IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Review On Finger Vein Recognition System

Rohit Raj[1], Jayant Kumar[2], Ayush Raj[3]
B.Tech Student[1,2,3]
Department of Computer Science Engineering
Galgotias University, Gautam BuddhNagar, India

Abstract: Using near-infrared (NIR) imaging to capture each person's vein patterns makes finger vein authentication incredibly secure and difficult to forge. These small near-infrared (NIR) sensors are ideal for use in many fields, including medicine, consumer electronics, and banking, thanks to the improved accuracy and efficiency brought about by modern machine learning and deep learning algorithms. The usage of this technology will be propelled by upcoming advancements in areas such as multi-modal biometrics, cloud computing, edge processing, and sensor technologies. Fingerprint vein authentication is a promising approach for future biometric systems because of its high level of accuracy, security, and user acceptability.

***Index Terms* -** Finger Vein Authentication, Vein Pattern, Image Processing, Deep Learning, Security, Privacy, Data Security

I. Introduction

The idea of using vascular patterns as a biometric identification system was first put up in the 1980s. The practicality of capturing and analyzing vein patterns for identification was the primary emphasis of early studies. Nevertheless, substantial technological progress did not permit practical implementation until the early 2000s.(1)

In 2004, Hitachi released a device that could authenticate users by their veins in the fingertips. The technology captured the vein patterns beneath the skin by illuminating the finger with near-infrared (NIR) light.(2) In order to facilitate identification and verification, the distinct vein patterns were extracted from the processed pictures.

Access control, online payment, bank account, and mobile device unlocking systems, among others, have seen tremendous growth in the security industry's use of identification and authentication technologies in the last several years. When making this option, it's crucial to think about both ease and security. Contactless biometric identification systems are perfect for use in payment and access control due to their dependability, resilience, convenience, and cleanliness. Contact with the subject is not necessary for many biometric procedures.(1) The following are only a few examples: vascular analysis, gait analysis, contactless fingerprinting, iris scanning, and more. Researchers are interested in studying vein recognition as a biometric identification method. A vein recognition system's main selling point is that it requires a live subject in order to work. It can take blood samples by illuminating veins with infrared light.(3)

The concept has been postulated by scientists since 1543, when Vesalius initially put it forward, that the configuration and course of our veins change over the years. A forensic medicine specialist has discovered that even in sets of identical twins, the vein pattern on the back of each hand is distinct. Researchers have looked at palm vein identification systems from both a theoretical and practical perspective. It is feasible to become an expert in both deep learning and handcrafting. Applications utilizing the palm vein identification method are currently accessible for purchase.(3) So, trade secrets allow architects and designers to keep their work private for real-world uses. Researchers and developers have had to spend more money on specialized equipment featuring near-infrared (NIR) sensors. If you hear about our system, it's because of VeinDeep. Someone else can't use your phone since their vein patterns can be used to identify them. Although it conceals venous patterns, it will not leave an imprint on your skin similar to a fingerprint. They have far better crowd-blending skills than the average person. Our gadget can take pictures of vein patterns since it has an infrared depth sensor. Infrared imaging allows for the illumination of veins using either conventional infrared or infra-red light sources. (4)

More and more, people are turning to biometric authentication technologies instead of using old-fashioned passwords and PINs. One of the most used biometric procedures, finger vein biometrics is known for its high level of security, precision, and user-friendliness. Since everyone's vein patterns are different, this procedure is incredibly difficult to replicate.(5) This article will examine finger vein biometric technology and go over its pros, cons, potential uses, and technical details.

Among the many benefits of biometrics are improved fraud detection, the removal of the need to memorize passwords, the use of distinct behavioral or physical traits, and the fact that they cannot be borrowed, stolen, forgotten, or left at home, among many others. Fingerprint, palm, and vein recognition, facial and voice recognition, and iris, palm, and vein recognition are some of the methods used in biometrics. However, a foolproof biometric technology has not yet arrived(6). Since it is possible to create a plausible fake fingerprint or palm print using a dummy print and modern fingerprint scanners are unable to tell the difference, it is straightforward to fabricate these biometric identifiers. Illnesses like a sore throat might make it difficult for people who should be able to use speech recognition to obtain their information. There isn't enough proof to deem iris scans unsuitable for use in background or watch list inspections, and patients may experience pain and vision problems throughout the process.

