IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 37, No. 3, June, 2023, pp. 709-718
Journal homepage: http://iieta.org/journals/ria

Advancements in Biometric Authentication Systems: A Comprehensive Survey on Internal Traits, Multimodal Systems, and Vein Pattern Biometrics

Jaya S. Mane[1], Snehal Bhosale[2*]

[1] Department of Computer Science and Engineering, Symbiosis Institute of Technology, Symbiosis International (Deemed University) (SIU) Lavale, Pune 412115, Maharashtra, India
[2] Department of Electronics and Tele-Communication, Symbiosis Institute of Technology, Symbiosis International (Deemed University) (SIU) Lavale, Pune 412115, Maharashtra, India

Corresponding Author Email: snehal.bhosale@sitpune.edu.in

https://doi.org/10.18280/ria.370319

Received: 21 January 2023
Accepted: 31 May 2023

Keywords:
biometric authentication, vein-based biometric features, multimodal biometric authentication

ABSTRACT

Biometric authentication systems, entities that leverage unique biological traits for individual identification, have become increasingly relevant in the digital age, addressing critical safety and security concerns. These biometric identifiers, being distinct and irreversible, uniquely differentiate individuals. Biometric recognition's significance extends to diverse domains, including forensics, defense, surveillance, personal identification, and banking. The impetus for advancements in biometric authentication systems is driven by the imperative need for resilience, high precision, and resistance against spoofing. This paper aims to elucidate the recent advancements in this evolving field. The fundamentals of biometric authentication systems, issues and vulnerabilities inherent in basic biometric systems, as well as the cutting-edge biometric systems developed in recent years, are thoroughly reviewed. The paper further explores how challenges can be mitigated through the deployment of Multimodal biometric systems and vein pattern-based systems. A synopsis of real-time face recognition incorporating morphing attack detection is also provided. This comprehensive survey concludes that the performance of biometric recognition systems is continually being augmented, predominantly through the incorporation of deep learning frameworks and 3D biometric imagery, which offer highly accurate representations of human biometric features.

1. INTRODUCTION

The cornerstone of any application requiring user access is robust and secure authentication, which serves as a bulwark against unauthorized access. Traditional authentication mechanisms, principally password management, typically involve the use of login IDs and passwords. However, the challenge of recalling multiple credentials often prompts users to note them down, consequently exposing the system to potential security breaches. These could occur through loss of credentials by the user or leakage and hacking of login information, underscoring the necessity for a more secure authentication approach [1, 2].

Biometric Authentication emerges as a robust alternative to traditional methods. This technique identifies individuals based on their unique features, which can be classified into Physiological or Behavioral biometric traits. Physiological traits encompass physical characteristics such as the face, ear, iris, retina, fingerprint, palm geometry, ECG, DNA, odour, palm vein, and finger vein. In contrast, behavioral traits include voice, signature, gait, and keystroke patterns, which reflect the individual's personality [1, 2].

Among the myriad biometric traits, face and fingerprint-based recognition systems have gained popularity due to their user-friendly nature. Since biometric authentication hinges on the individual's identity for validation, it supersedes traditional authentication methods that rely on login IDs and passwords. The inherent advantages include the elimination of password management, memorization, and concerns about password loss or hacking.

Despite the superiority of biometric authentication over traditional methods, it is not devoid of challenges. Concerns regarding aliveness detection, privacy protection, and security have been noted. Consequently, several researchers have proposed advanced systems to address these issues, which will be discussed in the subsequent sections of this paper.

- Proposed novel methodologies for verification.
- Use of better image acquisition devices and preprocessing techniques.
- By working on feature extraction methodologies.
- Introduce the use of unique biometric features or feature combinations.

According to the literature review vein pattern biometric recognition is one recent advancement in biometric authentication that handles the issue of aliveness detection. While multimodal authentication systems are based on a foundation of multiple biometric parameters, they are more dependable and accurate. The use of 3D images is a further advancement in biometric authentication that produces more precise and reliable results since human biometrics are more precisely represented in 3D images.

In this survey paper, section 2 is the literature survey of some biometric authentication systems published in recent years, section 3 summarizes attacks and issues on basic

biometric authentication systems, section 4 summarizes the morphing attack in real-time face recognition system, section 5 introduces the concept of multimodal biometric authentication systems, and section 6 covers vein pattern-based biometric authentication.

2. LITERATURE SURVEY

Zhang et al. [3] proposed an Android-based multimodal biometric authentication system with face and voice biometrics. This system takes a face and voice as input. The authors also introduced an improved LBP (Local Binary Pattern) feature extraction method which is coding-based to reduce time and space complexity and an enhanced VAD (Voice Activity Detection) method for voice recognition. They present an adaptive fusion strategy for combining matching scores for face and matching scores for voice to implement multimodal biometric authentication.

In the study [4], Mandalapu et al. have surveyed audio-visual biometric recognition techniques, Public databases available, and presentation attack detection algorithms. As mobile devices and laptops have inbuilt audio and face capture facilities, Audiovisual biometric systems are easy to implement. Data acquisition from users for such systems is in a user-friendly manner as compared to the collection of other biometric features.

Toygar et al. [5] introduced an open-access first multimodal vein database named FYO in which each letter is the first letter of each author's first name. This dataset contains a palm, dorsal, and wrist vein of the same individual; they also proposed multimodal deep learning-based CNN architecture using decision-level fusion. This deep learning approach showed improved performance compared to traditional hand-crafted feature extraction.

Obayya et al. [6] proposed a palm vein authentication model. Which uses Convolution Neural Network (CNN) with Bayesian Optimization. CNN is the most popular deep learning architecture. For image preprocessing, Jerman enhancement Filter is used. The proposed model is more computationally efficient as optimization of CNN avoids adding unnecessary convolution layers to network structure thus it also solves the overfitting problem.

