Int. J. Nonlinear Anal. Appl. 16 (2025) 5, 43–55
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2024.33566.5007

Biometrics based on deep learning: A survey

Bayda Zahid Kamil[a,*], Dhahir Abdulhadi Abdullah[a], Haraa Raheem Hatem[b]

[a] *College of Science, University of Diyala, Baqubah, Iraq*

[b] *College of Engineering, University of Diyala, Baqubah, Iraq*

(Communicated by Madjid Eshaghi Gordji)

Abstract

Biometrics is concerned with the identification and verification of people using their physiological and behavioral characteristics which are enduring and distinctive and these characteristics can distinguish one person from another. Systems for biometric recognition integrate intricate technological, operational, and definitional choices in a variety of scenarios. These systems combined with biometric strategies and authentication techniques will help to enhance the security of applications that rely on user collaboration. They aid in locating a specific person inside a set of industrial networks, office buildings, and control systems. This paper focused on convolutional neural networks, deep learning in biometrics, Unimodal and Multimodal Biometrics, template security, and general challenges of biometrics. This article examines a comprehensive and in-depth survey that succinctly and methodically on fingerprint and vein biometrics, analyzed, and compared to determine which is more effective in verifying the identification of a specific user and to highlight a biometric authentication system and the challenges of biometrics. We discuss each method and dataset used as well as their efficacy. The key difficulties in using these biometric recognition models as well as prospective directions for future study in this area are also covered.

Keywords: Biometrics, Deep Learning, Convolutional Neural Networks, Fingerprint, finger vein, multimodal
2020 MSC: 68T07

1 Introduction

There are several methods for identifying a person, and biometrics has shown to be one of the safest ones so far. The distinct, quantifiable traits that are used to identify and categorize people are called biometric identifiers [36]. They are typically split into two groups: behavioral characteristics and physiological characteristics. Each category has benefits and drawbacks [54, 56]. Since fingerprints and veins have biometric qualities, they are of particular interest to scientists conducting studies in this field such as for mobile payments, financial security, and smart cities [13]. Our fingerprints would remain the same after death. Our fingers will get bigger as we get older, but their prints won't ever alter. Even if the children are twins, their prints won't match exactly [62]. Because each person's fingerprint is distinct and constant, they have become a crucial biometric attribute. Due to the acquisition device's relatively modest size, this biometric modality is more popular and accepted by consumers. Additionally, compared to other biometric recognition systems based on the retina, ear shape, iris, etc., the recognition accuracy is comparably extremely good [4]. The finger vein biometric modality is typically utilized in biometric recognition due to various benefits over other

*Corresponding author
Email addresses: scicompms2206@uodiyala.edu.iq (Bayda Zahid Kamil), dhahir@uodiyala.ude.iq (Dhahir Abdulhadi Abdullah), haraa_altaie1980@yahoo.com (Haraa Raheem Hatem)

Received: March 2024 *Accepted:* June 2024

modalities, i) it is can be obtained in a simple and easy way, using a Near-Infrared light source (NIR); ii) Because the vein structure is concealed beneath the skin and the human identification system may be fooled in many different ways, it is extremely secure; iii) each person's veins are unique and different [3]. The recognition of a person's finger veins is based on the characteristics of human veins used for verification and identification of the person. As a result, the ability of humans and computers to recognize finger veins is a study area with potential for both scientific inquiry and widespread application [15].

One can categorize the traits derived from biometric data into unimodal and multimodal systems. For biometric authentication, unimodal methods only use one person's biometric characteristic. Although the technical aspects of unimodal authentication seem quite strong, unimodal has several drawbacks when working with a big population. However, several papers, including [8, 49, 65], among others, have demonstrated the drawbacks and shortcomings of biometric systems that rely on a single physical characteristic or biosignal to carry out recognition. The system's modality is this characteristic or bio signal, and different modes result in various behaviors and performances. Although pupil dilation and gaze angle may have an impact, iris-based systems are thought to offer some of the finest performance levels [27]. Additionally, iris biometrics may be subject to spoofing techniques such as the use of textured contact lenses [18, 37]. These flaws include the biometric sensor's susceptibility to distortion or incomplete data, as well as inter- and intraclass. Additionally vulnerable to fake attacks where the data can be copied or created are unimodal biometric devices. As a result, the limitations of the unimodal system are taken into account while designing multimodal systems [19]. is becoming the standard security solution for personal identification [16]. A neural network is a collection of techniques that let a computer learn to perform particular tasks by analyzing training models. It closely resembles the neural network in the human brain where neurons function as nodes to collect and categorize input based on building type. Therefore, receiving the data from one layer and delivering data to another, these nodes are closely coupled. For the intended output, each node has a movable weight (simply a number that shows the strength of the relationship between the components) [23, 48].

Shallow networks and deep networks are the two main categories of neural networks. Only a few buried layers make up conventional networks, commonly referred to as shallow networks. For performing appropriate classification, they rely on well-made handcrafted features. Though task of feature extraction in image recognition requires a knowledgeable specialist to complete it successfully. Shallow networks are given features that are retrieved from each of the samples for categorization [11, 41]. Deep learning approaches may learn to disengage these variables while examining discriminating representations if appropriate samples adequately describe the many variables that affect identification. As a result, disparities in the noisy biometric data and interclass data will be managed [14]. The model must be sufficiently complicated to capture all of these variances, which necessitates enormous training massive data [1, 30]. It might need a lot of work to collect data that would eventually change over time [17]. The rest of the article is divided as follows: Section 2 provides an insight into convolutional neural networks, which are extensively used in biometric identification. In section 3, the identification of basic background using a single biometric trait, i.e., unimodal biometrics, is discussed. Identification using deep learning for nine important traits is discussed. In section 4, literal review, at the end of sections 3 and 4, overviews of work done in biometrics using deep learning discussed are summarized in tabular form. In the end, challenges faced in biometric identification and conclusions drawn are discussed in section 5.

2 Convolutional neural networks

The Convolutional neural networks are effective in identifying fingerprints and finger veins. As deep learning technology has improved, CNNs have gained popularity in the field of image identification. CNNs are trained using the pixel-level label data produced by conventional texture extraction techniques.

The automated feature learning and classification steps make up CNNs. Its performance routinely beats that of other machine learning methods in complicated picture recognition challenges. Based on the feature data, the photos of finger veins are categorized using a template-matching technique [22]. CNN was used to extract the finger vein and print patterns, and a Fully Convolutional Network FCN was used to reconstruct them [22], as shown in figure 1.

