Information Security Journal: A Global Perspective

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uiss20

Challenges and opportunities in biometric security: A survey

Shefali Arora & M.P.S Bhatia

To cite this article: Shefali Arora & M.P.S Bhatia (2021): Challenges and opportunities in biometric security: A survey, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2021.1873464

To link to this article: https://doi.org/10.1080/19393555.2021.1873464

Published online: 14 Jan 2021.

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
https://doi.org/10.1080/19393555.2021.1873464

Challenges and opportunities in biometric security: A survey

Shefali Arora [a] and M.P.S Bhatia [a]

[a]Department of Computer Engineering, Netaji Subhas Institute of Technology, Delhi, India

ABSTRACT

Biometric systems identify individuals based on unique traits such as the face, fingerprints, iris etc. The main objective of the study is to understand the role of deep learning in the process of authentication as well as its application in the enhancement of security of biometric systems. We highlight the studies using deep learning approaches to authenticate enrolled users under ideal and non-ideal environmental conditions. We summarize these approaches and explore the challenges that continue to restrict the full potential of biometric systems. The foremost are: building robust algorithms for authentication, ensuring the security of enrolled templates and protecting systems against spoofing attacks. In this paper, we review the performance achieved by various studies in overcoming the aforesaid challenges, along with the potential improvements and future directions in this domain.

KEYWORDS

biometrics; security; privacy; deep Learning; convolutional Neural Networks; spoofing

1. Introduction

Biometric systems offer a reliable solution to identify individuals in scenarios that require secure authentication. Their sensors work on human traits such as fingerprint, iris and face to grant access to a system (Pagnin & Mitrokotsa, 2017). Earlier, passwords and PINs were used for such mechanisms. One of the main advantages of using biometrics as an entry mechanism is that it does not require memorizing complicated tokens or passwords. Authentication in these systems refers to the automated recognition of individuals based on their behavioral and biological characteristics (Jain et al., 2016).

The development of automated biometric systems started in the 1960s. These systems can be used in surveillance, forensics and other security-related activities. However, they are vulnerable to attacks and also incur extra hardware and software costs. The enrollment process can lead to false matches due to unconstrained environments. It is also possible to tamper with the enrolled templates.

Multimodal biometric systems combined with the use of passwords can help to enhance the security of such systems. The use of deep learning approaches can build robust algorithms to recognize individuals. For biometric systems to be effective, they should comply with the following properties (Sundararajan & Woodard, 2018):

- They should be able to capture the identities of millions of individuals, by understanding the variations in the multiple samples collected from each.
- They should be prone to spoofing and should be able to deal with noisy and distorted data collected in unconstrained environments.
- Distinctiveness and permanence of human traits are important parameters in such systems (Ross et al., 2006).

The main objective of this paper is to review the studies exploring the role of deep learning in the field of authentication using biometric systems. We also highlight the strengths and potential improvements in these works. This assessment would help us to underlying the gaps and challenges. The use of deep learning would not only automate these systems but also detect possible security vulnerabilities like spoofing and attacks on enrolled templates.

Section 2 discusses the process of biometric authentication and the applications of such systems. Section 3 discusses the core challenges and potential gaps which can be overcome in the field of biometric research. Section 4 describes the deep learning approaches that would benefit researchers to build robust algorithms and performances achieved on different traits in existing studies. Section 5 discusses

CONTACT Shefali Arora arorashef@gmail.com Department of Computer Engineering, Netaji Subhas Institute of Technology, Delhi.

the role of deep learning in enhancing the security of biometric systems in various scenarios. Section 6 illustrates a case study on the detection of spoofing in fingerprints using our proposed framework. Section 7 concludes the paper.

2. Framework of biometric systems

2.1. Recognition process

There are two phases in a biometric system: registration (or enrollment) and recognition. The first step involves pre-processing and feature extraction. These features are stored as templates in the database. During verification or identification (i.e. authentication), feature extraction is followed by the process of decision-making by matching the identity with the stored templates.

The system is regulated using a threshold t. During the process of matching identities with templates, if sample pairs generate scores higher than t, it signifies that they belong to the same person. Otherwise, they belong to different persons.

A biometric system can mistake inputs from various individuals to be from the same one (this is known as False Match Rate or FMR). Inputs from the same individual can be treated to be from different ones (this is known as False Non-Match Rate or FNMR). Other metrics used to determine the performance of a biometric system are Failure to Capture (FTC) and Failure to Enroll (FTE). FTC is defined as the percentage of times the biometric system fails to capture a user's trait. FTE is defined as the number of times an individual fails to register in the biometric system.

The choice of a human trait for such systems depends on the degree to which the conditions of uniqueness, distinctiveness, permanence, user acceptance, etc., are satisfied. These days, fingerprint, face and iris are the three commonly used traits for authentication. While several facial and fingerprint datasets have been collected by governments and agents, the iris is being increasingly used for large-scale authentication as it can help to achieve high accuracy in such systems.

In a face authentication system, the process is completed by finding similarity between two faces and identifying a match. The detection process can include face edge detection, localization and segmentation for pre-processing images. Face patches can be taken from different camera alignments leading to occlusion and distortion. Therefore, feature extraction, noise cleaning and dimension reduction of images must be done before the final matching. (Jain et al., 2001)(Cho & Jeong, 2014).

Feature extraction may signify procurement of the image features such as visual, statistical and transform coefficients (Hassaballah & Aly, 2015).

Figure 2 shows the different traits used in biometric systems for authentication (Jain et al., 2016).

