Biometric Authentication System For Access Control

Jaimit Patel, Anubhav, Ayush Kumar Singh, Rachit Kumar Tiwari, Abhi Singh and Bhupinder Kaur*

School of Computer Science and Engineering, Lovely Professional University Phagwara, Punjab, India

Abstract

Biometric Authentication System isacrucialneed in everyday security protocols, providing reliability through security and efficiency for identity verification. This paper introduces a comprehensive framework for fingerprint recognition within system addressing the critical challenges like rotation, scaling variations, noise, and distortions efficient in large datasets, accuracy, real-time performance, and reliability.Capitalizing on fingerprint scanner, captured templates are stored in database securely and matched with Python libraries. AES-256 encryption is applied to store templates and enhances protection against unauthorized access. Testing is conducted using various dataset sources like Kaggle, all-inclusive various fingerprint variation and noise levels. The proposed system demonstrates robustness, achieving the accuracy of 58% to 98% across different conditions. The efficiency of the algorithm ensures scalability even when processing the large dataset with real-time performance.

Keywords

Biometric Authentication, Access Control, Data Security, Biometric Authentication, Fingerprint Recognition

1. Introduction

Physical access security to restrict areas is one of the topmost priorities for an business, organizations and personal space. Currently available methods like key cards, RFID cards and simple pin passwords are vulnerable to loss, theft, cloning and unauthorized sharing. Biometric authentication offers a secure alternative which utilizes biometric signatures and components like face recognition, fingerprint recognition, retinal scan etc. This research paper will talk about how we created a fingerprint scanner and a matching algorithm for security access control. The components which are used to create fingerprint scanner are, R307 Optical fingerprint reader which is utilized to extract and verify human fingerprint data. This data, along with other user information, was collected by the ESP8266 Wi-Fi Module and transmitted over the internet to a designated destination which can be a cloud or a drive with connected network. A 0.96" I2C OLED Display is used to display the data. The system uses the Python environment and libraries for real-time fingerprint matching to grant access. The images captured by scanner

ACI'23: Workshop on Advances in Computational Intelligence at ICAIDS 2023, December 29-30, 2023, Hyderabad, India

*Corresponding author.

*Corresponding author.

†These authors contributed equally.

†These authors contributed equally.

jaimitpatel.1432@gmail.com (J. Patel); anubhavojha06@gmail.com (Anubhav); ayush9446286@gmail.com (A. K. Singh); rachittiwari03@gmail.com (R. K. Tiwari); abhisinghkirad7@gmail.com (A. Singh); bhupinder.23626@lpu.co.in (B. Kaur)

is compared with templates stored in the database. Access is granted only if a successful match is established with a good score and accuracy. Fingerprint templates stored within the database are encrypted using the latest and secured AES-256 bit encryption, safeguarding sensitive information against unauthorized access or potential breaches. It added an extra layer of security in database of fingerprint and protect the integrity of biometric data and the security of access control system. An open source algorithm is implement for the fingerprint matching algorithm on this biometric authentication for access control work which delivers quick and accurate results. This work utilizes SIFT (Scale Invariant Feature Transform) which is used to detect key points in images that are resistant to changes in size/scale, rotation, and brightness. Key points are just distinctive, or we can say unique location which are different from other points available in the image. It also utilizes Fast Library for Approximate Nearest Neighbours (FLANN) which is used to efficiently find the nearest neighbours between key points between images and for that it provides an accuracy rate about how much confident it is that images are the same or have the same key points. Upcoming sections of this paper will delve deeper into the system design, by outlining the fingerprint reader technology,fingerprint template creation process, and the Python-based fingerprint matching algorithm. Additionally, the paper will discuss the chosen encryption technique and its significance in securing the stored fingerprint data. Finally, the paper will present the results obtained from the system implementation and address potential limitations and future advancements. Several security and video based authentication techniques were proposed by the researchers in the recent years [1, 2, 3, 4].

2. Common Challenges and General Issues

In this section, issues and challenges related to noisy fingerprints and its efficiency are mentioned.

