ISSN2224-087X. Електроніка та інформаційні технології. 2022. Випуск 19. С. 58–65
Electronics and information technologies. 2022. Issue 19. P. 58–65

UDC 004.056.52 DOI: https://doi.org/10.30970/eli.19.5

DEVELOPMENT OF A FINGERPRINT PATTERN MATCHING METHOD USING K-MEANS

M. Nazarkevych[1], A. Petrov[1], O. Onopriychuk[1], N. Oleksiv[2], Y. Kis[2]

[1]Ivan Franko National University of Lviv,
107 Tarnavsky St., UA–79017 Lviv, Ukraine
mariia.nazarkevych@lnu.edu.ua

[2]Lviv Polytechnic National University,
12 Bandery St., UA-79013, Lviv, Ukraine

Biometric identification methods wstudied. Biometric identification of fingerprints and methods of their use are analyzed. As a recognition, fingerprint-based intelligent analysis identification is preferred, in particular the matching of a scanned fingerprint to a template. The paper analyzed the main filtering algorithms of the K-Means clustering method. The the study result of the program operation with the presented method of filtering the fingerprints were obtained. The developed identification system is based on Arduino Nano in combination with a DY50 fingerprint scanner. The software of this system is implemented using the C++ language and integrated using the Arduino IDE.

Keywords: filtering, Ateb-Gabor filtering, biometric images.

Methods of intellectual analysis and comparison of fingerprints

One of the urgent development tasks of information technologies at the current stage is the provision of reliable information protection. Actual methods of information protection are divided into: hardware, software, mixed (combines both hardware and software) [1].

As an alternative to the password system or its addition, user identification based on biometric characteristics and signs can be considered. Biometric technologies of identification and authentication have a number of advantages over traditional ones and are increasingly used in computer systems and various spheres of information activity [2]. Biometric verification of your biological data, and not just verification of a password that can be stolen, intercepted or guessed, is the key to the expansion of e-commerce, the creation of new information security systems in corporate networks and other modern systems.

There are two main categories of fingerprint comparison methods: point-by-point comparisons and whole-pattern fingerprint comparisons. The pattern identification method involves comparing two images to see how similar they are. This method is commonly used in fingerprint reading systems to find duplicates [3]. The most common technology is recognition based on the comparison of certain points.

The template-based algorithm compares the master fingerprint template between the pre-stored template and the candidate fingerprint. To do this, you need to be able to align the image in one direction. For this, the algorithm finds the central point of the fingerprint image and centers itself. In a pattern-based algorithm, the pattern contains the pattern type, size, and orientation within the aligned fingerprint image. The candidate's fingerprint image is graphically compared to the template to determine the level of match.

When comparing at special points, a template is formed, on which end points and branching points are distinguished. On the scanned image of the print, special points are also highlighted, which are compared with the pattern. The main advantage of this algorithm is its speed of operation and ease of implementation. Disadvantages of the comparison algorithm for special points include high requirements for image quality and sensor size.

The essence of the correlation comparison method is that the obtained fingerprint is superimposed on each standard from the base in turn, after which the difference between them is calculated by pixels. The comparison process must involve many iterations, each time the image is rotated by a small angle or shifted slightly. Therefore, this method is the slowest and requires high computing power.

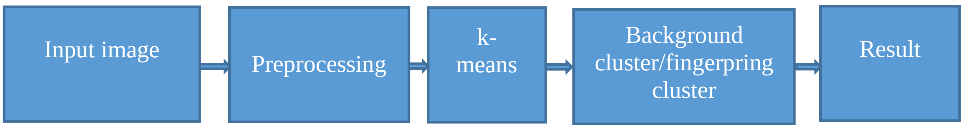

Fig. 1. Functional scheme of recognition

The image comparison algorithm takes into account not only individual points, but also general characteristics of the fingerprint, such as the thickness of the stripes, their curvature or density. The advantage of this method is that it can work with lower print quality. However, this method is not suitable for many database searches.

