DOI: https://doi.org/10.26565/2304-6201-2022-53-04

УДК 681.3.07

# Analysis Of Biometric-Based Identification Algorithms In Electronic Trust Services Systems

V.O. Podhaiko, S.G. Rassomakhin

**Rassomakhin S.G.** *Doctor of Technical Sciences, Associate Professor, Head of the Department of BIST,*
*V. N. Karazin Kharkiv National University,*
*Maidan Svobodi, 6, c. Kharkiv,61022*
*e-mail: bist@karazin.ua;*
**https://orcid.org/0000-0003-1394-3588**

**Podhaiko V.O.** *Postgraduate*
*V. N. Karazin Kharkiv National University,*
*Maidan Svobodi, 6, c. Kharkiv,61022*
*e-mail: podhaiko2020pg@student.karazin.ua;*
**https://orcid.org/0000-0001-5905-9400**

The article is devoted to the usage of identification algorithms based on biometric personal data (biometrics) in the electronic trust services. This theme is of considerable interest due to the fact that it is becoming one of the most used tools in everyday life. It can include such things as fingerprint and facial scanners in modern cell phones as well as more official aspects such as a personal passport or signature.

The main problem of electronic identification is that the most effective algorithms: based on abstract-minutiae cylindrical codes, where minutiae are unique to each fingerprint and determine the points of change in the structure of the capillary lines (ending, splitting, breaking, etc.), the orientation of capillary lines and coordinates at these points.

Also, algorithms based on fuzzy extractors, where by fuzzy extractor we mean the system (object, algorithm) which transforms biometric data into random sequences, providing the opportunity to apply encryption methods for biometric security. Although they perform their role, they do not always work correctly and present a possible danger to a user. A comprehensive analysis of the advantages and disadvantages of such algorithms requires further investigation and combination of these algorithms to solve existing problems and improve overall response.

Not only could that provide a higher level of protection, but also greatly simplify the mathematical complexity of data processing, as well as lead to an increase in the number of correct triggers and overall increase the efficiency of using biometric technology in electronic trust services.
***Keywords***: *biometry, minutiae, imprecise extractor, algorithm, code*.

# Анализ алгоритмов идентификации на основе биометрии в системах электронных доверительных услуг.

**Рассомахін С.Г.** *Доктор технічних наук, доцент, завідувач кафедри БІСТ,*
*Харківський національний університет ім. В.Н. Каразіна*
*Майдан Свободи, 6, м. Харків, 61022*
*e-mail: bist@karazin.ua;*
**https://orcid.org/0000-0003-1394-3588**

**Подгайко В.О.** *Аспірант,*
*Харківський національний університет ім. В.Н. Каразіна*
*Майдан Свободи, 6, м. Харків, 61022*
*e-mail: podhaiko2020pg@student.karazin.ua;*
**https://orcid.org/0000-0001-5905-9400**

Дана стаття присвячена актуальній на сьогоднішній день темі використання алгоритмів ідентифікації на основі біометричних даних особистості (біометрії) у системі електронних довірчих послуг. Це викликає значний інтерес через те, що це стає одним з найбільш використовуваних засобів в повсякденному житті. До нього можна віднести таке, як сканери відбитків пальців і обличчя у сучасних мобільних телефонах, так і більш офіційні аспекти, наприклад, особистий паспорт або підпис.

Основна проблема застосування електронної ідентифікації виражається в тому, що найбільш ефективні алгоритми: на основі абстрактно-мінуативних циліндричних кодів, де мінуція – це унікальні для кожного відбитку ознаки, що визначають пункти зміни структури папілярних ліній (закінчення, роздвоєння, розрив та ін.), орієнтацію папілярних ліній та координати в цих пунктах. Також алгоритми на основі нечітких екстракторів, де під нечітким екстрактором ми розуміємо систему (об'єкт, алгоритм), яка перетворює біометричні дані в випадкові послідовності, що надають можливість застосувати шифрувальні методи для біометричної безпеки. Вони хоча й виконують свою роль, але спрацьовують не завжди коректно, наражаючи на можливу небезпеку користувача.

