Journal of Intelligent System and Applied Data Science (JISADS)

Journal homepage : https://www.jisads.com

ISSN (2974-9840) Online

ENHANCING BIOMETRIC ACCESS SECURITY IN PHARMACEUTICAL COMPANIES THROUGH CONTACTLESS MULTIMODAL FUSION: A PROPOSED MODEL FRAMEWORK AND SYSTEMATIC REVIEW

Boniface Mwangi Wambui[1],, John Kamau1 and Faith Mueni Musyoka[2]*

[1]*School of Computing and Informatics, Mount Kenya University, Thika, 342-01000, Kenya*

[2]*School of Pure and Applied Sciences, University of Embu, Embu, 6-60100, Kenya*

***Corresponding Author**: Boniface Mwangi Wambui; Email: bonniemwangi91@gmail.com; mwangib@mku.ac.ke; jkamau@mku.ac.ke; mueni.faith@embuni.ac.ke

ABSTRACT

The recent advancements in contactless multimodal biometric fusion in respect to the pharmaceutical company's secure access are discussed in the systematic review. The article proposes a new hybrid model framework for secure access. Recent articles that have been published between the year 2020 to 2025 are considered using the using the PRISMA approach. From the findings deep learning such as the CNN architectures have shown a decrease in false acceptance rates and in increase in the recognition accuracy (95–99%). However, most models have not been validated in real-world pharmaceutical contexts, are still unimodal, and do not optimize hybrid settings. To bridge these gaps, the proposed Hybrid CNN–Gabor–PSO architecture integrates feature engineering, data augmentation, and hyper parameter tuning. Adaptative learning rate is incorporated in the model after the new feature generation. CNN layers collect spatial patterns, Gabor filters capture frequency and orientation information, and Particle Swarm Optimization (PSO) optimizes the fused feature subset to minimize intra-class variation. In order to guarantee the security of the pharmaceutical companies, the proposed integrated hybrid feature fusion model guarantees secure, reliable, adaptable and effective authentication.

Keywords: Multimodal fusion, Contactless biometrics, pharmaceutical environments, deep learning, Model.

1. INTRODUCTION

The need to safeguard sensitive information, valuable assets, and controlled substances while preserving environments free from contamination presents the pharmaceutical industry with increasing challenges in providing safe and hygienic facility access. Contactless biometric technologies like facial, iris, and palm vein recognition are becoming more popular as a result of the growing inefficiency and unhygienic nature of traditional access control systems and contact-based biometrics. Traditional access control techniques are usually inadequate in the rapidly evolving threat environment of today, requiring more robust and adaptable security measures [1]. Systems for biometric authentication are now essential for enhancing access control. For safe identification, they use distinguishing physiological and behavioral characteristics such as voice, iris patterns, palm or finger vein patterns, facial structure, and fingerprints [2]. Nevertheless, problems like occlusions, lighting fluctuations, and spoofing continue to restrict unimodal systems. Contactless multimodal biometric fusion combines several biometric characteristics to improve accuracy, security, and dependability in order to overcome these shortcomings. Despite advancements, there is a dearth of comprehensive data regarding the architecture, functionality, and implementation of such systems in pharmaceutical settings, which have stringent hygienic, environmental, and regulatory requirements. Because pharmaceutical facilities need authentication systems that support workers wearing protective gear, operate

dependably in cleanrooms, and adhere to stringent regulatory and contamination-control standards, this gap is operationally significant. Lack of implementation-focused research makes it more difficult to make well-informed decisions and raises the possibility of implementing biometric solutions that don't adhere to operational and compliance standards. In order to improve access security in pharmaceutical companies, this study aims to review and analyze the literature on contactless multimodal biometric fusion techniques. It seeks to pinpoint the most recent developments, obstacles, and weaknesses in biometric authentication and offer a theoretical framework that enhances precision, hygienic practices, and dependability in safe facility access.

Pharmaceutical firms were specifically chosen as the application environment because of their strict security, cleanliness, and regulatory requirements, even though this study is a systematic literature analysis. Traditional contact-based or unimodal authentication methods are insufficient in pharmaceutical environments because they contain controlled drugs, sensitive intellectual property, and regulated cleanroom activities. The study critically assesses current biometric solutions against realistic operational restrictions by placing the review into pharmaceutical settings, which increases the synthesized findings' practical significance.

2. LITERATURE REVIEW

According to [3] the automated identification of people based on their distinct biological and behavioral characteristics is known as biometrics. These characteristics fall into one of two categories: behavioral or physiological. Features that are specific to a person's body, like fingerprints, facial features, iris patterns, and DNA, are examples of physiological biometrics. Behavioral biometrics, on the other hand, look at patterns in an individual's actions or behaviors, such as gait, typing speed, and voice patterns. One type of biometric technology is non-contact biometrics, which gathers behavioral or physiological information without making physical contact with the system. In contrast to conventional fingerprint scanning, contactless biometrics use remote sensing techniques to collect data rather than requiring direct contact with a sensor. Iris scanning, voice recognition, and facial recognition are a few examples.

[4] lists a number of benefits of multimodal biometric fusion, including increased accuracy, better resistance to spoofing attacks, increased usability, and a lower rate of incorrect acceptance or rejection. Combining multiple biometric traits reduces the shortcomings of individual parameters, such as noise, appearance fluctuations, or a lack of distinctiveness, making identification techniques more accurate and dependable. Additionally, the fusion process can offer a more thorough and trustworthy evaluation of a person's identity, enhancing the overall security of the authentication system.

2.1 Contactless biometrics

Contactless biometric methods, including face, iris, voice, palm vein, and finger vein recognition, show clear advantages and disadvantages in all of the examined research. Although facial and voice-based systems are more convenient for users, they are more vulnerable to spoofing attacks, illumination changes, and ambient noise. On the other hand, because of the internal nature of the biometric characteristics, vascular biometrics such as the recognition of veins in the palm and finger consistently report superior accuracy and lower false acceptance rates, even though they frequently need for specialized imaging equipment and regulated acquisition settings. The impetus for multimodal fusion, which combines complimentary modalities to balance usability, robustness, and security, is highlighted by these contrasting findings.

In the wake of the COVID-19 pandemic and the growing demand for touchless interactions in high-security and healthcare settings, contactless biometrics has become a crucial development in safe and hygienic authentication. Contactless biometrics use modalities like voice recognition, palm vein imaging, iris scanning, and facial recognition to identify people without making physical contact, in contrast to conventional contact-based systems like fingerprint or hand geometry scanners. The increasing use of deep learning and multimodal fusion techniques to enhance recognition accuracy, robustness, and spoof resistance under variable conditions like lighting, pose, and occlusion is highlighted in recent literature. Research highlights that contactless biometric systems provide hygienic and operational advantages, making them appropriate for regulated settings like medical and pharmaceutical facilities ([5];[6].

