Raw and Noisy Fingerprint Image Classification with Natural Language Processing Techniques and Ensemble Machine Learning Methods

Milan Panić[1], Nemanja Maček[2], Branimir Trenkić[3], Daniel Menićanin[4]

[1]*Pan-European University "APEIRON", Faculty of Information Technology, Banja Luka, Bosnia and Herzegovina, milan.v.panic@apeiron-edu.eu, https://orcid.org/0009-0006-9270-7354*

[2]*University Business Academy in Novi Sad, Faculty of Social Sciences, Belgrade, Republic of Serbia, macek.nemanja@gmail.com, https://orcid.org/0000-0002-3465-7524*

[3]*Academy of Technical and Art Applied Studies, School of Electrical and Computer Engineering, Belgrade, Republic of Serbia, trenkic.branimir@gmail.com, https://orcid.org/0009-0006-8795-3040*

[4]*Pan-European University "APEIRON", Faculty of Information Technology, Banja Luka, Bosnia and Herzegovina, danijel.menicanin@gmail.com, https://orcid.org/0009-0001-6311-4043*

Original scientific paper

https://doi.org/10.7251/JIT2501005P UDC: 37.018.43:004.738.5

Abstract: This paper presents a raw and noisy fingerprint image recognition system based on natural language processing feature extraction methods and ensemble machine learning methods. The main goal of the proposed model is to reach state-of-the-art classification accuracy, even with the noisy images, eliminate false acceptance rates, and cancel the possibility of recreating a fake fingerprint image from a generated template. To achieve this, we omit preprocessing phase such as application of gradient vectors and multiple filter banks that are typically employed in traditional fingerprint recognition systems. Instead, we employ machine learning methods that classify biometric templates as numeric features. The biometric templates are generated by converting raw fingerprint image into a one-dimensional set of fixed-length codes, which then undergoes stylometric extraction of features further being used for classification. The experimental evaluation shows that the system performs as intended. In addition, the computational and storage costs are significantly decreased with respect to traditional systems, which makes it suitable for use in practical applications.

Keywords: biometrics, ensemble learning, fingerprint, machine learning, natural language processing, stylometry

Introduction

Fingerprint recognition represents a biometric technology based on unique fingerprint characteristics aimed at identifying and verifying an individual's identity. Given that human fingerprints have been discovered on a large number of archaeological artifacts [1, 2], it has been considered one of the most popular technique for human recognition as well as identification for over a century.

Each person has unique fingerprints, even twins do. This makes fingerprints extremely reliable for individual identification. Fingerprints can be relatively easily collected using various devices, making the collection process quick and non-invasive. Fingerprint recognition technology enables rapid identification and verification of an individual's identity. In forensics, fingerprints are often used as key evidence. They can be found at crime scenes, on items used in criminal activities, or on evidence found at the crime scene. Using fingerprint recognition technology, forensic experts can compare fingerprints to databases to identify suspects or confirm the identities of victims. Fingerprints are less susceptible to theft or misuse compared to traditional identification methods such as passwords or cards. Therefore, in many banks, government and military institutions, access to sensitive information is based on the application of fingerprint recognition technology to improve security.

The method of identification and authentication is based on the analysis of unique fingerprint characteristics. To create a unique biometric profile of a person, details found on the surface of the skin of the fingers, such as ridges and valleys, are used. Using optical, capacitive, or ultrasonic scanning techniques, characteristics are collected from the surface of the finger skin (ridges and valleys). After the collection process, the fingerprint image undergoes preprocessing, which involves noise removal, normalization, and segmentation, to improve its quality.

Extracting characteristic points from the preprocessed or enhanced image is a key step. Each fingerprint contains a large number of characteristic points called minutiae. Depending on the type, minutiae indicate branching and changes at the ends of ridges. Characteristic points of the fingerprint are stored in a database as a biometric profile. The accuracy of the minutiae extraction process directly affects the accuracy of fingerprint matching notably disrupting the identification process, where the template is compared with all fingerprint template in the database to find a best match.

The paper describes a new approach to fingerprint recognition that avoids the use of traditional filter banks and wavelet transformations. The described approach is based on converting a fingerprint image into a textual format using the Base64 encoding algorithm as presented in [3]. The use of a textual format eliminates the detection of the region of interest (ROI) segment of the image and the application of gradient vectors for identifying changes in pixel intensity in the edge or contour detection process of the fingerprint. Extraction of numerical characteristics is realized by applying a stylometric (natural language processing, NLP) extraction methods. By using appropriate ensemble machine learning techniques, classification of the extracted numerical characteristics is conducted. The described process excludes the preprocessing phase, which involves extracting numerical characteristics from raw data. The main contribution of the solution described in the paper relates to increasing the accuracy of fingerprint recognition by eliminating the False Acceptance Rate (FAR) and minimizing False Rejection Rate (FRR). Exclusion of the preprocessing phase, which involves applying appropriate image enhancement algorithms, significantly reduces the time in the fingerprint recognition and verification process. Additionally, the proposed approach enables the realization of a system on a low cost hardware.

