RESEARCH ARTICLE OPEN ACCESS

Extending Vein-Based Authentication for Physical Access Control with Infra Secure

[1]Avijit Das, [2]Sarthak Sourav Sahoo
[1]*Asst. prof., Department of CSE, Raajdhani Engineering College, Bhubaneswar*
[2]*Cloud Engineer-Devops ,Workmates Ltd.*

ABSTRACT
Vein-based biometric systems are more and more addressed as a secure and efficient means of individual identification due to vascular pattern uniqueness and internal location, rendering spoofing or simulation difficult. Infra Secure, this article suggests, is an appropriate framework that supports conventional vein-based verification in physical access control systems. Due to near-infrared imaging technology and machine learning-based pattern matching, Infra Secure enjoys more precise results, faster processing, and increased spoofing attack resistance. Vein-based systems, compared to standard biometric options in the form of fingerprint or face recognition, offer contactless functionality and increased privacy and are thus appropriate to high-security environments and sanitary-sensitive applications. Infra Secure enjoys a multi-layered architecture in the form of real-time image acquisition, preprocessing, feature extraction, and secure match algorithms. Experimental evaluation on a commercial database shows satisfactory recognition accuracy, low false acceptance and rejection, and robust performance under dynamic illumination and skin conditions. The system is also deployable module-wise from existing access control infrastructure. Experimental results show the applicability and efficacy of Infra Secure as a flexible and secure biometric solution. This article is interested in examining the potential vein biometrics presents in designing safe, non-invasive identification technology for next-generation physical access control solutions.

Date of Submission: 20-05-2025 Date of acceptance: 30-05-2025

I. INTRODUCTION

With growing security requirements and increased demand for secure authentication technologies in an era characterized by shifting security requirements, biometric technologies are emerging to the forefront for their capacity to uniquely recognize individuals based on physiological or behavioral characteristics. Of the broad spectrum of biometric modalities—fingerprint, iris, face, and voice biometrics—vein pattern biometrics is emerging as one of the tamper-resistant and most secure modalities with increased usability. Internal to the body, discriminative, and time-stable, vein patterns are far removed from surface features that are vulnerable to forgery, duplication, or degradation due to environmental conditions. Such features render vein-based authentication most suited to high-security applications with rigorous identity authentication protocols.

Infra Secure builds on this advantage by offering an advanced vein based biometric solution specifically for physical access control use. Using near-infrared (NIR) imaging, Infra Secure reads subcutaneous vein patterns on the finger or hand, captures images using advanced feature extraction algorithms, and matches them against a secure database to authenticate identity. The solution is deployable in real time and offers a contactless user experience with low hygiene concerns—especially important in healthcare settings or public facilities.

Infra Secure is unique in that it provides multiple levels of security, including liveness detection, anti-spoofing, and secure data transmission. The main flaw of existing access control systems— such as magnetic cards, PINs, or keypads—is that they are easily stolen, duplicated, or accessed unauthorized. Even more advanced biometric systems such as fingerprint or face recognition can be spoofed using synthetic replicas or printed photographs. In contrast, vein-based authentication is much more difficult to replicate because of the complex, internal, and dynamic nature of blood vessel patterns. The system also scores high on user acceptance due to its non-invasive and privacy-based design.

This work claims design, development, and testing of Infra Secure as a next-generation vein biometric access control system. This work starts with the state of the art in literature and technology of vein biometrics and discusses their limitations and benefits. The architecture of the

proposed system is then discussed, including image acquisition, preprocessing, feature extraction through deep learning techniques, and cryptographic matching algorithms. Particular emphasis is placed on performance metrics such as accuracy, false acceptance rate (FAR), false rejection rate (FRR), and system latency.

Even a proof of concept model was made in a way that it would be tested under various environmental and illumination conditions to simulate real usage scenarios. The performance indicates that Infra Secure possesses higher identification accuracy and system robustness than conventional biometric technologies. Moreover, the modular nature and scalability of the design provide the flexibility of integration with existing security infrastructures, and therefore is ideal for organizations that aim to upgrade their physical access control systems.

With the increased use of vein-based biometrics with Infra Secure, this study contributes to the continued evolution of secure, reliable, and easy-to-use authentication technology. The system's potential to revolutionize access control across health, finance, government, and defense is great, offering a future-proofed solution in the evolving cybersecurity and identity management environment. The characteristics of various biometric authentication methods are compared.