When users wear personal protective equipment, such as masks or gloves, issues with data privacy, template protection, interoperability, and performance consistency still exist. The literature emphasizes that although contactless biometrics improve security and user convenience, more research is needed to optimize multimodal fusion techniques, privacy-preserving algorithms, and practical deployment frameworks to satisfy the demanding needs of crucial industries like healthcare and pharmaceuticals.

The contatless authentication consists of:

Finger vein Recognition: According to [7], finger vein recognition is a biometric technology that recognizes an individual based on the vein patterns on their fingertips.

Online: https://doi.org/10.64680/jisads.v3i2.48

Finger vein biometrics uses a person's unique vein patterns to verify their identity. Vascular biometrics are biometrics that rely on blood vessels beneath the skin. Hemoglobin, a protein in our blood that contains iron, changes color when exposed to visible or near-infrared light. This enables the reader to examine each user's vein patterns. The vein pattern is digitally recorded in the cloud and secured.

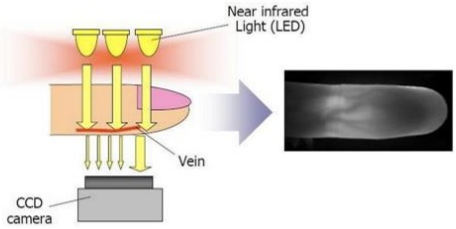

Figure 1: Finger Vein Data Capturing

Source (Shadhar, [7])

Figure 1 above shows that specialized capture equipment is used to gather data from the finger vein. Near-infrared light, a lens, a light filter, and picture capture technology make up the majority of the capture apparatus. Because finger veins are located beneath the skin's surface, they are invisible to the unaided eye. This device uses near-infrared light, which is capable of penetrating human tissue. Near-infrared light can be blocked by pigments like melanin and hemoglobin.

Palm Vein Recognition: [8] states that vein recognition, also known as vascular biometrics, is based on the hemoglobin vessels' ability to absorb light in the 750–960 nm wavelength range. Veins seem darker as a result of this impairing light reflection. According to preliminary study, vein patterns are recorded and compared to enrolled samples in order to confirm identity.

Vein recognition is believed to be more secure than other biometric methods since the authentication data is concealed beneath the skin. [9] claims that the method utilizes characteristics of inside body veins. Despite being identical twins, this distinguishes them from one another. Developing these attributes is really difficult. This technology is based on the special network of blood vessels located beneath the skin of the human finger. Infrared light and a monochrome CCD camera are used by vein identification reconnaissance systems to take pictures of the palm patterns. Through your finger, the hemoglobin in your deoxygenated blood absorbs infrared light, allowing a camera to capture an image. The vein pattern on the fingers is depicted in the figure by black lines. Before being used for authentication, these data are processed and transformed into a digital representation.

The vein pattern is extremely difficult to duplicate since it is hidden within the tissues of the palm and can only be confirmed using advanced equipment. The palm vein images are reprtesented in figure 2 below.

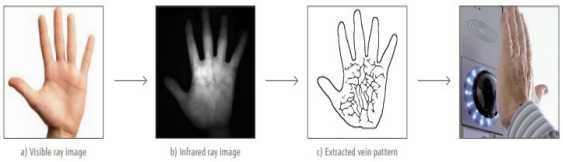

Figure 2: Palm vein Scanner

Source: Image retrieved from Fujitsu Identity Management (white paper) [10].

The examined literature increasingly highlights performance outcomes, fusion issues, and dataset heterogeneity as important research concerns, even as extensive descriptions of various biometric modalities provide technical footing. According to studies, system generalizability is greatly impacted by elements including uneven acquisition settings, a lack of cross-dataset validation, and inadequate dataset diversity. In order to address these issues, feature-level fusion, data augmentation, and optimization strategies are given priority in contemporary research, which emphasizes the necessity of analytically driven assessments as opposed to merely descriptive ones.

2.2 Security systems level in Pharmaceutical Companies

Digital health is a quickly expanding subject that enables more effective, precise, and efficient patient treatment, according to [11]. Pharmaceutical companies may now produce customized drugs based on unique genomic sequences thanks to digitization. Additionally, it makes it possible to effectively monitor drug absorption, plasma concentration, and bioavailability, strengthening the bond between businesses and patients. Sophisticated businesses are seriously threatened by cyber security breaches by hackers, thieves, and country states. Intellectual property, medical records, and medication contents are stolen. Emails that are private are visible to the public. Medical records are used to create false identities. Examples of recent data breaches include Anthem's theft of client and employee personal data earlier this year, Target's 2014 breach of 70 million credit card records, and JP Morgan Chase's 76 million account breach. The U.S. Food and Drug Administration (FDA) has issued cyber security advisories for specific goods due to an increase in medical device breaches within the last six months. Infusion pumps, for example, give patients preset amounts of fluids [11]. Strict environmental and hygienic regulations, such as ISO 14644, which governs cleanroom

contamination management, exacerbate these cyber-physical vulnerabilities in pharmaceutical settings. In order to prevent contamination, these legal frameworks require contactless and cyber-resilient access control measures. The requirement for safe, contactless, and multimodal biometric solutions is thus increased because authentication systems used in pharmaceutical facilities must concurrently handle cybersecurity risks, regulatory compliance, and cleanroom hygiene.

Medical devices on hospital networks are susceptible to future breaches as they can be found online. Information that has been compromised damages one's reputation. Although the effects are very different, both industrial and information systems are susceptible to exploitation. Manufacturing process disruptions can have potentially fatal outcomes in addition to monetary losses and damage to one's reputation. Pharmaceutical and medical technology cybersecurity breaches endanger the availability and integrity of these vital systems in addition to jeopardizing the privacy of personal information and intellectual property. [12] advise businesses, particularly pharmaceutical companies, that use networked computer systems to scout out and then close security vulnerable areas before it is too late, rather than waiting until an attacker stops or is informed that an attack is imminent. Cyberattacks can occur at any time and spread so quickly that most victims are unaware of the alerts. It is not a good idea to wait until a cyberattack occurs before fixing critical infrastructure flaws.