- Rotation and Scaling Variations:Templates which are in database or capture can have rotation of some degree or the scale may be different for each template.
- Noise and Distortions:Template may also contain noises like blurring, fuzziness due to some problems which capturing templates.
- Large Dataset Matching Efficiency:When working with large dataset, if algorithm is not efficient it can make matching process highly computational.
- Accuracy and Reliability: if algorithms are efficient in matching there can be an issue with accuracy and reliability of matching.
- Real Time Performance: there is also an issue with how much time does the whole process takes which is an issue.

3. Review of Literature

In this section literature review is discussed authors have done the work by using different approaches.

Leyu, Z. et.al. [5] came with an idea to implement an RFID access control system, by utilizing both hardware and software components in the work. Biometric recognition technologies like

fingerprint scanners and face recognition is used and highlighted as main aspect. This work integrates biometrics with IC cards while addressing pros and cons regarding data security and privacy. The architecture of work is composed of different modules where each module is designed to perform specific task like Card Issuing module, which is a software design, broken into components such as Face Recognition, Fingerprint Identification, and Windows client. The card reding and verifying uses modules like RFID Input-Output driver, and Voice broadcasting module which complements face and fingerprint recognition. The system employs AES-246 encryption and hardware based password authentication to strengthen data security and mitigating the risks.

Cheng, H. et.al. [6] talked about a plan for getting data in cloud computing. It focuses on keeping things safe by using identity based encryption (IBE) and body measurement checks. It talks about worries on safety of getting data in cloud places and ways to use IBE with ECC and body checks for safety. IBE lets any set of letters be a public key, making it easy to pass keys around and keep things safe. The end point they came to shows that because of growth in wireless talks and body checks, the plan they came up with is doable. Plus, RBAC (Role Based Access Control) is used to show how well it keeps data safe from many dangers.

Anisha Poojary et al. [7] presented a biometric authentication system using the unique vein patterns present in the dorsal hand. the paper shows the limitations of traditional authentication methods by showing enhanced security using hand vein recognition method. For this system authors have used cost effective scanning equipment such as No IR camera and NIR LEDs. These components have ability to capture high quality vein images without direct contact of hand. The paper shows the system's capability to accurately identify individuals based on the unique vein patterns. This feature makes it well suited for a wide range of uses which require strong security measures. In the end authors have given a detailed discussion of the implementation step of the system including camera initialization, image capture, pre-processing operations, and template matching procedures.

Natalya Kharina et al. [8] presented an calculation for selecting palm vein pictures for biometric confirmation frameworks, especially centring on utilizing multidimensional Markov chains. The strategy includes approximating the biometric format picture through a discrete Markov handle and leveraging conditional Markov handle hypothesis. The algorithm follows a number of specified steps. Initially it will be based on the calculation of transition matrices, which analyses local configurations. As a result, for the purpose of determining transition matrix indices, state vectors are established in the neighbourhood. In addition to palm vein authentication, it suggests applications such as riverbed detection or ultrasound image processing. In addition, it points to the algorithms low computational resource requirements and its potential use of precalculated transition matrices in order to further reduce complexity.

Tanya Ignatenko et. al. [9] presents the biometric privacy-authentication system was examined. The system utilized BHC code 13.5dB to introduce fuzzy commitment, but its limitations were attaining optimal privacy leakage. The paper's study recommends using turbo and convoluted codes to improve privacy control. The main emphasis of the practical coding method implementations is the use of vector quantization of the encoder for better trade-offs. Advanced coding techniques need to be implemented to increase privacy protection in biometric authentication systems. Many important elements are needed for needed for footprint recognition, including techniques for extraction, classification, matching, and data storing. It is emphasized

that matching and classifying footprints is highly essential in obtaining a precise biometric identity. Nevertheless, face recognition also concentrates on issues related to face biometric including illumination, body posture, expressions, image quality and more. The paper focuses on the advancements, drawbacks, and applications of biometric recognition technology in various domains like access control systems.

