁵

Valeriy Bezruk, Dr. habil., Prof. Kharkiv National University of Radio Electronics, Ukraine. valerii.bezruk@nure.ua

Yuliia Skoryk, Ph.D., Kharkiv National University of Radio Electronics, Ukraine. yuliia.skoryk@nure.ua

Veronica Kobtseva, Kharkiv National University of Radio Electronics, Ukraine. veronika.kobtseva@nure.ua

Abstract. Biometric authentication methods used to protect information in computer networks are considered. A comparative analysis of the main methods is carried out taking into account the totality of quality indicators using the hierarchy analysis method.

Keywords: Biometric authentication methods, quality indicators, multicriteria analysis.

ПОРІВНЯННЯ МЕТОДІВ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ЗА СУКУПНІСТЮ ПОКАЗНИКІВ ЯКОСТІ

Безрук В.М., д.т.н., проф., Харківський національний університет радіоелектроніки, Україна. valerii.bezruk@nure.ua

Скорик Ю.В., к.т.н., Харківський національний університет радіоелектроніки, Україна. yuliia.skoryk@nure.ua

Кобцева В.М. Харківський національний університет радіоелектроніки, Україна. veronika.kobtseva@nure.ua

Анотація. У статті розглядається багатокритеріальний підхід до порівняльного аналізу різних біометричних методів аутентифікації в порівнянні з іншими методами ідентифікації. Для якісного аналізу біометричної системи контролю доступу необхідно використовувати сукупність показників якості і відповідні методи багатокритеріальної оптимізації. Тому існує необхідність порівняльного аналізу біометричних методів аутентифікації з урахуванням сукупності показників якості. У роботі проводиться порівняльний аналіз деяких біометричних систем контролю і управління доступом за сукупністю показників якості, зокрема, коефіцієнт помилкового пропуску (FAR), тобто відсоток виникнення ситуацій, коли система дозволяє доступ користувачу, незареєстрованому в системі, і коефіцієнт помилкового відмови (FRR), тобто відсоток відмови в доступі справжньому користувачеві системи. Обидва параметри розраховуються методами математичної статистики. Чим менше значення цих показників, тим вище якість аутентифікації користувачів. У статті методом аналізу ієрархій проводиться багатокритеріальне порівняння і вибір переважного варіанту для найпопулярніших на сьогоднішній день методів біометричної ідентифікації на основі аналізу відбитка пальця, розпізнавання особи

⁵ Valeriy Bezruk, Yuliia Skoryk, Veronica Kobtseva
Infocommunication and computer technologies, № 1 (01), 2021

2D, радужної оболонки ока, сітківки ока, малюнка вен, клавіатурного почерку, голосу. Метод аналізу ієрархій полягає в декомпозиції проблеми вибору єдиного проектного варіанту деякої системи на прості складові частини і отриманні суджень експертів по парним порівнянь різних елементів проблеми вибору. Після обробки чисельних даних визначається кращий варіант методу біометричної ідентифікації. Застосування біометрії дозволить вирішувати проблему надійності і може збільшити достовірність аутентифікації і ідентифікації об'єктів при організації доступу до систем з великим числом користувачів, а також до критично важливих систем як частини системи контролю та управління фізичним доступом або як додатковий фактор аутентифікації.

Ключові слова: методи біометричної аутентифікації, показники якості, багатокритеріальний аналіз.

СРАВНЕНИЕ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ПО СОВОКУПНОСТИ ПОКАЗАТЕЛЕЙ КАЧЕСТВА

Безрук В.М., д.т.н., проф. Харьковский национальный университет радиоэлектроники, Украина. valerii.bezruk@nure.ua

Скорик Ю.В., к.т.н. Харьковский национальный университет радиоэлектроники, Украина. yuliia.skoryk@nure.ua

Кобцева В.М. Харьковский национальный университет радиоэлектроники, Харьковский национальный университет радиоэлектроники, Украина. veronika.kobtseva@nure.ua

Аннотация. В статье рассматривается многокритериальный подход к сравнительному анализу разных биометрических методов аутентификации по сравнению с другими методами идентификации. Для качественного анализа биометрической системы контроля доступа необходимо использовать совокупность показателей качества и соответствующие методы многокритериальной оптимизации. Поэтому существует необходимость сравнительного анализа биометрических методов аутентификации с учетом совокупности показателей качества. В работе проводится сравнительный анализ некоторых биометрических систем контроля и управления доступом по совокупности показателей качества, в частности, коэффициент ложного пропуска (FAR), т.е. процент возникновения ситуаций, когда система разрешает доступ пользователю, незарегистрированному в системе и коэффициент ложного отказа (FRR), т.е. процент отказа в доступе настоящему пользователю системы. Оба параметра рассчитываются методами математической статистики. Чем меньше значения этих показателей, тем выше качество аутентификации пользователей. В статье методом анализа иерархий проводится многокритериальное сравнение и выбор предпочтительного варианта для самых популярных на сегодняшний день методов биометрической идентификации на основе анализа отпечаток пальца, распознавания лица 2D, радужной оболочки глаза, сетчатки глаза, рисунка вен, клавиатурного почерка, голоса. Метод анализа иерархий состоит в декомпозиции проблемы выбора единственного проектного варианта некоторой системы на простые составляющие части и получении суждений экспертов по парным сравнениям различных элементов проблемы выбора. После обработки численных данных определяется предпочтительный вариант метода биометрической