In brief, the main contributions of this paper are listed as follows:

- no preprocessing phase whatsoever, i.e. no region of interest detection or gradient vector application, resulting in lower computational cost (please note that additional filters are neither applied);
- no tradeoff between FAR and FRR or seeking equal error rate, as FAR is zero;
- FRR ranging from 0,01% to 0,001%;
- applicability to raw and noisy images and
- providing a system that makes biometric template (a NLP feature vector) resilient to attackers that use artificial neural networks and genetic algorithms for malicious reverse processing (regenerating sample from template).

METHODS AND MATERIALS

Before we present methods used here, we need to clarify for a reader why fingerprint recognition systems may be computationally expensive. And has tradeoffs. But, first, one shall provide an insight in how they work, and what mathematics is behind the engine that slows them up, provides impostors a grant to a system as well as unwanted false rejections for genuine users.

The fingerprint recognition system typically goes through several key stages to provide accurate identification or verification: acquisition, image preprocessing, feature extraction and classification. Based on the classification results, the system makes a decision regarding the user's identity typically using some kind of a threshold. In identification, one or more potential identities may be returned, while in verification, the decision is based on the degree of feature match.

The fingerprint recognition system is used for both verification and identification purposes. In verification, a registered fingerprint is compared with an identified user to determine if two prints are from the same finger (1-1 matching). In identification, an input fingerprint is compared with all registered fingerprints in the database to determine if it matches any (1-N matching). In this context, systems have been developed relying on two key phases: enrollment and identification. The enrollment phase involves registering an individual's identity, or fingerprint, in the database for future use. On the other hand, the identification phase aims to extract an individual's identity from the database based on the user's claim of identity.

Although fingerprint acquisition, preprocessing, and feature extraction are common steps for both enrollment and identification, fingerprint matching represents an additional mandatory step in the identification phase. This step enables the identification of a person based on their fingerprint from a previously collected database. It is important to emphasize that processing time and identification accuracy are key factors in improving the performance of these systems.

Traditional fingerprint recognition

Fingerprint recognition systems operate as follows: first, an enhancement algorithm is applied to increase the clarity of ridges and valleys. These algorithms use visual characteristics such as continuity and orientation of ridges to improve image quality. Subsequently, the enhanced fingerprint image undergoes segmentation, separating the background from the fingerprint areas containing essential information. Segmentation is achieved by observing local intensity variations in the original grayscale image. In the minutiae identification process, the segmented image is first binarized, converting grayscale to a black-and-white image. Then, the image is thinned to reduce ridge thickness to a single pixel and isolate pixels corresponding to minutiae.

Gabor wavelets and filters are signal processing techniques commonly used in image analysis and shape recognition. Gabor wavelets are complex sinusoidal signals that are spatially and frequency limited. They can be oriented in specific directions and scaled to certain sizes, making them useful for detecting different orientations and frequencies in images. When applied to an image, Gabor filters produce an output that emphasizes regions similar to the local characteristics of the wavelet shape the filter is designed to detect. This enables the identification of textures, edges, and other details in the image. In the context of fingerprint recognition, Gabor filters are used to extract key fingerprint features such as ridges and valleys, facilitating further analysis and fingerprint identification. However, the use of Gabor wavelets and filters can be computationally demanding. It is important to note that systems based on Gabor technique implementation face challenges such as a high false acceptance rate, template size, and reliability, further complicating the fingerprint identification process.

Extraction of minutiae is a crucial step in fingerprint recognition systems, where distinctive features of the fingerprint are identified and extracted for further analysis. Minutiae are specific points where ridge lines in the fingerprint pattern end or bifurcate. These points serve as unique identifiers for fingerprint matching and are essential parts of the fingerprint recognition process. Minutiae extraction typically involves several steps: preprocessing, segmentation, orientation field estimation, image enhancement, and minutiae detail extraction. After capturing the fingerprint image using a fingerprint scanner or sensor, minutiae details are extracted from the biometric fingerprint before generating a pattern in which unwanted effects and components are removed.