Devices capable of utilizing more than one physical or mental unimodal biometric trait for authentication, confirmation, and identification are known as multimodal biometrics. Due to the use of fusion techniques, multimodal solutions allow for the merging of data from one or more biometric sensors to calculate many independent biometric features at the attribute, comparison, or decision level [23]. Figure 2 shows typical of existing Biometric features.

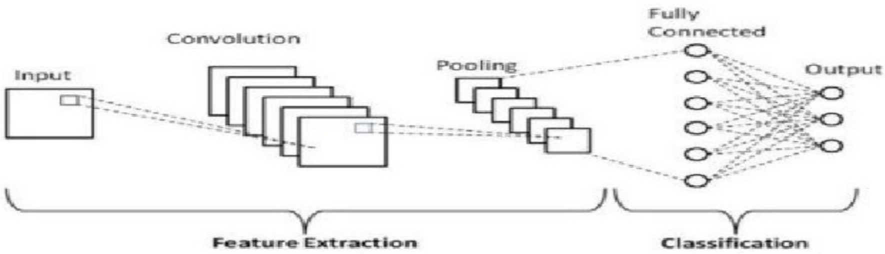

Figure 1: Architecture convolutional neural network (CNN) [33].

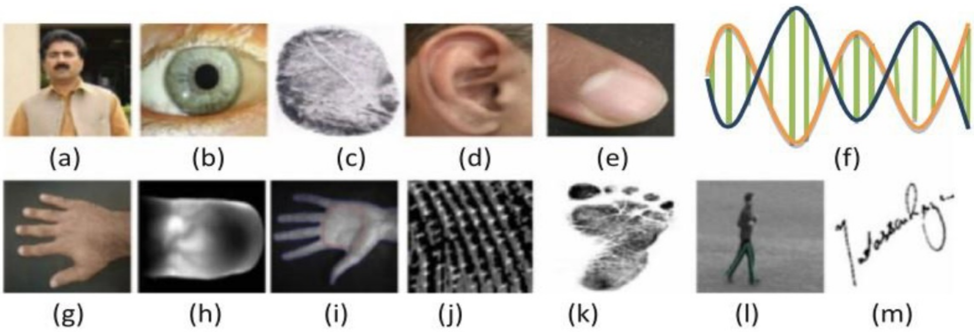

Figure 2: Represents biometric types [51].

3 Basic background

A biometric system has two stages:

1. Enrollment, which is the learning stage.
2. Recognition, which is the verification or identifying stage. Various modules used in a biometric system:

Authentication is an operational mode in the biometric recognition process. The authentication procedure involves comparing the extracted characteristics with the database's stored template [46].

In biometric recognition systems, people are recognized using protected biometric data. There are two ways to carry out recognition. (a) verification system: always accept a genuine user while rejecting all impostors, it is mean one to one matching [1:1] or (b) identification systems: accurately identify the presenting users with the registered identities in the database is regarded as its highest ideal performance, it is mean one to many matching [1:M] [5, 34].

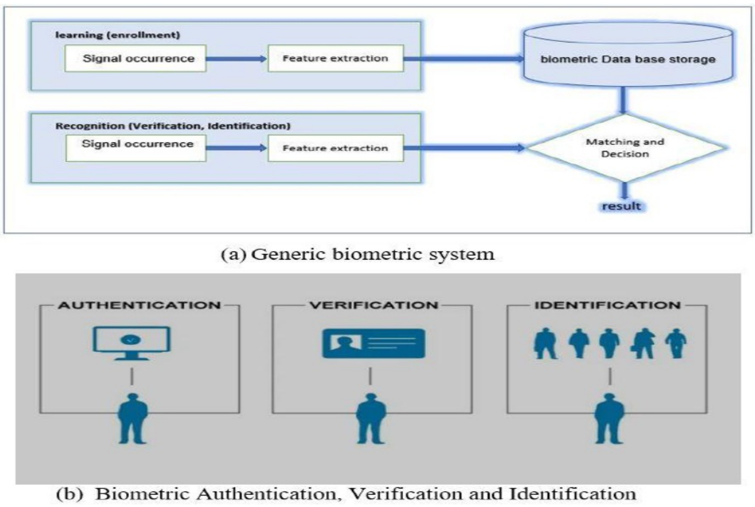

Figure 3: a) Generic biometric system b) Authentication, Verification and Identification.

3.1 Framework of biometric systems

According to the needs of the biometric characteristic, there are several feature extraction methods and classification methods accessible, and the user may create a brand-new feature extraction method and classifier for the same. Therefore, the objective is to increase the accuracy of identification rates by using either independent classifiers or hybrid classifiers using numerous feature extraction techniques [28]. The needed steps begin with the input of biometric attributes and continue via pre-processing, locating the region of interest, feature extraction techniques, developing and ultimately executing matching algorithms, followed by the decision-making process. Following input preprocessing, the next stage is to focus on the region of interest for using the feature extraction methods and matching approaches for a particular biometric characteristic or traits. There are several feature extraction and classification techniques that may be used to meet the needs of the biometric characteristic, and the user can create a unique feature extraction technique and classifier for the same [32, 55]. Figure 4 framework steps of biometric system operate.

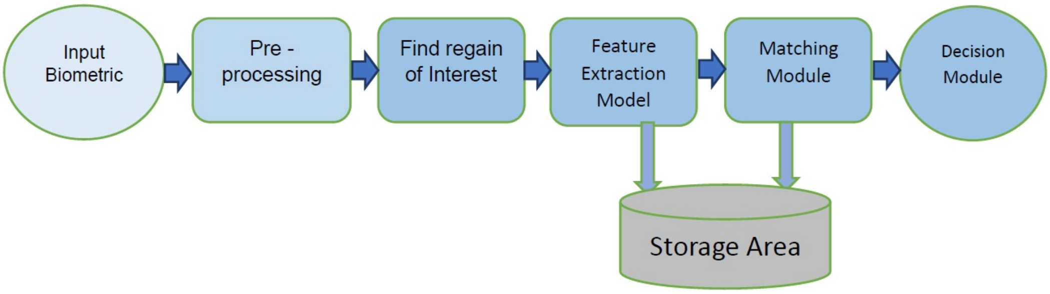

Figure 4: General framework of biometric system.

3.2 Biometric modality

Biometrics types are generally classified under two main categories behavioral and Physiological [50]. The measuring of an individual's traits for precise identification and verification is a biometric attribute. The use of biometric technology allows for the automatic recognition and validation of people based on their behavioral and psychological characteristics, such as face, palm print, iris, retina, fingerprint, voice, signature, gait, hand geometry, handwriting, ECG, brain print, and keystroke dynamics [33], as shown in figure 5.