The pattern comparison method uses the peculiarities of the structure of the papillary pattern. The resulting image is divided into many small cells, in each of which the location of the lines is described by the parameters of the sinusoid. The print obtained for comparison is aligned and reduced to the same type as the template. The main advantages of this algorithm are quite high speed and low image quality requirements.

In a graph-based comparison algorithm, the original fingerprint image is transformed into an orientation image of the papillary line field, indicating areas with the same line orientation. Then the centers of these areas are determined and a graph is obtained. Further actions are similar to the method of comparison in special points..

Comparing fingerprints using pattern-matching algorithms

The pattern identification method involves comparing two images to see how similar they are [4]. This method is commonly used in fingerprint reading systems to find duplicates. The most common technology is recognition based on the comparison of certain points.

- Normalization of the image: at this stage, we perform the process of scaling the print to a uniform scale and geometric dimensions with a clearly defined resolution;
- Local Orientation Calculation: This refers to scaling the footprint to the origin and rotating the impression to establish the basis and polar axis. Tilt your fingers at any angle while scanning. To recognize a print, it is necessary to have a visible reference to the coordinate system.
- Fingerprint segmentation: It is necessary to construct a fingerprint mask by dividing the normalized image into blocks and performing the task of classifying each block into those that match and do not match the trunk. After that, we use a mask with a Gabor filter [5].

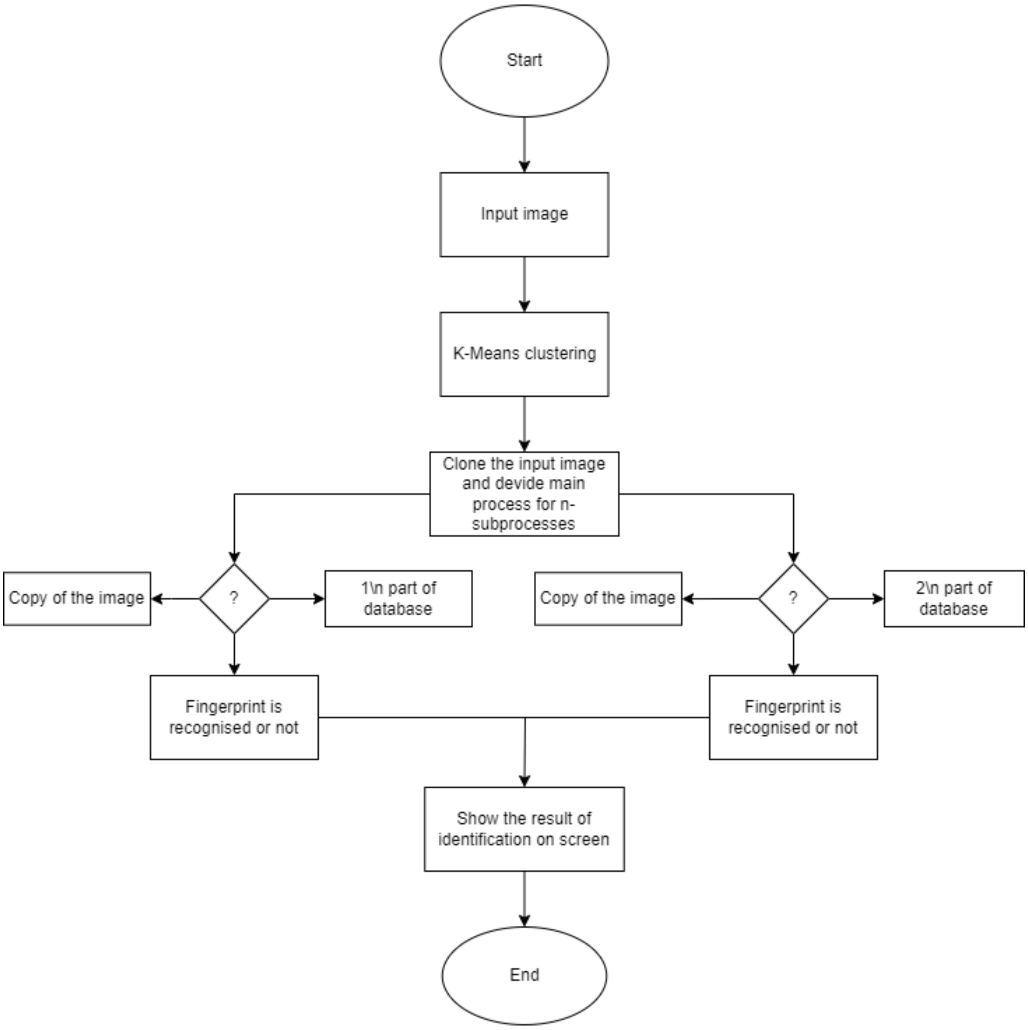
Start
Input image
K-Means clustering
Clone the input image and devide main process for n-subprocesses
Copy of the image
?
1\n part of database
Copy of the image
?
2\n part of database
Fingerprint is recognised or not
Fingerprint is recognised or not
Show the result of identification on screen
End