Bhattacharya et al. [7] developed a new deep learning-based algorithm named "vein and periocular pattern-based CNN (VP-CNN)". They proposed a "forehead vein and periocular pattern-based biometric system (FPPBS)", which takes the forehead subcutaneous vein pattern and periocular biometric pattern as input. They also developed the FSVP-PBP database based on captured images of forehead veins and periocular patterns. The system is developed for entry control and it works in a contactless manner. The proposed system is low-cost and portable and introduces the use of new biometric features in the field of biometric authentication.

Table 1. Literature review summary table

Advanced Biometric Authentication System	Biometric Traits Used	Methodology Used	Advantages of the System	Future Scope
[3] Multimodal biometric authentication	Face and voice	Improved local binary pattern (LBP) Improved voice activity detection (VAD) Adaptive fusion strategy	Less time and space complexity Lower misjudgment ratio Improved authentication performance	A multimodal system using other biometrics with reduced training data and a deep learning framework for mobile terminals can be developed to improve accuracy.
[5] Multimodal biometric authentication based on vein pattern	Palm, Dorsal, Wrist Vein pattern	Deep learning-based Convolutional Neural Networks (CNN) architecture and decision-level fusion	proposed CNN architecture has superior performance compared to hand-crafted methods.	Spoofing attacks can be tested on FYO dataset. Different Deep learning architecture can be implemented in the system.
[6] Contactless Authentication System	Palm vein	Deep Learning with Bayesian Optimization	computationally efficient as Bayesian optimization avoids unnecessary training models and finds the best model in fewer iterations.	Enhance the system to work with a larger dataset with a larger number of identities and introduce a Precise and strong segmentation method for accurate vascular pattern extraction
[7] Biometrics System based vein pattern	forehead region vascular structure and the edge patterns of the periocular region.	Deep learning-based algorithm named Vein and Periocular Pattern-based Convolutional Neural Network (VP-CNN).	Portable and low-cost entry control system	Performance accuracy can be enhanced further. Enhance the system for Multimodal biometric applications to address security issues.
[8] Multimodal Biometric Recognition Based on 3D images	3D hand geometry and 3D palmprint	Global features, mean features, weighted mean features.	Improved recognition performance due to fusion	The system can be extended to improve system's universality, recognition accuracy, and resistance to fraudulent attacks

Iula and Micucci [8] proposed a multimodal biometric system that uses 3D ultrasound palm print and hand geometry images. Ultrasound images help to obtain gravimetric images of the human body which give a more accurate representation

of characteristics and verify liveness. The proposed system also improved recognition accuracy. Ultrasound images are not affected by environmental factors as well as stains of hand like grease or ink, as well these extract under-skin features, so make the system non-spoofable.

A novel wrist vein pattern-based biometric recognition system embedded in smartphones is introduced [9]. This contactless biometric authentication system is proven to be hygienic. It is basically for unlocking screens and making online payments more secure using smartphones. For Image capturing a near-infrared LED with a near-infrared camera already implemented in smartphones is used. Two algorithms are also introduced for guiding proper wrist vein pattern recognition as follows:

- "Three-Guideline Software for Contactless Vascular Biometric Recognition (TGS-CVBR)" and
- "Preprocessing and Identification Software for Contactless Vascular Biometric Recognition (PIS-CVBR)"

TGS-CVBR provides video on the smartphone's screen and guides users to place their wrists properly for good quality image acquisition during enrollment as well as recognition phases. PIS-CVBR consists of three parts: Image preprocessing and verification by feature extraction and matching of features. Thus it is responsible for the identification of users.

Table 1 summarizes the findings from a literature survey done for advancement in biometric systems and also enumerates their future enhancement. It is found that deep learning framework is widely used to improve the accuracy and performance of the system. Vein pattern biometrics is difficult to forge so avoid fake authentication. Multimodal systems improve recognition performance due to the fusion of multiple biometric modalities and also address security issues. Many public datasets are available but while developing application-specific multimodal systems researchers developed their own dataset. The use of 3D images is a future trend in biometric authentication.

3. ATTACKS AND ISSUES ON A BIOMETRIC AUTHENTICATION SYSTEM

Dargan and Kumar [10] have summarized different attacks possible on biometric systems. Although biometric authentication is strong and secure enough as compared to traditional authentication systems based on login credentials, it is susceptible to many direct or indirect attacks. These attacks are on the overall working of authentication systems such as feature extraction algorithms or modules, and template matching algorithms or modules which are the two major components of any biometric authentication system. Rui and Yan [11] also summarized some attacks depending on the biological characteristics used for biometric authentication. For example:

- Face recognition systems can be cheated by using photographs of users obtained easily from the internet, or social media, or can be stolen by some means. Attackers can use video or face images to do false authentication.
- The Iris recognition system can be attacked by capturing iris images of the user using a high-resolution camera. These images later can be used by attackers to do fake authentication.
- Fingerprint and palmprint are easily available on the surfaces the user has touched. Many materials are available to collect them. These collected samples can be later used by the attacker for false authentication.
- Recognition systems based on ECG signals are susceptible to attack in which attackers use users' ECG signals collected using infrared sensors.

Voice recognition systems can be cheated using the user's voice, which can easily be recorded and used later.

As discussed in the study of [12] the deepfake attack is one more frequent way that a digital ID system might be compromised. Deepfakes are artificial intelligence (AI) created fake images that are easily deceptive to human sight. This is a presentation attack of some sort. Deepfakes are becoming more and more capable of deceiving even the greatest facial recognition systems due to the rapid advancement of deep learning. Face swapping with the Face Swapping Generative Adversarial Network (FSGAN) makes it simpler to create deep fakes because the FSGAN doesn't need to be trained with source and target photos for some hours. It implies that deepfakes can spread faster and more easily than ever before because anyone with a working knowledge of this technology can now produce them. Thus to overcome these attacks and protect biometric recognition systems from fake or collected data some countermeasures have been suggested by researchers.