Prashant Johri et al. [10] described that in today's time, strong security measures are essential to tackle the emerging threats of cyber attackers. These attackers are looking for different ways to get into the system and access the data for malicious purpose. The authors also talked about various ideas such as using biometric authentication as a robust security mechanism. The tools such as ID cards, username credentials like password, pin numbers have been in use for a pretty long time now and have been proved to not enough as they can be easily stolen or abused hence we need better alternatives and that's where biometric authentication come into play. Biometric technology is generally based on the psychological or behavioural traits. They are generally used in the form of fingerprints, facial, and eye contour identification. It covers the evolution of biometric technology across time, from earliest used techniques for collecting fingerprints to the most recent deep learning based strategies as well as the integration of ai in this. It also further explores about the new developments happening in this field such as multimodal biometric, global cooperation, and passive biometric data collection. The paper highlights the potential and ongoing progress of biometric authentication system across sectors.

Diptadeep Addy et al. [11] proposed a system of several layers of security to integrate biometrics and GSM communication in vaults. The proposal provides for a system whereby each layer of security is progressively transferred to access the vault, addressing growing concerns about security breaches. The four layers include account username/password matching, facial recognition, fingerprint matching, and One Time Password (OTP) verification through GSM communication. the system uses biometric data, a unique finger impression filter and remote communications. The paper examines the architecture of the framework, its equipment plan and usage, and analyses each organization of confirmation. Furthermore,to improve the accuracy and strength of the system, it recommends possible improvements and adjustments.

R. T. Hans et al. [12] explained about how biometric authentication system can be implemented from vehicle being theft. Due to this aid employment will also be created. This model diagram is important This diagram shows the benefit of implementing this model which Contributing to green computing, Cost effective, Better efficient and effective authentication of vehicle owner After implementing this model Shopping mall owners don't have to worry about vehicle theft, business opportunities will also be created which would develop and buy off-shelf systems. there is only one limitation to this model that is the approval of using such systems at the shopping mall because it deals with the usage of individual private sensitive information which should always be protected. So the usage of this approach should negotiate the perceived privacy.

Spanakis, E.G. et al. [13] described that most of the user authentication in ICT service/systems in application identity tools are passkey/personal identification number(PINs).This idea focuses to overcome weakness and flaws under improved under authentication with high level security and privacy. Speech-Xray's implementation regarding e-Health provided and analyzed report which explores security and privacy issues which offers a comprehensive summary of biometrics technology applications pointing towards the e-Health security challenges. Biometrics

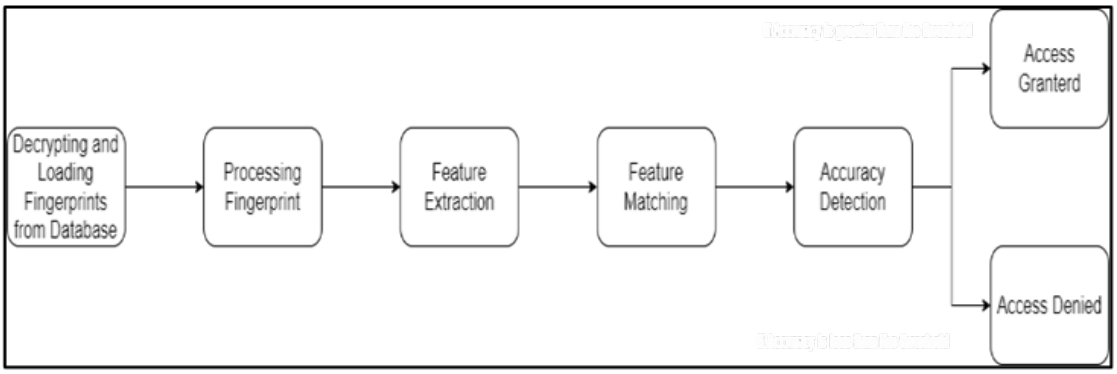

Figure 1: Flow Diagram

authenticates or verifies a person's identity and sorts it in two categories, physiological namely fingerprints, palm print, face and iris recognition, and DNA behavioral namely typing rhythm or voice.These things are also used as supplementary ID cards and passkeys, like communicating an extra level of security like multi factor authentication.Data like these will be stored in template database, placed inside the hospital which will achieve all the required characteristics regarding security, privacy, usability & cost-efficiency.