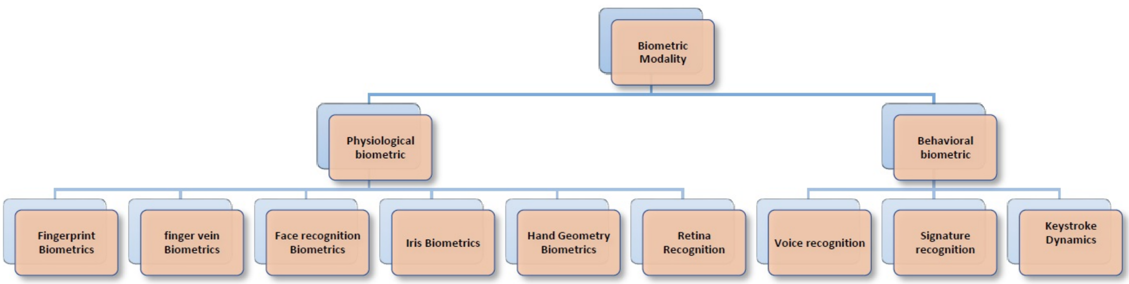

Figure 5: Overview of Biometrics Methods.

3.2.1 Finger print

For a given application, the system designer needs to decide which of the sources should be used in designing the multibiometric system. A different source of multimodal biometric is shown in Figure 6. Represents the overview of biometric methods can be based on one or more of the most developed biometric characteristics is the fingerprint, which is accepted as legal evidence in courts across the world As a result, fingerprints are employed in forensic departments for criminal investigations all over the world.Due to a greater knowledge of fingerprints and their demonstrated matching performance compared to any other biometric technology, more contemporary civilian and business applications are either adopting or actively investigating using fingerprint-based authentication [2].

Figure 6: Sample image Fingerprint captured [43].

3.2.2 Finger vein biometrics

The biometric technology and study area of finger-vein identification is relatively young. The finger-vein pattern is distinctive to a single individual, challenging to fake, contactless, unaffected by race or skin discolorations, and it does not alter with age. The finger-vein can be utilized to identify a certain person, according to a lot of research that has been done in this area. But since blood flow and lighting can cause a finger-vein picture to be unsteady and have poor contrast, it can be difficult to accomplish accurate finger-vein detection [29, 64], as shown in figure 7.

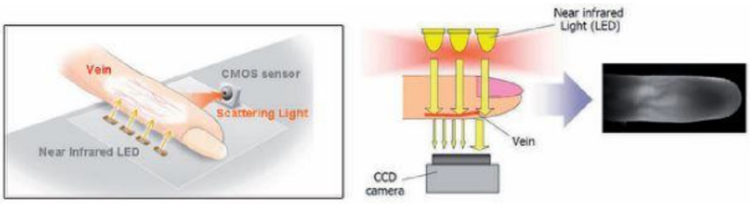

Figure 7: Sample image of Finger vein capture [29].

3.2.3 Face recognition biometric

Face recognition is a new field that is constantly evolving and becoming better. The study of face recognition has drawn researchers in the fields of security, psychology, optics, neural networks, machine learning, image processing, computer vision, and pattern recognition [6]. The most significant use is image analysis and understanding, and its development has included contributions from neuroscientists as well as engineers.

Popular and unobtrusive, face recognition is a technique. Face recognition is built on the size, ratio, and other physiological characteristics of the face. Humans are able to recognize and distinguish between faces based on the size, placement, and form of facial features such the nose, lips, eyes, chin, and jaw, as well as their spatial connections [61], as shown in figure 8.

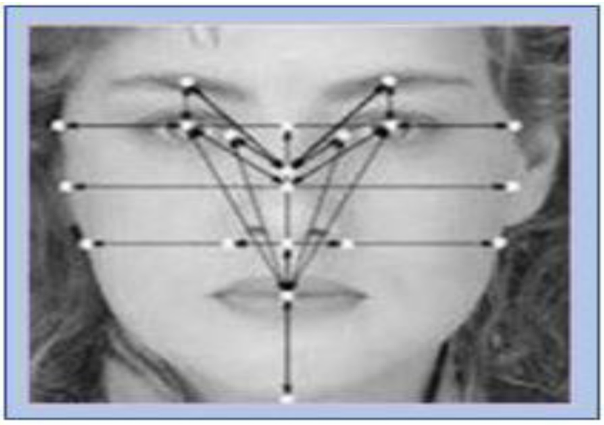

Figure 8: Sample image of Face recognition captured [40].

3.2.4 Iris biometrics

Iris Recognition is a biometric technique for personal identification and verification that uses iris scans to identify individuals in actuality; iris patterns exhibit a great degree of consistency and uniqueness. Each person has a distinctive iris, and even identical twins and a person's left and right eyes might differ from one another [60], as shown in figure 9.

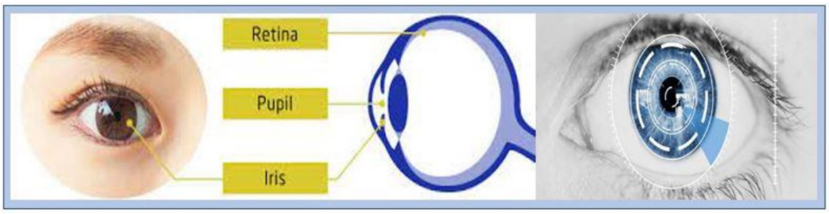

Figure 9: Sample Image of Iris recognition [60].

3.2.5 Retina recognition biometric

The thin nerve at the back of the eyeball's retina, which processes light arriving via the pupil, is captured and examined by Retina Recognitions. Highly distinguishing characteristics are retinal patterns. Each eye has a completely distinct blood vessel arrangement. Even identical twins' eyes differ from one another. The difficulty of eliminating its characteristics is the retina's power in feature identification [12, 25], as shown in figure 10.