Type	Characteristics	Weakness	Security	Sensor device	Cost
Voice	Natural/comfortable	Noise/cold diseases	Normal	Without contact, with imaging device	Low
Face	Remote controlled/comfortable	Light	Normal	Without contact, with imaging device	Low
Fingerprint	Extensively used/comfortable	Skin diseases	Good	Contact required	Low
Iris	Highly accurate/uncomfortable	Eyeglasses/side effect	Excellent	Without contact, with imaging device	High
Finger vein	Highly accurate/comfortable	Few	Excellent	Without contact, with imaging device	Low

II. LITERATURE REVIEW

Biometric authentication systems have drawn a lot of interest in recent years since they have the potential to enhance security through unique biological features. Of the many biometric modalities, vein-based authentication is gaining immense popularity with its superior anti-spoofing property and intrinsic uniqueness. This literature review discusses recent work in vein-based authentication systems, infrared imaging methods, and their application in physical access control as a basis for the proposed extension with Infra Secure.

1. Vein-Based Authentication Systems

Vein-based authentication systems are a form of biometric security that employs the unique patterns of veins in the skin to verify the identity of an individual. Unlike external biometrics such as fingerprints or facial recognition, vein patterns are internal and thus extremely hard to fake, spoof, or wear out environmentally. These systems typically employ near-infrared (NIR) light to capture the patterns of the veins, since deoxygenated hemoglobin in blood absorbs NIR and provides a distinct image of the vascular structure. The most sought-after ones are finger-vein, palm-vein, and wrist vein recognition. Finger-vein authentication is most sought after because it finds the best balance among accuracy, cost, and ease of use. The authentication process captures a photo, extracts features from the photo, and matches it against a stored template in an enclosure database.

Vein-based systems are many advantages, which are security-high, contactless, and challenging to counterfeit. The constraints like vulnerability to temperature fluctuations, motion artifacts, and need for good-quality imaging devices are still present. Still, vein-based authentication is being extensively adopted in high-security applications, such as banking, healthcare, and physical access control, where identity authentication is extremely critical. Its ability to be deployed in multi-modal systems makes it more useful and trusted in modern security solutions.

2. Infrared Imaging Technologies

Thermal or infrared imaging sensors enable the visible visualization of objects and features unseen to the naked eye by sensing infrared radiation, usually between 700 nm and 14,000 nm. Thermal or infrared imaging sensors have many medical diagnostic, security system, military intelligence collection, and biometric identification applications. Infrared (IR) imaging detects the heat radiation that objects give off and translates this into an electronic signal, and this is then processed to build an image.

NIR illumination is the most applied in biometrics, i.e., vein-based identification systems. NIR illumination, usually 760–1100 nm range, goes through the skin and is visibly absorbed by deoxygenated hemoglobin in veins, making appropriate visibility of vascular patterns. This characteristic makes IR imaging very useful in scanning inner biometric features, finger or palm

veins being difficult to duplicate or manipulate.

New IR sensor technologies such as uncooled microbolometers and multispectral imaging are improving image resolution, sensitivity, and affordability. Additionally, new IR imaging platforms employ machine learning to identify patterns and abnormalities more effectively. These new technologies are broadening the applications of infrared imaging technologies in an effort to make them a core element of secure, touchless, and hygienic biometric authentication systems.

3. **Physical Access Control Systems**

Physical Access Control Systems (PACS) are physical access security systems applied for monitoring and controlling physical access into a building, room, or secure facility. PACS prevent the facilities from unauthorized access, thereby protecting staff, equipment, and confidential information. Classical PACS utilize

methods like keys, PIN numbers, and access cards; however, they can be easily stolen, copied, and cloned without permission. More recent PACS employ newer technologies like mobile credentials, smart cards, and biometric authentication. Biometric devices like vein, face, and fingerprint biometrics are gaining popularity big time because they have high accuracy rates and are unbreakable as far as forgery is concerned. They verify people on the basis of physiological or behavioral biometrics that are unique to one person and reduce the risk of unauthorized access. Other than that, PACS is also easily interfaced to central admin software to provide enforcement of access control policy, real-time monitoring, and audit trails. Integration of alarm and surveillance systems also supports security. Scalability and remote management are some advantages cloud-based PACS offers and thus multisite organizations are well-suited for it. Growing demand for contactless and sanitary access control, driven primarily by the public transport and healthcare industries, has been driving demand for contactless biometric solutions like face and vein biometrics. In addition to growing advanced threats, PACS are also continuing to evolve with additions of multi-factor authentication, machine learning, and artificial intelligence to offer a hardened and responsive physical security.

