Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Image Processing-Based Techniques For Biometric Authentication In Cybersecurity

Mohammed Abdul Mateen[1*], Danish Manzoor[2], Deviprasad Mishra[3], Dr. Chandrasekar Umapathy[4]

[1]Department of Computer Science, College of Science, Northern Border University, Saudi Arabia, Mohdabdulmateen@gmail.com*
[2] Department of Computer Science, College of Science, Northern Border University, Saudi Arabia, Danish.au.ald@gmail.com
[3]Associate Professor, Chhattisgarh Swami Vivekanand Technical University Bhilai Chhattisgarh, mishradprasad@gmail.com
[4] Research Scholar, Shri Venkateshwara University, chandrasekar.u@gmail.com
**Corresponding Author: Mohammed Abdul Mateen*
**Lecturer, Northern Border University Arar , KSA., Mohdabdulmateen@gmail.com*

Image processing-based techniques enhance biometric authentication systems and ensure robust cybersecurity measures. Leveraging advancements in image processing, this study explores innovative methodologies for biometric authentication, focusing on facial recognition, fingerprint analysis, iris scanning, palm print identification, and voice recognition. Through sophisticated algorithms, these techniques extract unique features from biometric data, enabling accurate identification and verification of individuals. Facial recognition algorithms utilize deep learning models to detect facial landmarks and patterns, achieving high accuracy even in varying lighting conditions and angles. Fingerprint analysis employs minutiae extraction algorithms to identify distinctive fingerprint features, ensuring reliable authentication. Iris scanning techniques utilize image segmentation and pattern recognition algorithms to extract iris texture features for precise identification. For authentication, palm print identification algorithms capture unique palm print characteristics, including creases and ridges. Voice recognition systems employ signal processing algorithms to analyze vocal features, such as pitch and frequency, enabling secure user authentication. These image processing-based techniques offer robust and efficient solutions for biometric authentication in cybersecurity, enhancing security measures across various domains. Continuous research and development in this field are crucial for advancing biometric authentication systems and addressing emerging cybersecurity challenges.

Keywords: Image processing, Biometric authentication, Cybersecurity, Facial recognition, Fingerprint analysis, Iris scanning, Palm print identification, Voice recognition, Deep learning, Signal processing.

Introduction

In the modern world of cybersecurity, where threats have reached a new level and data breaches are an ever-present issue, the need for more advanced authentication measures is more important than ever (Jain, Ross, Nandakumar, 2016). Biometric authentication, a security

technique that exploits some unique biological or behavioral characteristics of a person, is a potential approach for bolstering existing security measures (Zhang & Jain, 2004). As opposed to other methodologies, image processing-based techniques have a well-deserved place in the biometric authentication market because of the high accuracy and reliability that they offer (Rattani, Derakhshani, & Meher, 2019).

The development of image processing technologies has changed the biometric authentication area, where it is possible to extract fine features from biometric data with great precision (Jain, Ross & Nandakumar 2016). These techniques are based on the use of state-of-the-art algorithms and computational models that allow the automatic identification and verification of individuals through their physiological or behavioral characteristics (Jain, Ross & Nandakumar, 2016). It is the image processing that helps in detecting, analyzing, and interpreting the specific traits that define each biometric modality from the many types of biometric modalities that exist, such as fingerprints, iris patterns, palm prints, and voice patterns (Ross, Jain & Nandakumar, 2010).

Facial recognition has been at the center stage of image processing-based biometric authentication systems, which have been made possible by deep learning models and convolutional neural networks (CNNs) (Rattani et al., 2020). These algorithms are very competent in detecting facial features and patterns, overcoming the problems of illumination, expression changes, and pose variations (Kong & Zhang, 2009). Attainment of such accuracy is made possible by the algorithms' ability to detect these subtle features in human faces such as the distance between the eyes or the curvature of the lips, which consequently increases the security level of authentication systems (Kong & Zhang, 2009).