The main difficulty in biometrics is to improve recognition performance in terms of efficiency and accuracy while also eliminating biased practices. Researchers have been working tirelessly to produce highly customized biometrics in an effort to boost dependability and dissuade spoofers. It would be wise for consumer devices to implement simple and inexpensive biometric authentication methods.

One biometric pattern that shows promise for individual identification is the finger-vein. Some benefits of the finger-vein biometric system as compared to others are:

1. The fact that no one can see the vein makes it extremely difficult, if not impossible, to steal or manufacture.
2. Because it is cleaner and less intrusive, more people are opting to have their finger veins taken.
3. To obtain the finger-vein pattern, one must utilize a live specimen. Thus, it is demonstrated by natural and convincing ways that the patient whose finger-vein was successfully caught is alive.

Using a person's unique vein patterns, finger-vein biometric technology can confirm their identification. While it is possible to duplicate traditional biometrics like fingerprints and facial features away from the original spot, vein patterns cannot. Further benefits of utilizing veins in the fingers include A person's fingertips may hold the key to identifying an identical twin in the future, thanks to their distinct system of veins and arteries. Also, our vein patterns remain the same as we get older.(3) This form factor for biometric identification is becoming the standard because of its tiny size and high recognition accuracy. The veracity of finger-vein patterns cannot be questioned.(3) The 10 fingers and contactless, non-invasive sensors make it easy to operate, and the extra ones can be used for identification in case of an accident or other emergency.

Biometric systems, which are pattern-recognition systems, boil down to identifying an individual's unique pattern of behavioral or physiological attributes and comparing it to a feature vector. Research has shown that vein pattern detection not only fits this description but also provides a plethora of important biometric features:

- the pattern's distinctiveness and durability
- a method for detecting without touching
- very difficult to counterfeit or duplicate.
- No one can see the biometric parameter.
- Even if two patients have the same vein pattern, it is still feasible to positively identify them.

In comparison to traditional, unreliable security measures like PINs and passwords, biometric authentication systems have clear advantages. Finger vein authentication is one of various biometric methods, but it stands out due to its dependability, simplicity, and high degree of security.(7) A person's fingerprint is a biometric because of the unique vein patterns observed on each finger. This paper delves into the details of finger vein authentication systems, covering their background, present state, and possible future advancements.

There has been a lot of study in this field since 1992, when the concept of exploiting vein pattern was first proposed. The complex network of capillaries that lies just under the surface of human skin is known as the vein pattern.(8) The ulnar and dorsal veins of the hand and fingers make up this vein-based sensory system. Compared to other veins, the finger vein has a far more complex and convoluted arrangement.

There are several benefits to using finger vein as opposed to other options:

- Variegated vein patterns in the fingers are unique to each individual. The fact that every single human being, including identical twins, has a distinct vein pattern makes this method exceptionally secure for sensitive information.
- Due to its subcutaneous location, the finger vein is both unnoticeable and challenging to treat or remove.
- User-friendly and clean, it captures images of vein patterns without invasive procedures.
- Because vein patterns remain constant throughout a person's life, they do not show signs of aging.
- If there is an epidermal injury, the vein pattern will also remain unchanged.

Since only live samples are collected from finger veins, it is completely impossible to steal someone's identity.(9) Using the unique crisscrossing vein patterns visible beneath the skin's surface, a biometric method called finger vein authentication can identify an individual. There are three main advantages to using finger vein authentication:

1. It is very difficult to forge or steal veins because of their deep location inside the body; also, their authenticity is unaffected by outside influences, such as the condition of the hands.
2. Contactless, non-invasive imaging made possible by infrared light is user-friendly and sanitary.
3. Being steady and well-defined, vein patterns may be captured using low-resolution cameras, making them ideal for handling small-size, simple data images.