2.3 Review of E-Health Cyber security Models

The adoption of smart devices has altered how healthcare organizations collect data, according to [13]. Wearables with sensors generate enormous amounts of data, which must be efficiently gathered, stored, and analyzed for trends. To protect sensitive and private information, the enormous volume of data collected should only be accessible to those who are permitted. Private information, particularly e-health data, is often sought after by unauthorized individuals. Numerous scholars have investigated different cybersecurity models for electronic health systems. A Modular Access Control (MAC) system was created by [14] especially for use in medical settings. Their approach extended the Role-Based Access Control (RBAC) model by adding access allocation to nodes and maintaining medical context to include patient conditions. This architecture ensured the safe implementation of data in medical sensor networks.

[15] introduced a biometric data authentication-based security architecture for Wireless Body Area Networks (WBAN). Their method places a strong emphasis on the use of the sender's electrocardiogram (ECG) as a crucial component in avoiding patient data confusion. This technique improves cryptographic key distribution and reduces computational mistakes since biometric characteristics are specific to each individual. The framework also has robust security mechanisms and is reasonably priced.

2.4 Multimodal Biometric System (MBS)

An enhanced authentication framework known as a multimodal biometric system uses two or more of a person's biometric characteristics to confirm their identification. When compared to single (unimodal) biometric systems, a multimodal biometric system increases the accuracy, dependability, and security of identity verification by combining various forms of biometric data, such as fingerprint, face, iris, voice, palm vein, or gait. In practical applications, multimodal biometric systems are becoming more and more common. To improve accuracy and security, a multimodal biometric system makes use of several biometric characteristics. Even though multimodal biometric systems use numerous modalities to improve accuracy and reliability, scalability issues could still affect them.

Scalability issues can arise from managing data from multiple modalities, guaranteeing interoperability across diverse components, and maintaining performance under growing workload. For large-scale deployment scenarios to function well, scalability must be addressed. However, as multimodal systems may also display comparable traits, scalability problems might not be unique to unimodal systems 16]. A multibiometric system can greatly reduce the overlap between the picture features of different people (inter-class similarities) by combining biometric traits and employing a fusion approach. While gathering information from multiple sources will make the feature vector more dimensional, the biometric system's overall accuracy will rise. For example, two family members may have a similar voice, yet their fingerprints or iris characteristics may differ.

Table 1 presents a consolidated summary of the studies included in this systematic literature review, highlighting their methods, key findings, and limitations. The table directly corresponds to the reviewed literature and supports the comparative analysis by mapping existing approaches to identified research gaps. Its placement within the literature review section ensures alignment with the SLR narrative and improves interpretability.

Online: https://doi.org/10.64680/jisads.v3i2.48

Table 1 below shows the reviewed articles on contactless biometric authentication.

Author(s)	Year	Title	Method	Key Findings	Limitation
[17]	2025	RSNet: Region Specific Network for Contactless Palm Vein Authentication	CNN	RSNet regional learning	Unimodal limitation
[18]	2024	IOT Contactless or biometric recognition using CNN	CNN	Improved recognition accuracy	No integration with hybrid fusion
[19]	2025	Enhancing Ad Hoc Network Security using Palm Vein Biometric Features	CNN+ key generation (AFBKG)	Achieved 98% authentication accuracy, 0.1% FAR, 95% spoof resistance	Unimodal limitation lacked wrapper-based feature selection
[20]	2025	Deep Learning Techniques for Hand Vein Biometrics: A Comprehensive Review	CNN	Multimodal fusion advances	No hybrid model wrapper model proposed
21]	2024	StarLKNet: Star Mixup with Large Kernel Networks for Palm Vein Identification	CNN	High Accuracy achieved using novel architecture	Single modality No Wrapper Model
[22]	2024	Mobile Contactless Palmprint Recognition : Use of Multiscale, Multimodal Embeddings	CNN + ViT hybrid Embeddings	High accuracy & low latency in mobile world	Unimodal limitation
[23]	2024	Utilizing Biometric Authentication to Prevent Private Sharing of Physician Information for Prescription System Access	CNN	Proven reduction in the unauthorized access to physician credentials	No exploration of hybrid palm and finger vein
[24]	2021	Palm Vein Identification Based on Hybrid Feature Selection Model	SVM+KNN +DT+NB	Hybrid selection improves accuracy	No usage of augmented data
[25]	2024	Semantic-based approach for medical cyber-physical system (MCPS) with biometric	wearable sensors (WBANs)	high accuracy levels (97.6% for EEG + eye blinking	Interoperability and standardization issues across heterogeneous

		authentication for secured privacy			medical devices and protocol
[26]	2025	Multimodal biometric authentication system leveraging optimally trained ensemble classifier using feature-level fusion	Bi-LSTM + DCNN ensemble classifier	Achieved high accuracy (98.23% and 97.92%) and low Equal Error Rates (EERs of 3.23% and 3.62%).	deployment in real-world settings remains untested (no field trials) adversarial robustness in varying environmental conditions
[27]	2020	Contactless Multi-biometric System Using Fingerprint and Palmprint Selfies	SVM+LBP	better accuracy and lower error rates	Score-level fusion limits feature synergy.
[28]	2020	Wrist vascular biometric recognition using a portable contactless system. Sensors,	SIFT+SURF +ORB	low Equal Error Rate (EER = 0.08 %)	system is sensitive to environmental lighting variance High computational overhead

A clear methodological evolution from general CNN architectures to region-specific and hybrid learning methodologies can be seen in an analysis of the papers compiled in Table 1. For instance, by concentrating feature extraction on discriminative vascular regions rather than processing the entire image uniformly, RSNet's regional learning strategy outperforms previous CNN models in terms of resilience and recognition performance. This pattern is indicative of a larger movement toward efficient architectures and targeted feature learning, which tackle issues like computational inefficiency, feature redundancy, and background noise seen in previous models

CNN: Convolutional Neural Network

SVN: Support Vector Machine

KNN: K Nearest Neighbor

DT: Decision Tree

NB: Naïve Bayes

LBP: Local Binary Pattern

SIFT: Scale-Invariant Feature Transform

SURF: Speeded-Up Robust Features

ORB: Oriented FAST and Rotated BRIEF

The CNN's scheme: From raw input data, the feature extraction layers are in charge of extracting meaningful groups; for example, feature extractors in face recognition CNN extract facial features like the nose, eyes, palm and so on. The retrieved features are mapped to the appropriate classes by the classification layers (the features are transferred to the corresponding individual in the facial recognition example). To create smaller data, the input is passed through several convolution layers in figure 6 below where a filter is applied. To make the data even more compact, a pooling layer is frequently added to take the maximum (or average, in the case of average pooling) of nearby data components. The output is then produced by feeding the final filtered data via a network that is fully connected [29].

