
Вибір переважного методу біометричної автентифікації

Юлія Скорик

Інфокомунікацій, Харківський національний університет радіоелектроніки, Харків, Україна
ORCID 0000-0003-1729-1003

Валерій Безрук

Інфокомунікацій, Харківський національний університет радіоелектроніки, Харків, Україна
ORCID 0000-0003-2349-7788

Для цитування цієї статті:

Скорик Юлія, Безрук Валерій. Вибір переважного методу біометричної автентифікації. International Science Journal of Engineering & Agriculture Vol. 2, No. 4, 2023, pp. 28-34. doi:10.46299/j.isjea.20230204.04.

Надійшла до редакції: 21 травня 2023 р.; **Схвалено:** 26 червня 2023 р.;

Опубліковано: 01 серпня 2023 р.

Анотація: У даній статті застосовується багатокритеріальна методика для порівнювального аналізу деяких біометричних методів з автентифікації та інших методів ідентифікації. Щоб якісно провести аналіз біометричних систем контролю доступу потрібно враховувати характеристики систем, а також застосовувати певні методи по багатокритеріальній оптимізації. Отже, необхідно проводити порівняльний аналіз біометричних методів з автентифікації враховуючи сукупність показників якості. В роботі наводиться порівняння певних біометричних систем контролю та керування доступом по сукупності показників якості, а саме, коефіцієнт помилкового пропуску (FAR), мається на увазі певний відсоток при виникненні ситуації, коли система може дозволити доступ користувачеві, незареєстрованому у системі, та коефіцієнт помилкової відмови (FRR), це відсоток відмови у доступі справжньому користувачеві системи. Обидва параметри розраховуються методами математичної статистики. Чим буде менше значення по цим показникам, тим вище буде якість з автентифікації певних користувачів. У статті наводиться порівняння і з застосуванням метода аналізу ієрархії та вибір бажаного варіанта відомих засобів біометричної ідентифікації на основі аналізу відбитку пальця, розпізнавання людини 2D, райдужною оболонкою ока, сітківки ока, малюнок вен, клавіатурного почерка і голоса. В основі метода аналізу ієрархії є декомпозиція завдання по вибіру бажаного проектного варіанта певної системи та поділення цього завдання на більш прості частинки з урахуванням отриманих оцінок від експертів по парним порівнянням простих частин завдання. Після проведення обробки певних даних визначається бажаний переважний метод біометричної ідентифікації. При застосуванні біометрії можна буде вирішувати проблеми з надійністю та можна покращити достовірність автентифікації та ідентифікації певних об'єктів при доступі до системи з великою кількістю користувачів, а також й до дуже важливих та необхідних систем як частини систем контролю та керування фізичним доступом.

Ключові слова: біометричні системи, автентифікація, порівняння, оптимізація.

1. Вступ

Швидкий розвиток інфокомунікаційних технологій вимагає постійного вдосконалення систем захисту інформації. Безпека у комп'ютерних мережах – це умова захисту конфіденційних даних від різного роду загроз.

Існує велика різноманітність методів ідентифікації. Найпоширеніші технології верифікації та ідентифікації базуються на використанні паролів та персональних ідентифікаторів (персональний ідентифікаційний номер PIN-код) або документів, таких як паспорт та водійські права. Однак такі системи є надто вразливими і можуть легко постраждати від підробки, крадіжки та інших факторів. Тому все більший інтерес викликають методи біометричної ідентифікації, які дозволяють визначати особу людини за її фізіологічними характеристиками шляхом розпізнавання за раніше збереженими зразками [1-4].

2. Об'єкт і предмет дослідження

Біометричні системи доступу дуже зручні у використанні та надійні для захисту інформації. Тому у даній статті об'єктом дослідження обрано методи біометричної ідентифікації на основі аналізу відбитку пальця, розпізнавання людини 2D та 3D, райдужною оболонкою ока, сітківки ока, малюнок вен, клавіатурного почерка і голосу.

3. Мета і задачі дослідження

Метою дослідження є зробити порівняльний аналіз методів біометричної автентифікації з урахуванням сукупності показників якості.

4. Аналіз літератури

Розпізнавання особистості стає невід'ємною складовою частиною життя суспільства, оскільки в багатьох видах людської діяльності необхідною умовою є гарантія ідентичності особистості. Надійна ідентифікація стає необхідним атрибутом повсякденного життя [1, 2].

Під час аналізу біометричних технологій розглядалися системи, які набули широкого поширення. Як варіанти для пошуку кращого розглядалися: відбиток пальця, розпізнавання обличчя 2D і 3D, райдужна оболонка ока, сітківка ока, малюнок вен [3,4].