Всебічний аналіз переваг і недоліків таких алгоритмів потребує подальшого їх розвитку та використання своєрідного симбіозу цих алгоритмів для вирішення існуючих проблем та покращення загального спрацьовування. Це повинно не тільки забезпечити більш високий рівень захисту, але й значно спростити математичну складність обробки даних за алгоритмами. І саме це призведе до підвищення кількості вірних спрацьовувань та підвищення ефективності використання біометричних технологій у системах електронних довірчих послуг.

***Ключові слова***: *біометрія, мінуція, нечіткий екстрактор, алгоритм, код*.

## Introduction

Nowadays different identification systems are increasingly being used. We use them for electronic payments, for limiting access to objects, for identity authentication, etc.

Nowadays, the problem of correct identification and authentication of a person is more important than ever. And what can be more personal than individual biometric features, such as voice, retina, gait, fingerprints and, of course, DNA. All of these things together are covered by the term "biometrics." Today, the idea of using biometrics for the authentication and identification is very relevant. Moreover, almost all of us use them, for example, to unlock the phone screen with our fingerprint, or the so-called "Face ID" or face identifier. Biometric mechanisms are also applied in the modern identification documents, both foreign and Ukrainian. But unfortunately, the above-mentioned methods, especially the more complex ones, do not work quite correctly. For example, "Face ID" can unlock the screen only if a person’s photo is presented to its scanner. And the fingerprint doesn't work when the fingers are wet or something else makes it difficult to access the fingerprint pattern.

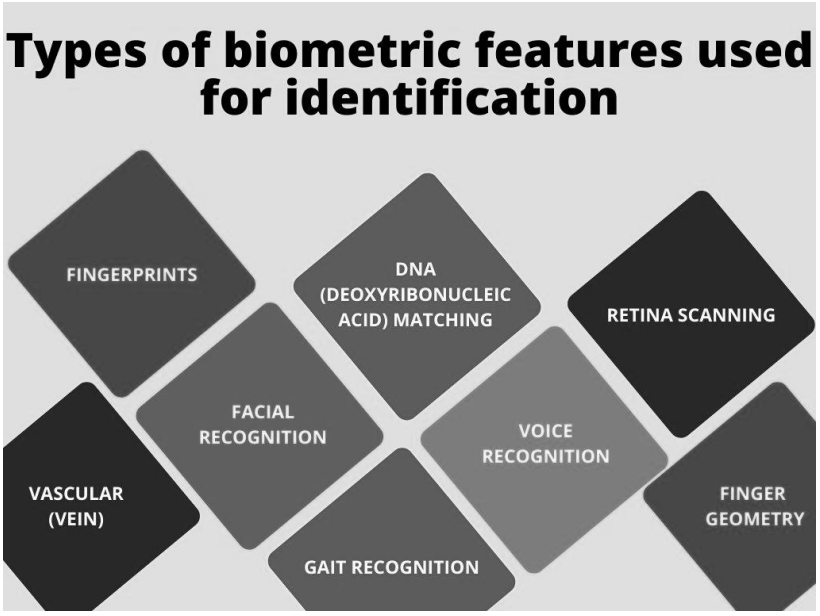


*Fig.1 The types of biometric features used for identification*

Such systems require more detailed study, all-around improvement and further development in order to avoid false positives and achieve a fully correct identification and authentication, where an error can be an extremely "costly".

## 1. Problem Statement

To analyze potentially better identification algorithms and determine directions for their further development in order to solve existing problems:

- confidentiality and delimitation (data obtained during biometric registration can be used for purposes that the registered individual did not consent to (was not aware of);

- dangers to owners of protected data (there is a possibility of an attempt on the part of the holder of biometric identifiers to gain access);

- the possibility of cancelling biometric data (the advantage of a password over biometrics is the possibility of changing it). Mainly, the cancellation of biometrics is a distortion of the biometric image or properties prior to their approval.

**2. Main points**

Fingerprint identification (dactyloscopy) is the most common technology used in biometric access control systems today. The technology is based on the unique pattern of fingerprints on people's fingers. The fingerprint obtained with the scanner is converted into a digital code, which is stored in a database, and then compared to previously entered and converted fingerprint codes.