2.5 CNN Model

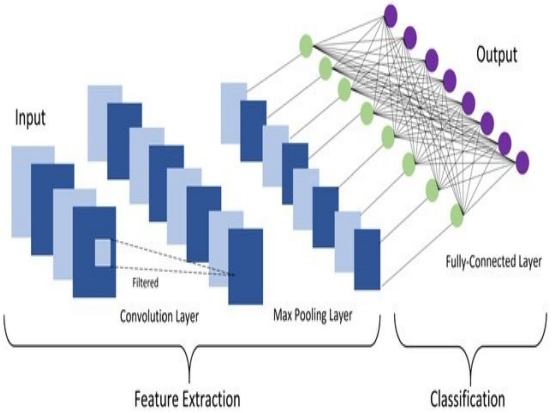

Figure 3 CNN Model

To improve the extended CNN model's feature extraction in figure 3 above various variances are added to the input data, data augmentation is used to enhance feature extraction and strengthen the model. During the preprocessing stage, it is used before the input layer. As reported [30] data augmentation improves performance and accuracy of the model. Feature engineering is applied in the creation or selection of such features that improve model functionality. Within CNNs this is normally completed before the Convolution Layer using the preprocessing techniques like color space conversion, edge detection and normalization. Optimization of hyper parameter adjust occurs to the learning rates, activation functions as well as the filter size and convolutional layers. This affects various elements of the networks like the convolutional layer, pooling layers, fully connected layer and the learning process and need to be applied when training the model to boost efficiency and accuracy.

While the Following section presents a suggested hybrid framework that is based on the gaps and limitations found in the examined literature, the preceding sections methodically review the body of research on contactless multimodal biometric authentication.

3. METHODOLOGY

To guarantee transparency, rigor, and reproducibility, this study uses a Systematic Literature Review (SLR) methodology that is guided by the PRISMA framework. In order to incorporate recent developments in contactless and multimodal biometric technologies, especially those that emerged following a surge in the need for hygienic authentication systems worldwide, a five-year assessment window (2020–2025) was chosen. Due to their poor applicability to contemporary deep learning-based methods, earlier research was disregarded.

Prominent scientific databases, such as IEEE Xplore, SpringerLink, and ScienceDirect, which index excellent peer-reviewed research in biometrics, artificial intelligence, and security systems, were used for the literature search. Peer-reviewed journal articles and a few high-impact conference papers that focused on contactless biometric authentication or multimodal fusion that were published in English between 2020 and 2025 met the inclusion criteria.

Research that was only unimodal, lacked technical rigor, or had nothing to do with secure facility access was eliminated. Relevance and methodological consistency were guaranteed by this procedure.Identification, screening, eligibility evaluation, and inclusion were the four organized phases of the SLR. Using predetermined keywords, pertinent articles were found during the identifying process. Abstract-level filtering and duplicate removal were used in the screening process.

Using predetermined search terms, a total of pertinent records was obtained from chosen electronic databases during the identification stage. Studies that did not address contactless biometric authentication or multimodal fusion were eliminated after duplicates were eliminated and the remaining publications were screened using titles and abstracts. Twelve articles that satisfied all methodological and thematic requirements for in-depth analysis were found after a full-text eligibility assessment utilizing specific inclusion and exclusion criteria. The final group of studies assessed was the outcome of the eligibility assessment, which comprised full-text evaluation against the inclusion criteria. To ensure uniformity and prevent technical content from being misunderstood, only English-language articles were taken into consideration. A PRISMA flow diagram (figure 4) is supplied to visually illustrate the selection process, showing the number of records identified, excluded, and included at each stage, in order to improve transparency and reproducibility.

Online: https://doi.org/10.64680/jisads.v3i2.48

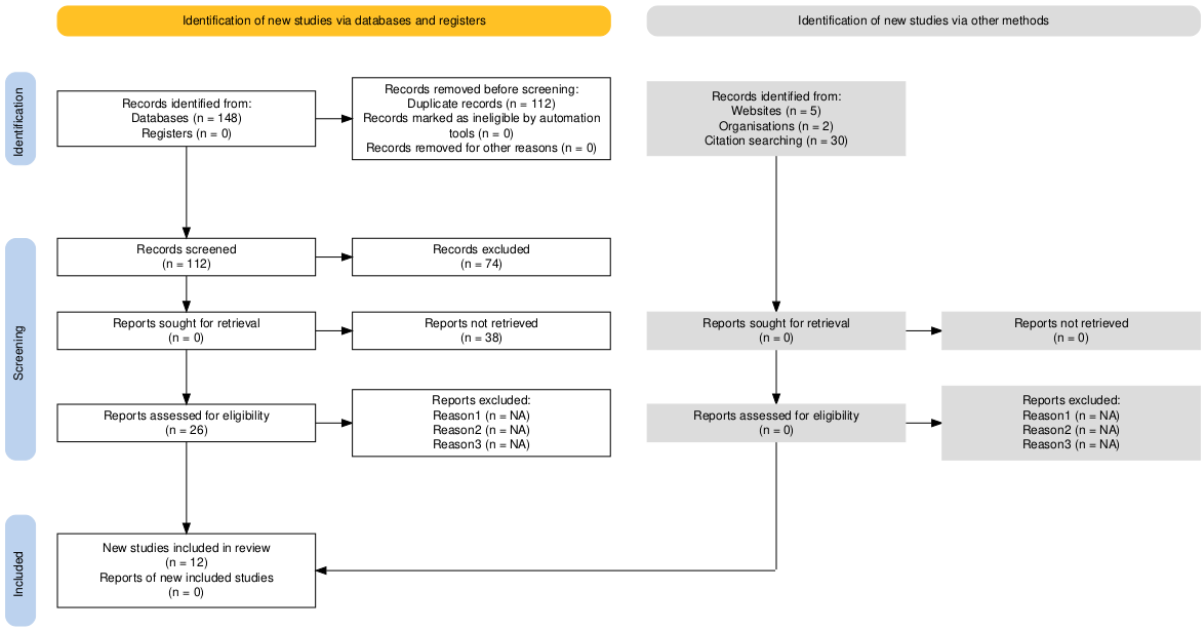

Figure 4: PRISMA Flow Diagram

4. RESULTS

The Results section presents synthesized findings derived from the systematic literature review rather than experimental or implementation-based outcomes. It summarizes reported performance metrics, fusion strategies, and architectural trends across the reviewed studies to identify dominant approaches and persistent limitations. No new dataset or empirical evaluation is introduced at this stage, as the primary objective is evidence synthesis.