Fig. 2. Image comparison algorithm for biometric identification

Preprocessing algorithm

Preprocessing [6] improves image quality by filtering and removing unwanted noise. The papilloma-based algorithm worked well only with 8-bit grayscale fingerprint images. This is because the 8-bit gray image of the fingerprint is the basis for converting the image to a 1-bit image with a value of 0 for spines and 1 for ridges. As a result, the ridges were highlighted in black, and the grooves in white. the process partially denoised the image and improved this edge detection.

In addition, there are two more steps to improve the highest quality of the input image. This is feature extraction and removal of damaged features. Detail extraction was performed using a trunk decimation algorithm, which requires the removal of redundant trunk pixels. As a result, the disappearing haircuts in the fingerprint image receive a unique certificate and can be used further. The wrong parts after the extraction step were removed as well. Lack of ink and connection between pins can lead to defective parts and incorrect fingerprint recognition.

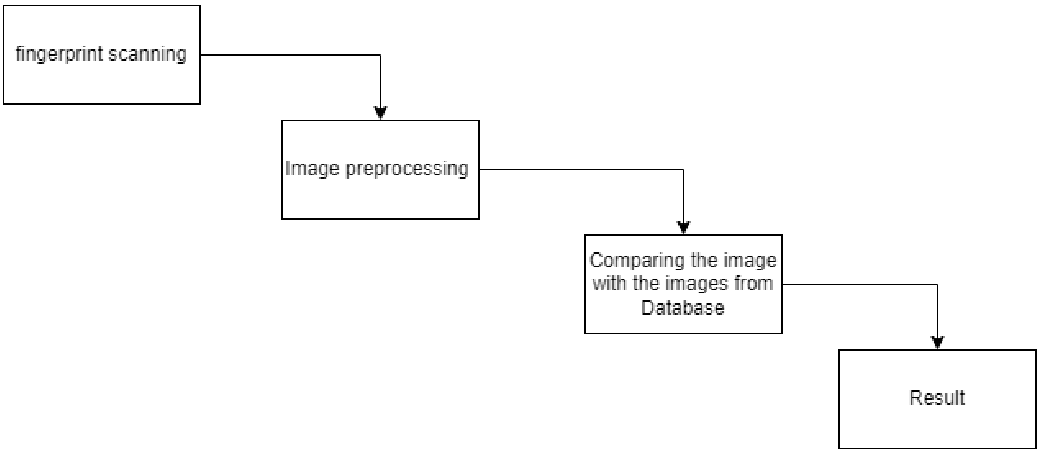

Fig. 3. Structural diagram of the comparison method

Methods of K-Means clustering and parallel processing

Clustering generally aims to group data points of reference points in biometric images. The technique involves first determining the number of clusters and randomly assigning cluster centroids to each cluster from entire data sets; this step is the initialization of the cluster centroids. The distance between each point in the entire data sets and each cluster is determined by k-means. The centroid is then calculated using a distance metric (e.g. Euclidean distance) [7]. Then, a minimum distance is determined for each data point, and this point is assigned to the nearest cluster [8]. This stage is called cluster assignment, and it is repeated until all data points have been assigned to one of the clusters.

While working with the software languagePythonand OpenCV library, a program was developed to identify fingerprint images from a corresponding fingerprint database [9, 10].