Here is a system that we call VeinDeep. An authentication method for smartphones that makes use of the user's vein patterns. Since veins are located just under the skin's surface, they do not leave any visible imprints like fingerprints.(10) As a viable solution to the present high level of security requirements, biometrics systems are presently gaining worldwide adoption. These systems use a part of the body and are extremely exact. A person's vascular patterns are unique, hard to replicate, contactless, age-and race-independent, and skin-color-independent, according to the research.

II. Literature Survey

S. Nandhini et al 2014: As consumer electronics continue to advance in sophistication, there will be a greater need for straightforward authentication systems that prioritize both security and usability. Passwords, PINs, and cards are the authentication methods used by modern systems. There is, however, always the risk of card theft and exploiters guessing passwords and PINs. Therefore, biometric solutions are necessary for the protection of sensitive data. The planned system's biometric identification mechanism is based on the detection of veins in the user's fingers. In this case, the centerlines are extracted using the approach for extracting features with the highest curvature, which disregards variations in vein brightness and width. Processing results are sent to administrators or owners via GSM. Some of the numerous potential applications of the system include automated attendance registers, systems for controlling the locking of doors, and identification and verification processes for automated teller machines. (3)

Rahul Dev et al 2017: The security of people's private data is paramount in the modern day. Despite the proliferation of novel methods, biometric identification remains the gold standard. A person's unique physical traits and behavioral patterns form the basis of biometric technologies. This process makes use of a variety of human identifiers, including fingerprints, veins, iris, and hands. When it comes to biometric security, the vast majority of individuals put their faith in fingerprint scanners. Methods for extracting features that identify finger veins are covered on this page. Topics such as feature extraction, pre-processing, and obtaining images of finger veins constitute the bulk of the current literature. In this section, we will compare and contrast these three sections from a functional standpoint. (11)

Caixia Liu et al 2013: Finger vein identification has been making headlines recently due to its widespread use and high level of security. Our approach involves using an improved adaptive Niblack threshold segmentation technique to extract features from photos of human finger veins. The parameter and correction factor for the Niblack window are provided here. To guarantee reliable feature extraction of the finger vein, the image is first filtered and adaptively histogram equalized. Future vein recognition approaches can benefit from this method's simplicity and ease of application, as shown in the experimental results. (12)

Jose Anand 2013: One sort of biometric authentication is verification using veins in the fingers. When combined with other biometric methods, this one can confirm a person's unique characteristics. This study aims to provide a template-matching technique for authenticating finger veins. The Matlab implementation verifies the user identification system's success by using finger vein authentication. (13)

Ajay Kumar 2009: This study introduces a new method for personal identification verification by combining three-dimensional hand vein images with data extracted from the contour of the knuckles at the same time. The proposed method involves automated palm dorsal vein imaging employing cost-effective near-infrared contactless imaging. When it comes to picture normalization and ROI extraction, the knuckle tips are crucial landmarks. To begin, a hierarchical matching score is generated using the four triangulation topologies found in the binarized vein structures. Concurrently, the perimeter distances between knuckle points in the acquired images are used as a geometrical characteristic to create the matching scores. A weighted combination of these two matching scores enables individual authentication. The trial results using contactless palm dorsal-hand vein photos of the proposed method show that it is a more user-friendly option for user identification, with an equivalent mistake rate of 1.14%. (14)

MOHAMED I. SAYED et al 2021: The combination of biometric recognition with telephony is the only way to make online payments and other types of financial transactions safer. Because of its bigger surface area and lack of wrinkles, the dorsal hand is better for vein detection than the palm, finger, or wrist. Dorsal hand vein recognition is currently used by systems, however it isn't always reliable and can't work in real-time. This work proposes a real-time dorsal hand detection system that is both effective and has a high frame rate. The data set was collected using a contactless device that was synced with a smartphone. Infrared light-emitting diodes and a USB camera were some of its features. There were 2,000 photos of 100 people's hands in the set. Light methods were applied to the obtained images in order to boost the frame rate and real-time performance. An ORB match with K-nearest neighbors (K-NN) was employed in the feature extraction and recognition technique. Additional data used to evaluate the suggested approach comes from the Poznan University of Technology (PUT) dataset. A respectable 29 fps was attained by the suggested method, which had an experimentally demonstrated EER of 4.33%. This is just mind-blowing. (15)