Table 2: Results Synthesized and Weaknesses Found in Contactless Multimodal Biometric Fusion Research (2020–2025)

Category	Key Findings / Results	Current Weaknesses / Research Gaps
Model Type	CNN-based models dominate the field, showing improved accuracy (95–99%) across palm, finger, and wrist vein recognition. Hybrid deep models (CNN + Bi-LSTM, CNN + ViT) achieve better spoof resistance and faster convergence.	Most studies remain unimodal; limited hybrid integration (e.g., palm + finger vein). Few models combine classical ML with deep learning for optimization.
Fusion Level	Feature-level fusion yields higher recognition performance than score- or decision-level approaches. Ensemble fusion (Bi-LSTM + DCNN) achieved EERs below 3.5%.	Lack of standardized fusion frameworks; limited comparative testing across datasets.
Performance Metrics	Several studies achieved accuracy above 97% with FAR below 0.5%, indicating strong potential for secure facility access systems.	Results are often dataset-specific; absence of cross-dataset validation and robustness testing under real-world conditions.

Optimization Techniques	Feature selection and optimization (e.g., PSO, wrapper-based selection) improve computational efficiency and accuracy when applied.	Most CNN models do not include optimization layers; high computational cost and model complexity persist.
Deployment & Validation	Systems demonstrate potential for secure, contactless pharmaceutical facility access; CNN-based fusion enhances hygiene and usability.	Limited field implementation, interoperability issues with existing systems, and absence of lightweight, energy-efficient architectures.
Security & Privacy	Deep learning models significantly improve spoof resistance and identity verification confidence.	Few studies address privacy-preserving techniques (e.g., homomorphic encryption, cancelable biometrics) or regulatory compliance frameworks.

Table 2 above shows that CNN-based architectures routinely outperform conventional models in contactless biometric authentication, especially in palm and vein recognition tasks, across the 12 reviewed studies (2020–2025). Nevertheless, the majority of frameworks are still in the laboratory evaluation stage, with limited multimodal integration, no field validation, and high computational overhead, even though they have achieved high accuracy and low error rates. The most promising approaches for future implementation in pharmaceutical settings where security and hygienic conditions are crucial are hybrid fusion and optimization techniques. CNN is still in the lead, recognizing palm and hand veins with high accuracy (up to 98%). From the findings recent research on hybrid multimodal systems using the classical machine learning models such as the Support vector machines(SVM) and K-Nearest Neighbours(KNN) have shown better perfomance and robustness than the unimodal biometric systems. Ensemble-based and feature-level fusion techniques improved spoof resistance and generalization, but their practical application is still limited.

From the findings most of the studies never employeed the feature optimazing features which increases the systems acuracy. Despite these improvements, common problems persisted, including a large computational overhead, no field validation, and a limited range of wrapper-based features. Emerging applications such as wearable EEG and eye-blink sensors for secure access showed significant potential in healthcare settings, despite challenges with interoperability and standardization. The hybrid multimodal feature-level fusion with the optimized feature generation is the most promising model for enhancing the relibility and secure access of biometric systems in pharmaceutical companies.

4.1 Security Extensions

By combining contactless biometrics with secure tokens or behavioral biometric cues for anomaly detection, the suggested architecture can be expanded to include multi-factor authentication. This multi-layered security strategy improves defense against unauthorized access and insider threats. Additionally, it is advised to stress-test system robustness against presentation attacks using generative adversarial network (GAN)-based spoofing simulations in order to improve resistance under realistic threat situations.

5. PROPOSED MODEL FRAMEWORK

The following is the proposed authentication framework. The proposed framework model in Figure 5 above entails a concept of combination of CNN and 2D Gabor filters of feature extraction and integration of Wavelet Transform and Autoencoders as features representations enhancing scheme. Hybrid feature selection, that is, applying Particle Swarm Optimization (PSO) has been adopted to optimize feature selection, and then is trained and tested along with hyperparameter tuning, data augmentation, and feature engineering.

Online: https://doi.org/10.64680/jisads.v3i2.48

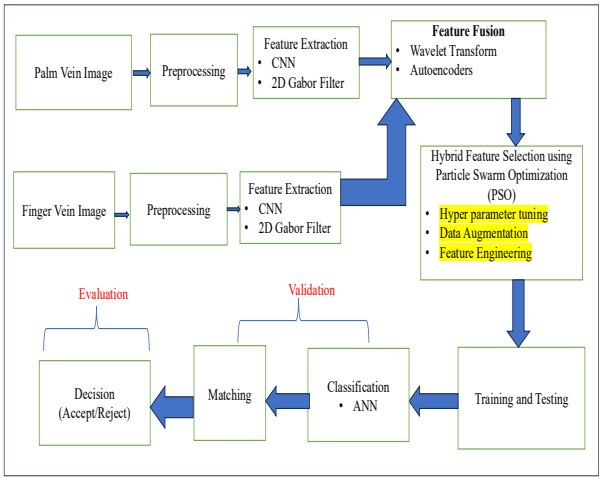

Figure 5 : Proposed Model Framework
Source: (Self, 2025)

ANN takes care of classification where the identity of the user is predicted prior to the matching procedure where extracted features are compared against registered biometric templates. The last stage is the determination stage (Accept/ Reject) which determines the authenticity of the authentication process, this is done on the basis of the results in the classification and matching stages. This biometric authentication workflow increases precision, resilience and computation before a biometric.

The proposed mathematical equations for the optimized Hybrid Feature-Level Biometric Model

a) Input and Preprocessing

Let:
P: Palm vein image
F: Finger vein image
After processing
P = Preprocess (P), F =Preprocess*(F)*

b) Feature Extraction using CNN and Gabor Filters

Extracted feature maps from each modality:

$\Phi\ P$=CNN (P) ⊕Gabor (P)

$\Phi\ F$=CNN (F)⊕ Gabor (F)

Where:

⊕ Concatenation of CNN and Gabor features

c) Feature Fusion using Wavelet Transform and Autoencoder

Fused feature representation

$$\Phi = Autoencoder(WaveletTransform(\phi\_P \cup \phi\_F))$$

Where:

∪: Union of feature vectors from both modalities.