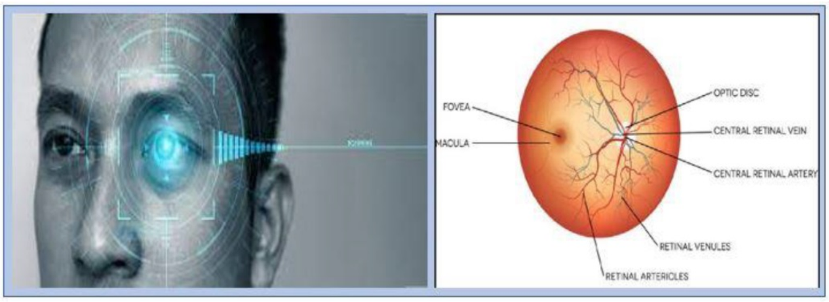

Figure 10: Sample of Image of Retina Recognition [25].

3.2.6 Hand geometry biometrics

Regarding user acceptability, cost, performance, and other factors, all biometric approaches vary. Given that every human hand is different, one of the physiological traits for recognition is hand geometry. Every human being differs from every other individual in terms of their relative placement, finger length, width, thickness, and curvatures. The medium security that hand geometry is thought to provide comes with a number of benefits over other methods, including: medium cost because it only requires a platform and a medium-resolution reader or camera. It also uses a low-computational cost algorithm that produces quick results and a small template size (between 352 and 1209 bytes), which reduces the need for storage. Finally, it is very simple and appealing to users, which results in high user acceptance [21, 52], as shown in figure 11.

Figure 11: Sample image of hand geometry [52].

4 Literal review

The many proposed approaches in the last few years, with public datasets, feature extraction and recognition methods, are based on a comparison of finger vein and fingerprint biometrics dependent on accuracy (Acc) and Error Rate (EER) values. Compared to the existing literature, the basic contributions of this paper are as follows:

1. B. Pandya et al. in [42]: proposing a new deep learning architecture for fingerprint recognition. The proposed architecture comprises a preprocessing stage for extracting texture features from fingerprints, and this stage is performed by using histogram equalization, Gabor enhancement and fingerprint thinning. The pre-processed fingerprints are input into a Deep Convolutional Neural Network classifier (DCNNC). A dataset was created in the laboratory using a Futronics FS88 scanner device with 56 users participating. The proposed approach has achieved 98.21% classification accuracy with 0.9 loss.
2. C. Lin and A. Kumar in [31]: A Robust Thin-Plate Spline (RTPS) based generalized fingerprint deformation correction model (DCM) is proposed in this work. The usage of DCM results in the accurate alignment of key minutiae features observed on the contactless and contact-based fingerprints. RTPS and DCM use the Gabor filter to enhance the image which is followed by binarization and thinning to generate the ridge image. This paper has also developed a database of 2D contactless fingerprint images and their corresponding contact-based fingerprint images. The proposed RTPS and DCM method achieves the best performance with 14.33% EER (Equal Error Rate).
3. B. Bakhshi and H. Veisi, in [10]: an end-to-end CNN-based fingerprint matching method has been developed using FVC2002 (Fingerprint Verification Competition2002) dataset. No prepossessing is required in the proposed method and the model directly learns fingerprint patterns from raw pixels of images. A work-flow for verification using an end-to-end CNN approach was proposed and two CNN modules have been tested: CNN-1 and trained Alex Net. Using trained Alex Net increased the speed of the training phase. The model has reached the EER of 17.5% which is a better result in comparison to the MinutiaSC and A-KAZE methods.
4. F. Wu et al. in [63]: proposed a New Convolutional Neural Network (CNN) model to identify patterns of real fingerprints. In this work, fingerprint patterns are divided into six categories: arc (A), whorl (W), double whorl (DW), ulnar loop (UL), radial loop (RL), and peacock eye (PE). The authors collected and chose nearly 4000 pictures of each fingerprint category. The best accuracy the model achieved was 94.87% for a six-category fingerprint database. Another important finding is that after 30 times repeated experiments, the proposed model shows its stability, which can be seen from the standard deviation of accuracy (0.31) and test loss (0.01).
5. W. Jian et al. in [26]: proposes a lightweight CNN structure based on a singularity ROI pattern. Firstly, all raw images go through a series of preprocessing procedures to obtain singularity ROI (Region of Interest) patterns. Secondly, ROI patterns serve as input data for NN (neural network) classifiers. Three sets of control experiments are used to demonstrate the superiority of the proposed model in classification performance and calculation amount based on NIST SB4 (National Institute of Standards and Technology Special Database 4). The experimental results of the proposed method show that the accuracy achieved is 93%, which is far better than classic non-NN (neural network) classifiers.
6. A. Takahashi et al. in [58]: proposed a novel CNN architecture to extract features from fingerprint images by combining texture, minutiae and frequency spectrum. A minutia attention module to pay attention to the position of the minutiae was proposed. Also, the authors introduced novel data augmentation methods specific to fingerprint images for efficient training with a small number of classes of training data. In the FVC2004 DB1 dataset, the EERs of the proposed method obtained 1.41% and in the FVC2004 DB2 dataset, the EERs of the proposed method obtained 1.10
7. M. Ahsan et al. in [4]: introduces an intelligent computational approach to automatically authenticate fingerprints for personal identification and verification. The feature vector is formed using combined features obtained from the Gabor filtering technique and Convolutional Neural Network (CNN). Principle Component Analysis (PCA) has been performed on the feature vectors to reduce the over-fitting problems in order to make the classification results more accurate and reliable. Experiments performed using standard public databases with 9000 fingerprint images demonstrated that the proposed approach showed better performance with regard to accuracy (99.87%) compared to the more recent classification techniques such as Support Vector Machine (97.86%) or Random Forest (95.47%). However, the proposed method also showed higher accuracy compared to other validation approaches such as K-fold (98.89%) and generalization (97.75%).
8. M. Dincă Lăzărescu et al. in [7]: presents an algorithm for fingerprint classification using a CNN (convolutional neural network) model and making use of full images belonging to four digital databases, the proposed model consists of the following steps: a preprocessing stage which deals with edge enhancement operations, data resizing, data augmentation, and finally a post-processing stage devoted to classification tasks. Primarily, the fingerprint

images are enhanced using Prewitt and Laplacian Gaussian filters. This investigation used the fingerprint verification competition with four databases (FVC2004, DB1, DB2, DB3, and DB4). The accuracy varies from 67.6% to 98.7% for the validation set and between 70.2% and 75.6% for the test set.

9. F. Saeed et al. in [47]: introduced a technique for automatically creating a custom-designed CNN model for multi-sensor fingerprint categorization. Since CNN models contain a large number of parameters and are designed randomly, we used the FKT approach to build a low-cost, high-speed CNN model tailored for the target fingerprint dataset. The developed DeepFKTNet model is data-dependent using two public datasets namely Finger Pass and FVC2004. The DeepFKTNe obtains higher accuracy (98.89%) compared with previous works.
   Table 1 shows a summary of the previous work presented above. This summary is based on the dataset, feature extraction and recognition methods, and the recognition metrics' accuracy (Acc.) and Error Rate (EER) values.