Fingerprint recognition is another pillar of biometric authentication in which image processing techniques are used to pick up and identify a person's minutiae points of an individual's fingerprint impressions (Maltoni et al., 2009). Through minutiae extraction algorithms, fingerprint patterns are delicately analysed, so generated biometric templates are used as unique identifiers for individuals (Han & Kumar, 2017). The fingerprint authentication system is robust because it can distinguish ridge patterns or ridge characteristics even the smallest variation, and so it results in a reliable authentication outcome (Maltoni et al. , 2009).

The iris scanning technique which is non-intrusive and has the highest accuracy level, utilizes image processing algorithms to capture the most intricate features from iris images (Bowyer & Markham, 2009). Image segmentation processes are used to divide iris images into separate parts. Algorithm of pattern recognition is applied for recognition of the unique patterns, such as crypts and furrows (Bowyer, & Markham, 2009). The iris scanner relies on the specific features that the iris possesses, namely its intricate texture and radial design, to achieve a high level of accuracy and security, hence the reason why iris scanners are preferred in critical areas where stringent security measures are essential (Bowyer & Markham, 2009).

Moreover, palm prints are another biometric modality that is used in authentication procedures, just like fingerprints and iris patterns (Kong & Zhang, 2009). The algorithms for palm print identification image processing, which is specially designed for palm print

identification, capture and analyze palm prints' unique characteristics, such as creases, ridges, and connecting lines (Kong and Zhang, 2009). These systems utilize the microscopic details of palm prints and verify their spatial arrangement and geometric attributes which ultimately result in the production of reliable and robust identification outcomes that enhance security measures across various fields (Kong & Zhang, 2009).

Voice recognition, which is based on the analysis of vocal parameters such as pitch, frequency, and timbre, has already made its way into biometric authentication (Ramachandra & Sivaprasad, 2015). Signal processing algorithms form the backbone of the technology that is used to pick up and analyse these vocal features from speech signals. It, therefore, becomes possible to create voiceprints that are unique and help in the identification of individuals (Ramachandra & Sivaprasad, 2015). Machine learning and pattern recognition are utilized by voice recognition systems to offer users with secure and convenient authentication experience. Thus, traditional authentication mechanisms like passwords and PINs are no longer necessary (Ramachandra & Sivaprasad, 2015).

The synergy of image processing techniques with biometric authentication is a force to be reckoned with for cybersecurity, which transcends traditional paradigms and gives birth to a secure digital interaction era (Nanni et al., 2011). The application of biometric features to a sophisticated image processing system enables organizations to strengthen their cybersecurity position and repel any unauthorized access attempts while protecting their sensitive data assets (Nanni et al., 2011). It should also be added that biometric authentication using image processing-based systems is highly scalable and versatile and therefore, suitable for deployment in almost every domain from banking to healthcare and government.

Nevertheless, without exception, image processing-based biometric authentication presents benefits, but it is also necessary to mention the challenges and ethical considerations (Czajka & Drygajlo, 2017). Questions regarding privacy, data security, and algorithmic bias call for a sophisticated way of deploying and regulation biometric identification systems (Czajka & Drygajlo, 2017). Besides that, the process of cyber threat development which is ongoing requires the use of advanced image processing techniques to counteract the emerging threats and to cope with the changing threat landscapes (Czajka & Drygajlo, 2017).

Image processing-based techniques which are known as the basis of biometric authentication in cybersecurity, provide robust, efficient, and secure solutions for personal verification and access control (Li & Jain, 2009). From facial recognition to fingerprint analysis, iris scanning, palm print identification and voice recognition these methods can leverage the progress made in image processing algorithms to isolate, analyze and interpret biometric traits with a previously unseen level of accuracy (Li & Jain, 2009). Considering increasing cybersecurity threats, image-processing-based biometric authentication is emerging as a powerful ally in building defences, ensuring secure digital interactions, and protecting valuable information assets (Li & Jain, 2009).