Однак, у всіх літературних джерелах, присвячених огляду біометричних технологій, зазначалося, що вибір кращої з них – окреме завдання, яке має вирішуватися безпосередньо для кожного конкретного випадку окремо.

Метод аналізу ієрархії описується в [5], але немає прикладу вибору біометричних систем.

Однак, у всіх літературних джерелах, присвячених огляду біометричних технологій, зазначалося, що вибір кращої з них – окреме завдання, яке має вирішуватися безпосередньо для кожного конкретного випадку окремо.

Тому, актуальним є провести вибір біометричної системи методами багатокритеріальної оптимізації та методом аналізу ієрархії.

5. Методи дослідження

У статті наводиться порівняння і з застосуванням метода аналізу ієрархії. В основі метода аналізу ієрархії є декомпозиція завдання по вибору бажаного переважного варіанта певної системи та поділення завдання на більш прості частини з урахуванням отриманих оцінок від експертів по парним порівнянням простих частин завдання, як показано на рисунку 1.

Результати попарних порівнянь частин системи записуються до матричної форми.

Після виконання деякої обробки матриць попарних порівнянь частин в ієрархії на рівнях 2 і 3 проводиться обчислення вектора глобальних пріоритетів \vec{C} порівнюваних частин системи (1) і (2). Але спочатку знаходяться компоненти власного вектора V_i та вектори пріоритетів P_i на кожному рівні ієрархії.

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

де n – кількість показників якості, N – кількість порівнювальних систем.

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

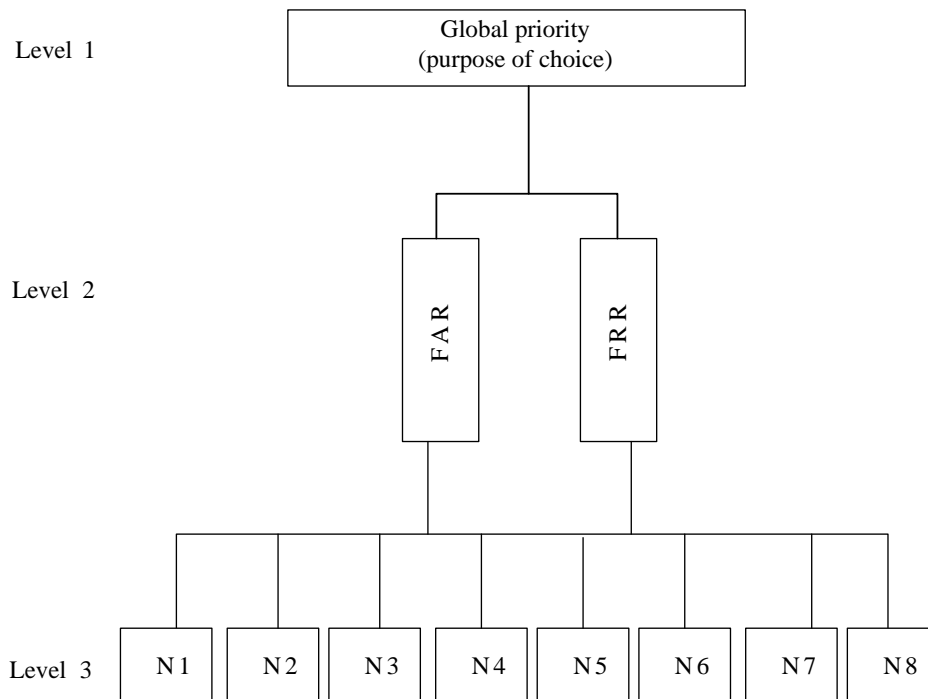


Рисунок 1. Декомпозиція завдання вибору в ієрархію методів біометричної автентифікації.

За максимальним значенням компонент вектора \vec{C} обирається бажаний варіант певної системи.