аутентификации. Применение биометрии разрешит решать проблему надежности и может увеличить достоверность аутентификации и идентификации объектов при организации доступа к системам с большим числом пользователей, а также к критически важным системам как часть системы контроля и управления физическим доступом или как дополнительный фактор аутентификации.

Ключевые слова: методы биометрической аутентификации, показатели качества, многокритериальный анализ.

Introduction

The rapid development of information technology requires continuous improvement of information security systems. Security in computer networks is a condition for protecting confidential data from various kinds of threats.

There is a wide variety of identification methods. The most common verification and identification technologies are based on the use of passwords and personal identifiers (personal identification number PIN) or documents such as a passport and driver's license. However, such systems are too vulnerable and can easily suffer from forgery, theft and other factors. Therefore, methods of biometric identification, which make it possible to determine a person's identity by its physiological characteristics by recognition by previously stored samples, are of increasing interest [1].

Biometric access systems are very user-friendly and reliable for protecting information. The main advantages of biometric technologies are the following factors:

- rid users of problems associated with the loss of keys and identity cards, as well as the need to remember the identification code and passwords;
- the uniqueness of the biometric characteristics of each person makes it impossible to use them by third parties;
- the process of user communication with a biometric scanner is easy and requires minimal time costs;
- the recognition process, thanks to the intuitiveness of the software and hardware interface, is understandable and accessible to people of any age and does not know language barriers;
- in the case of each appeal to the system, you can prove the authorship of a particular action, for example, save the biometric data of the attacker.
- prevent intruders from entering protected areas and premises by falsifying, stealing documents, cards, passwords;
- restrict access to information and ensure personal responsibility for its safety;
- provide access to responsible facilities only certified specialists;

Therefore, there is a need for a comparative analysis of biometric authentication methods, taking into account the totality of quality indicators [1-5].

Comparative analysis of biometric systems by hierarchy analysis

When comparing systems, the following quality indicators were selected: false acceptance rate (FAR), i.e. the percentage of situations when the system allows

access to a user who is not registered in the system and the false rejection rate (FRR), i.e. The percentage of denied access to the current user of the system. Both parameters are calculated using mathematical statistics methods. The lower the values of these indicators, the higher the quality of user authentication. Other quality indicators of systems are also considered, in particular, the probability that the system is mistaken in determining matches between the input sample and the corresponding template from the database (FNMR - False Non-Match Rate); receiver operational characteristic (ROC) is a visualization of a compromise between the FAR and FRR characteristics; Failure to enroll rate (FTE or FER) - coefficient of unsuccessful attempts to create a template from the input data; Failure To Capture (FTC) - the probability that the automated system is not able to determine biometric input data when it is presented correctly; template capacity - the maximum number of data sets that can be stored in the system; counterfeiting resistance is an empirical characteristic generalizing how easy it is to deceive a biometric identifier; environmental resistance is a characteristic empirically evaluating the stability of a system under various environmental conditions.

In particular, in the work by the method of hierarchy analysis, a multicriteria comparison was made and the preferred option was selected for biometric identification methods based on fingerprint analysis, 2D face recognition, iris of the eye, retina, vein pattern, handwriting, voice. In the table 1 shows the average values of the FAR and FRR indicators for different biometric access control and management systems (ACMS) [1-5].

Table 1.
Quality indicators FAR and FRR for various biometric access systems

№	Type of biometric ACMS based on analysis	FAR, %	FRR, %
N1	fingerprint analysis	0,001	0,6
N2	2D face recognition	0,1	2,5
N3	3D face recognition	0,0005	0,1
N4	iris of the eye	0,00001	0,016
N5	retina	0,0001	0,4
N6	vein pattern	0,0008	0,01
N7	handwriting	0,01	3,0
N8	voice	1	3

For convenience, the initial values of the FAR and FRR quality indicators given in table 2 were converted. In particular, the operation of normalizing quality indicators.

The method of analyzing hierarchies consists in decomposing the problem of choosing the only project version of a certain system into simple components and obtaining expert judgments on pairwise comparisons of various elements of the choice problem [6].

Table 2.