Just to illustrate the needs of mathematics behind traditional fingerprint recognition system, we present some of it below. Preprocessing of the sample involves analyzing the image histogram, i.e., the distribution of pixel intensities (histogram equalization), to enhance the local contrast of the image. The process of removing blurring and additional noise from the fingerprint image, without altering the structures of the biometric sample, is based on the implementation of a Wiener filter. The Wiener filter [4] in the frequency domain can be represented by the equation:

$$W(u,v) = \frac{H^*(u,v)}{|H(u,v)|^2 + \frac{P_n(u,v)}{P_s}(u,v)}, \tag{1}$$

where $H(u,v)$ is the Fourier transform of the point spread function $h(x,y)$, $H^*(u,v)$ is the complex conjugate of this function, $P_n(u,v)$ is the spectral power density of the noise, and $P_s(u,v)$ is the spectral power density of the under-graded image,

$$W(u,v) = \frac{P_s(u,v)}{P_s(u,v) + \sigma_n^2}, \tag{2}$$

where σ_n^2 is the noise variance.

Segmentation involves extracting significant parts from the rest of the image, i.e., ridge structures from the background and other artifacts. The process is based on dividing the resulting output of the Wiener filter into blocks of the same size that do not overlap. Let N denote the block size, and $\mu(I)$ represent the mean pixel value of the block. Block I is considered a foreground block if its noise variance is greater than the threshold τ_s:

$$\sigma^2(I) = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\big(I(i,j) - \mu(I)\big)^2 > \tau_s\,, \qquad (3)$$

Estimation of the orientation field, i.e., the local orientations of ridge and valley structures, is also performed on a block-by-block basis. One way of estimating it is based on gradient vectors that show the greatest intensity deviation perpendicular to the ridge lines [5]. The orientation θ of each block is given by the equation:

$$\theta = \frac{1}{2}tan^{-1}\left[\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}2g_x(i,j)g_y(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N}(g_x{}^2(i,j)-g_y{}^2(i,j))}\right] + \frac{\pi}{2}\,, \qquad (4)$$

where g_x and g_y denote the gradient vectors of a block centered at pixel (i, j) in the horizontal and vertical directions, respectively. To enhance the image, a Gaussian low-pass filter is used, followed by a 2-D Gabor filter [6] defined by:

$$G(x,y,\theta,f_0) = e^{-\frac{1}{2}\left(\frac{x_\theta{}^2}{\sigma_x{}^2}+\frac{y_\theta{}^2}{\sigma_y{}^2}\right)}\cos(2\pi f_0 x_0)\,, \qquad (5)$$

$$x_0 = xsin\theta + ycos\theta\,, \qquad (6)$$

$$y_0 = -xcos\theta + ysin\theta\,, \qquad (7)$$

where f_0 denotes the ridge frequency, θ the orientation of the filter, σ_x and σ_y the standard deviations of the Gaussian envelope along the x and y axes, $[x_\theta, y_\theta]$ the coordinates $[x, y]$ after rotating the coordinate axes by $0.5\pi-\theta$ clockwise. Considering that point feature extraction algorithms work with images in binary format, the output of filtering is binarized. The grayscale level of each pixel is compared with a global threshold, resulting in an image with two levels of interest: ridges and valleys. Narrowing the width of ridge lines is achieved by applying a thinning algorithm described in [7]. According to the Hilditch's definition, the number of transitions represents the measure of transitions from white to black pixels while passing through points in a certain order. The result of the algorithm is an image composed of ridge lines one pixel wide, with clearly visible ridge endings and bifurcation points (valley endings). For each pixel in the resulting image, according to the Rutovitz's definition, the number of transitions is calculated as the number of transitions from white to black and vice versa as points are passed in sequence. Pixel is identified as a ridge end point if number of transitions equals two, and as a bifurcation point if number of transition equals six. Reader may cf. [8, 9] for more details.

Related work

There is a wealth of research describing techniques for fingerprint recognition. Contemporary studies increasingly involve the application of various machine learning techniques to improve accuracy, performance, and system stability. In this chapter, we analyze relevant research exploring fingerprint recognition methods using machine learning techniques for feature extraction, fingerprint image enhancement, classification, and matching.

In the work by Xie and Qi [10], a backpropagation neural network method is proposed for grayscale fingerprint image quality assessment. Their methodology involves segmenting fingerprint images into blocks, which requires additional computational resources.

Zhu et al. [11] use a neural network to estimate the quality of fingerprint images, focusing on the orientation of fingerprint ridges. Precise ridge orientation is estimated using trained neural networks.

Labati et al. [12] proposed using neural networks to measure image quality in wireless fingerprint scanning. They identified a new set of features and developed a neural network for extracting complex characteristics for future fingerprint matching.

Liu et al. [13] propose using backpropagation neural network method for detecting singular points on grayscale fingerprint images divided into blocks of size 35 times 35 pixels.