Arduino IDE development environment

The Arduino Integrated Development Environment [11] – or Arduino software (IDE) – contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions, and a series of menus. It connects to Arduino hardware to download and communicate with programs.

Programs written using the Arduino software (IDE) are called sketches. These thumbnails are saved in a text editor and with the .ino extension. The editor has features for cut/paste and find/replace text. The message area provides feedback during saving and exporting, and displays errors. The console displays the text displayed by the Arduino software (IDE), including full error messages and other information. The configured board and serial port are displayed in the lower right corner of the window. Toolbar buttons let you test and load programs, create, open, and save thumbnails, and open the serial monitor.

The fingerprint sensor has its own flash memory where it stores data. This data, called templates, is 512 bytes; The sensor memory can store up to 127 patterns.

In order for the sensor to recognize a fingerprint, it must first store patterns for comparison. Therefore, first-time users should always run the "registration" program first.

Layout board and connection of contacts

A mock-up board is a universal printed circuit board for modeling prototypes of electronic devices. With the help of a breadboard, you can easily design the necessary circuit.

The board is a plastic board with a lot of holes. Jumper wires, microcircuits, resistors, LEDs, buttons and other elements with thin, sharp metal tips can be inserted into these holes. The distance between the holes is 2.54 mm. This is a standard spacing, so many electronic components fit perfectly into this board.

A solderless breadboard is very convenient for making breadboards.

The system is connected via a breadboard. The connection to the computer is made directly from the ArduinoNano using a USB adapter (Fig. 4).

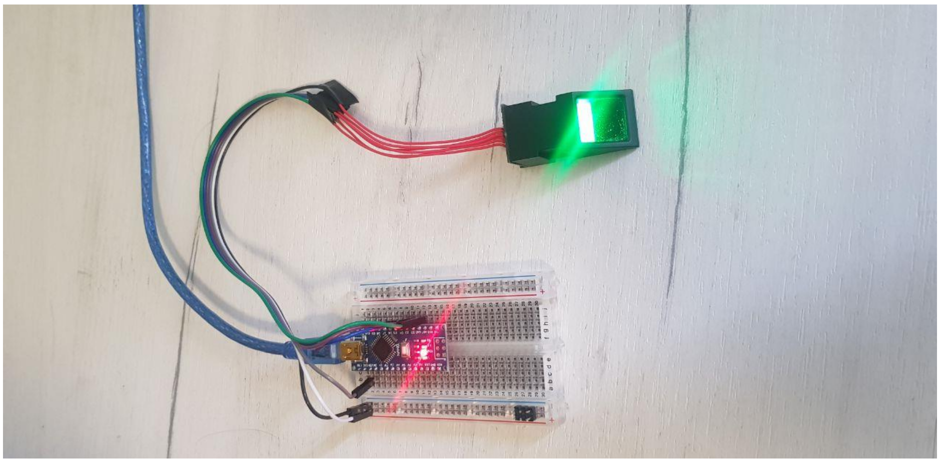

Fig. 4. Fingerprint scanning system

The important point is to connect the fingerprint scanner to the ArduinoNano. In fig. 4, it is difficult to understand the order of connecting the cables to their ports, so it is shown in Fig. 5.

To demonstrate the operation of the fingerprint verification system, two firmwares were created for our system: a custom firmware that searches the fingerprint database and searches for the corresponding user fingerprint; and administrator firmware to register fingerprints. Enroll allows you to add fingerprints to the database under one of the indexes, the number of indexes is limited by the maximum number of scanner memory (127 templates). The program gives the opportunity to choose under which identifier we will save our fingerprint (Fig. 4), after which the fingerprint reading script is launched. For the reliability of a correct reading, the system requires repeated application of the finger to verify the stored print (Fig. 5).