Shabab BAZRAFKAN: This research presents a novel biometric method that makes use of the structure of veins. One way to verify a person's identity is by analyzing their vein structure in the middle phalanx of the finger. It ought to be feasible to implement the hardware notion with handheld devices. Software installation and device configuration will be covered. The temporal median filter was used to merge the finger pictures, and the Gabor filter bank was used to recover the maps of the veins in the fingers. (16)

Shi-Jinn Horng et al 2022: There has been a significant uptick in R&D activity concerning biometric access controls and mobile online payment systems. This article presents a novel, inexpensive method for detecting veins in the palm of the hand using RGB photos captured by smartphones. Starting from scratch, we improve upon previous methods that relied on the red channel by detecting and enhancing palm vein patterns using the saturation channel. Our subsequent presentation covers a new approach to convex hull-based region of interest extraction and a fresh use of key vectors; these methods tackle the difficult contactless capture issues with smartphones, such as scale variants, rotation, closed fingers, rings on hand, and so on. When compared to other palm vein recognition research, our novel algorithm—based on deep learning and designed for smartphones—stands out. An accuracy-enhancing fusion approach, an inverted residual bottleneck, a spatial pyramid pooling module, an appropriate convolution block, and depthwise separable convolution are all components of the suggested model. When contrasted with similar models, the outcomes show that the proposed model is more concise and accurate. An inference time of 8 ms and a best-equal-error rate of 0.49% were both accomplished by the integrated model that was suggested. (17)

Syafeeza AHMAD RADZ et al 2016: This research presents a new method for identifying blood and fingerprint samples using a convolutional neural network (CNN). Given their intracellular position, recreating vein patterns is exceedingly difficult, in contrast to two existing biometric procedures: fingerprints and facial recognition. Because they are impossible to alter, damage, or forge, biometrics based on finger veins provide an extra layer of protection. In order to achieve high performance accuracy, traditional algorithms for finger-vein detection undergo intensive image processing, which involves removing noise, extracting and improving features, and conducting picture classification. With CNNs, you can categorize data, extract features, and reduce data dimensionality all inside the same network structure, which is a huge benefit over more traditional methods. We don't need to conduct any photo preparation for the method because CNN handles noise and tiny image misalignments well. Using a fused convolutional-subsampling architecture, this paper proposes a four-layer CNN for finger-vein recognition that is simplified. The stochastic diagonal Levenberg-Marquardt algorithm's convergence time has been decreased via optimization and its application to network training. A fifty-person in-house finger-vein database was used to evaluate the proposed CNN, with ten samples taken from each finger. After dividing the samples in half for testing and training, we achieved a perfect identification rate of 100%. After further testing with a larger sample, 81 individuals had a success rate of 99.38%. (18)

Yi Liu et al 2017: There are more applications than ever before that could potentially expose sensitive biometric authentication data, which is a very serious concern. In order to stop these kinds of assaults, a lot of researchers are looking into the problem and creating new authentication methods. However, the most significant obstacle is ensuring the privacy of biometric data without rendering identity verification procedures unworkable. This paper's authors set out to address this issue by presenting FVR-DLRP, a deep learning-based, randomly projected biometric template-based approach to finger vein recognition. The fundamental biometric data will be safeguarded by FVR-DLRP even if the user's password is hacked. The experimental results demonstrate that the FVRDLRP algorithm improves biometric authentication security by keeping biometric identification accurate while increasing transformation uncertainty. (12)