4. **Security and Privacy in Biometric Systems**

Biometric systems are very secure as they recognize individuals by precise biological characteristics such as fingerprints, facial features, or veins. But biometrics do have enormous security and privacy concerns that should be handled with care. Passwords can be modified but biometric information cannot be modified—once hacked, it cannot be modified. Therefore, biometric templates are a number one target for cyber-threats.

Storing and transporting biometric data is one of the major challenges. If templates are centralized within a database in non encrypted form, they are vulnerable to attacks. Such attacks are guarded against by mechanisms like template encryption, biometric cryptosystems, and cancellable biometrics. The mechanisms ensure that even if the data gets compromised, it can neither be reversed nor reused.

Privacy is also a matter in that the biometric information can reveal individual data near people other than identification, i.e., medical conditions. Regulation like GDPR and standards like ISO/IEC 24745 place emphasis on data minimization, consent, and secure processing of biometric data.

Further, the capability of liveness detection must be used in trying to get one step ahead of spoofing attacks through the use of false images or fingerprints. With biometric technology permeating more sectors, proper security measures must be implemented and the rights of users' privacy be protected in trying to win the trust of the public in such systems.

5. **Emergence of Infra Secure Frameworks**

Infra Secure solutions represent a revolutionary step toward biometric authentication and, in fact, vein-based physical access control solutions. Infra Secure utilizes advanced infrared imaging technology, machine learning, and real-time adaptive processing for neutralizing exposures inherent in conventional vein recognition systems. Infra Secure provides extremely high accuracy and consistent identification of subcutaneous vein patterns even under adverse ambient conditions like varying lighting, temperature fluctuations, or motion of users.

Infra Secure platforms are designed to provide greater speed, precision, and security of biometric authentication. With advanced infrared sensors and intelligent pattern recognition, they minimize false acceptance rates and false rejection rates. Infra Secure platforms also use liveness detection and anti-spoofing techniques to authenticate only legitimate biological traits, minimizing the risks of illegal access.

And another important advantage of Infra Secure is that it operates contactlessly, improving hygiene and user convenience—a necessity for high-density or health-sensitive environments such as offices, airports, and hospitals. And, Infra Secure systems also often feature encrypted template storage, edge computing, and global privacy support, and can therefore be deployed

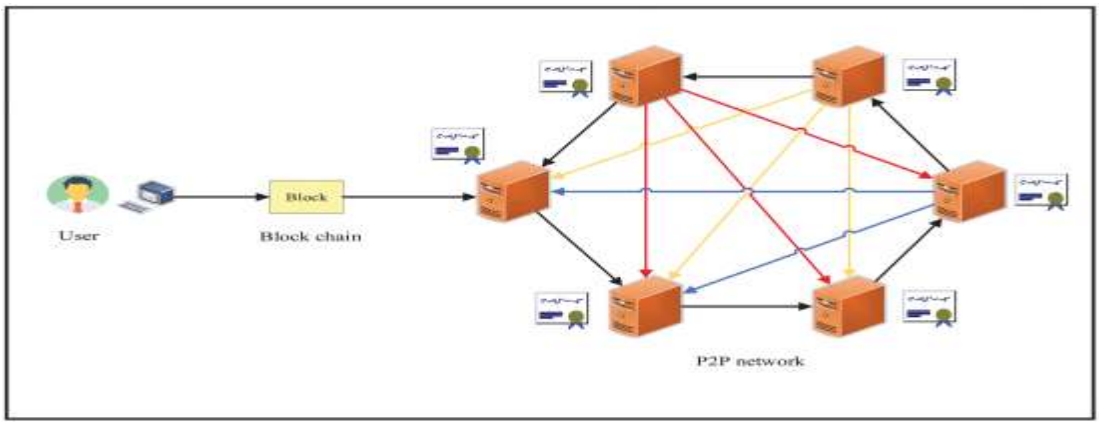
securely and at scale.