6. Результати досліджень

При порівнянні систем були обрані наступні показники якості: коефіцієнт помилкових прийняттів (FAR), тобто відсоток ситуацій, коли система дозволяє доступ користувачеві, який не зареєстрований в системі, і коефіцієнт помилкових відмов (FRR), тобто відсоток відмов у доступі поточному користувачеві системи. Обидва параметри розраховуються за допомогою методів математичної статистики. Чим нижчі значення цих показників, тим вища якість автентифікації користувачів. Розглядаються також інші показники якості систем, зокрема, ймовірність того, що система помиляється у визначенні збігів між вхідною вибіркою та відповідним шаблоном з бази даних (FNMR – False Non-Match Rate); робоча характеристика приймача (ROC) – візуалізація компромісу між характеристиками FAR та FRR; коефіцієнт

невдалих спроб (FTE або FER) – коефіцієнт невдалих спроб створити шаблон з вхідних даних; Failure To Capture (FTC) – ймовірність того, що автоматизована система не зможе визначити біометричні вхідні дані при їх коректному пред'явленні; ємність шаблону – максимальна кількість наборів даних, які можуть зберігатися в системі; стійкість до підробки – емпірична характеристика, що узагальнює, наскільки легко підробити біометричний ідентифікатор; стійкість до впливу навколишнього середовища – характеристика, що емпірично оцінює стабільність роботи системи в різних умовах навколишнього середовища.

Зокрема, в роботі методом аналізу ієрархій було проведено багатокритеріальне порівняння та обрано бажаний переважний варіант для методів біометричної ідентифікації на основі аналізу відбитків пальців, 2D розпізнавання обличчя, райдужної оболонки ока, сітківки ока, малюнку вен, почерку, голосу. У таблиці 1 наведено середні значення показників FAR та FRR для різних біометричних систем контролю та управління доступом (СКУД) [1-5].

Таблиця 1. Середні значення показників FAR та FRR.

№	Тип біометричної системи	FAR, %	FRR, %
N1	аналіз відбитку пальця	0,001	0,6
N2	розпізнавання людини 2D	0,1	2,5
N3	розпізнавання людини 3D	0,0005	0,1
N4	райдужна оболонка ока	0,00001	0,016
N5	сітківка ока	0,0001	0,4
N6	малюнок вен	0,0008	0,01
N7	клавійатурний почерк	0,01	3,0
N8	голос	1	3

Для зручності вихідні значення показників якості FAR та FRR, наведені в таблиці 2, були преобразовані. Зокрема, проведена операція нормалізації показників якості.

Таблиця 2. Преобразовання початкових значень показників якості FAR та FRR.

№	Тип біометричної системи	FAR	FRR
N1	аналіз відбитку пальця	0,01	0,016
N2	розпізнавання людини 2D	0,0001	0,004
N3	розпізнавання людини 3D	0,02	0,1
N4	райдужна оболонка ока	1	0,625
N5	сітківка ока	0, 1	0,025
N6	малюнок вен	0,0125	1
N7	клавійатурний почерк	0,001	0,003
N8	голос	0,0001	0,003

У табл. 3 наведено розраховані значення компонент вектора \vec{C} пріоритетності варіантів технологій за кожним показником якості, а також компонент вектора глобальних пріоритетів з (компонента вектора пріоритетів за показниками якості), (компонента вектора пріоритетів за показником якості FAR), (компонента вектора пріоритетів за показником якості FRR), (компонента вектора пріоритетів за показником якості FRR).

Таблиця 3. Розраховані значення компонент вектора

Тип біометричної системи	Q_{ij}		\vec{C}
	FAR	FRR	
аналіз відбитку пальця	0,071	0,075	0,077
розпізнавання людини 2D	0,025	0,037	0,031
розпізнавання людини 3D	0,153	0,157	0,165
райдужна оболонка ока	0,35	0,349	0,373
сітківка ока	0,108	0,112	0,117
малюнок вен	0,235	0,239	0,252
клавіатурний почерк	0,044	0,018	0,036
голос	0,012	0,015	0,014
P_i	0,667	0,399	

На основі максимального значення \vec{C} обрано бажаний метод біометричної автентифікації.

Це – райдужна оболонка ока, з характеристиками FAR 0,00001% та FRR 0,016%.

7. Перспективи подальшого розвитку досліджень

Використання біометрії дозволить вирішити проблему достовірності і може підвищити надійність аутентифікації та ідентифікації об'єктів при організації доступу до систем з великою кількістю користувачів, а також до критично важливих систем в складі системи контролю і управління фізичним доступом або в якості додаткового фактора аутентифікації.

8. Висновки

Проведено порівняльний аналіз деяких біометричних систем контролю доступу за набором показників якості. За допомогою методу аналізу ієрархій знайдено бажаний переважний метод біометричної автентифікації. Це метод райдужної оболонки ока.

9. Список літератури

1) 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.