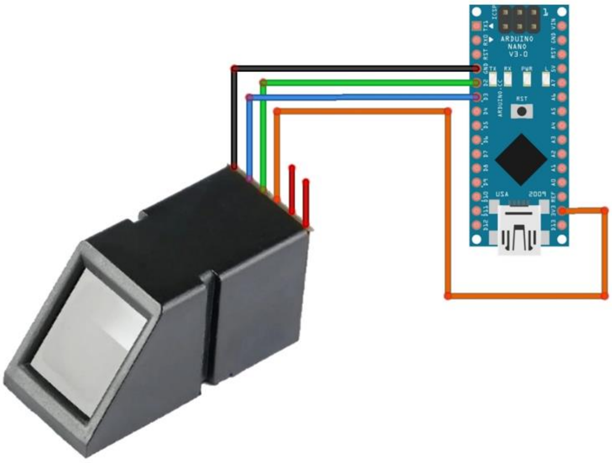

Fig. 5. Connection diagram of the fingerprint scanner

Fig. 6 shows the fingerprint identification process. Algorithm verification is performed by the same function as adding a fingerprint. The only difference is that the fingerprint template recorded in the database has already been processed and stored in the fingerprint skeleton image format. That is, the scanned fingerprint is first pre-processed, and only then is it checked against those present in the database.

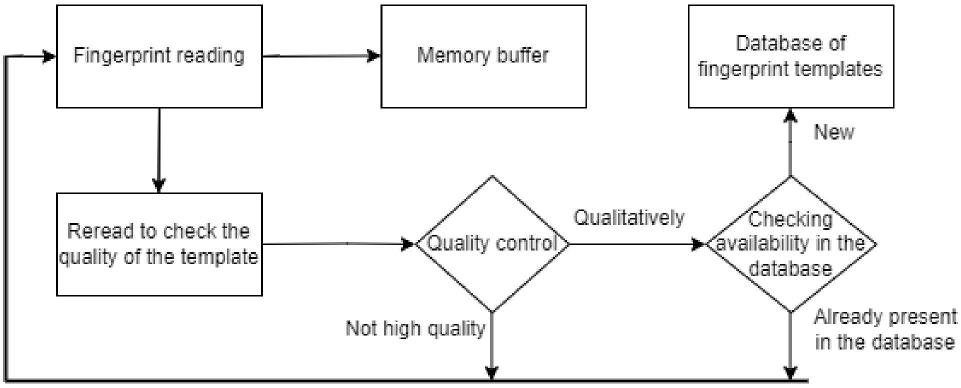
Fingerprint reading
Memory buffer
Database of fingerprint templates
New
Reread to check the quality of the template
Quality control
Qualitatively
Checking availability in the database
Not high quality
Already present in the database

Fig. 6. Schematic description of the process of adding fingerprints

Conclusion

The methods of defining a fingerprint on an image using the K-Means method proposed in the OpenCV library were analyzed. The fingerprint identification method was analyzed. This method is used in fingerprint reading systems to find duplicates. The most common technology is recognition based on the comparison of certain points.

The pattern matching algorithm, which is based on data analysis, considers not only individual segments, but also general characteristics of the fingerprint, such as the thickness of the papillomas, and their curvature or density. The advantage of this method is that it can work with a lower-quality print.

The developed identification system is based on Arduino Nano coupled with a DY50 fingerprint scanner; all hardware pins were connected using a breadboard. The software of this system is implemented using the C++ language and integrated using the Arduino IDE.

References

[1] *Jeon, S. J., Go, M. S., & Namgung, J. H.* (2022). Use of personal information for artificial intelligence learning data under the Personal Information Protection Act: the case of Lee-Luda, an artificial-intelligence chatbot in South Korea. *Asia Pacific Law Review*, 1-18.

[2] Luo, S. (2022). User Sensitive Information Protection Scheme Based on Blockchain Technology. *Mobile Information Systems*, *2022*.

[3] *Hrytsyk, V., Grondzal, A., & Bilenkyj, A.* (2015, September). Augmented reality for people with disabilities. In 2015 Xth International Scientific and Technical Conference" Computer Sciences and Information Technologies"(CSIT) (pp. 188-191). IEEE.

[4] *Gulekci, Y., Efeoglu Ozseker, P., Cavus Yonar, F., & Daglioglu, N.* (2022). Comparison of methods to develop fingerprints on papers impregnated with AB-PINACA and AB-FUBINACA. Journal of Forensic Sciences, *67*(2), 524-533.