The biometric access by fingerprint is easy to use, convenient and reliable. The devices that scan the fingerprints are very reliable and cheap. The disadvantages include distortion of the papillary pattern by small scratches, cuts, chemical reagents; inability to read the fingerprint by some scanners if the skin is too wet.

Two types of features can be identified in each fingerprint – global and local. Global features are those that can be seen with the naked eye.

Papillary pattern:

- pattern area – a highlighted fragment of the fingerprint in which all global features are localized;

- core or center – a point localized in the middle of the imprint or some selected area;

- the "delta" point – the starting point. The place where there is a separation or joining of the papillary furrows, or a very short furrow (can reach to a point);

- line type – the two largest lines that start as parallel and then diverge and circle the entire image area;

- line count – the number of lines on the image area, or between the core and the "delta" point.

Papillary pattern types:

- "loop" type patterns (left, right, central, double),

- "delta" or "arc" type patterns (simple and sharp),

- "spiral" type patterns (central and mixed).

Another type is local features. They are called minutiae (peculiarities or special points) which are unique for each fingerprint and determine the points of capillary lines structure changes (ending, splitting, breaking etc.), the orientation of capillary lines and coordinates in these points. Each fingerprint can contain up to 70 or more minutiae.

Practice shows that the fingerprints of different people may have the same global features, but it is completely impossible to have the same minutiae micropatterns. Therefore, global features are used to separate the database into classes and at the stage of authentication. At the second stage of recognition local features are used.

Comparisons of prints by local features (minutiae) include:

1. Improving the quality of the original image of the print. Sharpness of the borders of the lines of strokes is increased.

2. Calculation of the orientation field of the fingerprint's lines. The image is divided into square blocks with sides more than 4 pixels, and the angle t of line orientation for a fragment of the fingerprint is calculated using brightness gradients.

3. Binarizing the image of the print. Binning to a black and white image (1 bit) by thresholding.

4. Thinning the lines of the fingerprint image. Thinning is performed until the lines are 1 pixel wide.

5. Minutiae extraction. The image is divided into blocks of 3x3 pixels. After that, the number of black (non-zero) pixels around the center is counted. The pixel in the center is considered to be a minutia if it is non-zero, and there are one (minutiae "ending") or three (minutiae "branching") neighboring non-zero pixels. Coordinates of detected minutiae and their orientation angles are written in a vector. When registering users, this vector is considered a reference and is written to the database. During recognition, the vector determines the current fingerprint.

6. Matching minutiae. Two fingerprints of the same finger will differ from each other by rotation, offset, change in scale, and/or area of contact, depending on how the user places the finger on the scanner.

Therefore, it is impossible to tell whether a fingerprint belongs to a person or not by a simple comparison (the vectors of the reference and the current fingerprint may differ in length, contain mismatched minutiae, etc.). Because of this, the comparison process must be implemented for each minutia separately.

Comparison stages include data registration, searching for pairs of matching minutiae, evaluating the print matching.

During registration the parameters of affine transformations (rotation angle, scale and shift) are determined, at which some minutiae from one vector correspond to some minutiae from the second vector.

The results of a search are up to 30 rotation values (from -15 to +15 degrees), 500 shift values (from -250 px to +250 px, though sometimes even smaller limits are chosen), and 10 scale values (from 0.5 to 1.5 in steps of 0.1) for each minutia, up to 150,000 steps for each of the 70 possible minutiae in total. (In practice, all possible options are not enumerated – after selecting the right values for one minutia, there is an attempt to substitute them for the other minutiae, otherwise it would be possible to match almost any prints to each other).

The assessment of print matching is done by the formula

$$K = \frac{D^2}{pq} * 100,$$

where $D$ – the number of matching minutiae,
$p$ – the number of minutiae of the reference,
$q$ – the number of minutiae in the recognized print). If the result exceeds 65%, the prints are considered identical (the threshold can be lowered by setting another level of vigilance).