Z. Ishak et al. [14] experimented about fingerprint biometric systems. These were categorized by small size, ease of use and less power consumption like Apple touch id. If this system is implemented, we can work upon multi-factor authentication plan and improve encryption algorithm. Other biometric system like retina and face recognition not enough researched in depths so there is less trust in uniqueness.This system implements position-based accesses control, develop stronger authentication mechanism. Long-term use will increase security of database and eliminate backdoor entry.There are 3 main problems with this system: first is identification of unauthorized user for access in the absence of any limitation in the security company, next is confidential data might slip out by any intruder since of weak security part, last up is security software to protect internal data which are not carefully unforced. The system reach is divided in two parts: user scope and system scope. In user scopes,users can optimize the data in Secure Biometric Lock System for Files and Applications. Simultaneously, the system scope consists of features in the Biometric Lock System namely login settings and enter control panel. Approaches are modern fingerprint readers, facial recognition, eigen face (black and white) [15] and hand geometry [16].

4. Methodology

This Work is divided into six parts which explain about the hardware components which gives insight about the circuit connection, and algorithms which are used for encryption, decryption, and fingerprint matching. COmplete flow diagram of proposed work is shown in fig. 1.

4.1. First: Integration of Fingerprint Sensor Module:

The integration of a fingerprint sensor module is done with Transistor-Transistor Logic (TTL) Universal Asynchronous Receiver-Transmitter(UART) interface for direct connections to microcontroller UART or to a PC through MAX232 / USB-Serial adapter. Module diagram is shown in figure 2. This module allows users to store fingerprint data and configure it in 1:1 or 1:N mode for identifying individuals. The fingerprint sensor is flexible and suitable for applications like marking attendance, safety boxes and securing devices like car doors and monitoring applications. It can interface directly with any microcontroller or Arduino board.The complete setup and module structure are shown in Fig. 2 and Fig. 3. The fingerprint sensors used in the IoT setup have the following functions:

Table 1
IoT Modules

Parameter	**Value**
Sensor Type	Optical
Sensor Lifespan	100 million scans
ESD Protection	15KV
Backlight	Bright green
Interface	USB1.1/UART (TTL Logical level), RS232
Communication Baud Rate	4800BPS 115200BPS (adjustable)
Dimensions	55 x 32 x 21.5mm
Image Capture Surface	15-18(mm)
Verification Speed	0.3 seconds
Scanning Speed	0.5 seconds
Character File Size	256 bytes
Template Size	512 bytes
Storage Capacity	250
Security Level	5 (ranging from 1 to 5, highest being 5)
False Acceptance Rate	0.0001%
False Rejection Rate	0.1%
Resolution	500 DPI
Voltage	3.6-6.0 VDC
Working Current	Typical: 90mA, Peak: 150mA
Matching Method	1: N
Operating Temperature	-20 to 45 degrees Celsius

A thin, multilayered organic film is positioned between an anode and a cathode to create the self-emitting OLED (Organic Light-Emitting Diode) technology. OLED is thought to be the next-generation technology for flat-panel displays since it doesn't require a backlight like LCD technology does. It also offers great application potential for a variety of display kinds.

4.2. Second: Data Encryption:

This step involves encryption of the images which are being taken for the censors. The algorithm used for this is AES-256. By creating a key with random generation, we generate a secure key,