$\Phi \in \mathbb{R}^n$: Combined feature vector

d) Feature Engineering and Data Augmentation

Let:
E: Engineered features
A: Augmented training samples

Enhanced features after engineering:

$$\Phi' = \Phi \cup E \cup A$$

e) Adaptive Learning Rate Optimization

Update learning rate dynamically using cosine annealing

$$\eta_t = \eta_{min} + \frac{1}{2}(\eta_{max} - \eta_{min})\left(1 + cos\left(\frac{t\pi}{T}\right)\right)$$

Apply learning rate in weight update

$$w_t + 1 = w_t - \eta t \cdot \nabla L(w_t)$$

Where:

η_t = Learning rate at time t

Lw_t= Loss function such as cross-entropy

f) Hybrid Feature Selection using Particle Swarm Optimization (PSO)

Let:

$\Phi' \in R^n$: full feature set

$S \subseteq \Phi'$: candidate feature subset

$J(S)$: fitness function (e.g., ANN accuracy

PSO optimization:

$$S^* = argmax_{S \subseteq \Phi'} J(S)$$

Each particle's position and velocity update

$$v_i^{t+1} = \omega v_i^t + c_1 r_1 (p_i^* - x_i^t) + c_2 r_2 (g^* - x_i^t)$$
$$x_i^{t+1} = x_i^t + v_i^{t+1}$$

Where:

v_i : Velocity

x_i : Current position (feature subset)

p_i^*: Best Local Solution

g^* : Best Global Solution

ω, c_1, c_2 : inertia and acceleration constraints

$r_1, r_2 \sim (0,1)$: Random Values

g) Classification using Artificial Neural Network (ANN)

Feed selected features S^* into ANN

$$\hat{y} = ANN(S^*) = \sigma(W \cdot S^* + b)$$

Where:

$\hat{y}$:predicted Probability

σ: Activation function such as SoftMax or sigmoid.

W,b: Weights and biases.

Online: https://doi.org/10.64680/jisads.v3i2.48

h) Biometric Matching and Decision Rule

Compare output with stored template T using Euclidean distance:

$d = ||\hat{y} - T||_2$

Decision rule:

$$Match = \begin{cases} Accept, & if\ d \leq \theta \\ Reject, & if\ d > \theta \end{cases}$$

Where θ is the acceptance threshold.

General Equation for the Hybrid Contactless Biometric Authentication Model

$$\text{Decision} = \begin{cases} Accept, & if\ ||ANN\ (PSO(AE(WT(\text{CNN} \oplus \text{Gabor (P)}\ \cup\ CNN \oplus \text{Gabor (F)})\ \cup\ E\ \cup\ A))) - T||_2 \leq \theta \\ Reject, & otherwise \end{cases}$$

General Equation (with Learning Rate Optimization)

$$\text{Decision} = \begin{cases} Accept, & if\ ||ANN_{\eta_t}\ (PSO(AE(WT(CNN_{\eta_t} \oplus \text{Gabor (P)}\ \cup\ CNN_{\eta_t} \oplus \text{Gabor (F)})\ \cup\ E\ \cup\ A))) - T||_2 \leq \theta \\ Reject, & otherwise \end{cases}$$

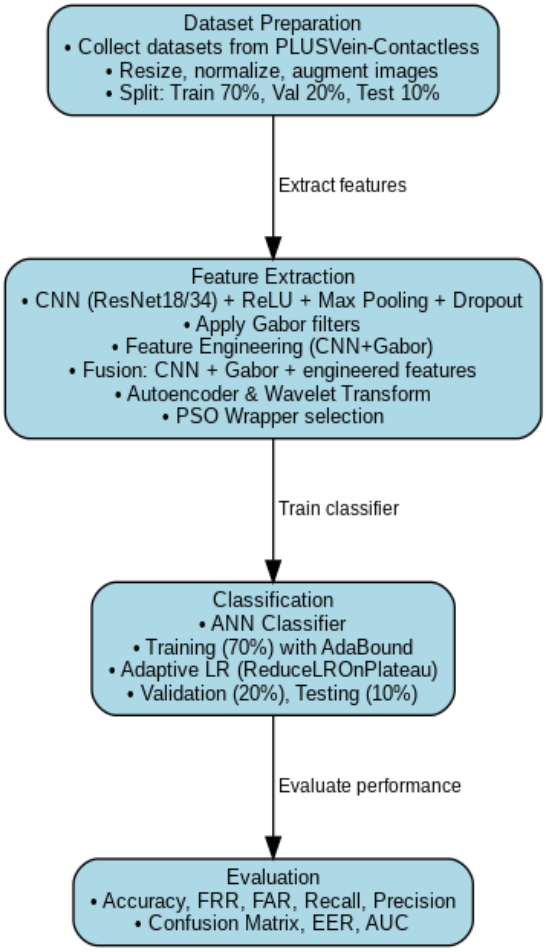

Figure 4 : Proposed Hybrid model Experiment Flowchart Source: (Self, 2025)

Figure 4 above shows the proposed experimental flowchart to implement the proposed contactless hybrid feature-level fusion authentication model.

The dataset will be split into taining(70%), validation(20%) while 10% will be used for model taining. It will entail feature extraction using CNN+Gabor filters. Several layers such as convolutional, dropout and flatter layers will be applied. The fusion will entail the new engineered features with the CNN and Gabor filters and Particle Swam optimization(PSO) will be applied to optimized the new model. Artificial Neural Networks(ANN) will be used for classification while various metrics such as False acceptance rate(FAR), False rejection rate(FRR),Recall and the confusion matrix.

5.1 Practical Deployment and Strategic Considerations

The suggested hybrid contactless biometric framework should be implemented gradually to ensure successful real-world adoption in pharmaceutical settings. This should start with pilot implementation in high-security areas like drug storage areas and research and development vaults before expanding to entire facilities. With the least amount of disturbance, this method allows for the controlled assessment of system performance, usability, and operational impact. In order to reduce cyber risks, which are still a major problem in pharmaceutical information systems, secure middleware integration and robust network designs are essential for backend compatibility.

Biometric acquisition may be hampered by the personal protection equipment (PPE) that is frequently required in pharmaceutical work situations. The suggested system addresses this by supporting backup authentication methods, such as secure credentials or secondary biometric modalities, to guarantee business continuity. Rapid user onboarding and re-enrollment modules are also prioritized in order to reduce downtime and accommodate changing workforce needs without interfering with regulated procedures.

By combining contactless biometrics with secure tokens or behavioral biometric cues for anomaly detection, the architecture can be expanded to accommodate multi-factor authentication from a security standpoint. Furthermore, adding anti-spoofing techniques, such as generative adversarial network (GAN)-based simulations, improves resistance under realistic threat scenarios and permits robustness testing against presentation attacks. Energy-efficient edge computing architectures for on-device biometric matching should be taken into account in future system evolution to lower latency and increase reliability. Additionally, modality options beyond palm and finger vein recognition, like gait or radar-based signatures, should be expanded to strengthen redundancy.