Table 1: A summary of the previous work

Ref.	**Year**	**Dataset**			**Method**	**Metrics**
		Name	Image size	No. of users or images		
[42]	2018	New dataset was collect by authors	350 × 233	56	DCNNC, Convolution layer=2 and kernel size =5×5	Acc.=98.21%
[31]	2018	The HKPU Contactless 2D to Contact-based 2D	1400 × 900 and 356 × 328	300	RTPS and DCM	EER=14.33%
[10]	2019	FVC2004 DB1	300 × 300	110	CNN and AlexNet with Convolutional layer=3 and Kernel size=3 × 3	EER=17.5%
		FVC2004 DB2	256 × 364			
		FVC2004 DB3	448 × 478			
		FVC2004 DB4	240 × 320			
[63]	2020	New dataset was collect by authors	256 × 256	100,000 images	New CNN with Convolutional layer=4 and kernel size=11 × 11	Acc.=94.87%
[26]	2020	NIST SD4	512 × 512	4000 images	lightweight CNN with Convolution layer =3 and kernel size= $7\times7, 5\times5, 3\times3$	Acc.=93%
[58]	2020	FVC2004 DB1	640 × 480	800	Novel CNN with Convolution layer=4 and kernel size= $7\times7, 5\times5, 3\times3$	ERR=1.41%
		FVC2004 DB2	328 × 364			EER=1.10%
[4]	2020	standard public databases	227 × 227	9000 images	CNN with Convolution layer=5 and kernel size= $11\times11, 5\times5, 3\times3$	Acc.=99.87%
[7]	2022	FVC2004DB1	640 × 480	110	CNN with Convolution layer=4	Acc.= from 70.2% to 75.6%
		FVC2004DB2	328 × 364			
		FVC2004DB3	300 × 480			
		FVC2004DB4	288 × 384			
[47]	2022	FVC2004	–	110	DeepFKTNet-5 with Convolution layer =4 and kernel size =7 × 7	98.89%

10. S.A. Radzi, et al. in [3]: proposed a novel model using a convolutional neural network (CNN) for finger-vein biometric identification. In this work, a reduced-complexity four-layer CNN with fused convolutional-subsampling architecture is proposed for finger-vein recognition. For network training, the authors have modified and applied the stochastic diagonal Levenberg–Marquardt algorithm, which results in a faster convergence time. The database used in this research was developed by the VeCAD Laboratory of Universiti Teknologi Malaysia which contains 50 subjects with 10 samples from each finger. An identification rate of 100.00% is achieved, with an 80/20 percent ratio for the separation of training and test samples, respectively.
11. G. Meng et al. in [35]: applied a convolutional neural network (CNN) finger vein recognition method. The image samples are directly input into the CNN model to extract its feature vector so that the authors can make authentication by comparing the Euclidean distance between these vectors. Finally, the Deep Learning Framework Caffe is adopted to verify this method. The proposed method used the DataTang finger vein image database and it consists of 64 subjects with 15 samples each for finger, which were captured in three months and 5 images per month. The results achieved 99.4% accuracy, obtaining a very low error rate of 0.21.
12. R. Das et al. in [9]: propose a convolutional-neural-network-based finger-vein identification system and investigate the capabilities of the designed network over four publicly available databases. The main purpose of this work is to propose a deep-learning method for finger-vein identification, able to achieve stable and highly accurate performance when dealing with finger-vein images of different quality. The reported extensive set of experiments shows that the accuracy achievable with the proposed approach can go beyond 95% correct identification rate for all the four considered publicly-available databases.
13. H. Qin and P. Wang in [44]: proposes a deep learning model to extract vein features by combining the Convolutional Neural Networks (CNN) model and Long Short-Term Memory (LSTM) model. Firstly, we automatically

assign the label based on a combination of the known state-of-the-art handcrafted finger-vein image segmentation techniques and generate various sequences for each labelled pixel along different directions. Secondly, several Stacked Convolutional Neural Networks and Long Short-Term Memory (SCNN-LSTM) models are independently trained on the resulting sequences. Thirdly, propose a supervised encoding scheme to extract the binary vein texture. The proposed method used HKPU dataset includes 3132 images from 156 subjects using an open and contactless imaging device. Experimental results show that the proposed approach extracts robust vein features and significantly improves the verification error rate EER =0.95%.

14. D. Gumusbas et al. in [24]: proposed the Capsule Network for the finger-vein-based biometric identification method to take advantage of using convolutions with a limited number of samples on four finger-vein benchmark sub-databases. The proposed method aims to extract finger-vein features that are more definable and rationally augmented without using any pre-trained weights. Secondly, it compares the CNN-based equivalent and LeNet-5 models to show how Capsule Network is better at approaching representing features. This capsule-based finger-vein identification approach using 32×32 image resolutions achieves an average 95.5% accuracy on four benchmark sub-databases.
15. J.M. Song et al. in [57]: suggest two recognition finger vein systems based on CNN: using a difference image as the input to the network and calculating the distance between feature vectors extracted from the CNN. Difference images can be susceptible to noise as they are generated by differences in pixel values. To address this issue, this paper examined a method less susceptible to noise and which uses the entire network; a composite image of two finger-vein images was used as the input to a deep, densely-connected convolutional network (DenseNet). Two open databases, namely Shandong University homologous multi-modal traits (SDUMLA-HMT) finger-vein database and The Hong Kong Polytechnic University finger image database (version 1), were the proposed system obtains error rate EER= 0.33.
16. K.J. Noh et al. in [39]: offered rough finger-vein regions in an image are detected to reduce the effect of mis-segmented regions, to complement the drawbacks of shape image-based finger-vein recognition. Furthermore, score-level fusion is performed for two output scores of deep convolutional neural network extracted from the texture and shape images, which can reduce the sensitivity to noise, while diverse features provided in the texture image are used efficiently. Two open databases, SDUMLA-HMT and HKPU, are used for experiments. The proposed method shows better recognition performance with error rate =0.05.
17. S.M.M. Najeeb et al. in [38]: suggests a new Deep Learning (DL) model called the Re-enforced Deep Learning (RDL). This approach provides another way of personal verification by using the Finger Veins (FVs). The RDL consists of multiple layers with a feedback. Two FV fingers are employed for each person, FV of the index finger for first personal verification and FV of the middle finger for re-enforced verification. The used database is from the Hong Kong Polytechnic University Finger Image (PolyUFI) database (Version 1.0). The result shows that the proposed RDL achieved a promising performance of 91.19%.
18. I. Boucherit et al. in [13]: offered an improved deep network, named Merge Convolutional Neural Network (Merge CNN), which uses several CNNs with short paths. The scheme is based on the use of multiple identical CNNs with different input images qualities, and the unification of their outputs into a single layer. The authors conducted different experiments using different network parameters and layers. The most optimal model took a combination of original images and images enhanced with the contrast limited adaptive histogram (CLAH) method. The model was trained using the FV-USM, SDUMLA-HMT, and THU-FVFDT2 datasets, and it achieved a recognition rate of 96.75%, 99.48%, and 99.56%, respectively.
19. L.D. Tamang and B.W. Kim in [59]: designed a feature extraction network in which each block consists of a convolutional layer followed by hybrid pooling, whose output activation maps are concatenated before passing features to another block within the network. In the hybrid pooling layer, two subsampling layers of maxpooling and average pooling are placed in parallel where the former activates the most discrete features of the input, and the latter considers the complete extent of the input volume so better localization of features can be accessed. After the features are extracted, they are passed to three fully connected layers (FCLs) for classification. The experiments results are applied on two public dataset HKPU and FVUSM, the proposed model achieves outstanding recognition performance with accuracies of up to 97.84% and 97.22% for good and poor-quality images, respectively.