SUNGCHUL CHO et al 2020: In this paper, we present a new method for biometric identification verification using fingerprint and palm-vein images captured in both the near-infrared (NIR) and ambient-light (ARG) regions of a photograph. With visibility library access, we may use the red and blue spectra as gallery examples and the near-infrared (NIR) spectra as probe sources while keeping generalizability. To improve the discriminative capability of the palmprint templates, we extract palm-vein and palmprint features and use a simpler Local Binary Pattern (LBP) encoding approach. Lastly, we compile the similarity scores for the NIR palm-vein templates compared to the recorded RGB palm-vein templates and the scores for the NIR palmprint codes compared to the registered RGB palmprint codes. Using two publicly available multi-spectral palm databases, we show that the proposed technique consistently yields promising verification results in our tests. (5)

Paula López-González et al 2022: One modern method that shows promise is vein pattern biometrics. Vein patterns are very desirable due to their exceptional performance, resistance to circumvention, distinctiveness, longevity, and versatility. Both collectability and acceptability might use some work. These two attributes are closely related to the acquisition methods. This approach is usually employed to obtain images of veins because hemoglobin within veins absorbs a greater amount of near-infrared (NIR) light compared to the surrounding tissues. Specialized equipment is typically utilized to obtain superior vein pictures. The decrease in popularity of these devices has an adverse effect on their collectability value. (19)

Kashif Shaheed et al 2021: A relatively new area of study, biometrics examines methods of human identification that rely on distinct physiological and behavioral traits. This study documents new developments in physiological-based biometric multimodalities and focuses on processing methods that use fingerprints, palm and finger veins, faces, lips, iris, and retina. Biometric technology's operational mode, performance metrics, and architecture were also evaluated by the writers. This article discusses and analyzes physiological biometric modalities that are based on deep learning as well as others that are more traditional. This article does a thorough exploration of biometric techniques that include a variety of modalities. Extracting features, classifying data, and performing preliminary processing are all examples of such methods. An exhaustive overview of the present and future trends in traditional and deep learning approaches, together with their respective strengths and weaknesses, is offered to the researcher. Furthermore, we take a look at the traditional and cutting-edge methods for evaluating biometric systems that use high-level physiological data. A robust physiological-based strategy can still be employed to improve and advance the biometric system, according to the comparisons and analyses offered in the article. (1)

III. METHODOLOGY

DATA ACQUISITION AND PROCESSING

1. Finger Vein Image Processing Stages

Infrared (NIR) cameras take pictures of the veins in the fingers and send them to the computer for processing. In response, the infrared LED's brightness is dynamically adjusted by a central processing unit (CPU), which fine-tunes the image quality. Preprocessing of the acquired image will follow acquisition. Following that, the image processing will be applied to the finger-vein region for post-processing. Reducing noise and smoothing it out are part of this process, as is determining a local threshold for every vein. The recorded finger vein template is compared to a reference template as part of this process. A block diagram depicting the processing stage is shown in Figure 1.