6. DISCUSSIONS

The design of the suggested hybrid CNN–Gabor–PSO framework is informed by practical deployment issues in pharmaceutical applications, despite the fact that it involves substantial mathematical and algorithmic depth. Hygienic access control is supported by contactless biometric modalities, and resilience under changing lighting, occlusion, and user mobility is improved through feature-level fusion and optimization. Additionally, the framework's modular design enables integration with current pharmaceutical access control systems, addressing both operational viability and security. Original datasets or preliminary experimental measures like accuracy, FAR, or FRR are not presented in this paper. Rather, it methodically combines published findings from previous research to create performance standards and support the suggested hybrid framework. Future research to empirically evaluate the suggested model must include experimental validation and dataset-based assessment.

Integrating cutting-edge technologies is extremely difficult for pharmaceutical organizations, especially when it comes to supply chain management, patient data protection, and access control. The intricacy of operational procedures, the demand for interoperability between historical and contemporary systems, and strict regulatory requirements are frequently the causes of these difficulties. In order to ensure both operational integrity and legal compliance, compliance frameworks like Good Manufacturing Practices (GMP), ISO 27001 for information security, and HIPAA for patient data protection set stringent requirements that must be followed. Therefore, effective integration necessitates solutions that balance innovation and compliance while simultaneously improving security and efficiency and adhering to these regulatory criteria.

For biometric and access control systems used in high-risk settings like pharmaceutical companies, security strengthening is a crucial prerequisite. In order to combat evolving cyberattacks, [31] points out that intrusion risks in contemporary digital infrastructures require "robust security measures," such as sophisticated intrusion detection methods, real-time monitoring, and adaptive machine learning-based defenses. The authors also stress that resilience against illegal access and data breaches is strengthened by combining anomaly detection methods with intelligent threat intelligence systems. In order to guarantee operational dependability and regulatory compliance in delicate pharmaceutical settings, these insights highlight the necessity of integrating anti-spoofing methods, multi-factor authentication, and adaptive security layers within contactless biometric frameworks.

By facilitating intelligent feature learning, optimization, and anomaly detection, the synergistic integration of artificial intelligence improves the efficacy of biometric fusion and access control systems. According to [32] "enhanced security, efficiency, and transparency" are made possible by AI integration, which enables complex systems to dynamically adjust to changing operating and threat conditions. This synergy facilitates strong fusion methods and better decision-making in controlled contexts when applied to contactless multimodal biometrics.

7. CONCLUSION

From the findings of the systematic review, the proposed contactless hybrid model ensures a secure, adaptable and efficient model for enhancing the security of the pharmaceutical’s companies. The combination of several biometric characteristics such as facial recognition, finger vein, and palm vein significantly improves operational efficiency, spoof resistance, and identification accuracy. Achieving high security and complying with the industry standards is vital for these companies since they deal with medicine and formulas that are very confidential. The proposed hybrid CNN Gabor filters model framework is able to overcome the current challenges due to the

Online: https://doi.org/10.64680/jisads.v3i2.48

incorporation of feature engineering, data augmentation and hyper parameter tuning.

PSO's mathematical feature optimization improves generalization and minimizes redundancy, guaranteeing trustworthy access verification even in a variety of environmental circumstances. In addition to improving authentication accuracy, this integrated approach satisfies the pharmaceutical industry's operational requirements and strict hygiene standards.

Biometric authentication solutions must be implemented in pharmaceutical settings in accordance with industry-specific compliance standards, HIPAA-like frameworks, GDPR, and other data protection and privacy regulations. The suggested model's practical practicality is strengthened by incorporating privacy-by-design principles, secure biometric template management, and audit measures to ensure regulatory compliance while upholding user confidence.

8.0 RECOMMENDATIONS

In order to reduce latency and increase reliability in network-constrained contexts, future developments of this work should look into energy-efficient edge computing architectures that allow on-device biometric matching. Further strengthening redundancy and improving system robustness across a range of operational conditions can be achieved by extending the selection of biometric modalities beyond palm and finger vein detection, such as adding gait-based or radar-based signatures.

To confirm the proposed hybrid CNN–Gabor–PSO model's computational effectiveness and robustness, future studies should concentrate on putting it into practice and assessing it in actual pharmaceutical settings. The creation of standardized multimodal datasets will make it possible to compare and benchmark outcomes. Using sophisticated data augmentation pipelines and automated hyperparameter tuning (like Bayesian optimization) will increase flexibility in response to changing circumstances. To guarantee adherence to data protection regulations, researchers should also investigate lightweight CNN architectures for edge deployment and incorporate privacy-preserving features like homomorphic encryption or cancelable biometrics. Lastly, it is advised that industry and academia work together to convert the suggested hybrid framework into scalable, deployable, and legally compliant pharmaceutical facility Access control solutions.

REFERENCES

[1] Poonia, P., & Ajmera, P. K. (2024). Robust Palm-print Recognition Using Multi-resolution Texture Patterns with Artificial Neural Network. Wireless Personal Communications, 1-19. DOI: 10.1007/s11277-023-10819-0

[2] Kumar, K. P., Prasad, P. K., Suresh, Y., Babu, M. R., & Kumar, M. J. (2024). Ensemble recognition model with optimal training for multimodal biometric authentication. Multimedia Tools and Applications, 83(23), 63497-63521. DOI: 10.1007/s11042-024-18541-0

[3] Xaba, S. L., Aworinde, H. O., & van Niekerk, B. (2025). A systematic literature review on integrating contactless biometrics into online learning environments. Edelweiss Applied Science and Technology, 9(9), 172-194. DOI: 10.55214/2576-8484.v9i9.9781

[4] Abozaid, A., Haggag, A., Kasban, H., & Eltokhy, M. (2019). Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion. Multimedia tools and applications, 78(12), 16345-16361. DOI: 10.1007/s11042-018-7012-3

[5] Chowdhury, A. M., & Imtiaz, M. H. (2022). Contactless fingerprint recognition using deep learning—a systematic review. Journal of Cybersecurity and Privacy, 2(3), 714-730. DOI: 10.3390/jcp2030036

[6] Matsuda, S., & Yoshimura, H. (2022). Personal identification with artificial intelligence under COVID-19 crisis: a scoping review. Systematic Reviews, 11(1), 7. DOI: 10.1186/s13643-021-01879-z

[7] Shadhar, A. M. (2022). The finger vein recognition using deep learning technique. Wasit Journal of Computer and Mathematics Science, 1(2), 1-7. Doi: 10.31185/wjcms.43

[8] Nakisa, B., Ansarizadeh, F., Oommen, P., & Shrestha, S. (2022). Technology Acceptance Model: A case study of palm vein authentication technology. IEEE Access, 10, 120436-120449. Doi: 10.1109/ACCESS.2022.3221413

[9] Shaheed, K., Liu, H., Yang, G., Qureshi, I., Gou, J., & Yin, Y. (2018). A systematic review of finger vein recognition techniques. Information, 9(9), 213.