The Table 2 shows Summary of the Previous Works for Finger Vein Recognition. This summary is based on the dataset, feature extraction and recognition methods, and the recognition metrics' accuracy (Acc.) and Error Rate (EER) values.

Table 2: A summary of the previous work

Ref.	Year	Dataset			Method	Metrics
		Name	Image size	No. of users or images		
[3]	2016	Own	55×67	50	CNN with Convolution layer =4 and kernel size $=7 \times 7$	ACC.=100%
[35]	2017	DataTang	256×256	64	CNN with Convolution layer =5 and kernel size $=11 \times 11$	ACC.=99.4%
[9]	2018	HKPU	513×256	156	CNN with Convolution layer =5 and kernel size $=5 \times 5$	ACC.=95%
		FV-USM	640×480	123		
		SDUMLA	320×240	106		
		UTFVP	672×380	60		
[44]	2018	HKPU	513×256	156	CNN+LSTM with convolution layer=2 and kernel size=11×11	EER=0.95%
[24]	2019	HKPU	513×256	156	Capsule Network	Acc.=88%
		SDUMLA	320×240	106		Acc.=100%
		UTFVP	672×380	60		Acc.=94%
		MMCBNU-6000	320×240	100		Acc.=100%
[57]	2019	HKPU	513×256	156	Deep Dense Net161 with convolution layer=7 and kernel size= $1 \times 1, 2 \times 2, 3 \times 3$	EER=0.33
		SDUMLA-HMT	320×240	106		
[39]	2020	HKPU	513×256	156	Deep Dense Net161 with convolution layer=3 and kernel size=7×7	EER=0.05
		SDUMLA-HMT	320×240	106		
[38]	2021	PolyUFI	513×256	156	RDL with convolution layer=1 and kernel size $=3 \times 3$	Acc.=91.19%
[13]	2022	FV-USM	300×100	6	Merge CNN with convolution layer = 3 and kernel size=$3 \times 3, 5 \times 5, 7 \times 7$	96.75%
		SDUMLA-HMT	320×240	3816		99.48%
		THU-FVFDT2	200×100	610		99.56%
[59]	2022	HKPU	513×256	156	CNN with convolution layer = 5 and kernel size=$3 \times 3, 5 \times 5$	97.84%
		FVUSM	640×300	494		97.22%

5 General Challenges of the biometrics

When we consider that, unlike passwords or keys, we do not have the opportunity to modify our biometric qualities when they are taken, spoofing and data security—two significant and important issues appear even more urgent [20, 53]. The need to adequately and thoroughly address the issues of spoofing and data security is more important than ever as the field of biometrics develops from specialized research to widely used commercial products. In fact, some commercial systems that have already been deployed store sensitive information on the enrolled users [45]. Future studies should focus on finding and reducing weaknesses and preventing spoofing attacks. Additionally, methods like cancelable biometrics or cryptosystems.

6 Conclusions

With the increase in workplace safety and comfort, biometric recognition technologies are continually improving. Deep learning, pattern recognition, and machine learning approaches enable the advancement. Smart cards, computers, and mobile devices are among the diverse uses. The purpose of this study is to introduce researchers to the methodologies for feature extraction, various classifiers, various datasets, and accuracy rates in the creation of biometric systems for novel applications. In order to cover as many qualities as feasible, the study discusses the thorough and methodical scanning of a single-modal and multi-modal biometric system based on several attributes. The objective is to provide a concise summary of each attribute together with the results of recent biometric fingerprint and finger vein research. In addition to offering the community security, monitoring, and investigative levels measures at cheap cost and higher accuracy, this will enable gullible users with the most recent innovations and advantages. By observing how well-liked and widely accepted certain identification systems are by users. As future work, enhanced results are planned. High accuracy and greater reliability are obtained if biometric systems are used to identify an individual. Since the cost of obtaining a finger vein and fingerprint is the lowest among biometric systems in general, and as we mentioned earlier in this research paper, the time to obtain multiple systems is longer if the systems are single, so we proposed to integrate the fingerprint and finger vein with a multiple biometric system so that we can obtain the two characteristics (finger vein and fingerprint) at the same time.

References

[1] C. Affonso, A.L.D. Rossi, F.H.A. Vieira, and A.C.P. de Leon Ferreira, *Deep learning for biological image classification*, Expert Syst. Appl. **85** (2017), 114–122.

[2] D.M Ahmed, S.Y. Ameen, N. Omar, S.F. Kak, Z.N. Rashid, H.M. Yasin, I.M. Ibrahim, A.A. Salih, N.O. Salim, and A.M. Ahmed, *A state of art for survey of combined iris and fingerprint recognition systems*, Asian J. Res. Comput. Sci. **10** (2021), no. 1, 18–33.

[3] S. Ahmad Radzi, M. Khalil-Hani, and R. Bakhteri, *Finger-vein biometric identification using convolutional neural network*, Turkish J. Electr. Eng. Comput. Sci. **24** (2016), no. 3, 1863–1878.