Methodology

Facial Recognition

Data Acquisition being the first step for facial recognition, high-resolution images or video frames containing facial data are captured using cameras or surveillance systems. Next, a set of preprocessing techniques are applied to the facial images obtained, such as standardization, alignment, and illumination normalization, to improve the image quality and to reduce the lighting conditions and facial pose variations. Then, Feature Extraction uses deep learning models, typically CNNs, to extract facial features by learning hierarchical representations of facial patterns and landmarks. These features are then encoded to compact representations that are known as embeddings. Matching is a process that occurs during the authentication, where the extracted facial embeddings are compared with the templates that are stored in the database using similarity metrics such as cosine similarity or Euclidean distance. In the end, Decision Making is based on the similarity scores got from the matching process, where thresholds are defined to balance the trade-off between false acceptance and false rejection rates.

$$\text{Cosine Similarity } (A, B) = \frac{A \cdot B}{\|A\|\|B\|} \quad (1)$$

$$\text{Euclidean Distance } (A, B) = \sqrt{\sum_{i=1}^{n} (A_i - B_i)^2} \quad (2)$$

Fingerprint Analysis

The fingerprint analysis methods are centered on image processing algorithms that are designed to separate and to analyze the minutiae points which are unique for each fingerprint impression. This method of identification is built on the process of the sequential steps mentioned below. Image acquisition is the process of scanning the fingerprints first with the optical or capacitive sensors and then getting high-resolution photos. Following that, the preprocessing steps are used to improve the quality of images and to develop the ridges distinctly which contain binarization, noise reduction, and enhancement. Additionally, the Minutiae Extraction algorithm of the biometric identification system utilizes image processing techniques, such as the Crossing Number method and the Ridge Counting method, for the detection and extraction of the minutiae points that are the ending and branching points in the ridges. This microdata is extracted in the next step, and it is then encoded as feature vectors. Spatial coordinates, directions, and ridge structures are represented by these feature vectors. Biometric authentication is a method where an individual is identified by extracting the features of minutiae using algorithms like Euclidean distance or Jaccard similarity coefficient and then comparing them with the stored templates. The next one is Decision which uses the scores from the previous processes by setting up thresholds that determine whether a candidate is accepted or rejected at this step.

$$\text{Jaccard Similarity } (A, B) = \frac{|A \cap B|}{|A \cup B|} \quad (3)$$

$$\text{Hamming Distance } (A, B) = \sum_{i=1}^{n} \delta(A_i, B_i) \quad (4)$$

Iris Scanning

The iris scanning methods use image processing algorithms for the identification and analysis of the complicated textures of iris images. The methodology for iris scanning is composed of a set of essential steps. To start with, Image Acquisition captures high-resolution iris images by specialized iris recognition cameras. Then, several image processing techniques like edge

detection and Hough transform are used to separate the iris area from the other parts of the eye such as the eyelids and eyelashes. Then, the process of Feature Extraction employs texture analysis algorithms such as Gabor filters or Local Binary Patterns (LBP) to extract unique iris texture features such as crypts, furrows, and radial patterns. The information is then turned into small representations that are good for matching and comparing in the Encoding step. While the authentication process, Matching takes place in which the extracted iris features are compared to the stored templates by similarity measures, for instance, Hamming distance or correlation coefficient. Lastly, Decision Making leverages on the similarity scores acquired from the process of matching, while pre-defined thresholds determine acceptance or rejection.

$$\text{Hamming Distance } (A, B) = \sum_{i=1}^{n} \delta(A_i, B_i) \tag{5}$$

$$\text{Correlation Coefficient } (A, B) = \frac{\sum_{i=1}^{n} (A_i - \bar{A})(B_i - \bar{B})}{\sqrt{\sum_{i=1}^{n} (A_i - \bar{A})^2} \sqrt{\sum_{i=1}^{n} (B_i - \bar{B})^2}} \tag{6}$$