Bartunek et al. [14] used a backpropagation neural network for extracting minutiae from fingerprint images. Minutiae detection was performed using a sliding window of size 5 times 5 pixels to access the entire fingerprint image.

Yang et al. [15] used fuzzy logic-based neural networks for extracting minutiae from grayscale images, with a high degree of rotation and grayscale invariance.

In the research described in [16], Kumar and Vikram described the application of multidimensional artificial neural networks (MDANN) for fingerprint matching using minutiae points. This algorithm achieved a maximum recognition rate of 97.37%.

Liu et al. [17] used the SVM method with a five-dimensional feature vector to determine the quality of fingerprint images. Fingerprints were classified into high, medium, and low-quality images with an accuracy of 96.03%.

Li et al. [18] proposed using the SVM technique for fingerprint classification into 5 classes using a combination of singular points and image orientation. Using only orientation coefficients achieved an accuracy of 87.4%, while using only singular points achieved an accuracy of 88.3%.

In the study described in [19], the authors presented the development of a fingerprint classification model based on the SVM algorithm. The algorithm was tested on the FVC2000 and FVC2002 datasets, achieving a fingerprint classification accuracy of 92.5%.

Kahraman et al. [20] proposed a methodology for extracting characteristic minutiae from fingerprint images using a multilayer artificial neural network based on orientation maps. This algorithm was evaluated on the UPEK and FVC2000 datasets, achieving significant results. Specifically, an accuracy of 95.57% was achieved for UPEK, while an accuracy of 91.38% was achieved for FVC2000.

Zeng et al. [21] proposed an algorithm for recognizing partial fingerprints based on deep learning. The Deep Neural Network (DNN) was trained and evaluated using the NIST-DB4 dataset, achieving an accuracy of 93%.

In the research conducted by Saponara et al. [22], an autoencoder architecture based on Convolutional Neural Network (CNN) for reconstructing fingerprint images is proposed. The proposed architecture was evaluated on four different fingerprint image datasets, achieving accuracies of 98.1%, 97%, 95.9%, and 95.02%, respectively, for each of the four datasets.

In the work by Elsadai et al. [23], a method for fingerprint recognition based on machine learning techniques and stylometric features is proposed. For the evaluation of machine learning algorithms, the CASIA-FingerprintV5 database was used. The application of random sampling before and during the cross-validation process was analyzed. The CatBoost algorithm for classification, along with the over-sampling method SMOTE during cross-validation, achieved accuracies of 99.95% and 99.98% for the All_features and GRRF datasets, respectively.

In the work by Sun et al. [24], the authors propose an APFI model based on deep learning focused on feature extraction from partial fingerprint images. Experimental results on their dataset and the NIST SD4 dataset show that the proposed method achieves an accuracy of 98.9% for the complete image, 98.6% when the effective fingerprint area is 75%, 94.9% when the effective fingerprint area is 50%, 88.9% when the effective fingerprint area is 75%, and 94.9% when the effective fingerprint area is 25%.

Further, we will let a reader screen a summary table in the discussion section with a brief comparison of fellow researchers aforementioned.

Natural language processing based feature extraction

Traditional fingerprint recognition systems utilize minutiae extraction methods that employ Gabor wavelet transformations or filters, segmentation, binarization, thinning, and generation of binary fingerprint templates for individual recognition. This process, besides being based on a complex mathematical apparatus, requires more time and better computational performance to optimize parameters to balance the FAR and FRR values in the matching phase. In this work, we propose a framework (Fig. 1) that is based on encoding raw data representing fingerprint images and converting them into raw textual data without modifying statistical characteristics.

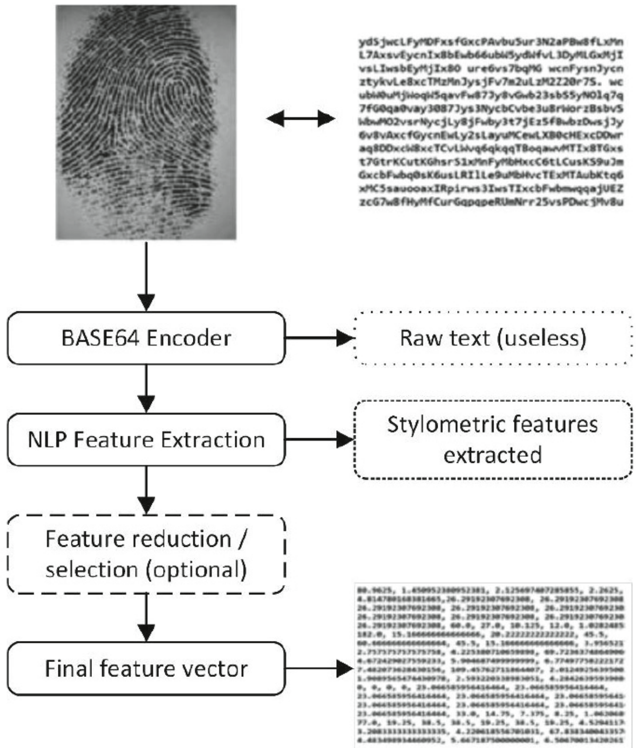

Figure 1. *Fingerprint data acquisition framework.*
Source: *author's contribution. Fingerprint image is adopted from [25].*