[4] M. Ahsan, M.A. Based, J. Haider, and M. Kowalski, *An intelligent system for automatic fingerprint identification using feature fusion by Gabor filter and deep learning*, Comput. Electr. Eng. **95** (2021), 107387.

[5] M.M.H. Ali, V.H. Mahale, P. Yannawar, and A.T. Gaikwad, *Overview of fingerprint recognition system*, Int. Conf. Electr. Electron. Optim. Tech. ICEEOT 2016, pp. 1334–1338.

[6] S. Almabdy and L. Elrefaei, *Deep convolutional neural network-based approaches for face recognition*, Appl. Sci. (Switzerland) **9** (2019), no. 20.

[7] D.L. Andreea-Monica, S. Moldovanu, and L. Moraru, *A fingerprint matching algorithm using the combination of edge features and convolution neural networks*, Inventions **7** (2022), no. 2, 1–13.

[8] S. Anton, T. Artem, P. Andrey, and K. Igor, *Modification of VGG neural network architecture for unimodal and multimodal biometrics*, IEEE East-West Design and Test Symposium, EWDTS Proc., 2020, pp. 1–4.

[9] A. Avci, M. Kocakulak, and N. Acir, *Convolutional neural network designs for finger-vein-based biometric identification*, ELECO 11th Int. Conf. Electr. Electron. Eng., 2019, pp. 580–584.

[10] B. Bakhshi and H. Veisi, *End to end fingerprint verification based on convolutional neural network*, ICEE 27th Iran. Conf. Electr. Eng., 2019, pp. 1994–1998.

[11] M.M. Bejani and M. Ghatee, *A systematic review on overfitting control in shallow and deep neural networks*, Artif. Intell. Rev. **54** (2021), 6391–6438.

[12] T.R. Borah, K.K. Sarma, and P.H. Talukdar, *Retina recognition system using adaptive neuro fuzzy inference system*, IEEE Int. Conf. Comput. Commun. Control. IC4 2015, 2016, pp. 1–6.

[13] I. Boucherit, M. Ould, H. Hentabli, and B. Affendi, *Finger vein identification using deeply-fused Convolutional Neural Network*, J. King Saud Univ. Comput. Inf. Sci. **34** (2022), no. 3, 646–656.

[14] L. Cai, J. Gao, and D. Zhao, *A review of the application of deep learning in medical image classification and segmentation*, Ann. Transl. Medicine **8** (2020), no. 11, 713–713.

[15] E. Cherrat, R. Alaoui, and H. Bouzahir, *Convolutional neural networks approach for multimodal biometric identification system using the fusion of fingerprint, finger-vein and face images*, PeerJ Comput. Sci. **2020** (2020), no. 1, 1–15.

[16] T.Z. Chin, A. Saidatul, and Z. Ibrahim, *Exploring EEG based authentication for imaginary and non-imaginary tasks using power spectral density method*, IOP Conf. Ser. Mater. Sci. Eng. **557** (2019), no. 1, 012031.

[17] A.M.M. Chowdhury and M.H. Imtiaz, *Contactless fingerprint recognition using deep learning & mdash: A systematic review*, J. Cybersecurity Priv. **2** (2022), no. 3, 714–730.

[18] M. Choudhary, V. Tiwari, and U. Venkanna, *Iris anti-spoofing through score-level fusion of handcrafted and data-driven features*, Appl. Soft Comput. J. **91** (2020).

[19] S. Dargan and M. Kumar, *A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities*, Expert Syst. Appl. **143** (2020), 113114.

[20] L.M. Dinca and G.P. Hancke, *The fall of one, the rise of many: A survey on multi-biometric fusion methods*, IEEE Access **5** (2017), 6247–6289.

[21] K. Fatima, S. Nawaz and S. Mehrban, *Biometric authentication in health care sector: A survey*, 3rd Int. Conf. Innov. Comput. ICIC, 2019, pp. 1–10.

[22] P.L. Galdámez, W. Raveane, and A.G. Arrieta, *A brief review of the ear recognition process using deep neural networks*, J. Appl. Log. **24** (2017), 62–70.

[23] U. Gawande and Y. Golhar, *Biometric security system: A rigorous review of unimodal and multimodal biometrics techniques*, Artic. Int. J. Biomet. **10** (2018), no. 2, 142–175.

[24] D. Gumusbas, T. Yildirim, M. Kocakulak, and N. Acir, *Capsule network for finger-vein-based biometric identification*, IEEE Symp. Ser. Comput. Intell. SSCI, 2019, pp. 437–441.

[25] S. Haware and A. Barhatte, *Retina based biometric identification using SURF and ORB feature descriptors*, Int. Conf. Microelectron. Devices, Circuits Syst. ICMDCS, 2017, pp. 1–6.

[26] W. Jian, Y. Zhou, and H. Liu, *Lightweight convolutional neural network based on singularity ROI for fingerprint classification*, IEEE Access **8** (2020), 54554–54563.

[27] M. Karakaya and E.T. Celik, *Effect of pupil dilation on off-angle iris recognition*, J. Electr. Imaging, 28 (2019), no. 3, 033022.

[28] N. Kaur, *A study of biometric identification and verification system*, Int. Conf. Adv. Comput. Innov. Technol. Eng. ICACITE, 2021, pp. 60–64.

[29] I. Kovač and P. Marák, *Openfinger: Towards a combination of discriminative power of fingerprints and finger vein patterns in multimodal biometric system*, Tatra Mt. Math. Publ. **77** (2020), no. 1, 109–138.

[30] Y. Li, *Research and application of deep learning in image recognition*, IEEE 2nd Int. Conf. Power, Electron. Comput. Appl. ICPECA, 2022, pp. 994–999.

[31] C. Lin and A. Kumar, *Matching contactless and contact-based conventional fingerprint images for biometrics identification*, IEEE Trans. Image Process. **27** (2018), no. 4, 2008–2021.

[32] J. Mason, R. Dave, P. Chatterjee, I. Graham-Allen, A. Esterline, and K. Roy, *An investigation of biometric authentication in the healthcare environment*, Array **8** (2020), 100042.

[33] H. Mehraj and A.H. Mir, *A survey of biometric recognition using deep learning*, EAI Endorsed Trans. Energy Web **8** (2021), no. 33, 1–16.

[34] P. Melzi, C. Rathgeb, R. Tolosana, R. Vera-Rodriguez, and C. Busch, *An overview of privacy-enhancing technologies in biometric recognition*, arXiv preprint arXiv:2206.10465, (2022).