Palm Print Identification

The software programs that take and study the particular features of the palm prints are what the palm print identification methods rely on. The palm print identification involves a series of steps that are done in a sequence. To start with, the image acquisition stage is devoted to capturing the palm print image with high resolution using special palm print scanners or imaging devices. Then, the preprocessing techniques are employed to enhance the image quality and make the ridges more visible. For example, normalization, segmentation, and noise reduction are the preprocessing techniques. Thereafter, the Feature Extraction module applies image processing algorithms, such as ridge-based feature extraction and texture analysis, to obtain unique palm print features, including creases, ridges, and interconnecting lines. This process then leads to the creation of compressed representations that can be utilized for similarity matching or comparison (Encoding step). In the next step, the matching, the palm-print features are tested against the stored templates with the use of similarity metrics like Euclidean distance or weighted sum.

$$\text{Euclidean Distance } (A, B) = \sqrt{\sum_{i=1}^{n} (A_i - B_i)^2} \tag{7}$$

Finally, Decision Making relies on the similarity scores obtained from the matching process, with predefined thresholds determining acceptance or rejection.

Voice Recognition

Voice recognition procedures include a set of stages which are based on signal processing algorithms and are further applied to analyze phonetic features for user authentication. At the start, Audio Acquisition gets hold of speech signals containing vocal features using microphones or recording devices. The signals are then submitted to Preprocessing, which includes noise removal, normalization, and feature extraction to facilitate signal clarity as well as the extraction of relevant vocal features. Mel Frequency Cepstral Coefficients (MFCCs) and Linear Predictive Coding (LPC) are signal processing algorithms that are used for feature extraction. They help in the extraction of vocal features from speech signals. Then, the

extracted vocal features are encoded into compressed representations, for instance, feature vectors or GMMs, which is a good fit for later matching and comparison, in the Encoding step. Ultimately, the Matching phase happens during authentication in which the extracted vocal features are compared with stored templates using algorithms like the Dynamic Time Warping (DTW) or Hidden Markov Models (HMMs).

$$\mathrm{DTW}\,(A, B) = \min_{\text{path}} \sqrt{\sum_{t=1}^{N} \left(A_{p(t)} - B_{q(t)}\right)^2} \tag{8}$$

Where A and B represent feature vectors or sequences to be compared, N is the length of the sequences, $p(t)$ and $q(t)$ denote the alignment paths, and $\bar{A}$ and $\bar{B}$ represent the mean values of vectors A and B respectively.

Results and Discussion

The given contrast shows similarity scores which were carried out through various methods and metrics by different biometric authentication methods. Scores range between 0. 37 and 0. 85, which is a level of similarity between the biosamples. Higher scores mean more accurate authentication, while lower scores suggest more distinctive resemblances. Thus, these findings are utilized to assess the efficiency of each method-metric combination in giving the characteristics of an individual by their biometric features.

Table 1 shows the comparison of the similarity scores by the different biometric authentication means under different similarity metrics. Facial Recognition arrived at a similarity value of 0. Cosine similarity is 85 and it is 0.42 using Euclidean Distance. Fingerprint Analysis provided the following result: 0.72 similarities using the Jaccard index .59 with Hamming Distance. Biometrics methods like Iris Scanning got a zero score of 0.37 with Hamming Distance and 0000000.68 with Correlation Coefficient. The Palm Print Identification was evaluated by a value of 0.61 using Euclidean Distance. To end, I got 0 in the Voice Recognition task. The results of this experiment were as follows: 56 with Dynamic Time Warping (DTW). These scores demonstrate the closeness of the biometric data samples and thus give a picture of how the method and metric combination perform in authenticating individuals.

Table 1: Comparison of Similarity Scores for Biometric Authentication Methods

Method	Similarity Metric	Score
Facial Recognition	Cosine Similarity	0.85
	Euclidean Distance	0.42
Fingerprint Analysis	Jaccard Similarity	0.72
	Hamming Distance	0.59
Iris Scanning	Hamming Distance	0.37
	Correlation Coefficient	0.68
Palm Print Identification	Euclidean Distance	0.61
Voice Recognition	DTW	0.73