It has been observed that for such attack prevention and security of authentication systems, multimodal biometric systems are attracting researchers and it is becoming popular nowadays. Along with this Vein pattern recognition is also one of the recent trends observed in the field of biometric authentication.

In recent years many biometric recognition systems have been developed to satisfy specific application requirements, by using advanced algorithms and some new biometric features as discussed in section 2. Let us now discuss face morphing attack detection in a unimodal face recognition system.

4. FACE MORPHING ATTACK DETECTION IN THE FACE RECOGNITION SYSTEM

Face Recognition is the most popular way to identify a person. It is found to be in use in public security-based applications like automated border control (ABC), person identification at airports, in healthcare for monitoring patients as well as staff, security in the banking sector, access control in organizations, and in education sector for students and staff identification. Different types of attacks are possible on face recognition systems [12-14].

In many nations, the applicant must submit an analog or digital version of the facial image that will be utilized for the ePassport issuance process. A wanted criminal may swap his face with the face of a lookalike accomplice in a face-morphing attack scenario. A legitimate ePassport outfitted with the altered face image will be given to the accomplice if he applies for one with that feature. Remember that altered facial photos can be convincing enough to trick human assessors. The morphing image kept on the ePassport could then be used to successfully verify both the offender and the accomplice. Thus, the offender can pass through ABC gates (or human instructor at the border) using the ePassport supplied to the accomplice. The risk created by this attack, also known as a face morphing attack, is heightened by the ease with which non-experts can create realistic altered face photos

using readily accessible, either freely available or reasonably priced, face morphing software [15].

Face morphing is one of the most frequently found attacks on face recognition systems. The purpose of a face morphing attack is to fool a person's recognition system by producing a morphed face image. Morphed face images can be obtained by combining two or more personal face images. This synthetic image can help all these persons to get authenticated by the face recognition system. Most of the time person identification is done by verifying a person's live captured face image with the image stored in the database during enrolment or with a photograph present on the machine-readable document issued after enrolment [16, 17].

During enrolment itself, malicious users provide morphed images and get the genuine document issued. So it is possible for the malicious user to bypass the system and get authenticated using morphed images. To detect such malicious users, it is necessary to implement a morph attack detection system. Let us discuss face morphing generation and detection methods briefly [15, 16, 18, 19].

4.1 Face morph generation method

Face morphing nowadays is made very easy. Many online tools are available for generating face-morphing images [16]. The methods for morphing faces can be categorized into two categories as shown in Figure 1(a).

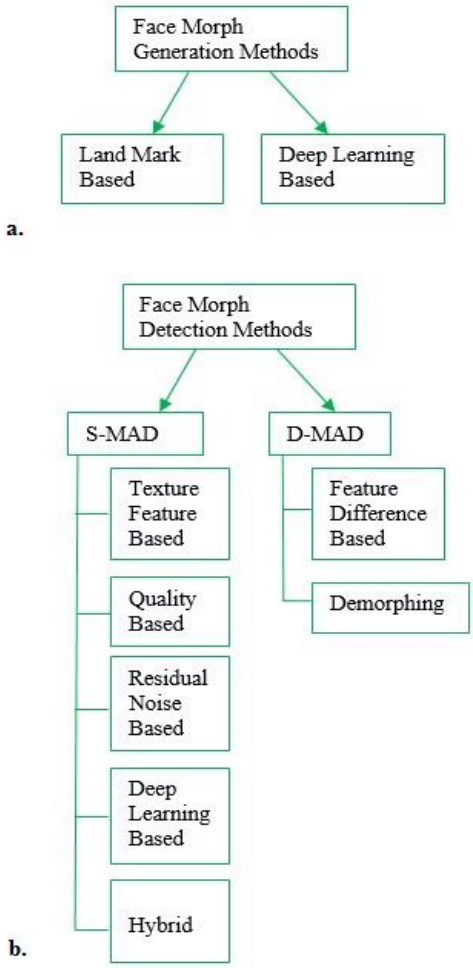

Figure 1. a. Face morph generation and b. face morph detection methods

4.1.1 Landmark-based method

The human face is identified by three main features: eye, nose, and mouth. The landmark-based method accesses these three feature-based regions for processing landmark points. Landmark points of both the face images involved in morphing are wrapped together by placing pixels in an average location. This movement of pixels is done using different methods. Sometimes images obtained by this type of wrapping lead to some uncommon image formation so some post-processing is needed to obtain realistic images.

4.1.2 Deep learning-based method

These are based on GAN (Generative Adversarial Networks). Due to advancements in deep learning, morph generation using GAN has become possible. Morph images are generated using two sample images. MorGAN architecture consists of a generator that generates an image of good quality from scratch. The deep learning-based method was found to be more effective as compared to landmark-based morphed image generation.

4.2 Face morph detection method

Face morphing attacks can be detected by two approaches: Single image-based MAD(S-MAD) and differential image-based MAD (D-MAD) [16] as shown in Figure 1(b).

4.2.1 Single image-based MAD (S-MAD)

Input morphed images can be in any of two forms digital or print-scan. S-MAD techniques can be categorized further based on features of images used for morph detection purposes as follows:

- Texture feature-based S-MAD- This approach uses the texture feature of the image. This approach was found to be effective and accurate for digital as well as print-scan-type images.

Limitations: picture resolution-sensitive, lack of ability to generalize image resolution and morph images, and performance degradation for print scan data.

- Quality-based S-MAD- These methods verify image quality to find the real or fake image. As morphed images are of poor quality compared to the real images. This approach was found to be effective and accurate for digital but not so accurate for print-scan-type images.