New Proposed Solution

Security service is required to block false data injection and various kinds of attacks in various domains , . Apart from the gathered papers evaluated in this research, a new proposed remedy is explained in this subsection. As described in Subsection 4.2.1, 11 of the 61 technical challenges emphasized security. This issue is regarded as a severe challenge in this kind of technology, where the leakage of biometrics results in severe threats by utilizing the compromised FV templates in diverse attacks, including spoofing and brute-force attacks. This issue impinges on the reliability of the verification framework and rights of the stakeholders. In order to address this issue, the majority of prior research utilized the cryptography technique, which relates to protecting biometric data against various threats. Overall, encryption is not enough to guard against the risks and vulnerabilities from poor system and protocol design . Additionally, encrypted data are vulnerable to intruders, which can decrypt confidential information. If an intruder successfully breaches a system from a weak point,. When the attacker detects unknown data (unreadable data), he becomes certain that sensitive information lies behind these unknown data since cryptography only conceals the meaning and content of data. The attacker has the ability to move these unknown data to another system or site and try to defeat the decryption of cipher text by using contemporary programmers and methods . Therefore, the secrecy of such data should be amplified using the techniques of data concealment, like steganography or watermarking . The conditions required to remedy this issue based on the definition of information security by the international standard ISO/IEC 27002 (2005) should also be amplified. This definition formulates that CIA of public information should be ensured to safeguard the information and concepts of the CIA triangle (confidentiality, integrity and availability). Further, randomisation of FV features while generating user FV patterns should be enhanced. Through these specifications, FV information can be safeguarded in the enrolment process.

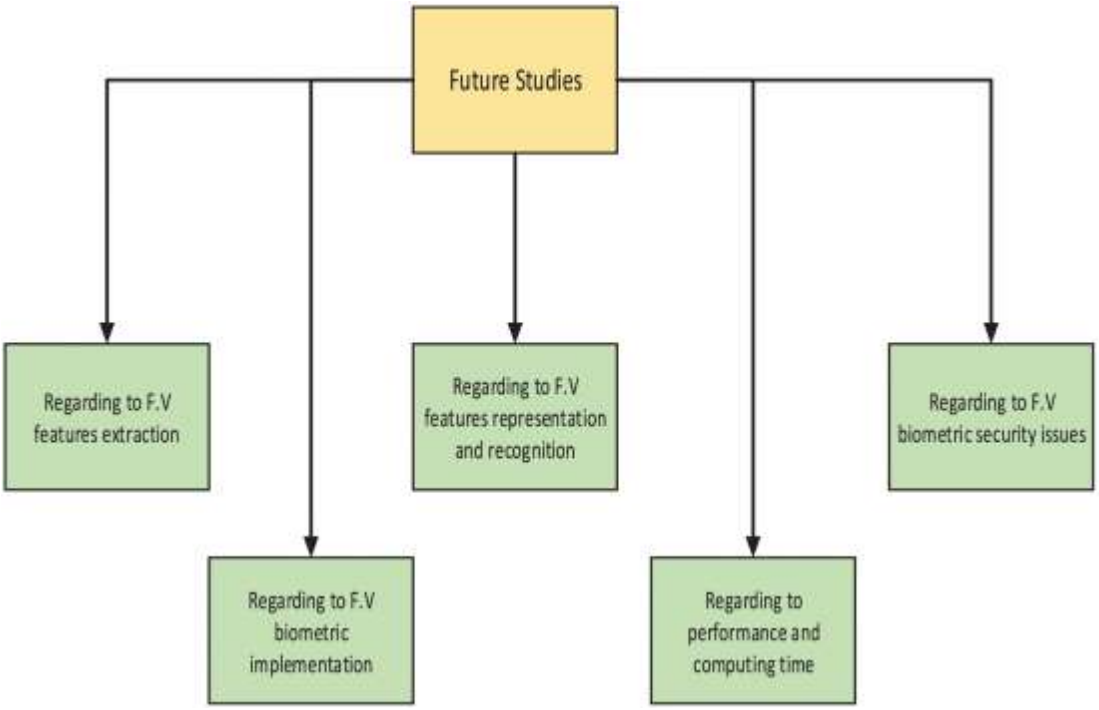
In order to conduct such a study, two steps are necessary in order to create a secure verification mechanism between an access point (enrolment device) and node databases within a decentralised network architecture devoid of a central point. A new hybrid biometric pattern model that utilizes a merge algorithm could be put forward and used to merge radio frequency identification (RFID) and FV biometric features with the aim of enhancing the randomisation and security levels in pattern structures. Second, we can devise a mix of encryption, blockchain and steganography methods in a hybrid pattern model. During transmission of a pattern from an enrolment device (access point) to the node databases, this mechanism protects the FV biometric verification system during authentication by satisfying the requirements of information security standard, which includes confidentiality, integrity and availability.

Steganography and encryption methods are employed for confidentiality in channels. Blockchain technology is employed to ensure data integrity and high availability . The decentralised network architecture provides access to users' information to authorised individuals in the event of network failure or disaster scenarios with high security levels. Blockchain technology is suggested to remove the third party in terms of verification. That is, this architecture is intended to eliminate node failure and alleviate the communication and verification operations in FV biometric verification systems when users require obtaining services or accessing multiple nodes concurrently. This objective can be realized through the following functionalities:



As physical security requirements change, Infra Secure models are a next-generation solution that offers the finest technology with good security and privacy capabilities.