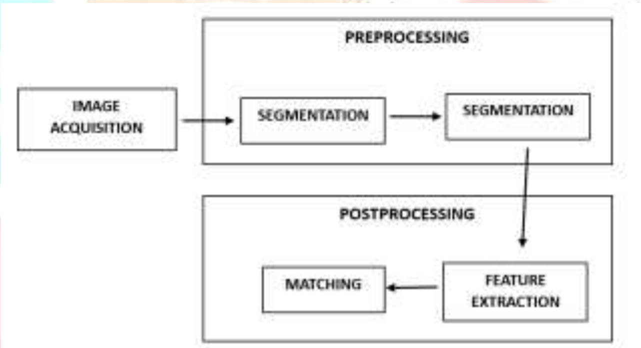


Fig.1 Data Structure for the Processing Phase

2. Image Acquisition

The accuracy and reliability of the system are determined by the picture collection step of finger vein detection, which is therefore critically important. An infrared (IR) light source, such as a light-emitting diode (LED) or a laser that operates in the near-infrared range (700 nm to 1000 nm), is used to initiate the process. It is possible to see veins using a near-infrared camera because blood carries light from the skin to the sensor. The intricate vein patterns can only be captured with a high-resolution camera. Usually, these devices come with grips or guides that you may use to keep your finger at a constant angle to the camera. This way, you can take consistently high-quality images. By manipulating the lighting in a dark room or chamber, you may isolate the finger and ensure that the infrared light is spread out evenly throughout its surface. Taking numerous shots at once may help a high dynamic range camera handle different lighting conditions. Nonetheless, evaluating quality is of utmost importance. In the event that the captured images are of poor quality, users will be instantly informed through feedback systems. After that, the photographs will be checked to make sure they are up to par by automated algorithms. If you want your infrared light source and camera to keep working as they should and provide you consistent, accurate photos, you need to calibrate your imaging system often. Pictured in Figure 2 is a simplified representation of the process that takes pictures.

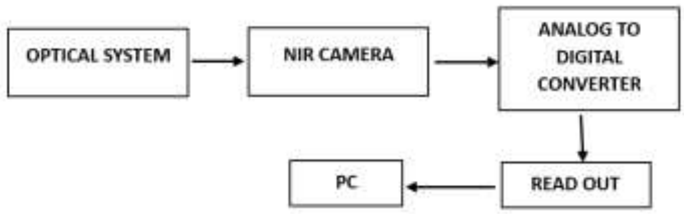


Fig.2 Acquiring Images

3. Image preprocessing

For improved recognition results from your finger vein recognition system, image pretreatment is a must. First things first, we need to quiet down. This is achieved by applying image smoothing techniques and removing artifacts created during capture utilizing tools like median and Gaussian filtering. To make sure all the photos are the same contrast and brightness, the next stage is normalization, which usually uses histogram equalization to scale the intensity values to a given value. Then, we use morphological techniques, such as edge detection, to isolate the part of the image that contains the vein pattern. This is called ROI extraction, to put it simply. Consistency is also ensured by making sure the ROI is aligned accurately. Lastly, the vein patterns are made more apparent using contrast enhancement techniques and adaptive histogram equalization. This makes the features easier to see in the future when it comes time to extract and match them.

4. Finger Vein Segmentation

By dividing a digital image into smaller, more manageable pieces, it can be segmented. Common applications include object detection and edge identification for photometric curves and lines. What we mean when we say "binarization of finger vein image" is to divide the image into two distinct layers. Distinct from the landscape is the object, which is the region surrounding the finger. There is a white item part and a black backdrop. The current database provides near-infrared pictures of finger-vein to feed the suggested system.

5. Vein Pattern Extraction

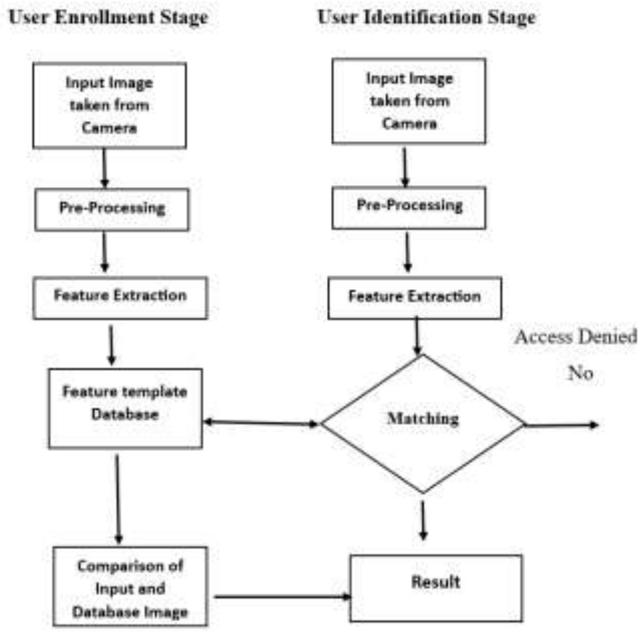
In finger vein recognition, vein pattern extraction is all about separating and improving the distinct vein structures in a preprocessed picture so that they may be utilized for matching and recognition later on. The first step is to improve the vein pattern by drawing attention to the vein structures using methods such as matched filtering, Gabor filtering, and repeated line tracking. Gabor filtering increases particular frequencies and orientations that correspond to vein patterns, whereas matched filtering convolves the picture with filters that match the expected vein shapes. Tubular structures are highlighted and identified through repeated line tracking. After the veins have been improved, the following stage is to use these patterns to extract characteristics. One approach is to use thresholding to make the image binary, which allows the veins to stand out from the backdrop. Another is to use more advanced approaches, such as local binary patterns (LBP) or minutiae extraction, to capture the vein bifurcations and endpoints. Each person's unique template is created using these extracted features; this template can then be compared against templates saved for recognition.