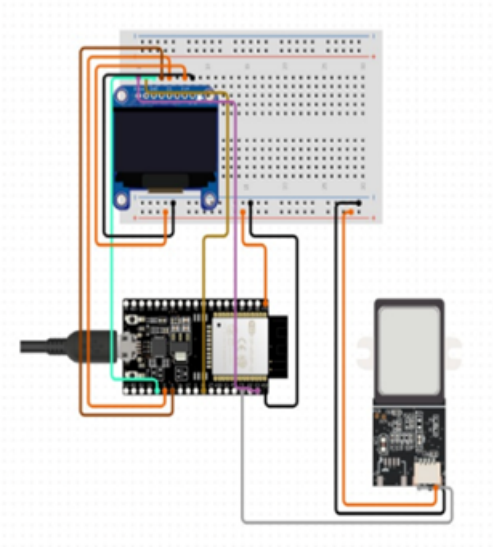

Figure 2: Module Diagram

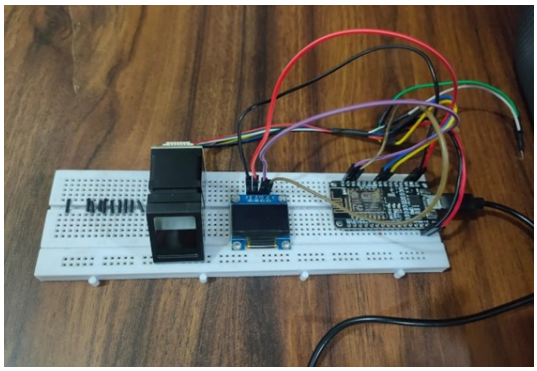

Figure 3: Practical implementation

and when the incoming data is received it gets encrypted by the program and then stored in the database.

4.3. Third : Database Access and Decryption

By using AES-256decryption we can access data from the database. It requires a stored and protected key which is used for both encryption and decryption.

4.4. Fourth: Fingerprint Processing:

This step involves improving the quality of images, as in size formatting or removing some blurriness, and lastly applying grayscale conversion as shown in Fig. 4.

Figure 4: Grayscale and Resized Fingerprint

Figure 5: FLANN based matching

4.5. Fifth: Fingerprint Loading and Extracting Features:

By using Pythons OS module we will move to the directory where all the fingerprints are stored, and we will store location in a variable which will hold the paths. After this we will extract all the features using SIFT (Scale Invariant Feature Transformation) by using SIFT create() function, It will detect all the features like, Scale invariance: SIFT detects features at multiple scales within an image. Rotation invariance: SIFT descriptors are invariant to image rotation.

4.6. Sixth: Matching Features:

By initializing a FLANN (Fast Library for Approximate Nearest Neighbours) matcher with proper parameters, the Matched fingerprint function will match by using Knn-Match method. This method finds the two nearest neighbours (key points) for each descriptor in the query image within the database descriptors, as shown in the Fig. 5.

5. Results

The Sift descriptors are used to determine accuracy of the system. These photos depict various fingerprints with different types of variations and noises as shown in fig. 6, fig. 7 and fig. 8. The

Figure 6: Fingerprint with Rotational Region

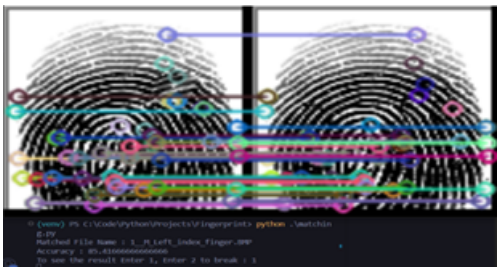

Figure 7: Fingerprint with Z-cut Region

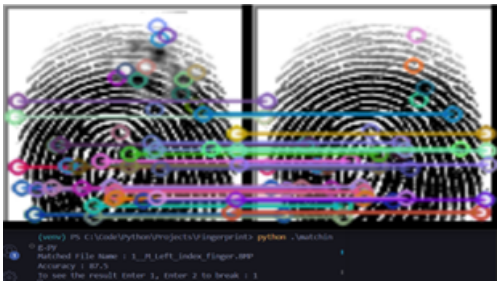

Figure 8: Fingerprint with Faded Region

purpose of this study, which deal with both security aspects of fingerprint and noise cancellation. More than 17,000 photos are used in the testing process to ensure that it can withstand large dataset and gives good accuracy. The resultant accuracy varied from 58% to 98% according to level of noise present in the image. If the image is in perfect condition and without any noise the resultant accuracy comes in the range of 89% to 99% depending upon the level of noise in the fingerprint image.

By using OpenCV's Euclidean distance method we got different results when matching fingerprints. As shown in Fig. 9. The time taken by Euclidean distance is much shorter when compared to SIFT+FLANN matching and as the number of templates increases this time of matching also increases.