[10] Fujitsu. (n.d.). Fujitsu Identity Management and PalmSecure (White Paper). Fujitsu. Retrieved from https://www.fujitsu.com/my/imagesgig5/PalmSecure%20Whitepaper.pdf

[11] Jaithliya, T. (2017). Cyber security in pharmacy and pharmaceutical companies. J Pharm Sci, 2. Doi: 10.29011/2574-7711.100021

[12] Kannan, U., & Swamidurai, R. (2023). INDIRECT CYBER ATTACK ON PHARMACEUTICAL COMPANIES. Journal of Pharmaceutical Negative Results, 1766-1782. Doi: 10.47750/pnr.2023.14.02.222

[13] Sari, A., & Sopuru, J. (2021). E-Health Threat Intelligence Within Cyber-Defence Framework for E-Health Organizations. Smart Systems for E-Health: WBAN Technologies, Security and Applications, 161-179. Doi: 10.1007/978-3-030-14939-0_7

[14] Garcia-Morchon, O., & Wehrle, K. (2010, March). Efficient and context-aware access control for pervasive

medical sensor networks. In 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops) (pp. 322-327). IEEE.doi: 10.4108/ICST.PERCOMWORKSHOPS2010.6832

[15] Ramli SN, Ahmad R, Abdollah MF, Dutkiewicz E (2013) A biometric-based security for data authentication in wireless body area network (wban). In: 2013 15th international conference on advanced communication technology (ICACT), IEEE, pp 998–1001. Available at https://opus.lib.uts.edu.au/handle/10453/120960?

[16] Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2024). A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection. IEEE Access, 12, 64300-64334. Doi: 10.1109/ACCESS.2024.3395417

[17] Luo, D., Huang, J., Yang, W., Shakeel, M. S., & Kang, W. (2025). RSNet: Region-Specific Network for Contactless Palm Vein Authentication. IEEE Transactions on Information Forensics and Security. Doi: 10.1109/TIFS.2025.3544029

[18] Hasan, M., Hoque, T., Ganji, F., Woodard, D., Forte, D., & Shomaji, S. (2024). A Resource-Efficient Binary CNN Implementation for Enabling Contactless IoT Authentication. Journal of Hardware and Systems Security, 8(3), 160-173.doi: https://doi.org/10.1007/s41635-024-00153-7

[19] Mohamed, A., Salama, A., & Ismail, A. (2025). Enhancing Ad Hoc Network Security using Palm Vein Biometric Features. Engineering, Technology & Applied Science Research, 15(1), 20034-20041. Doi: https://doi.org/10.1007/s41635-024-00153-7

[20] Hemis, M., Kheddar, H., Bourouis, S., & Saleem, N. (2025). Deep learning techniques for hand vein biometrics: A comprehensive review. Information Fusion, 114, 102716. Doi: https://doi.org/10.1016/j.inffus.2024.102716

[21] Jin, X., Zhu, H., Yacoubi, M. A. E., Li, H., Liao, H., Qin, H., & Jiang, Y. (2024). Starlknet: Star mixup with large kernel networks for palm vein identification. arXiv preprint arXiv:2405.12721. available at: https://arxiv.org/abs/2405.12721?utm_source=chatgpt.com

[22] Grosz, S. A., Godbole, A., & Jain, A. K. (2024). Mobile contactless palmprint recognition: Use of multiscale, multimodel embeddings. IEEE Transactions on Information Forensics and Security, 19, 8428-8440. Doi: https://doi.org/10.1109/TIFS.2024.1234567

[23] Hosseini, A., Khalil Loo, B., & Aghsami, A. (2024). Utilizing Biometric Authentication to Prevent Private Sharing of Physician Information for Prescription System Access. Journal of Industrial Engineering and Management Studies, 11(2), 105-122. Available at: https://jiems.icms.ac.ir/article_219394.html

[24] Alfoudi, A., Alsaeedi, A., Abed, M., Otebolaku, A., & Razooqi, Y. (2021). Palm vein identification based on hybrid feature selection model. International Journal of Intelligent Engineering and Systems, 14(5), 469-478.doi: 10.22266/ijies2021.1031.41

[25] Vashisht, C., Kaushik, R., & Kaushik, E. (2024). Semantic-based approach for medical cyber-physical system (MCPS) with biometric authentication for secured privacy. Digital Transformation in Healthcare 5.0: Volume 2: Metaverse, Nanorobots and Machine Learning, 237. Doi: 10.1515/9783111398549-010

[26] Jha, K., Jain, A., & Srivastava, S. (2025). Multimodal biometric authentication system leveraging optimally trained ensemble classifier using feature-level fusion. Technology and Health Care, 09287329251363424. Doi: 10.1177/09287329251363424

[27] Herbadji, A., Guermat, N., Ziet, L., Akhtar, Z., Cheniti, M., & Herbadji, D. (2020). Contactless Multi-biometric System Using Fingerprint and Palmprint Selfies. Traitement du Signal, 37(6). Doi: 10.18280/ts.370602

[28] Garcia-Martin, R., & Sanchez-Reillo, R. (2020). Wrist vascular biometric recognition using a portable contactless system. Sensors, 20(5), 1469. Doi: 10.3390/s20051469

[29] Hashemi, B., Talebi, A. F., & Janghorbani, A. (2025). Generative adversarial networks based synthetic biology: A promising approach to sars-cov-2 mutations prediction. Engineering Applications of Artificial Intelligence, 148, 110395.

[30] Benegui, C., & Ionescu, R. T. (2020, November). To augment or not to augment? Data augmentation in user identification based on motion sensors. In International Conference on Neural Information Processing (pp. 822-831). Cham: Springer International Publishing.

[31] Komar, R., Patil, A., & Ali, W. A. (2023). Emerging Trends in Cloud Computing: A Comprehensive Analysis of Deployment Models and Service Models for Scalability, Flexibility, and Security Enhancements. Journal of Intelligent Systems and Applied Data Science, 1(1).

[32] Aloun, M. S. (2024). Synergistic Integration of Artificial Intelligence and Blockchain Technology: Advancements, Applications, and Future Directions. Journal of Intelligent Systems and Applied Data Science, 2(2).