6. Matching

Last but not least, matching compares the retrieved vein patterns to stored templates to establish an individual's identity in finger vein recognition. After each person's vein patterns have been extracted, a one-of-a-kind template is made using the attributes. The unique vein patterns of each individual are captured by this template. In order to find a match, many techniques are used to compare the newly made template to templates that are already in the database. The geometric distance between feature points and the bit-counting Hamming distance are two popular ways to compare binary templates. More sophisticated approaches can be employed to enhance precision, such as machine learning models and correlation-based matching. Once the matching algorithm generates a similarity score, it checks it against a threshold that has already been set. The templates have been recognized when the score is greater than the threshold. This technique is a crucial part of the system that can detect veins in the fingers and guarantees accurate identification.

IV. PROPOSED SYSTEM

The suggested system's flow diagram is shown in Figure 3.



V. RESULT

In order for the system to authenticate users or manage their access, it uses finger vein identification. However, if a user's vein patterns don't match those of an enrolled user, the system will not be able to accomplish either. The patterns that emerge from the processed vein images are compared to previously saved templates utilizing specific algorithms after acquisition and processing. By comparing the generated similarity score to a predefined threshold, these algorithms arrive at a final score. When the score is higher than the threshold, it means there is a positive match, and access is granted to verify the person's identity. Conversely, if the score is below the cutoff, entry will be denied because there is no match.

An indicator of the system's efficacy is the False Acceptance Rate (FAR), which measures how often the system accepts a rejected request. Both FAR and FRR assess the possibility that the system might incorrectly grant access to an unauthorized user, while FAR also assesses the possibility that it might miss the mark when identifying an authorized user. A safe and user-friendly system must strike a balance between the two rates; ideally, there should be less incorrect acceptances and denials.

The recognition mechanism relies heavily on user feedback. After receiving a confirmation message or being allowed access, users can often proceed with their intended duties after a match is identified. If it doesn't, though, the user is encouraged to give it another go and may even receive advice on how to better position their fingers. After a certain number of failed login attempts, the system may prompt the user to provide further biometric information or answer security questions.

Security and system logging are important supplementary features. Accurate time stamps, match scores, and the outcomes of identification efforts are scrupulously documented for the sake of auditing and security monitoring. For the purpose of keeping tabs on system performance, possible mistakes, and security protocol compliance, these logs are invaluable.

Efficient error management is crucial to the system's reliability and user happiness. Temporary problems, such low image quality or misalignment, may be resolved by the system through multiple efforts. An additional layer of security is in place to ensure the user's identification in the event that the first two fail. So, even if the first two don't work, access can still be managed. The reliability and safety of the authentication technique are directly affected by how well the finger vein recognition procedure works.

VI. Conclusion

Lastly, a major indicator of the system's user authentication capabilities is the result of the finger vein identification test. Following a comparison of the recorded vein patterns to pre-existing templates, the software calculates a similarity score in order to ascertain authorization. False Acceptance Rate (FAR) and False Rejection Rate (FRR) are metrics that quantify how effectively this strategy combines security with user practicality. Strong error management, thorough system recording, and reliable feedback mechanisms can enhance the system's reliability and user experience. Modern identity verification and access control systems greatly benefit from fingerprint vein recognition because of the strong biometric security it offers. The unique and long-lasting characteristics of vein patterns are used to their advantage in this way.