The Base64 encoding algorithm was implemented to encode original fingerprint images into raw textual form without modifying their statistical characteristics. From the raw textual data, significant features listed below were extracted:

- the average sentence length in a text;
- the percentage of capital letters in relation to the number of lower-case letters;
- the percentage of lower-case letters in relation to the total number of characters in a text;
- the percentage of punctuation signs in relation to the total number of blank spaces in a text;
- the percentage of the numeric characters in relation to the total number of letter characters in a text;
- the average word length per sentence in a text;
- the frequency of the most frequent stop word in a text;
- the frequency of the most frequent starting word of a sentence in a text;
- the frequency of the most frequent starting letter of a starting word;
- the frequency of the most frequent starting letter of a stop word;
- the number of words occurring only once in a text;
- the number of words occurring twice in a text;
- the number of words of a given length in a text;
- the number of words whose lengths are within a given range and
- the number of vowels in a text.

This list includes language-independent features selected from the stylometry tagging model proposed in [26]. Additionally, we employ:

- the Deflate algorithm - text compression in the best compression mode and
- the Kolmogorov complexity of text fragments of a given length.

The transformation of a fingerprint image into a source of information via a finite alphabet induced by Base64 encoding has a significant impact on the accuracy of the proposed biometric system. Spatial correlations are easier to detect in text generated using Base64 than from a fingerprint image. This argument particularly applies to properties based on global information measures, such as Kolmogorov complexity and structural stylometric properties. These measures, calculated for the textual representation of a fingerprint image, actually include structural spatial interdependencies within the given image, indirectly encoded in the corresponding text. On the other hand, Base64 encoding preserves enough information related to local spatial properties, encoded in stylometric properties. Since text is considered a biometric source, it generates biometric characteristics in our proposed method. The obtained information enables verification or authentication of authorship based on extracted characteristics. Generated feature templates based on input text obtained from raw data will ensure achieving higher accuracy.

The intuition behind using stylometric features is that the spatial structure of fingerprint images, when encoded into text, introduces statistical regularities similar to those found in natural language. These regularities can be captured using language-independent features, providing a novel representation for classification.

Elsemble learner classification

In the proposed approach described in the paper, data preprocessing is reduced to the extraction of feature vectors, which are then forwarded to the classifier when the fingerprint is loaded into the system for testing. No noise reduction, normalization, oversampling, or filter application procedures were conducted on the raw data. This approach significantly improves the performance of the proposed fingerprint recognition system framework.

For the selection of significant feature vectors, dimensionality reduction, and generation of classifier models, several machine learning methods were used, such as:

- Multiboost [27] from the Weka system [28] named *MultiboostAB*,
- Random Forest [29] from the R package *randomForest* (the original Breiman and Cutler's Fortran code ported to R) and
- Gradient boosting (CatBoost) [30] from the Python package *catboost*.

Results

The procedure was implemented on data obtained from the CasiaV5 fingerprint image database [25] developed by the Chinese Academy of Science, Institute of Automation (Fig 2). The database has been offe43red free of charge for the biometric research community. The fingerprint samples were captured using the URU4000 sensor during one session. CASIA-FingerprintV5 database consists of 20,000 fingerprint images of 500 individuals, including graduate students, waiters, workers, etc.

Figure 2. *Fingerprint data acquisition.*

Source: *Chinese Academy of Science, Institute of Automation [25]. Used with permission.*

The analyzed dataset was divided into training and test sets using the 10-fold cross-validation method. The performance of the generated classifier models was evaluated using the measures accuracy, precision, recall, F-measure, and the area under the curve (AUC). In addition, two important biometric measures are taken into account: the FAR and FRR. In the binary classification considered in our approach, they are equivalent to the False Positive Rate (FPR) and False Negative Rate (FNR), respectively.

The proposed approach can be briefly described by the following procedure: each of the two fingerprint images is represented by a feature vector. The array representing the first image is denoted as A, and the array representing the second image is denoted as B. Feature vectors A and B are classified as Y (the observed fingerprints belong to the same person) or N (the observed fingerprints belong to different individuals).

Results are presented in Table 1. Reader may find these comparable to aforementioned studies.