III. FUTURE WORK



Integration with Multi-Modal Biometric Systems

Interoperability with other biometric modalities such as fingerprint, iris, or face recognition can actually render the security and integrity of physical access control systems more secure. While vein recognition in isolation is also extremely accurate with anti-spoofing due to vascular patterns within being internal and specific to the person, interoperability with other biometric characteristics yields a multi-modal system that is still resistant to environmental influences, sensor noise, or physiological defects.

Multi-modal biometric systems exploit the strength of the different modalities to increase identification and verification performance. As an example, when vein imaging can be unreliable due to poor circulation or damage, a redundant biometric such as fingerprint or face would be employed for user verification. This redundancy is what adds strength to the system and limits its exposure to false acceptance or rejection.

In Infra Secure-based systems, multiple mode integration is possible through sensor fusion or decision-level fusion algorithms wherein different inputs are processed in parallel or sequential form to identify an authentication result. These systems are most effectively employed in highly secure locations like government buildings, laboratories, and airports. Seamless integration, usability, speed and accuracy, as well as privacy of the data for all biometric modes, are the areas that need to be addressed by future work.

Real-Time Performance Optimization

Real-time optimization of performance is critical to the practical deployment of vein-based authentication systems, particularly high throughput applications where speed and correctness of access decisions are critical. Infra Secure technology, working through near-infrared imaging to capture vascular patterns, must rapidly process biometric information without compromising accuracy. Slow processing can lead to frustration on the part of users, queues, and reduced efficiency in systems—particularly in venues like airports, business corporations, or secure zones where throughput is critical.

To be executed in real-time, several areas need to be addressed. First, the image capture process would have to be streamlined to take images fast with reduced motion blur or outside interference. This can be achieved through the use of high-end sensors and adaptive illumination systems. Second, the vein recognition algorithms would have to be computational efficient. Utilizing lightweight deep models or hardware acceleration techniques such as GPU or FPGA based processing can significantly reduce response time.

Moreover, system software also needs to

be able to handle parallel processing and concurrent processing of authentication requests. Local processing of data through edge computing can also be utilized to reduce latency caused by data transmission to distant servers. Finally, system performance has to be monitored continuously and updated with the implementation of machine learning techniques to learn new usage patterns in order to ensure smooth real-time authentication performance.

Scalability and Deployment in Large Infrastructures

Scalability is a critical factor when deploying vein-based authentication systems, particularly in large infrastructures such as corporate campuses, airports, government facilities, or smart cities. As the number of users and access points increases, the system must maintain high performance, reliability, and security without degradation in speed or accuracy. Infra Secure-enhanced vein authentication must be architected to support distributed environments where numerous authentication terminals operate concurrently.

To achieve scalability, a modular and decentralized architecture is essential. Edge computing can be employed to process authentication locally at each terminal, reducing latency and minimizing reliance on central servers. This approach not only accelerates decision-making but also enhances fault tolerance and system availability. Cloud integration may also be leveraged for centralized data storage, analytics, and system-wide updates, provided it complies with stringent data privacy standards.

Effective database management is equally important. Biometric templates should be efficiently indexed and encrypted to allow fast retrieval and matching, even as the user base grows into the thousands or millions. Load balancing, network optimization, and the use of scalable communication protocols ensure seamless operation across multiple sites. Future work should focus on intelligent system orchestration, predictive maintenance, and automated deployment tools to support the long-term scalability of vein-based access control systems.

Anti-Spoofing and Liveness Detection Mechanisms

Anti-spoofing and liveness detection are two of the key elements in keeping vein-based authentication systems secure and unbroken. Though vein patterns themselves are difficult to fake because they are unseen and personal, advanced spoofing technologies like artificial hands with replicated vein patterns or thermal print remain possible loopholes. It makes it a necessity to introduce advanced anti-spoofing and liveness detection techniques in an attempt to defend systems against unauthorized use and protect sensitive infrastructure. Liveness detection ensures that the sample of the biometric offered to the system is from a living individual and not a picture, mold, or replica.

Infra Secure technology can be upgraded by innovation of this ability by near-infrared imaging-based real-time blood flow or very small vascular temperature changes detection. Pulse detection, thermal pattern changing, and dynamic hand gesture recognition can be done in a manner that liveness determination can be done without losing the convenience of users. Machine models learned from real and spoof vein data can also be employed to enhance the capability of the system for real and spoofed input detection.