[35] G. Meng, P. Fang, and B. Zhang, *Finger vein recognition based on convolutional neural network*, MATEC Web Conf., 2017.

[36] S. Minaee, E. Azimi and A. Abdolrashidi, *FingerNet: pushing the limits of fingerprint recognition using convolutional neural network*, arXiv preprint arXiv:1907.12956, (2019).

[37] J.C. Moreno-Rodriguez, J.C. Atenco-Vazquez, J.M. Ramirez-Cortes, R. Arechiga-Martinez, P. Gomez-Gil, and R. Fonseca-Delgado, *BIOMEX-DB: A cognitive audiovisual dataset for unimodal and multimodal biometric systems*, IEEE Access **9** (2021), 111267–111276.

[38] S.M.M. Najeeb, R.R.O. Al-Nima, and M.L. Al-Dabag, *Reinforced deep learning for verifying finger veins*, Int. J. online Biomed. Eng. **17** (2021), no. 7, 19–27.

[39] K.J. Noh, J. Choi, J.S. Hong, and K.R. Park, *Finger-vein recognition based on densely connected convolutional network using score-level fusion with shape and texture images*, IEEE Access **8** (2020), 96748–96766.

[40] M.O. Oloyede and G.P. Hancke, *Unimodal and multimodal biometric sensing systems: A review*, IEEE Access **4** (2016), 7532–7555.

[41] M. Pak and S. Kim, *A review of deep learning in image recognition*, Proc. 4th Int. Conf. Comput. Appl. Inf. Process. Technol. CAIPT 2017, 2018, pp. 1–3.

[42] B. Pandya, G. Cosma, A.A. Alani, and A. Taherkhani, *Fingerprint classification using a deep convolutional neural network*, 4th IEEE Int. Conf. Inf. Manag., 2018, pp. 86–91.

[43] J. Priesnitz, C. Rathgeb, N. Buchmann, C. Busch, and M. Margraf, *An overview of touchless 2D fingerprint recognition*, EURASIP J. Image Video Process. **2021** (2021), 8.

[44] H. Qin and P. Wang, *Finger-vein verification based on LSTM recurrent neural networks*, Appl. Sci. **9** (2019), no. 8, 1–18.

[45] J. Ribeiro Pinto, J.S. Cardoso, and A. Lourenco, *Evolution, current challenges, and future possibilities in ECG Biometrics*, IEEE Access **6** (2018), 34746–34776.

[46] T. Sabhanayagam, V.P. Venkatesan and K. Senthamaraikannan, *A comprehensive survey on various biometric systems*, Int. J. Appl. Eng. Res. **13** (2018), no. 5, 2276–2297.

[47] F. Saeed, M. Hussain, and H.A. Aboalsamh, *Automatic fingerprint classification using deep learning technology (DeepFKTNet)*, Math. **10** (2022), no. 8, 1285.

[48] P. Saikia, R.D. Baruah, S.K. Singh, and P.K. Chaudhuri, *Artificial neural networks in the domain of reservoir characterization: A review from shallow to deep models*, Comput. Geosci. **135** (2020), 104357.

[49] R. Saini, B. Kaur, P. Singh, P. Kumar, and P.P. Roy, *Don't just sign use brain too: A novel multimodal approach for user identification and verification*, Inf. Sci. **430** (2018), 163–178.

[50] K. Shaheed, H. Liu, G. Yang, I. Qureshi, J. Gou, and Y. Yin, *A systematic review of finger vein recognition techniques*, Inf. **9** (2018), no. 9, 213.

[51] M. Sharif, M. Raza, J.H. Shah, M. Yasmin, and S.L. Fernandes, *An Overview of Biometrics Methods*, Handbook of Multimedia Information Security: Techniques and Applications, 2019.

[52] S.A. Shawkat, K.S.L. Al-Badri, and A.I. Turki, *The new hand geometry system and automatic identification*, Period. Engin. Natural Sci. **7** (2019), no. 3, 996–1008.

[53] K. Siddique, Z. Akhtar, and Y. Kim, *Biometrics vs passwords: A modern version of the tortoise and the hare*, Comput. Fraud Secur. **2017** (2017), no. 1, 13–17.

[54] G.K. Sidiropoulos, P. Kiratsa, P. Chatzipetrou, and G.A. Papakostas, *Feature extraction for finger-vein-based identity recognition*, J. Imag. **7** (2021), no. 5.

[55] M. Singh, R. Singh, and A. Ross, *A comprehensive overview of biometric fusion*, Inf. Fusion **52** (2019), 187–205.

[56] S. Socheat and T. Wang, *Fingerprint enhancement, minutiae extraction and matching techniques*, J. Comput. Commun. **8** (2020), no. 5, 55–74.

[57] J.M. Song, W. Kim, and K.R. Park, *Finger-vein recognition based on deep densenet using composite image*, IEEE Access **7** (2019), 66845–66863.

[58] A. Takahashi, Y. Koda, K. Ito, and T. Aoki, *Fingerprint feature extraction by combining texture, minutiae, and frequency spectrum using multi-task CNN*, IJCB IEEE/IAPR Int. Jt. Conf. Biometrics, 2020, pp. 1–8.

[59] L.D. Tamang and B.W. Kim, *FVR-Net: Finger vein recognition with convolutional neural network using hybrid pooling*, Appl. Sci. **12** (2022), no. 15, 7538.

[60] H.M. Therar, E.A. Mohammed and A.J. Ali, *Biometric signature based public key security system*, 3rd Int. Conf. Adv. Sci. Eng. ICOASE 2020, pp. 133–138.

[61] M. Wang and W. Deng, *Deep face recognition: A survey*, Neurocomput. **429** (2021), 215–244.

[62] K.N. Win, K. Li, J. Chen, P.F. Viger, and K. Li, *Fingerprint classification and identification algorithms for criminal investigation: A survey*, Futur. Gener. Comput. Syst. **110** (2020), 758–771.

[63] F. Wu, J. Zhu, and X. Guo, *Fingerprint pattern identification and classification approach based on convolutional neural networks*, Neural Comput. Appl. **32** (2020), no. 10, 5725–5734.

[64] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, *A fingerprint and finger-vein based cancelable multi-biometric system*, Pattern Recogn. **78** (2018), 242–251.

[65] J.C. Zapata, C.M. Duque, Y. Rojas-Idarraga, M.E. Gonzalez, J.A. Guzmán, and M.A. Becerra Botero, *Data fusion applied to biometric identification–A review*, Communicat. Comput. Inf. Sci. **735** (2017), 721–733.