[5] *Kasprowski, P., & Ober, J.* (2004, May). Eye movements in biometrics. In International Workshop on Biometric Authentication (pp. 248-258). Springer, Berlin, Heidelberg.

[6] *Giełczyk, A., Marciniak, A., Tarczewska, M., & Lutowski, Z.* (2022). Pre-processing methods in chest X-ray image classification. *Plos one*, *17*(4), e0265949.

[7] *Wang, C., Peng, G., & De Baets, B.* (2022). Class-specific discriminative metric learning for scene recognition. Pattern Recognition, 126, 108589.

[8] *Voznyi, Y., Nazarkevych, M., Hrytsyk, V., Lotoshynska, N., & Havrysh, B.* (2021). Проектування системи автентифікації біометричного захисту на основі методу K-середніх. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 4(12), 85-95.

[9] *Nazarkevych, M., & Nazarkevych, H.* (2022). Проектування захищеної інформаційної системи для створення продукту в умовах адаптації. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 3(15), 186-195.

[10] *Nazarkevych M., Marchuk A., Voznyi Ya.* Development of biometric identification methods based on new filtration methods // Electronics and information technologies. 2020. Issue 14. P. 55–64.

[11] *Minz, S., Singh, S., Aggarwal, A., Behl, N., Rajput, P., & Sharma, S.* (2022, January). A Gesticulation Superintend Arm with Arduino IDE. In 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 766-771). IEEE.

РОЗРОБКА МЕТОДУ ПОРІВНЯННЯ ВІДБИТКІВ ПАЛЬЦІВ З ВИКОРИСТАННЯМ K-MEANS

М. Назаркевич[1], А. Петров[1], І. Оноприйчук[1], Н. Олексів[2], Я. Кісь[2]

*[1]Львівський національний університет імені Івана Франка,
вул. Ген. Тарнавського, 107, 79017 Львів, Україна*
mariia.nazarkevych@lnu.edu.ua

*[2]Національний університет «Львівська політехніка»,
вул. Степана Бандери 12, 79013 Львів, Україна*

Досліджено методи біометричної ідентифікації. Проаналізовано метод кластеризації K-Means. Кластеризація групує опорні точки на біометричних зображеннях. Методика передбачає визначення кількості кластерів та присвоєння кластеру центроїдів до кожного кластера з цілих наборів даних. Відстань між кожною точкою у наборах даних та кластерами обчислюється розробленим методом. При порівнянні на спеціальних точках формується шаблон, на якому виділяються кінцеві точки і точки розгалуження. На сканованому зображенні відбитка також виділяються спеціальні точки, які порівнюються. При нормалізації зображення відбувається процес масштабування відбитка до однорідного масштабу та геометричних розмірів з визначеною роздільною здатністю. Обчислення локальної орієнтації: означає процес масштабування відбитка до початку координат та поворот відбитка із встановленням початку координат. Суть методу кореляційного порівняння полягає в тому, що отриманий відбиток пальця накладається на кожен еталон з бази по черзі, після чого обчислюється попіксельно різниця. Процес порівняння повинен включати багато ітерацій, на кожній з яких зображення повертається на невеликий кут або трохи зміщується. При виконанні сегментації відбитків: необхідно будувати маску, розділивши нормалізоване зображення на блоки, та виконавши завдання класифікації. Алгоритм узгодження шаблонів враховує не тільки окремі сегменти, а й загальні характеристики відбитка пальця, такі як товщина папілом, їх кривизна або щільність. Для демонстрації роботи системи створено користувацьку та адміністративну прошивки. Отримані результати дослідження роботи програми з представленим методом зображення відбитків пальців. Розроблена система ідентифікації базується на Arduino Nano у поєднанні з сканером відбитків пальців DY50. Програмне забезпечення даної системи реалізовано за допомогою мови C++ та інтегровано, використовуючи Arduino IDE.

Ключові слова: фільтрація, фільтрація Атеб-Габора, біометрична ідентифікація.

Стаття надійшла до редакції 05.10.2022.
Прийнята до друку 14.10.2022.