Limitations: Compressed data-sensitive, lack of ability to generalize image resolution and morph images, and performance degradation for digital and print scan data.

- Residual Noise-based S-MAD- These methods examined pixel disturbance in a morphed image, as morphed images generated by wrapping two images results in pixel movement. These methods are performing well on digital datasets but have not been tested yet on a print-scan morph image dataset.

Limitations: Compressed image-sensitive. Need high resolution images for good results. Applicable to only digital morph images.

- Deep Learning-Based S-MAD- For image classification different Deep learning approaches are found to be effective. This leads to the use of deep learning-based methods for face morph attack detection. These approaches have shown good performance on both digital as well as print-scan images.

Limitations: Large database needed for training, high cost of calculation, lack of ability to generalize morph images.

- Hybrid S-MAD- Hybrid approach makes use of different classifiers as well as feature extraction techniques together. This results in a good performance for both digital and print-scan morph images, but it leads to more computational costs.

Limitations: high cost of calculation, need to optimize a number of parameters so difficult to implement.

4.2.2 Differential image-based MAD (D-MAD)

The main goal of this technique is to find out whether the face image on a document like a passport is genuine or morphed. The comparison is done between real-time captured face images from the camera and images from the documents. These methods subdivided into two types Demorphing and feature difference-based D-MAD

- Feature difference-based D-MAD- These methods first extract features from both the images the one captured from the camera and the other which is on the document (maybe morph image). These extracted feature differences are calculated and used to detect face-morphing attacks.

Limitations: Its computational cost is high and performance is sensitive to the segmentation of face region, type of image data and features.

- Demorphing-This method discovers the image used for morph generation. This method is powerful for good-quality images but performance decline for real-time images captured by the camera is having light and pose variations.

Limitations: Performance is sensitive to facial pose and lighting variations. It also requires constrained image data.

In order to get reliable performance in practical application, MAD approaches must be generalized. But only known face morph generation methods and recognized sources of digitization (types of printer and scanner) are used to evaluate the current MAD procedures. When MAD approaches are tested on unidentified sources of generation, their performance degrades. If learning-based MAD approaches are not trained on a large-scale dataset containing all real-life variants, it limits their applicability. Therefore, developing a MAD method that is capable of spotting face-morphing attacks is crucial [16].

5. UNIMODAL AND MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEMS

Let us introduce unimodal and multimodal biometric authentication systems briefly [10, 20]. Unimodal biometric authentication systems are using only one biometric feature for authentication. Ex. Face recognition, and fingerprint recognition for biometric attendance in offices. As it is dependent on only one biometric feature, it may face challenges like poor recognition rate, less accuracy achieved, and high-security requirements. It also has drawbacks like what if the person has a physical disability with the biometric feature that is used for the biometric authentication or if some accidental cases happened with that biometric feature.

Multimodal biometric authentication systems use fusion of multiple biometric traits to authenticate users. These systems are therefore more accurate, have a good recognition rate, and are more secure as compared to unimodal.

Ryu et al. [21] published a survey on Continuous Multimodal Biometric Authentication schemes. It is observed that many Multimodal Biometric Authentication systems use a combination of only behavioral biometric traits, some use combinations of only physiological biometric traits, and some work on mixed combinations of behavioral and physiological traits to improve performance and security. Also, the number of modalities (Number of biometric features) used ranges from two to four. But there is no clear discussion about how many biometric traits could optimize the accuracy of the system.

To classify the features extracted from biometric traits, different types of machine learning Algorithms are used in various authentication systems, as they guarantee higher accuracy and security. These algorithms can be supervised, unsupervised, semi-supervised, and reinforcement learning. Supervised learning algorithms work on labeled dataset while unsupervised algorithms do not require any prior knowledge about training data. Supervised learning algorithms need a large amount of training data. Though most Multimodal systems apply supervised learning approaches for classification. An unsupervised learning approach i.e. PCA (Principal Component Analysis) is preferred for facial recognition.

Semi-supervised learning is combination both of supervised and unsupervised. It uses a large amount of unlabelled data and little amount of labeled data. These classification algorithms has not explored yet for multimodal biometric authentication system. Reinforcement learning is not suitable for limited resources available as they work in complex environments and do not require certain input output.

Through the literature survey, it is noted that for continuous multi-modal biometric authentication systems supervised machine learning algorithms (k-Nearest Neighbors, Naïve Bayes, Random Forest) are more commonly used as these algorithms are found to be more accurate than unsupervised learning techniques. But it has the limitation of over-training issues, unsupervised, semi-supervised machine learning approaches have not been explored yet by researchers, they could have the capability to be used in continuous authentication systems.

Researchers used different classifiers for their authentication system and compared the results obtained. According to survey done in the study [21], Gaussian Mixture Model (GMM) is found to be best classifier for voice and face authentication rather than Artificial Neural Networks (ANN) and Support Vector Machine (SVM).

For the specific multimodal biometric authentication systems researchers used their private dataset according to the system requirement, as the multimodal biometric system needs different features of the same person. Public datasets available are based on single feature samples like Face, fingerprint, finger vein, iris, etc. which could not be suitable for multimodal biometric systems.

Following are some trade-off need to be considered while implementing Multimodal biometric authentication system [10]:

- Selection of correct combination of biometric modalities is required as fusion of two or more biometric modalities can generate problem.
- Deciding the number of traits used is an important aspect for the system development.
- Fusion framework and efficient recognition algorithms need to be used.
- Biometric trait Capturing device cost and performance need to be considered.
- Input Capturing Device accuracy and reliability is playing a vital role for data acquisition.

- Designing a real time application specific system is needed.
- Application specific data set generation is required.
- There may be a need for generation of better data acquisition tools based on a combination of biometric traits used.
- User acceptance for the multimodal system is important.