SIFT+FLAAN based matching comes into highlight when we talk about accuracy as shown in Fig. 10. Not only SIFT+FLAAN is good with accuracy as compared to others, but it also tackles

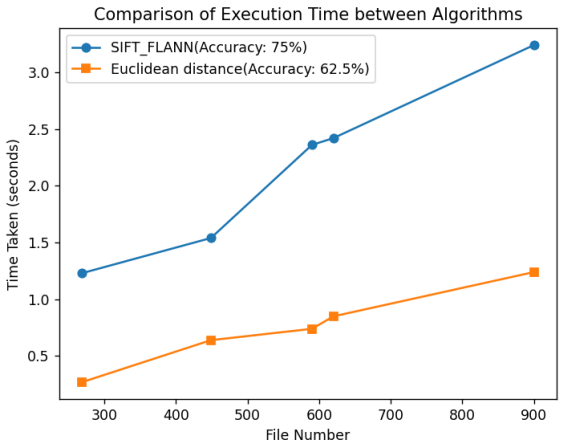

Figure 9: Time Execution graph between Algorithms

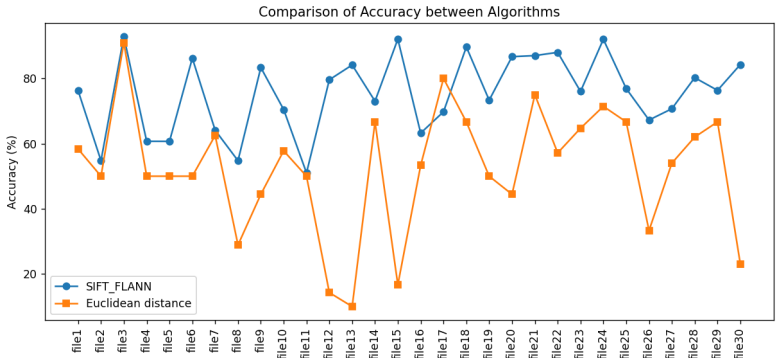

Figure 10: Accuracy graph between Algorithms

images with noises preset with it which makes this algorithm a little bit time consuming.

6. Conclusion

The Fingerprint Scanner and Matching is a technique which is used by multiple organizations in their daily life for adding a layer of security. Increased number of crimes has made people more aware about security and risks associated with it. In this work, with low computational complexity, faster matching and with relatively good accuracy, this model can be helpful in security.With the help of image processing techniques which are available in open source helped this work to be more secure. The resultant product can detect images with rotation (Fig 6), noises(Fig 7),blurriness(Fig 8) with good accuracy.

References

[1] G. Kaur, P. Agrawal, Optimisation of image fusion using feature matching based on sift and ransac, Indian Journal of Science and Technology 9 (2016) 47.

[2] V. Madaan, D. Sethi, P. Agrawal, L. Jain, R. Kaur, Public network security by bluffing the intruders through encryption over encryption using public key cryptography method, in: Advanced Informatics for Computing Research: First International Conference, ICAICR 2017, Jalandhar, India, March 17–18, 2017, Revised Selected Papers, Springer Singapore, 2017, pp. 249–257.

[3] S. Chauhan, P. Agrawal, V. Madaan, E-gardener: building a plant caretaker robot using computer vision, in: 2018 4th International Conference on Computing Sciences (ICCS), IEEE, 2018, pp. 137–142.

[4] N. Bhadwal, V. Madaan, P. Agrawal, A. Shukla, A. Kakran., Smart border surveillance system using wireless sensor network and computer vision, in: International Conference on Automation, Computational and Technology Management (ICACTM - 2019), https://ieeexplore.ieee.org/document/8776749, 2019, pp. 183–190.

[5] Z. Leyu, Z. Xinyou, F. Yunjia, L. Shuyao, B. Jun, H. Xijia, Design and implementation of rfid access control system based on multiple biometric features, in: 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), IEEE, 2021, pp. 570–575.

[6] H. Cheng, C. Rong, Z. Tan, Q. Zeng, Identity based encryption and biometric authentication scheme for secure data access in cloud computing, Chinese Journal of Electronics 21 (2012) 254–259.

[7] A. Poojary, A. Chourasiya, K. Jha, S. Ranbhise, Biometric authentication system using dorsal hand vein pattern, in: 2020 International Conference on Convergence to Digital World-Quo Vadis (ICCDW), IEEE, 2020, pp. 1–3.