The models analyze temporal and spatial characteristics hard to fake. Vein biometrics integrated with other biometrics or behavioral characteristics can also be employed in order to offer more security against spoofing. New-generation systems need to implement incessant learning as well as adaptive security models so they can combat dominant trends in spoofing.

User Privacy and Data Protection

User privacy and protection of data are the paramount considerations when deploying vein-based authentication systems, particularly where users' biometric data is stored and captured. The vein patterns are not erasable and are intimately connected with an individual, and hence their protection becomes paramount. Unintended exposure and usage of the data can lead to complete privacy violation and irretrievable loss of identity.

In order to eliminate these challenges, systems must catch up with global data protection law such as the General Data Protection Regulation (GDPR) and complementing national laws. It entails storing data in an encrypted form securely both in transit and at rest in a way that secures biometric templates and not disclosed to any third party. Additionally, template protection techniques such as cancellable biometrics and biometric cryptosystems could be employed to render data revocable and non-invertible.

Infra Secure-hardened systems will also have to offer transparency and consent in terms of allowing users to view what data is being collected, what it's collected for, and what access and deletion control they can exercise. Systems need to be developed in line with privacy-by-design principles that curtail data collection and retain only what's necessary. There needs to be

periodic auditing, access control, and effective authentication processes done to protect and handle the users' information. Privacy protection enforces user responsibility and enables ethical use of biometric systems.

Environmental and Situational Adaptability

Environmental and situational flexibility is also a major parameter to guarantee the reliability of vein-based authentication systems, especially when they are deployed in heterogeneous real-world environments. Infra Secure technology from near-infrared images of vascular patterns has to function under some lighting intensity range, skin type, hand poses, and ambient temperature. Failure to factor in these parameters may result in considerable false rejection rates or delays in authentication.

Uncontrolled or external environments induce interference caused by changes in lighting and reflections during imaging, and the aforementioned methods are thus employed here to provide clear and consistent imaging of veins. Infrared sensors also need to be calibrated for supporting different types of skin and environmental conditions like moisture, dust, or temperature fluctuations endangering the visibility of veins.

Environmental factors such as hand motion, direction, or partial occlusions must be accommodated as well. Preprocessing, normalization, and deep learning-based alignment methods can be used to compensate for these variations, enhancing the rate of recognition. Scanning with user feedback can help with correct hand placement and eliminate user error.

Future systems will need to be developed in such a way that they learn and adapt dynamically to diverse environments to attain robustness, reliability, and user satisfaction in all application environments.

Blockchain for Access Auditability

Blockchain can be used to store secure and immutable access logs. Every authentication event can be logged as a block, and this ensures an open and tamper-evident audit trail. This will be particularly beneficial in very secure environments such as government buildings, data centers, or research institutions where it is important to authenticate access history.

User Experience and Real-World Testing

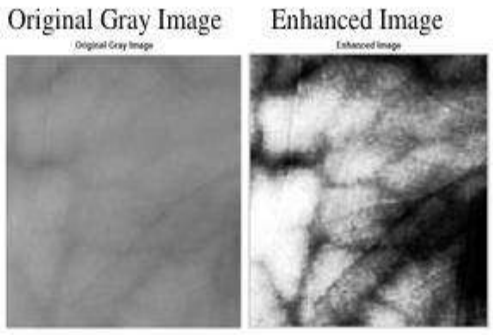
Future work must then focus on usability through the performance of real-world deployment field trials. These field trials will consider system responsiveness, usability, hygiene issues, and user satisfaction. Field trial feedback will be pivotal to iteratively improving system interfaces, training procedures, and enhancing user take-up in varying physical environments.

FV Feature Extraction

Study employed varying levels of fusion and increased the precision of feature extraction. The study declared that the biometric pattern databases should be managed efficiently to enhance verification system performance. Study proposed new features of extraction method utilization and building strong HHsMs in the future to enhance verification systems. The anatomical investigation verified the diameter of the FV difference between the fingertip and finger root and between the sub-branch and core branch. Hence, this research emphasized the enhancement of matching and discrimination of FVs by splitting the width of the core vein branch and the sub-vein branch individually during the matching process . Study considered FAR due to the misalignment of FV images at enrolment and rotation of the finger, which complicates feature extraction. To resolve this issue, a technique for extreme finger rotation and illumination change should be employed in future research. In addition, the ability to augment computation via the integration of multi-modal recognition, herein posited, with scattering blur-restoration techniques needs to be investigated to shed light on noise in FV images.