- 2) Bezruk V.M., Skoryk YU.V., Kobtseva V.M. Sravnenye metodov byometrycheskoy autentyfykatsyy po sovokupnosti pokazately kachestva / V.M. Bezruk // Mizhnarodna naukova konferentsiya High-Technologies in infocommunications. – Харків. Кам'янець-Подільський Університет, Україна, 2019. – С. 79-80.
- 3) Lebedenko YU. I. Biometricheskiye sistemy bezopasnosti / YU. I. Lebedenko // - Tula: Izd-vo TulGU, 2012. - 160 s.
- 4) Sayt Sovremennyye biometricheskiye metody identifikatsii [Elektronnyy resurs] Rezhim dostupa: [www/ URLhttp://masters.donntu.org/2013/fknt/fomenko/library/article4.htm](http://www.URLhttp://masters.donntu.org/2013/fknt/fomenko/library/article4.htm)
- 5) Saaty T.L. The Analytic Hierarchy Process / T.L. Saaty. – New York: McGraw Hill, 1980. – 270 s.
- 6) 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
- 7) Elizarov A., Ryabiy M., Elizarov A., Shkarupa D., Gorinshtein M. Review of modern methods of biometric identification and analysis of the effectiveness of their use to limit access / A. Elizarov // INFORMATION TECHNOLOGIES/4. Information Security. Kharkov: Khneu. – 2009.
- 8) Bryukhomitsky Y. Biometric technologies of personality identity / Y. Bryukhomitsky// textbook. Rostov-on-Don: South Federal University. – 2017. – 263 p.
- 9) James L. Wayman, Anil K. Jain, Davide Maltoni. Biometric Systems: Technology, Design and Performance Evaluation / L. James. – Springer, 2005. – 361 p.
- 10) Jiankun Hu, David Chek Ling Ngo, Andrew Beng Jin Teoh. Biometric Security / Hu Jiankun. – Springer, 2015. – 460 p.
- 11) Ruggero Donida Labati, Vincenzo Piuri, Fabio Scotti. Touchless Fingerprint Biometrics / Donida Labati Ruggero. – CRC Press, 2015. – 223p.
- 12) Dijana Petrovska-Delacrétaz, Gérard Chollet, Bernadette Dorizzi. Guide to Biometric Reference Systems and Performance Evaluation / Petrovska-Delacrétaz Dijana. – Springer, 2009. – 373 p.
- 13) Ted Dunstone, Neil Yager. Biometric System and Data Analysis: Design, Evaluation / Dunstone Ted. – Springer, 2008. – 263 p.
- 14) Anil K. Jain, Patrick Flynn, Arun A. Ross. Handbook of Biometrics / Jain Anil K. – Springer, 2007. – 550 p.
- 15) N. V. Boulgouris, Konstantinos N. Plataniotis, Evangelia Micheli-Tzanakou. Biometrics: Theory, Methods, and Applications / Boulgouris N. V. – WILEY. Canada, 2009. – 719p.

Selecting the preferred biometric authentication method

Yuliia Skoryk

Department of Infocommunications, Kharkiv National University of Radio Electronics,
Kharkiv, Ukraine
ORCID 0000-0003-1729-1003

Valeriy Bezruk

Department of Infocommunications, Kharkiv National University of Radio Electronics,
Kharkiv, Ukraine
ORCID 0000-0003-2349-7788

Abstract: In this article, a multicriteria methodology is used to compare some biometric authentication methods with other identification methods. In order to analyze biometric access control systems qualitatively, it is necessary to take into account the characteristics of the systems, as well as to apply certain methods for multicriteria optimization. Therefore, it is necessary to conduct a comparative analysis of biometric authentication methods, taking into account a set of quality indicators. This paper compares certain biometric access control systems by a set of quality indicators,

namely, the false-admission rate (FAR), which means a certain percentage when a situation arises when the system can allow access to a user who is not registered in the system, and the false-rejection rate (FRR), which is the percentage of access denied to a real user of the system. Both parameters are calculated using mathematical statistics. The lower the value of these indicators, the higher the quality of authentication of certain users. The article compares and uses the hierarchy analysis method to select the preferred option of known biometric identification tools based on the analysis of fingerprint, 2D human recognition, iris, retina, vein pattern, keyboard handwriting and voice. The hierarchy analysis method is based on the decomposition of the task of selecting the desired design option for a particular system and dividing this task into simpler parts, using the estimates obtained from experts for pairwise comparisons of simple parts of the task. After processing certain data, the preferred biometric identification method is determined. The use of biometrics can solve reliability problems and can improve the reliability of authentication and identification of certain objects when accessing a system with a large number of users, as well as very important and necessary systems as part of physical access control and management systems.

Keywords: biometric systems, authentication, comparison, optimization.