5.1 Working of a multimodal biometric system

Figure 2 describes the generalized working of a Multimodal Biometric System which uses a score-level fusion mechanism and 2 biometric features. Multiple Biometric Features are taken as input from users using different data acquisition devices. These collected features from the user are processed by the preprocessing module. These processed images in the next step are used by the feature extraction module. The matching score calculation is done separately for each biometric modality used. These matching scores are later combined by score level fusion and given to the authentication module. The authentication module is responsible to decide whether the user is authenticated or not.

5.2 Fusion level mechanisms

The basic requirement of any Multimodal Biometric Authentication scheme is what type of biometric features to be used in the system and which fusion level mechanism should be used for their fusion. There are mainly 4 fusion level mechanisms observed in the literature survey- score level, decision level, feature level, and rank level fusion [21, 22]. Score-level fusion is the widely used fusion technique due to its good performance.

There may be different fusion-level results in a good performance depending on the platform on which the authentication system is to be implemented such as mobile or computer and also on the biometric traits that are preferred for authentication. Table 2 summarizes all 4 fusion-level mechanisms.

Fusion levels used in a multimodal biometric authentication system decide at which stage and how the features extracted from different biometric traits will be combined.

In the study [23], researchers have proposed a multimodal system with fusion at two levels to improve the overall recognition accuracy of the system. Two fusion levels used are feature level and score level fusion. Three biometric traits used by the system are fingerprint, Palmprint, and earprint.

In the study [24], two multimodal biometric authentication systems are published.One uses feature-level fusion for ECG and fingerprint biometric fusion, and the Other based on decision-level fusion mechanisms for the same biometric traits. CNN is used for feature extraction. Two layers of CNN with different feature descriptors were selected and the highest accuracy was achieved.

In the study [25], fingerprint matching score and fingerprint liveness detection score are combined by score level fusion mechanism to avoid spoofing attacks. This approach is one kind of advancement in the traditional way of fingerprint recognition. This will prevent fake authentication attempts by attackers using collected or generated samples of user fingerprints.

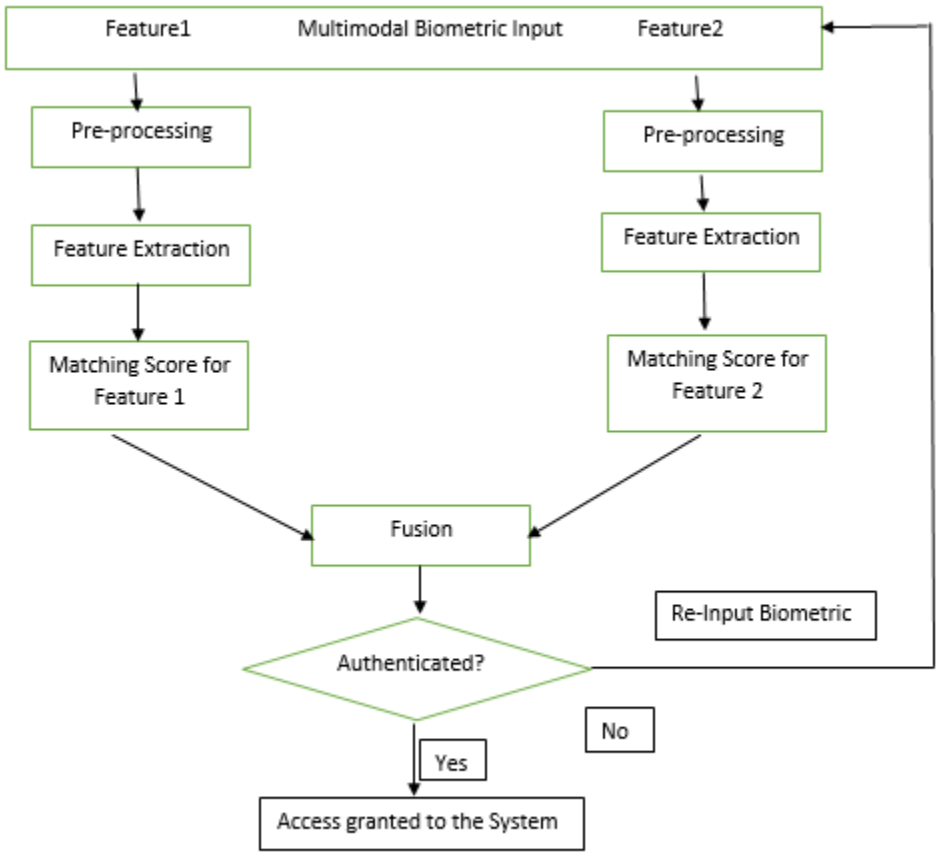

Figure 2. Multimodal biometric system working model

Table 2. Fusion level mechanisms

Fusion Level Mechanism	Method of Fusion Used	Key Characteristics
Score Level	Each modality matching score is calculated independently, these scores are then combined.	It is the most popular fusion method, the system is easily extensible by just adding another modality.
Feature Level	Combine different features extracted from different modalities to form a single template	Creating a single template removes noise in biometric images, allowing de-identification of the image but it generates high computational load.
Decision Level	Is the same as score level fusion, but the score is in the form of a feature match or non-match.	Recognition results are like rejected or accepted, so more convenient and easier to fuse rather than score fusion.
Rank Level	Enrolled users are ranked according to the output from multiple biometric recognition systems. Matching users are sorted using confidence. These ranks further decide the best match.	Processing time required is reduced as compared to feature-level fusion and it is easier than score-level fusion.

5.3 Performance measure

Accuracy is the major evaluation criterion used in the field of multimodal biometric authentication. Along with accuracy following are the commonly used measures according to a survey [21].

- False acceptance rate (FAR)- represents how the model blocks fake access.
- False rejection rate (FRR)- it shows how frequently legal users are rejected by the system.
- Equal error rate (ERR) -is the error rate at which FAR and FFR are equal.