FV Feature Representation and Recognition

Researches and sought to improve FV images for individuals who do not have vein intersection points to minimize false rejection outcomes. Research explored the applicability of using score-level fusion techniques and established a comparison between FV fusion and that of multi-sample recognition systems. Identifying the correlation between FV and finger dorsal in terms of recognition may be an area to pursue for the authors of Study.



IV. METHODOLOGY

Vein pattern images are captured via the infra red (IR) cameras. The images captured are blur in type since they represent the thermal

signature of the veins pattern. The captured images are usually in jpeg format and converted to gray scale format by using the rgb2gray command in matlab. The vein image patterns are enhanced by using the histogram equalization method where the histogram of the vein patterns are adjusted in sequence in order to increase the vein patterns from the back ground.

The histogram equalized image (O/P Img) is represented by:

O/P Img (x,y) = Where CDF(i), CDF(min) are the ith gray level and minimum cumulative distribution function. (M,N) is the image size and L is the maximum gray level intensity in image. Original Gray Image Enhanced Image The enhanced images are then binarized with the use of Otsu algorithm. Otsu algorithm is founded on choosing a threshold value based on minimum within class variance approach. Minimum within class variance is calculated for every gray level value i.e. from i=0 to 255 and for which gray level minimum class variance is minimum, that gray level is utilized as the threshold value. Depending on the calculated threshold value, the image is binarized i.e. the gray value below threshold value are mapped to back ground and above are mapped to pattern. The binary pattern thus obtained has salt and pepper type noise. It is eliminated by employing the following algorithm:

The histogram equalized image (O/P Img) is given by: O/P Img (x,y) = WHITE) Then P0 is the Background Pixel.

If (P0 = WHITE) & P1= P2 = P3 = P4 = P5 P6 = P7 = P8 = BLACK) Then P0 is the Object Pixel.

Lastly the binary images thus obtained are now thinned to single pixel width vein patterns. This is achieved by employing the pixel neighborhood connectivity algorithm and 8-neighbors of a pixel under scanner. This can be readily implemented with bimorph command in matlab**.**

V. CONCLUSION

Human biometric-based verification medical systems are extensively employed in several medical applications that need dependable verification/identification schemes. Various platforms utilizing FV authentication systems with high security and low verification error rates have gained more and more attention. The current study extends existing research by generating a taxonomy of existing literature. It distinguishes between the kind of research carried out based on FV biometric systems in development and categorizes them into two types (software- and hardware-based component development). Scholars can utilize this taxonomy to identify research gaps in FV biometric authentication system literature. We thoroughly reviewed related papers by underscoring the amount of publications, types of problems, suggested solutions, optimum results, evaluation techniques, existing datasets, reasons, issues and suggestions for further research. Some suggestions for managing and regulating FV biometric authentication healthcare systems are also presented. These guidelines should be adhered to by designers and developers to enable them to design strong and highly secure FV biometric authentication systems that are sufficient for the needs of organizations and companies in terms of security of information. Additionally, a newly suggested solution is described. This can be used in the future to manage the leakage of biometric information, leading to serious threats when stolen FV templates are utilized. The suggested solution will be simulated and deployed in the future to act as a reference for researchers who plan to test secure framework-based decentralized network architectures in health systems, such as access points and other database nodes without a point of centralization.

REFERENCES:

[1]. [Amirthavalli, 2014]Amirthavalli Kannika, and Kirubha D., "Thermal Imaging as a Biometrics Move Towards Facial Signature Substantiation", International Journals of Advanced Computational Engineering & Networking, Vol. 2, No. 1, pp.54-58.

[2]. [Anand, 2013]Anand Jose, Flora T. G. Arul and Philip Anu Susan, "Finger Vein Based Biometric Security System", International Journal of Research in Engineering and Technology, Vol. 2, pp. 197- 200.

[3]. [Arandjelovic, 2010] Arandjelovic Ognjen, Hammoud B. Riad and Cipolla Robberto, "Thermal and Reflectance Based Personal Identification Methodology Under Variable Illumination", Pattern Recognition, Vol. 43, No. 5, pp. 1801-1813.

[4]. [Badawi, 2006]Badawi Ahmed M., "Hand Vein Biometric Verification Prototype: A Testing Performance and Patterns Similarity", IPCV, pp. 3-9.