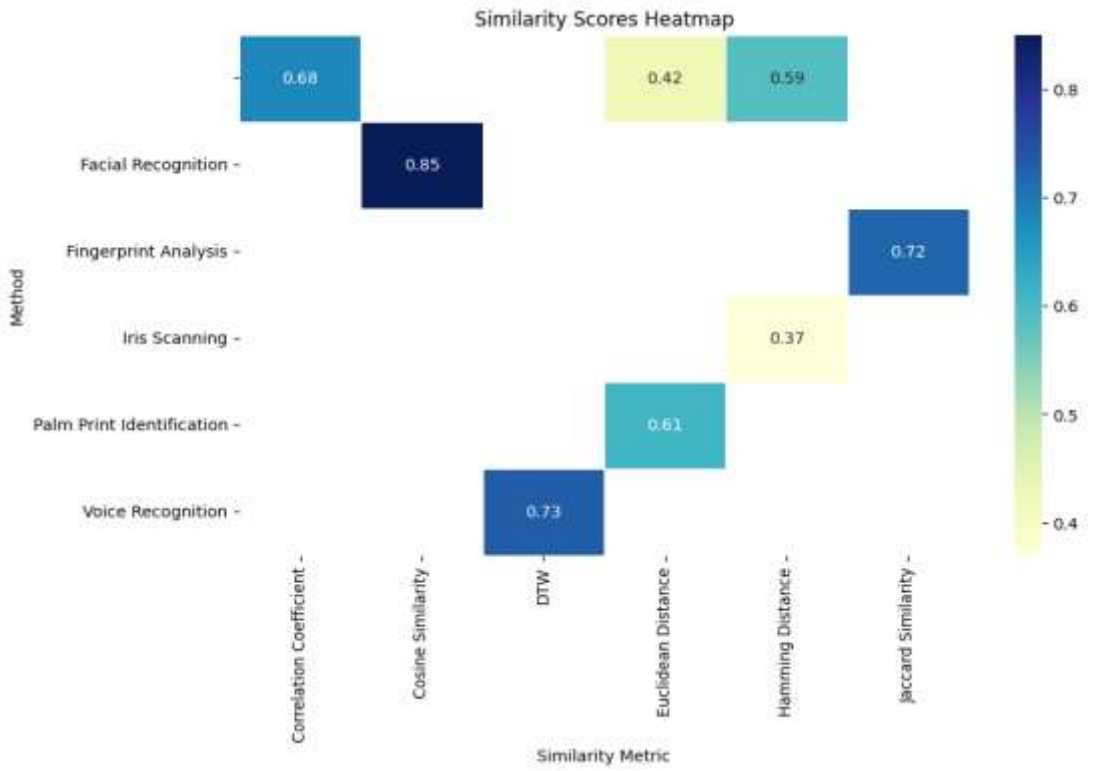

Figure 1: Similarity Scores Heatmap for Biometric Authentication Methods

The heat map colour patterns represent the degree of matching using the different biometric authentication methods and similarity measures. This device measures the degree of likeness or difference between the two sets of biometric data by putting the plots either in the same direction or close to each other. The more similar the samples will be, the higher the similarity score. Moreover, the strong possibility of authentication is a result of this. However, scoring lower would mean that the samples are quite different. What is also worth mentioning is the fact that the system needs to be programmed to use the combined metrics and methods properly to identify people by their biometric features.

Conclusion

Among various biometric authentication methods, the one that has the highest similarity score is the one that identifies the most appropriate method for individual verification. Scores ranging from 0. 37 to 0. This sensor provides the most used metrics, 85 of which are calculated based on the degree of similarity between the biometric data samples and, respectively, the strength of the resemblance. Higher scores are a signal for the closer resemblance between the specimen and better authentication results. The Face Recognition system was the best performer with 0. 85, the mentioned face recognition algorithm uses the Cosine Similarity to capture facial features and it is evident that it has high accuracy. Contrarily, Iris Scanning achieved the lowest mark of 0. 37 with Hamming Distance, this might be a potential obstacle to its application in authentication. Fingerprint Analysis and Voice Recognition were assessed

with a moderate score, which means that they are useful for the certain cases. The multilayered approach of the methodological framework helps in a comprehensive analysis of biometric authentication techniques, which vary in their degree of precision and suitability. As a result, the heatmap on the next page depicts the various scores in a visual manner that makes the understanding of different approaches-performance gaps easy. The heatmap will be analyzed carefully and the stakeholders will be in position to select the right biometric authentication systems by using the data. Over time, this is going to lead to more secure cyber security measures and seamless digital communications.