Discussion

This section of the paper will briefly deal with the following issues: finding the optimal hyper-parameters of the classification models, generalizability of the solution and the need for oversampling, introduction of filter bank preprocessing and the applicability and security issues.

Regarding the optimal hyper-parameters, authors may conclude that different parameters apply to other datasets. To put it simple, parameters will vary with different image acquisition device in real life scenario – be it with or without oversampling. Here, for example, forests are built with 150 trees, while CatBoost employs 500.

Regarding generalizability, the proposed method is tested by considering the average classification accuracy of the repeated cross-validation procedure (ten-fold cross-validation repeated ten times, every time with a different seed of a random number generator). Depending on the dataset properties, an over-

Table 1. *Experimental evaluation of CASIA samples with three ensemble learning algorithms.*

	Accuracy	Precision	Recall	F-measure	AUC
Multiboost	0.9946 ± 0.006	0.97 ± 0.03	0.99 ± 0.01	0.98 ± 0.01	0.98 ± 0.01
Random Forest	0.9982 ± 0.002	1.00 ± 0.00	0.99 ± 0.01	0.99 ± 0.01	1.00 ± 0.00
CatBoost	0.9967 ± 0.003	0.97 ± 0.01	1.00 ± 0.00	1.00 ± 0.00	0.99 ± 0.00

estimation of the performance is possible as a consequence of the applied approach for cross-validation after the over-sampling [31].

Although ROI estimation and gradient vectors could provide an additional image tuning in the preprocessing phase, the idea behind this research was to provide a proof that this method is applicable to raw images and is prone to errors originating from noise. Reader may consult [23] to compare results of the similar research that includes noise reduction and normalization with the results presented here.

To make the proposed approach suitable for an efficient algorithmic verification in embedded devices and IoT technologies, efforts are made to reduce the size of the fingerprint biometric template. The results of the feature extraction show that it is possible to reduce the size of an biometric template to 128 and 256 bits, which represent a significant reduction with respect to the biometric templates generated by the traditional methods.

Regarding applicability, this reduction of the computational costs and template size enables implementation of the proposed approach in devices with small memory capacity, it does not have a negative impact on the security of the biometric templates. In the proposed approach, a biometric template is stored as a set of numeric feature values in a database. In contrast to the traditional approaches, these templates cannot be used to reconstruct the original fingerprint images by using genetic algorithms or artificial neural networks, which cancels the possibility of performing a successful attack on the biometric system by using synthetic fingerprint images.

Last, but not least, we provide a comparison table with the other researchers (Table 2).

Conclusion

The disadvantages of the traditional fingerprint recognition systems include the existence of the FAR, which is unacceptable in most of authentication scenarios, the existence of a threshold in the authentication phase, the need to find a balance between the FAR and FRR, the fine-tuning of filter parameters, and large template sizes which are not suitable for some applications.

To overcome these disadvantages, we employ feature extraction approach based on an encoder that generates a set of stylometric features from a raw fingerprint image. As expected, the transformation of an image into an information source over a finite alphabet has a significant positive impact on the recognition accuracy, as spatial correlations are more easily detected, and thus more easily utilized, in a Base64-generated text than in an fingerprint image.

As for further work, we will provide the research on impact of traditional preprocessing phases on the confusion matrix as well as impact of oversampling techniques, such as oversampling before and during cross-validation.

Table 2. *Comparison to other researchers.*

Ref.	Methods	Pros.	Cons.
Xie and Qi [10]	ANN, grayscale fingerprint segmentation	N/A	Image segmentation leads to additional computational resources
Zhu et al. [11]	ANN, minutiae	N/A	Precise ridge orientation overhead
Labati et al. [12]	ANN, minutiae	New set of features	Complexity
Bartunek et al. [14]	ANN, minutiae	N/A	Sliding window application, low accuracy
Yang et al. [15]	Fuzzy logic, ANN	High degree of rotation and grayscale invariance	Low accuracy
Kumar and Vikram [16]	Multidimensional ANN	N/A	Low accuracy
Liu et al. [17]	SVM	Low dimensionality	Low accuracy
Li et al. [18]	SVM	N/A	Extremely low accuracy
Kahraman et al. [20]	Orientation maps ANN	N/A	Low accuracy
Zeng et al. [21]	Deep neural nets	N/A	N/A
Saponara et al. [22]	Autoencoder based on Convolutional Neural Network	High accuracy	N/A
Elsadai et al. [23]	Stylometry, preprocessing, machine learning	Very high accuracy	Preprocessing and oversampling
Panić et al. [this contribution]	Stylometry, ensemble machine learning	Very high accuracy	N/A

Acknowledgements
The presented study received no external funding. The responsibility for the content of this article lies with the authors.