"FMR (False Match Rate)" and "FNMR (False Non-Match Rate)" are two more performance measures widely used to evaluate biometric systems. Both of these are calculated in terms of probability. FMR and FNMR are the probability of incorrectly authenticating a false user and incorrectly rejecting legal users respectively.

The "Average Number of Genuine Actions (ANGA)" and the "Average Number of Imposter Actions (ANIA)" are new performance measures required for a continuous biometric authentication system.

6. VEIN PATTERN BASED BIOMETRIC SYSTEMS

Most biometric features used for authentication are external and can be easily captured like face, fingerprint, iris, voice, etc. It is observed that fingerprint recognition is the most popular system used for biometric authentication in academia and in Industry. Some common applications of it are biometric attendance systems, mobile device access, banking applications, etc. This system faces major challenges like aliveness detection and privacy protection.

Aliveness Detection and Privacy Protection: As discussed in the previous section fingerprint recognition systems can be cheated by using captured fingerprints through a specific material. Fingerprints can be captured from the surfaces the user touched. So in a fingerprint-based recognition system, it is difficult to identify whether the submitted fingerprint is real or captured (fake).

The survey done in the study [11], has summarized how these two challenges are addressed by researchers. For aliveness detection, to capture the thermal image of the hand dorsa a thermal camera can be used. A camera below captures palm prints or fingerprints and the camera above collects the thermal image. But this type of hardware support may not be possible in some mobile devices. For privacy protection, rather than depending on a single fingerprint two fingerprint images are captured.

One is the directional features of one fingerprint and the other is the minutiae of another fingerprint Both images are combined to form a composite image.

Hou et al. [26] have mentioned that Finger vein-based biometric recognition system has some advantages as follows:

- It is the most unique feature among humans.
- It is only active in the living body.
- It will not change in adulthood.
- It is more robust as finger veins are not visible, not leaving any traces behind.
- It can be captured only with a contactless infrared sensor.

Hence it improves system security and reliability, as well as spoofing attacks is not possible. Thus the new biometric authentication systems using finger vein patterns or palm veins [27] that are protected under the skin are proven to be more secure as they have a low forgery rate.

Table 3 shows the comparison of Some of the biometric traits that are frequently used for biometric authentication. Vein Patterns can comfortably be collected from the user. It provides excellent security medium performance and acceptability [10, 28].

Table 3. Vein biometric comparison with other popular biometric traits

Biometric Identifier	Collection from User	Weakness	Security	Performance	Acceptability
Voice	Comfortable	Noise/ Change of voice due to cold diseases	Normal	Low	High
Face	Comfortable	Light effects	Normal	Low	High
Fingerprint	Comfortable	May be affected by skin diseases	Good	High	Medium
Iris	Uncomfortable	Spectacles affect input from user	Excellent	Medium	Low
Hand/Finger vein	Comfortable	Weaknesses are related to some internal and external factor.	Excellent	Medium	Medium

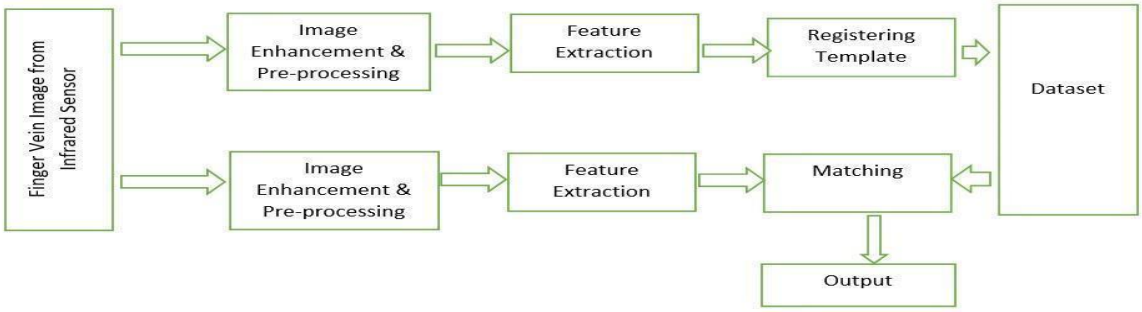

Figure 3. Finger vein biometric recognition system

Despite the advantages discussed earlier in this section, some internal and external factors affect the performance [26]. The most important internal factor is the configuration of the vein pattern-capturing device. External factors are humidity, dust, temperature, and misplacement of fingers. Both internal and external factors can be overcome by tuning the capturing device and processing the captured images before the verification process.

As per the review in the study [26], finger vein biometric recognition can be further improved by introducing better-designed capturing devices and image preprocessing methods. Introducing large-scale vein pattern datasets is also needed. Improving 3D finger vein recognition can be further advancement in vein pattern authentication systems.

6.1 Finger VEIN biometric recognition system steps

Finger vein-based biometric recognition systems have two main stages [10, 28, 29]: Enrollment and authentication of users. The user vein pattern is registered into the dataset in the enrollment stage. In this stage, the vein image is taken as input which is captured by an infrared sensor. The input image quality is enhanced by applying image processing methods. These enhanced and improved vein images are further processed by the feature extraction method to extract features. Extracted features are then stored in template format for future verification processes.

During the authentication or verification stage, the vein pattern of the biometric features of the user is taken as input by the system. This vein pattern is processed using image processing methods for image enhancement followed by feature extraction. The last step of authentication is matching these testing features with templates stored in a dataset during enrollment. Figure 3 represents the working of the finger vein biometric system.

As vein patterns are internal biological information of the body, image acquisition is different from the other biometric features [27]. Image acquisition is based on the concept that hemoglobin present in the vein vessels absorb near infrared light with more absorption rate than the tissues present in surrounding it. Thus it forms a vascular shadow which is treated as a vein pattern image for further processing.