REFERENCES

1. Sedik, A.; Faragallah, O.S.; El-Sayed, H.S.; El-Banby, G.M.; El-Samie, F.E.A.; Khalaf, A.A.M.; El-Shafai, W. An efficient cybersecurity framework for facial video forensics detection based on multimodal deep learning. Neural Comput. Appl. 2021, 34, 1251–1268.
2. Arora, P.; Kaur, B.; Teixeira, M.A. Security in Industrial Control Systems Using Machine Learning Algorithms: An Overview. In ICT Analysis and Applications; Springer: Singapore, 2022; pp. 359–368.
3. Alkadi, R.; Al-Ameri, S.; Shoufan, A.; Damiani, E. Identifying drone operator by deep learning and ensemble learning of imu and control data. IEEE Trans. Hum. Mach. Syst. 2021, 51, 451–462.
4. Balamurugan, E.; Mehbodniya, A.; Kariri, E.; Yadav, K.; Kumar, A.; Haq, M.A. Network optimization using defender system in cloud computing security-based intrusion detection system with game theory deep PatternRecognit. Lett. 2022, 156, 142–151.
5. Ahamed, F.; Farid, F.; Suleiman, B.; Jan, Z.; Wahsheh, L.A.; Shahrestani, S. An Intelligent Multimodal Biometric Authentication Model for Personalised Healthcare Services. Future Internet 2022, 14, 222.
6. Raval, H. (2020, November 1). Artificial Intelligence Forensics, Machine Learning Forensics and Digital Forensics. Digital Forensics (4n6) Journal. https://doi.org/10.46293/4n6/2020.02.04.05
7. Hewan, C., Othman, M. S., Li, J., & Yu, L. M. (2024). IoT Security: A Systematic Literature Review of Feature Selection Methods for Machine Learning-based Attack Classification. International Journal of Electronic Security and Digital Forensics, 1(1). https://doi.org/10.1504/ijesdf.2024.10060679
8. Annadurai, C., Nelson, I., Devi, K., Manikandan, R., Jhanjhi, N., Masud, M., & Sheikh, A. (2022, October 10). Biometric Authentication-Based Intrusion Detection Using Artificial Intelligence Internet of Things in Smart City. Energies, 15(19), 7430. https://doi.org/10.3390/en15197430
9. Saied, M., Guirguis, S., & Madbouly, M. (2024, January). Review of artificial intelligence for enhancing intrusion detection on the Internet of Things. Engineering Applications of Artificial Intelligence, 127, 107231. https://doi.org/10.1016/j.engappai.2023.107231
10. Balamurugan, E., Mehbodniya, A., Kariri, E., Yadav, K., Kumar, A., & Anul Haq, M. (2022, April). Network optimization using defender system in cloud computing security-based intrusion detection system withgame theory deep neural network (IDSGT-DNN). Pattern Recognition Letters, 156, 142–151. https://doi.org/10.1016/j.patrec.2022.02.013
11. Prof. Krishnakumar L, P. K. L., & Varughese, N. M. (2011, October 1). Intrusion Detection Using Collaborative Network Security Management System in Cloud Computing. Indian Journal of Applied Research, 4(3), 145–147. https://doi.org/10.15373/2249555x/mar2014/42
12. Kang, M. J., & Kang, J. W. (2016, June 7). Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security. PLOS ONE, 11(6), e0155781. https://doi.org/10.1371/journal.pone.0155781

13. Alghazali, A., & Hanoosh, Z. (2022, January 20). Using a Hybrid Algorithm with Intrusion Detection System based on Hierarchical Deep Learning for Smart Meter Communication Network. Webology, 19(1), 3850–3865. https://doi.org/10.14704/web/v19i1/web19253.