Conflict of Interests
Authors declare that there is no conflict of interest regarding the publication of this article.

References

[1] Moenssens, A. A. (1971). Fingerprint techniques [by] Andre A. Moenssens. *Chilton Book Co. Philadelphia*, [1st ed.] edition.

[2] Lee, H. C., & Gaensslen, R. E. (2001). Methods of latent fingerprint development. *Advances in fingerprint technology*, 2(105-176), 1.

[3] Adamović, S., Miškovic, V., Maček, N., Milosavljević, M., Šarac, M., Saračević, M., & Gnjatović, M. (2020). An efficient novel approach for iris recognition based on stylometric features and machine learning techniques. *Future Generation Computer Systems*, 107, 144-157.

[4] Furuya, H., Eda, S., & Shimamura, T. (2009). Image restoration via Wiener filtering in the frequency domain. *WSEAS transactions on signal processing*, 5(2), 63-73.

[5] Wang, Y., Hu, J., & Han, F. (2007). Enhanced gradient-based algorithm for the estimation of fingerprint orientation fields. *Applied Mathematics and Computation*, 185(2), 823-833.

[6] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition* (Vol. 2). London: springer.

[7] Lam, L., Lee, S. W., & Suen, C. Y. (1992). Thinning methodologies-a comprehensive survey. *IEEE Transactions on Pattern Analysis & Machine Intelligence*, 14(09), 869-885.

[8] Maček, N., Đorđević, B., Gavrilović, J., & Lalović, K. (2015). An approach to robust biometric key generation system design. *Acta Polytechnica Hungarica*, 12(8), 43-60.

[9] Lalović, K., Maček, N., Milosavljević, M., Veinović, M., Franc, I., Lalović, J., & Tot, I. (2016). Biometric verification of maternity and identity switch prevention in maternity wards. *Acta Polytechnica Hungarica*, 13(5), 65-81.

[10] Xie, R., & Qi, J. (2010, December). Continuous fingerprint image quality estimation based on neural network. In 2010 *International Symposium on Intelligent Signal Processing and Communication Systems* (pp. 1-4). IEEE.

[11] Zhu, E., Yin, J., Hu, C., & Zhang, G. (2005, August). Quality estimation of fingerprint image based on neural network. In *International Conference on Natural Computation* (pp. 65-70). Berlin, Heidelberg: Springer Berlin Heidelberg.

[12] Labati, R. D., Piuri, V., & Scotti, F. (2010, July). Neural-based quality measurement of fingerprint images in contactless biometric systems. In *The 2010 international joint conference on neural networks* (IJCNN) (pp. 1-8). IEEE.

[13] Yong-Xia, L., Jin, Q., & Rui, X. (2010, July). A new detection method of singular points of fingerprints based on neural network. In 2010 3rd *International Conference on Computer Science and Information Technology* (Vol. 1, pp. 301-305). IEEE.

[14] Bartunek, J. S., Nilsson, M., Nordberg, J., & Claesson, I. (2006, November). Neural network based minutiae extraction from skeletonized fingerprints. In *TENCON 2006-2006 IEEE Region 10 Conference* (pp. 1-4). IEEE.

[15] Yang, G., Shi, D., & Quek, C. (2005, May). Fingerprint minutia recognition with fuzzy neural network. *In International Symposium on Neural Networks* (pp. 165-170). Berlin, Heidelberg: Springer Berlin Heidelberg.

[16] Kumar, R., & Vikram, B. D. (2010). Fingerprint matching using multi-dimensional ANN. *Engineering Applications of Artificial Intelligence*, 23(2), 222-228.

[17] Liu, L., Tan, T., & Zhan, Y. (2008, December). Based on SVM automatic measures of fingerprint image quality. In 2008 *IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application* (Vol. 1, pp. 575-578). IEEE.

[18] Li, J., Yau, W. Y., & Wang, H. (2008). Combining singular points and orientation image information for fingerprint classification. *Pattern Recognition*, 41(1), 353-366.

[19] Alias, N. A., & Radzi, N. H. M. (2016, May). Fingerprint classification using support vector machine. In 2016 *Fifth ICT International Student Project Conference* (ICT-ISPC) (pp. 105-108). IEEE.

[20] Kahraman, N., Cam Taskiran, Z. G., & Taskiran, M. (2018). Novel feature extraction methodology with evaluation in artificial neural networks based fingerprint recognition system. *Tehnički vjesnik, 25(Supplement 1)*, 112-119.

[21] Zeng, F., Hu, S., & Xiao, K. (2019). Research on partial fingerprint recognition algorithm based on deep learning. *Neural Computing and Applications*, 31(9), 4789-4798.