According to the study [27], for palm vein pattern image acquisition there are two methods mainly used. These methods are named as transmission and reflection as shown in Figure 4. Both the method comprises two basic components namely illumination component and image capturing component. Illumination components lighten the user's palm and capturing components capture vein pattern images.

The target part is lightened from the palmar side of the palm in the reflection method and the capturing component is also placed on the palmar side of the palm. As both the components are present on the same side of the palm, these can be combined together in an image acquisition device as shown in Figure 4(a).

The target part is lightened from the dorsal side of the palm in the transmission method, and the image is captured from the palm's frontal side. As both the components are present facing each other as shown in Figure 4(b) these can not be combined together.

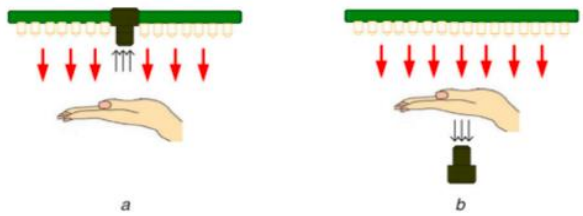

Figure 4. Palm Vein Pattern Image Capturing [27] a) Reflection Method b) Transmission Method

6.2 Performance measure

For vein-based biometric systems performance measures are FAR, FRR, EER, and Accuracy. These are calculated in the same way as per the discussion done for the multimodal biometric system. According to the study [26], one threshold value is decided for the feature matching score. The FRR is a false rejection probability i.e. valid user rejected access, this happens when the matching score of the finger vein is below the threshold value decided. The FAR false acceptance probability i.e invalid user gets access, this happens when the matching score of the finger veins is above the threshold value decided.

A comparison of different methods for dorsal hand vein image recognition is shown in the study [30] using three performance measures EER, STD (Standard Deviation of Accuracy), and ACC. "Deep learning" (DL) and "generative adversarial networks" (GANs) i.e., DL-GAN method proved to be better as compared to other recognition methods for dorsal hand vein images.

Researchers have presented a lightweight and "fully convolutional Generative Adversarial Network (GAN)" architecture, named FCGAN in the study [31], and a new scheme FCGAN-CNN for finger vein classification which proved to be more accurate, having higher GAR and Low EER compared to the previous methods for finger vein biometric recognition.

7. CONCLUSION

Biometric recognition is the field found to be continuously evolving in order to solve the issues like security, performance, accuracy, ease of use, liveness detection, and privacy protection. In this survey paper, we presented advancements done in the field of biometric authentication, we also reviewed some authentication systems published in recent years. It has been found that vein biometric and multimodal biometric authentication systems are attracting researchers to develop strong and unforged biometric authentication systems. Deep learning-based algorithms are improving system performance. Almost all biometric systems are making use of deep learning-based algorithms in recent years. It is noted that as per the need biometric features can be used and fused in multimodal biometric systems. Some public datasets are available but privately created datasets are preferred as they are generated to satisfy specific system demands. Thus better biometric systems can be developed by applying advanced data acquisition tools, image preprocessing methods, modified feature extraction, and fusion methods in order to improve performance, accuracy, and ease of use.

REFERENCES

[1] Rachapalli, D.R., Kalluri, H.K. (2020). Color QR pattern-driven cancelable biometric fingerprint system. Ingénierie des Systèmes d'Information, 25(2): 245-251. https://doi.org/10.18280/isi.250212

[2] Verma, G., Chakraborty, R. (2019). A hybrid privacy preserving scheme using finger print detection in cloud environment. Ingénierie des Systèmes d'Information, 24(3): 343-351. https://doi.org/10.18280/isi.240315

[3] Zhang, X.M., Cheng, D.X., Jia, P.K., Dai, Y.X., Xu, X.B. (2020). An efficient android-based multimodal biometric authentication system with face and voice. IEEE Access, 8: 102757-102772. https://doi.org/10.1109/ACCESS.2020.2999115

[4] Mandalapu, H., PN, A.R., Ramachandra, R., Rao, K.S., Mitra, P., Prasanna, S.M., Busch, C. (2021). Audio-visual biometric recognition and presentation attack detection: A comprehensive survey. IEEE Access, 9: 37431-37455. https://doi.org/10.48550/arXiv.2101.09725

[5] Toygar, Ö., Babalola, F.O., Bitirim, Y. (2020). FYO: A novel multimodal vein database with palmar, dorsal and wrist biometrics. IEEE Access, 8: 82461-82470. https://doi.org/10.1109/ACCESS.2020.2991475

[6] Obayya, M.I., El-Ghandour, M., Alrowais, F. (2020). Contactless palm vein authentication using deep learning with Bayesian optimization. IEEE Access, 9: 1940-1957. https://doi.org/10.1109/ACCESS.2020.3045424

[7] Bhattacharya, S., Ranjan, A., Reza, M. (2022). A portable biometrics system based on forehead subcutaneous vein pattern and periocular biometric pattern. IEEE Sensors Journal, 22(7): 7022-7033. https://doi.org/10.1109/JSEN.2022.3149286

[8] Iula, A., Micucci, M. (2022). Multimodal biometric recognition based on 3D ultrasound palmprint-hand geometry fusion. IEEE Access, 10: 7914-7925. https://doi.org/10.1109/ACCESS.2022.3143433

[9] Garcia-Martin, R., Sanchez-Reillo, R. (2020). Vein biometric recognition on a smartphone. IEEE Access, 8: 104801-104813. https://doi.org/10.1109/ACCESS.2020.3000044

[10] Dargan, S., Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications, 143: 113114. https://doi.org/10.1016/j.eswa.2019.113114