Conversion of initial values of quality indicators FAR and FRR for various biometric access systems

№	Type of biometric ACMS based on analysis	FAR	FRR
N1	fingerprint analysis	0,01	0,016
N2	2D face recognition	0,0001	0,004
N3	3D face recognition	0,02	0,1
N4	iris of the eye	1	0,625
N5	retina	0, 1	0,025
N6	vein pattern	0,0125	1
N7	handwriting	0,001	0,003
N8	voice	0,0001	0,003

As a result of processing the obtained numerical data of expert judgments according to a certain mathematical procedure, the components of the global priority vector are obtained that characterize the priority of the choice of options for the designed system and determine the choice of the only design option of the system from a given set of options. The decomposition principle provides for structuring the problem of choice in the form of a hierarchy of levels, which is the first stage of the application of MAH. The principle of comparative judgments of experts at the MAH is that objects of the problem of choice are compared by experts in pairs in importance. The importance of different systems options (at level 3) and different quality indicators (at level 2) is compared in pairs (Fig. 1).

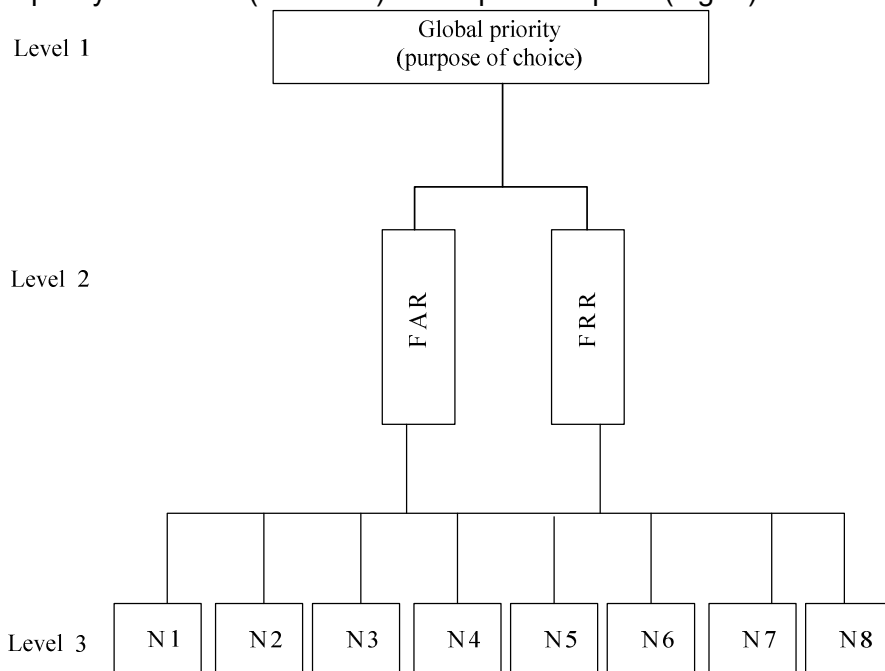


Fig. 1. Decomposition of a selection problem into a hierarchy of biometric identification methods

The results of pairwise comparisons of elements are reduced to matrix form.

Next, some processing of matrices of pairwise comparisons of hierarchy elements at levels 2 and 3 is performed. From a mathematical point of view, these processing tasks are reduced to calculating the main eigenvector, which after a certain normalization becomes the element priority vector at the corresponding hierarchy level [6].

To calculate the vector of global priorities of the compared system options, the processing of matrices of pairwise comparisons of alternatives is performed. The components of the main eigenvector are calculated V_i matrices and priority vectors P_i at each level of the hierarchy according to the relations

$$P_i = \frac{V_i}{S}, \quad V_i = n \sqrt[n]{\prod_{j=1}^n a_{ij}}, \quad S = \sum_{i=1}^n V_i, \quad i = \overline{1, n} \quad (1)$$

where n - number of quality indicators, N - the number variants compared systems.

Similarly, evaluation matrices are of pairwise comparisons variants of systems of 3 level individually with respect to each indicator of quality. On the basis of these matrices the corresponding main components are computed eigenvectors and priority vectors systems $\bar{Q}_j$ with relative to the quality indicators. Using these data, calculated values of the components of the vector of global priorities $\vec{C}$ according to:

Using this data, the values of the components of the global priority vector are calculated $\vec{C}$

$$C_j = \sum_{i=1}^n P_i Q_{ij}, \quad j = \overline{1, N} \quad (2)$$

By the maximum value of the components of the global priority vector (3), the only preferred variant of the system is selected.

Table 3 shows a matrix of paired comparisons of quality indicators at level 2.

Table 4 shows the matrix of paired comparisons of biometric technologies in relation to FAR.

Table 5 shows the matrix of paired comparisons of biometric technologies in relation to FRR.