If authentication has been performed, this is the end of the process. For identification this process must be repeated for all fingerprints in the database (then the user with the highest matching level is selected (of course, the result must be above the 65% threshold)).

**3. Current identification algorithms**

The main directions of solving the specified problems are the algorithms abstract-minutiae cylindrical codes, and the algorithms based on fuzzy extractors. They are the most used in biometrics to provide a high probability of a correct identification.

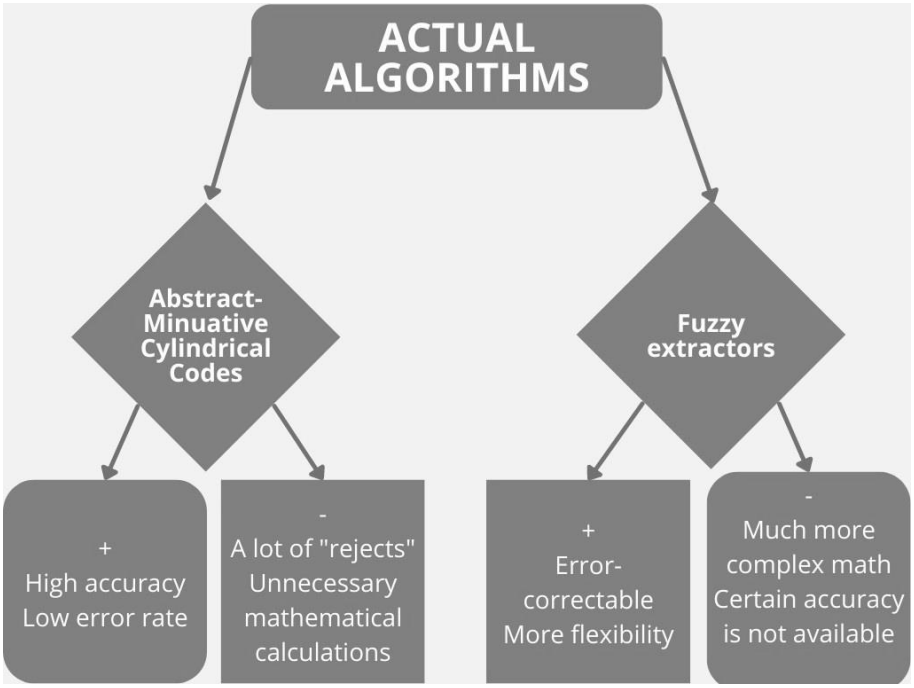


*Fig.2 The used algorithms*

*Abstract-Minutiae Cylindrical Codes.*

Abstract-Minutiae cylindrical codes are based on the small details of fingerprint descriptors, which take into account the smallest information in a fingerprint image to match them. Minutiae are features unique to each fingerprint, defining points of change in the structure of the capillary lines (termination,

bifurcation, break, etc.), the orientation of the capillary lines and the coordinates at these points. Each fingerprint can contain up to 70 or more minutiae. It is thanks to their comparison that the local features are compared.

The algorithm based on minutiae cylindrical codes uses three-dimensional data structures called cylinders, where each cylinder is oriented in the direction of the central minutiae throughout the image. Minor locations are spatial points where the orientation, frequency, and energy have a higher differential of change.

The orientation image computed by STFT analysis differs from traditional orientation images computed using simple derivatives. With the exception of the core and delta points, any local area of the fingerprint image provides consistent texture information using STFT. This is not the case in traditional gradient orientation estimation.

The approach by which it is created is called the default function, where not every cell in the cylinder will accumulate the specified contribution. Thus, cells that lie outside the valid territory mask are considered invalid, and cells without neighbors have zero contribution. The cylinder is kept or discarded according to validity constraints. These constraints include the minimum number of neighbors around the central minutiae at constant radius, as a percentage of the total number of valid cells. Only valid cylinders will be part of the imprint pattern.

The disadvantage of this approach is the complexity of mathematical calculations of a large number of minutiae and a significant number of cylinders that are processed but discarded for one reason or another (considered invalid).