VII. References

1. Shaheed K, Mao A, Qureshi I, Kumar M, Abbas Q, Ullah I, et al. A Systematic Review on Physiological-Based Biometric Recognition Systems: Current and Future Trends. Vol. 28, Archives of Computational Methods in Engineering. Springer Science and Business Media B.V.; 2021. p. 4917–60.
2. Kang W, Wu Q. Contactless palm vein recognition using a mutual foreground-based local binary pattern. IEEE Transactions on Information Forensics and Security. 2014;9(11):1974–85.
3. Nandhini S, Shyam D. Real-time finger-vein recognition for security and monitoring system. In: Applied Mechanics and Materials. Trans Tech Publications; 2014. p. 194–203.
4. Uhl A, Busch C, Marcel S, Veldhuis R. Advances in Computer Vision and Pattern Recognition [Internet]. Available from: http://www.springer.com/series/4205
5. Cho S, Oh BS, Toh KA, Lin Z. Extraction and Cross-Matching of Palm-Vein and Palmprint from the RGB and the NIR Spectrums for Identity Verification. IEEE Access. 2020;8:4005–21.
6. Zhang L, Cheng Z, Shen Y, Wang D. Palmprint and palmvein recognition based on DCNN and a new large-scale contactless palmvein dataset. Symmetry (Basel). 2018 Apr 1;10(4).
7. Mulyono D, Jinn HS. A Study of Finger Vein Biometric for Personal Identification. Vol. 4.
8. Horng SJ, Vu DT, Nguyen T Van, Zhou W, Lin CT. Recognizing Palm Vein in Smartphones Using RGB Images. IEEE Trans Industr Inform. 2022 Sep 1;18(9):5992–6002.
9. Miura N, Nagasaka A, Miyatake T. Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification. Mach Vis Appl. 2004 Oct;15(4):194–203.
10. Delac K, Grgic M. A SURVEY OF BIOMETRIC RECOGNITION METHODS. 2004.
11. Astya PN, Galgotias University. School of Computing Science and Engineering, Institute of Electrical and Electronics Engineers. Uttar Pradesh Section, Institute of Electrical and Electronics Engineers. IEEE International Conference on Computing, Communication and Automation (ICCCA 2017) : proceeding : on 5th-6th May, 2017.
12. Liu Y, Ling J, Liu Z, Shen J, Gao C. Finger vein secure biometric template generation based on deep learning. Soft comput. 2018 Apr 1;22(7):2257–65.
13. . JA. FINGER-VEIN BASED BIOMETRIC SECURITY SYSTEM. Int J Res Eng Technol. 2013 Dec 25;02(12):197–200.
14. Kumar A, Prathyusha KV. Personal authentication using hand vein triangulation and knuckle shape. IEEE Transactions on Image Processing. 2009;18(9):2127–36.
15. Sayed MI, Taha M, Zayed HH. Real-Time Dorsal Hand Recognition Based on Smartphone. IEEE Access. 2021;9:151118–28.
16. Bazrafkan S, Nedelcu T, Costache C, Corcoran P. Finger vein biometric: Smartphone footprint prototype with vein map extraction using computational imaging techniques. In: 2016 IEEE International Conference on Consumer Electronics, ICCE 2016. Institute of Electrical and Electronics Engineers Inc.; 2016. p. 512–3.
17. Mulyono D, Jinn HS. A Study of Finger Vein Biometric for Personal Identification. Vol. 4.
18. Ahmad Radzi S, Khalil-Hani M, Bakhteri R. Finger-vein biometric identification using convolutional neural network. Turkish Journal of Electrical Engineering and Computer Sciences. 2016;24(3):1863–78.
19. López-González P, Baturone I, Hinojosa M, Arjona R. Evaluation of a Vein Biometric Recognition System on an Ordinary Smartphone. Applied Sciences (Switzerland). 2022 Apr 1;12(7).