[22] Saponara, S., Elhanashi, A., & Zheng, Q. (2021). Recreating fingerprint images by convolutional neural network autoencoder architecture. *IEEE Access*, 9, 147888-147899.

[23] Elsadai, A., Adamović, S., Šarac, M., Saračević, M., & Kumar Sharma, S. (2022). New approach for fingerprint recognition based on stylometric features with blockchain and cancellable biometric aspects. *Multimedia Tools and Applications*, 81(25), 36715-36733.

[24] Sun, Y., Tang, Y., & Chen, X. (2023). A neural network-based partial fingerprint image identification method for crime scenes. *Applied Sciences*, 13(2), 1188.

[25] Biometrics Ideal Test, http://biometrics.idealtest.org

[26] Adamovic, S., Miskovic, V., Milosavljevic, M., Sarac, M., & Veinovic, M. (2019). Automated language-independent authorship verification (for Indo-European languages). *Journal of the Association for Information Science and Technology*, 70(8), 858-871.

[27] Webb, G.I., 2000. Multiboosting: A technique for combining boosting and wagging. *Machine learning*, 40(2), pp. 159-196.

[28] Witten, I.H., Frank, E., Hall, M.A. and Pal, C.J., 2016. *Data Mining: Practical machine learning tools and techniques*. Morgan Kaufmann.

[29] Breiman, L., 2001. Random forests. *Machine learning*, 45(1), pp. 5-32.

[30] Prokhorenkova, L., Gusev, G., Vorobev, A., Dorogush, A.V. and Gulin, A., 2018. CatBoost: unbiased boosting with categorical features. In *Advances in Neural Information Processing Systems* (pp. 6638-6648).

[31] Holte, R.C., 1993. Very simple classification rules perform well on most commonly used datasets. *Machine learning*, 11(1), pp. 63-90.

Received: April 29, 2025
Accepted: May 23, 2025

ABOUT THE AUTHORS

Milan Panić was born in Gradiška in 1999. He earned the title of Bachelor of Computer Science and Informatics Engineer in the field of computer security and information protection in July 2023 at the Pan-European University "Apeiron" Banja Luka as a top student with an average of 9.48 out of 10. Since 2021, he has been employed at the Pan-European University Apeiron in Banja Luka as a system administrator, and since 2024 as an assistant in the courses of computer forensics and mobile forensic. He holds a certificate from ISC2 (CC), which confirms his understanding of key principles in the field of cybersecurity, including network security, data protection and risk management.

Nemanja D. Maček is a senior lecturer at the School of Electrical and Computer Engineering and the full professor at the Faculty of Social Sciences. He also works, as a contractor, for the SECIT Security Consulting and as a senior AI researcher and scientific advisor for several companies. Nemanja graduated from University of Novi Sad in 2006 and received Advanced Security Systems PhD from Singidunum University in 2013. The research of Prof. Maček involves machine learning, pattern recognition and natural language processing applied to information security, as well as biometric systems, cryptology and designing novel security mechanisms. He is a passionate cat lover and a very lousy musician.

Branimir Trekić, Full Professor in Computer Sciences, was born in Ćuprija, Serbia, in 1961. Dr. Trenkić joined the Faculty of Computer Sciences in Belgrade as associate professor in 2011. In 2013 he became a full professor at the Faculty of Computer Sciences and in 2016 he joined the School of Electrical and Computer Engineering of Applied Studies. Throughout his career, he has authored numerous impactful publications in peer-reviewed journals, contributing valuable insights to the scientific community, projects etc. Area of work: performance analysis of communication networks, high-performance systems (HPC), IoT, queueing strategies for communication networks, software development and testing.

Daniel Menićanin, a student at the Faculty of Information Technology specializing in Programming and Software Engineering at Paneuropean University Apeiron, is an innovator recognized for developing groundbreaking solutions. In recognition of his exceptional contributions to education, science, and the arts, Daniel received the Plaque of the City of Banja Luka. He was also awarded the prestigious Butterfly Innovation Award in the Youth category, presented by the Regional Cooperation Council. Currently, Daniel's research focuses on robotics, industrial machinery, and automation, further advancing his expertise in developing cutting-edge technological solutions.

FOR CITATION

Milan Panić, Nemanja Maček, Branimir Trenkić, Daniel Menićanin, Raw and Noisy Fingerprint Image Classification with Natural Language Processing Techniques and Ensemble Machine Learning Methods, *JITA – Journal of Information Technology and Applications, Banja Luka*, Pan-Europien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 15(2025)1:5-14, (UDC: 37.018.43:004.738.5), (DOI: 10.7251/JIT2501005P), Volume 15, Number 1, Banja Luka, June (1-80), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004