[8] N. Kharina, A. Zemtsov, S. Chernyadyev, Algorithm of palm vein image selection for biometric authentication systems based on multidimensional markov chain, in: 2023 25th International Conference on Digital Signal Processing and its Applications (DSPA), IEEE, 2023, pp. 1–5.

[9] T. Ignatenko, F. M. Willems, Privacy-leakage codes for biometric authentication systems, in: 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2014, pp. 1601–1605.

[10] P. Johri, M. S. Arora, Review of the issues and a thorough investigation of biometric authentication systems, in: 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), IEEE, 2022, pp. 892–897.

[11] D. Addy, P. Bala, Physical access control based on biometrics and gsm, in: 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE, 2016, pp. 1995–2001.

[12] R. T. Hans, Using a biometric system to control access and exit of vehicles at shopping malls in south africa, in: 2014 4th International Conference on Engineering Technology and Technopreneuship (ICE2T), IEEE, 2014, pp. 148–151.

[13] E. G. Spanakis, M. Spanakis, A. Karantanas, K. Marias, Secure access to patient's health records using speechxrays a mutli-channel biometrics platform for user authentication,

in: 2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), IEEE, 2016, pp. 2541–2544.

[14] Z. Ishak, N. Rajendran, O. I. Al-Sanjary, N. A. M. Razali, Secure biometric lock system for files and applications: a review, in: 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), IEEE, 2020, pp. 23–28.

[15] P. Agrawal, R. Kaur, V. Madaan, M. S. Babu, D. Sethi, Moving object detection and recognition using optical flow and eigen face using low resolution video, Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science) 13 (2020) 1180–1187.

[16] S. K. Singh, M. Sharma, P. Agrawal, V. Madaan, A. Dhiman, Expar: A fuzzy rule based expert system for palmistry 9 (2016) 5207– 5214.

[17] J. I. Bhat, R. Yousuf, Z. Jeelani, O. Bhat, An insight into content-based image retrieval techniques, datasets, and evaluation metrics, in: Intelligent Signal Processing and RF Energy Harvesting for State of art 5G and B5G Networks, Springer, 2024, pp. 127–146.

[18] R. T. Hans, Using a biometric system to control access and exit of vehicles at shopping malls in south africa, in: 2014 4th International Conference on Engineering Technology and Technopreneuship (ICE2T), IEEE, 2014, pp. 148–151.

[19] R. J. Tazim, M. M. M. Miah, S. S. Surma, M. T. Islam, C. Shahnaz, S. A. Fattah, Biometric authentication using cnn features of dorsal vein pattern extracted from nir image, in: TENCON 2018-2018 IEEE Region 10 Conference, IEEE, 2018, pp. 1923–1927.

[20] R. R. Estacio, N. B. Linsangan, A rotation invariant algorithm for bimodal hand vein recognition system, in: 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), IEEE, 2018, pp. 1–6.

[21] H. Thakuria, A. Dutta, A. Sarkar, A. Ghosal, R. Saha, S. Pramanik, S. Mitra, C. Mukherjee, U. N. Thakur, D. Mukherjee, A comparative study of vein pattern recognition for biometrie authentication, in: 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), IEEE, 2017, pp. 689–694.

[22] A. Kuznetsov, I. Oleshko, K. Chernov, M. Bagmut, T. Smirnova, Biometric authentication using convolutional neural networks, in: Conference on Mathematical Control Theory, Springer, 2019, pp. 85–98.

[23] M. Xin, J. Xiaojun, Palm vein recognition method based on fusion of local gabor histograms, The Journal of China Universities of Posts and Telecommunications 24 (2017) 55–66.

[24] C. Kalyani, Various biometric authentication techniques: a review, Journal of Biometrics & Biostatistics 8 (2017) 371.

[25] L. Zhang, Z. Cheng, Y. Shen, D. Wang, Palmprint and palmvein recognition based on dcnn and a new large-scale contactless palmvein dataset, Symmetry 10 (2018) 78.

[26] E. Kurbatova, N. Kharina, A. Zemtsov, S. Plyaskin, Investigating palm vein pattern recognition methods, in: 2022 24th International Conference on Digital Signal Processing and its Applications (DSPA), IEEE, 2022, pp. 1–5.