*Fuzzy extractors.*

A fuzzy extractor is a system (object, algorithm) that converts biometric data into random sequences that provide the ability to apply encryption methods for biometric security. They are used to encrypt and authenticate user transactions. In this case, the biometric input is treated as a key. The word "fuzzy" in the extractor's name implies that the values of the resulting sequence have a form close enough to the original and can confirm the authenticity of the identity.

The algorithm using fuzzy extractors is a method that allows us to uniquely recover the secret key from inaccurately reproduced biometric data involving auxiliary data, which is open. According to the algorithm, a sequence of actions is performed:

- initialization, where a security parameter is specified that defines the length of the public and secret keys and the triggering threshold, based on which the algorithm generates a secret master key and public parameters;

- extraction, where a specific identity and the secret master key are specified, and the algorithm itself processes the data and returns the user's secret key;

- encryption, where the algorithm returns a ciphertext based on the user's secret key, his identity, and the embedded message;

- decryption, where by the secret key and the ciphertext encrypted with the identity, the algorithm returns the message if the identity data is confirmed, or stops working otherwise.

Subsequently, the stability of such an algorithm is evaluated from the point of view of force attacks, such as full brute force, collision creation, etc. The stability to them being obtained, the algorithm is moved to the analysis of its stability against analytical attacks.

The disadvantage of this approach is the complexity of mathematical apparatus of data processing in the presence of a significant number of errors and the inability to provide the necessary accuracy when it is necessary to correct these errors.

**Conclusions**

Thus, the most important and promising areas for further research are those related to the incorrect operation of fuzzy extractors and abstract-minutiae codes, which address the issues of correct identification and authentication of the person. The identification and authentication based on the synthesis of the "strengths" of both algorithms will balance their individual drawbacks.

## ЛІТЕРАТУРА

1. Подгайко В.О., Рассомахін С.Г. *Аналіз алгоритмів ідентифікації у системах електронних довірчих послуг*.// Зб. наук. праць І Міжнародної науково-технічної конференції “Системи і технології зв’язку, інформатизації та кібербезпеки: Актуальні питання і тенденції розвитку”, м. Київ, 25–26 листопада 2021 року. С. 239-240.

2. A. Menezes, P. van Oorschot and S. Vanstone. *Handbook of applied cryptography*. – Boca Raton, FL: CRC Press, 1996. P. 306-312.

3. Yen-Lung Lai, Jung-Yeon Hwang, Zhe Jin, Soohyong Kim, Sangrae Cho and Andrew Beng Jin Teoh. *A Symmetric Keyring Encryption Scheme for Biometric Cryptosystems*. – arXiv:1807.02251v1 [cs.CV], 6 Jul 2018. P. 1-15.

4. Wajih Ullah Baig, Umar Munir, Waqas Ellahi, Adeel Ejaz, Kashif Sardar. *Minutiae Texture Cylinder Codes for fingerprint matching*.// Information Sciences. V.502, October 2019. P. 492-509.

## REFERENCES

1. Podhaiko V.O., Rassomakhin S.G. *Analysis of identification algorithms in electronic trust services systems*. // Coll. of Scient. Papers of the First International Scientific and Technical Conference "Communication Systems and Technologies, Informatization and Cyber Security: Current Issues and Development Trends", Kyiv, November 25-26, 2021. – P. 239-240.

2. A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of applied cryptography*. – Boca Raton, FL: CRC Press, 1996. – P. 306-312.

3. Yen-Lung Lai, Jung-Yeon Hwang, Zhe Jin, Soohyong Kim, Sangrae Cho and Andrew Beng Jin Teoh. *A Symmetric Keyring Encryption Scheme for Biometric Cryptosystems*. – arXiv:1807.02251v1 [cs.CV], 6 Jul 2018. – P. 1-15.

4. Wajih Ullah Baig, Umar Munir, Waqas Ellahi, Adeel Ejaz, Kashif Sardar. *Minutiae Texture Cylinder Codes for fingerprint matching*.// Information Sciences. V.502, October 2019. – P. 492-509.

Надійшла у першій редакції 09.12.2021, в останній - 14.01.2022.