[5]. [Benziane, 2013]Benziane Sarah and Benyettou Abdelkader, "Biometric Technology Based on Hand Vein", Oriental Journal of Computer Science & Technology, Vol. 6. pp. 401-412. [Buddharaju, 2008] Buddharaju Pradeep, PavlidisLoannis and

[6]. ManoharChinmay, "Face Recognition Beyond The Visible Spectrum",

Advances in Biometrics, Springer London, pp. 157-180.

[7]. [Chekmenev, 2007]Chekmenev Sergey Y., Farag Aly A. and Essock Adward A., "Thermal Imaging of the Superficial Temporal Artery: An Arterial Plus Recovery Model" IEEE Conference on Computer Vision and Pattern Recognition, pp. 1-7.

[8]. [Chen, 2011]Chen Cunjian, and Ross Arun, "Evaluation of Gender Classification Methods on Thermal and Near Infrared Face Image", Biometric International Conference, IEEE, pp. 1-8.

[9]. [Chengbo, 2008]Chengbo Yu, Huafeng Qing, and Lian Zhang, "A Research on Extracting Low Quality Human Finger Vein Pattern Characteristics", The Second International Conference on Bioinformatics and Biomedical Engineering, pp.1876-1879.

[10]. [Chennamma, 2010]Chennamma H. R., Rangarajan Lalitha, and Veerabhadrappa, "Face Identification From Manipulated Facial Images Using SIFT", IEEE International Conference on Emerging Trends in Engineering and Technology, pp. 192-195.

[11]. [Cho Siu, 2011]Cho Siu Yeung, Ting Chan Wai, and Quek Chai, "Thermal Facial Pattern Recognition for Personal Verification Using Fuzzy CMAC Model", International journal of innovative, Information and Control, Vol. 7, pp. 203 - 222.

[12]. [Chu, 2007]Chu Rufeng, Liao Shengcai, Han Yufei, Sun Zhenan, Li Stan Z. and Tan Tieniu, "Fusion of Face and Plamprint for Personal Identification Based on Ordinal Features", IEEE Conference on Computer Vision and Pattern Recognition, pp. 1-2.

[13]. [Covavisaruch, 2006] Covavisaruch N. and Prateepamornkul P., "Personal Identification System Using Hand Geometry and Iris Pattern Fusion", IEEE International Conference on Electro/ Information Technology, pp. 597-602.

[14]. [Deepamalar, 2010] Deepamalar M. and Madheswaram M., "An Improved Multimodal Palm Vein Recognition System Using Shape and Texture Features". International Journal of Computer Theory and Engineering, Vol. 2, pp. 95-101.

[15]. [Ding, 2005]Ding Y., Zhuang D. and Wang K., "A Study of Hand Vein Recognition Method", Proceedings of the IEEE International Conference on Mechatronics & Automation, pp. 2106-2110. [E, 2014] E. Manjunathswamy B, J Thriveni, R Venugopal K and Patnaik L M, "Multi Model Personal Authentication Using Finger Vein and Face Images", IEEE International Conference on Parallel, Distribution and Grid Computing, pp. 341-344.

[16]. [Ferrer, 2007]Ferrer Miguel A., Morales Aythami, Travieso Carlos M. and Alonso Jesus B., " Low Cost Multimodal Biometric Identification System based on Hand Geometry, Palm and Finger Textures", in 41st Annual IEEE International Carnahan Conference on Security Technology, pp. 52-58.

[17]. [Fuksis, 2011]Fuksis R.,KadikisA.andGreitans M., "Biohashing and Fusion of Palmprint and palm vein Biometric Data", In Hand Based Biometric, pp. 98-110.

[18]. [Garbey, 2007]Garbey Marc, Sun Nanfei, Merla Arcangelo, and PavlidisLoannis, "Contact-Free Measurement of Cardiac Plus Based on The Analysis of Thermal Imagery", Biomedical Engineering, IEEE, Vol. 54, pp. 1418-1426.

[19]. [Gault, 2010]Gault Travis R., Blumenthal Nicholas, Farag Aly A., Starr Tom, "Extraction of the Superficial Vasculature, Vital Sign Waveform & Rates Using Thermal Imaging", Computer Vision and Pattern Recognition Workshops, IEEE, pp. 1-8.

[20]. [Ghiassa, 2014]Ghiassa Reza Shoja, Arandjelovi Ognijen, Bendadaa Abdelhakim, and Maldague Xavier, "Infrared Face Recognition", Audio – Video Based Biometrics Person Authentication, Springer Berlin Heidelberg, Vol. 47, pp. 2807- 2824.