[11] Rui, Z., Yan, Z. (2018). A survey on biometric authentication: Toward secure and privacy-preserving identification. IEEE Access, 7: 5994-6009. https://doi.org/10.1109/ACCESS.2018.2889996

[12] Mitra, A., Bigioi, D., Mohanty, S.P., Corcoran, P., Kougianos, E. (2022). iFace 1.1: A proof-of-concept of a facial authentication based digital ID for smart cities. IEEE Access, 10: 71791-71804. https://doi.org/10.1109/ACCESS.2022.3187686

[13] Ortega-Delcampo, D., Conde, C., Palacios-Alonso, D., Cabello, E. (2020). Border control morphing attack detection with a convolutional neural network de-morphing approach. IEEE Access, 8: 92301-92313. https://doi.org/10.1109/ACCESS.2020.2994112

[14] Khan, N., Efthymiou, M. (2021). The use of biometric technology at airports: The case of customs and border protection (CBP). International Journal of Information Management Data Insights, 1(2): 100049. https://doi.org/10.1016/j.jjimei.2021.100049

[15] Scherhag, U., Rathgeb, C., Merkle, J., Breithaupt, R., Busch, C. (2019). Face recognition systems under morphing attacks: A survey. IEEE Access, 7: 23012-23026. https://doi.org/10.1109/ACCESS.2019.2899367

[16] Venkatesh, S., Ramachandra, R., Raja, K., Busch, C. (2021). Face morphing attack generation and detection: A comprehensive survey. IEEE Transactions on Technology and Society, 2(3): 128-145. https://doi.org/10.1109/TTS.2021.3066254

[17] Hamza, M., Tehsin, S., Karamti, H., Alghamdi, N.S. (2022). Generation and detection of face morphing attacks. IEEE Access, 10: 72557-72576. https://doi.org/10.22214/ijraset.2023.52876

[18] Husseis, A., Liu-Jimenez, J., Goicoechea-Telleria, I., Sanchez-Reillo, R. (2019). A survey in presentation attack and presentation attack detection. In 2019 International Carnahan Conference on Security Technology (ICCST), pp. 1-13. https://doi.org/10.1109/CCST.2019.8888436

[19] Scherhag, U., Debiasi, L., Rathgeb, C., Busch, C., Uhl, A. (2019). Detection of face morphing attacks based on PRNU analysis. IEEE Transactions on Biometrics, Behavior, and Identity Science, 1(4): 302-317. https://doi.org/10.1109/TBIOM.2019.2942395

[20] Edwards, T., Hossain, M.S. (2021). Effectiveness of deep learning on serial fusion based biometric systems. IEEE Transactions on Artificial Intelligence, 2(1): 28-41. https://doi.org/10.1109/TAI.2021.3064003

[21] Ryu, R., Yeom, S., Kim, S.H., Herbert, D. (2021). Continuous multimodal biometric authentication schemes: A systematic review. IEEE Access, 9: 34541-34557. https://doi.org/10.1109/ACCESS.2021.3061589

[22] Singh, M., Singh, R., Ross, A. (2019). A comprehensive overview of biometric fusion. Information Fusion, 52: 187-205. https://doi.org/10.1016/j.inffus.2018.12.003

[23] Kabir, W., Ahmad, M.O., Swamy, M.N.S. (2019). A multi-biometric system based on feature and score level fusions. IEEE Access, 7: 59437-59450.

https://doi.org/10.1109/ACCESS.2019.2914992
[24] Hammad, M., Liu, Y., Wang, K. (2018). Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. IEEE Access, 7: 26527- 26542. https://doi.org/10.1109/ACCESS.2018.2886573
[25] Zhang, Y.L., Gao, C.H., Pan, S.Y., Li, Z.W., Xu, Y.Y., Qiu, H.Z. (2020). A score-level fusion of fingerprint matching with fingerprint liveness detection. IEEE Access, 8: 183391-183400. https://doi.org/10.1109/ACCESS.2020.3027846
[26] Hou, B.R., Zhang, H.J., Yan, R.Q. (2022). Finger-vein biometric recognition: A review. IEEE Transactions on Instrumentation and Measurement, 71: 5020426. https://doi.org/10.1109/TIM.2022.3200087
[27] Wu, W., Elliott, S.J., Lin, S., Sun, S.S., Tang, Y.D. (2020). Review of palm vein recognition. IET Biometrics, 9(1): 1-10. https://doi.org/10.1049/iet-bmt.2019.0034
[28] Mohsin, A.H., Zaidan, A.A., Zaidan, B.B., Albahri, O.S., Ariffin, S.A.B., Alemran, A., Enaizan, O., Shareef, A.H., Jasim, A.N., Jalood, N.S., Baqe, M.J., Alamoodi, A.H., Almahdi, E.M., Albahri, A.S., Alsalem, M.A., Mohammed, K.I., Ameen, H.A., Garfan, S. (2020). Finger vein biometrics: Taxonomy analysis, open challenges, future directions, and recommended solution for decentralized network architectures. IEEE Access, 8: 9821-9845. https://doi.org/10.1109/ACCESS.2020.2964788
[29] Shaheed, K., Mao, A., Qureshi, I., Kumar, M., Hussain, S., Zhang, X. (2022). Recent advancements in finger vein recognition technology: Methodology, challenges and opportunities. Information Fusion, 79: 84-109. https://doi.org/10.1016/j.inffus.2021.10.004
[30] Alashik, K.M., Yildirim, R. (2021). Human identity verification from biometric dorsal hand vein images using the DL-GAN method. IEEE Access, 9: 74194-74208. https://doi.org/10.1109/ACCESS.2021.3076756
[31] Zhang, J.F., Lu, Z.Y., Li, M., Wu, H.P. (2019). GAN-based image augmentation for finger-vein biometric recognition. IEEE Access, 7: 183118-183132. https://doi.org/10.1109/ACCESS.2019.2960411