In the table 6 shows the calculated values of the components of the priority vector of technology options with respect to each quality indicator, as well as the components of the vector of global priorities with P_i (component of the vector of priorities for quality indicators), Q_{1j} (component of the vector of priorities in relation to the quality indicator FAR), Q_{2j} component of the vector of priorities in relation to the quality indicator FRR.

Table 3.
Matrix of paired comparisons of quality indicators

	K_1	K_2	P_i
K_1	1	2	0,667
K_2	1/2	1	0,333

Table 4.
Matrix of paired comparisons of biometric technologies in relation to FAR

	1	2	3	4	5	6	7	8	Q_{1j}
N1	1	7	1/5	1/6	1/4	1/6	6	7	0,066
N2	1/7	1	1/9	1/9	1/8	1/9	1/2	2	0,019
N3	5	9	1	1/4	4	1/4	6	9	0,165
N4	6	9	4	1	5	3	7	9	0,341
N5	4	8	1/4	1/5	1	1/5	6	8	0,104
N6	6	9	4	1/3	5	1	7	9	0,259
N7	1/6	2	1/6	1/7	1/7	1/7	1	6	0,031
N8	1/7	1/2	1/9	1/9	1/9	1/9	1/6	1	0,014

Table 5.
Matrix of paired comparisons of biometric technologies in relation to FRR

K_2	N1	N2	N3	N4	N5	N6	N7	N8	Q_{2j}
N1	1	6	1/7	1/8	1/7	1/8	6	6	0,049
N2	1/6	1	1/8	1/9	1/8	1/9	3	3	0,025
N3	7	8	1	1/8	5	1/8	8	8	0,139
N4	8	9	8	1	5	1/2	9	9	0,296
N5	7	8	1/5	1/5	1	1/5	8	8	0,105
N6	8	9	8	2	5	1	9	9	0,353
N7	1/6	1/3	1/8	1/9	1/9	1/9	1	2	0,017
N8	1/6	1/3	1/8	1/9	1/9	1/9	1/2	1	0,015

Table 6.
The results of the calculation of the components of the global vector of priorities

Type of biometric ACMS based on analysis	Q_{ij}		$\vec{C}$
	FAR	FRR	
fingerprint analysis	0,071	0,075	0,077
2D face recognition	0,025	0,037	0,031
3D face recognition	0,153	0,157	0,165
the iris of the eye	0,35	0,349	0,373
retina	0,108	0,112	0,117

Type of biometric ACMS based on analysis	Q_{ij}		$\vec{C}$
	FAR	FRR	
vein pattern	0,235	0,239	0,252
handwriting	0,044	0,018	0,036
voice	0,012	0,015	0,014
P_i	0,667	0,399	

Based on the maximum value of the global priority vector, the preferred method of biometric authentication is selected.

This is number 4 - the iris of the eye, with indicators of quality FAR 0,00001% and FRR 0,016 %.

Conclusions

A comparative analysis of some biometric access control systems by a set of quality indicators is carried out in the work. Using the hierarchy analysis method, the preferred version of the biometric authentication method was found. This is the iris of the eye method.

The use of biometrics will solve the problem of reliability and can increase the reliability of authentication and object identification when organizing access to systems with a large number of users, as well as to critical systems as part of a physical access control and management system or as an additional authentication factor.

References

- [1] Saaty T.L. The Analytic Hierarchy Process / T.L. Saaty. – New York: McGraw Hill, 1980. – 270 s.
- [2] Lebedenko YU. I. Biometricheskiye sistemy bezopasnosti / YU. I. Lebedenko // . - Tula: Izd-vo TulGU, 2012. - 160 s.
- [3] Sayt Sovremennyye biometricheskiye metody identifikatsii [Elektronnyy resurs] Rezhim dostupa: [www/ URLhttp://masters.donntu.org/2013/fknt/fomenko/library/article4.htm](http://masters.donntu.org/2013/fknt/fomenko/library/article4.htm)
- [4] Matveyev YU.N. Tekhnologii biometricheskoy identifikatsii lichnosti po golosu i drugim modal'nostyam / YU.N. Matveyev. – Vestnik MGTU im. N.E. Bauman. – 2012. – S. 46-61
- [5] Bezruk V., Zelenin A., Vlasova V., Skorik J., Koltun Y. Select preferred of wireless sensor and actuator network / V. Bezruk // Eastern European Journal of Enterprise Technologies, 1/9 (79). – 2016. – P.4-9.
- [6] Bezruk V.M., Skoryk YU.V., Kobtseva V.M. Sravnenye metodov byometrycheskoy autentifikatsyy po sovokupnosti pokazateley kachestva / V.M. Bezruk // Mizhnarodna naukova konferentsiya High-Technologies in infocommunications. – Kharkiv-Kam"yanets'-Podil's'ky, Ukrayina, 2019. – S. 79-80.