2.2. Applications of biometric systems

Biometric systems are very commonly used in the following domains:

- They are commonly used for automated attendance of employees and students. The most common traits used in these systems are faces and fingerprints.
- Organizations like the Federal Bureau of Investigations (FBI) and Interpol have been using biometrics for forensic investigations to allow examiners to cross-check identities of suspects for possible matches with stored templates.
- Biometric authentication is widely used around the world for home access control, mobile phone access, vehicle access authentication, etc. (Zeng et al., 2014).
- Biometrics in banking has increased exponentially in recent years. Banks are implementing these technologies to increase security in transactions and reduce the chances of frauds. This would increase the convenience of customers.

Section 3 describes the various challenges faced in the design of biometric systems and the research gaps in existing studies, which can be overcome using deep learning.

3. Challenges and research gaps

For biometric systems to be efficient, the similarity between various inputs from one individual must be high, and it should be low between inputs taken from different individuals. Most of the research in

the field of biometrics is centered on two main problems:

i) To find the best representation scheme for a particular trait. The feature extractor must be capable of minimizing intra-subject variations.

ii) To design robust algorithms for feature extraction is another major challenge in biometric systems (Ding et al., ..2011). Matching algorithms should be chosen based on the characteristics of various traits.

iii) Permanence and distinctiveness of traits affect the performance of a biometric system. Hence it is important to analyze these properties while designing the system.

iv) Biometric templates can be compromised or stolen. In case an adversary replicates an individual's trait used for authentication, he could use it to gain access to crucial applications. Authors (Jain et al., 2001) identified different points of attacks in a system, including those at the interface, modules, template database, etc.

In this paper, we survey some of these challenges and the role of deep learning in tackling them. These include detection of spoofing attacks, protection of biometric templates and identification of traits in unconstrained conditions. We highlight the superiority of deep learning algorithms over state-of-the-art methods and potential future directions that would be useful for researchers. For example, the role of multimodal biometric systems to enhance security is becoming important these days.

3.1. Contribution

Our main contribution in the paper is as follows:

This paper gives an insight into the various studies which would prove helpful for fellow researchers in designing robust deep learning algorithms for biometric systems. These techniques would prove to be beneficial in authentication as well as for addressing some of the challenges that affect the security of biometric systems.

We study and summarize the strengths of various deep learning approaches that have been used in various researches to build efficient algorithms for biometric systems. We also highlight the potential improvements in the summarized techniques so as to provide future directions to researchers in this field.

We highlight the application of deep learning approaches to enhance the security of biometric systems. For this purpose, we summarize the various approaches which have been used for detection of spoofing attacks, attacks against templates etc. The open issues and future directions for research in these domains have been explored.

We highlight our contribution in the enhancement of security of biometric systems. We explain our proposed framework for detection of spoofed fingerprints in a biometric system. Further, the accuracy obtained is compared with some of the research works studied in this paper.

In the next section, we highlight the various deep learning architectures and their performance in biometric systems for authentication of human traits like face, fingerprint and iris.

4. Deep learning in biometrics

4.1. Deep learning architectures

4.1.1. Convolutional neural networks (CNN)

Convolutional neural networks are mainly used for image classification. Originally developed by Geoffrey Hinton (Geoffrey, 2010), they are ideal for detecting objects from different images. Given 1D input x and a filter k, this operation is defined as:

$$y[n] = (x*k)[n] \sum_{-\infty}^{\infty} x[m]k[n-m] \qquad (1)$$

Convolutional layers are followed by pooling layers and fully connected layers. In convolution, input image matrix is convolved with a filter matrix to create a feature map for the next layer. The use of kernels makes CNNs location-invariant and avoids overfitting. Figure 3 gives an example of the convolution process.

The final layer or fully connected layer connects the previous units and makes use of some nonlinear activation function (ReLu, tanh, sigmoid, etc.)

4.1.2. Deep belief networks (DBM)

DBN is a class of deep neural network with multiple layers of models with directed and undirected edges. There are multiple hidden units in a deep belief network. Layers are connected but units are not (Krizhevsky et al., 2017).

A belief network consists of stochastic binary unit layers with weight-associated to each connected layer. The units can have state 0 or 1, and the probability of unit attaining state 1 depends on the values of weighted units from other inputs along with a bias value. Figure 4 depicts a deep belief network (Salakhutdinov & Larochelle,).

Restricted Boltzmann machines (RBM) constitute a deep Belief Network, with various layers stacked to each other. DBMs have directed edges between lower layers (i.e. a Bayesian network) and undirected edges between top layers (i.e. RBM).

4.1.3. Long short term memory networks(LSTM)

LSTM is an advancement of recurrent neural networks used for learning input sequences. It is used to learn sequential data and is better than RNNs, which suffer from the problem of vanishing gradient. Long Short Term Network was proposed by (Ilya, 2013). In LSTM, gates are used to decide the information to keep and the one to forget. These gates act like neural networks. The gates used are input gate i_t, output gate o_t, forget gate f_t and a gate signifying the cell state c_t.

$$c_t = \ tanh(W_c(h_{t-1}, x_t) + b_c\ ) \tag{3}$$

$$c_t = f_t\ c_{t-1}\ + i_t\ c_t \tag{4}$$

$$h_t = \ o_t \tanh(c_t) \tag{5}$$

4.2. Deep learning on various traits in biometric systems

Deep learning approaches improve the performance of biometric authentication due to the following factors:

(1) Feature learning: Deep learning approaches have an edge over traditional state-of-the-art methods because they can efficiently learn features from data. They are suitable for traits like face and voice which require feature learning in a hierarchical manner.
(2) Invariant representations. The robust representations obtained using deep learning approaches are useful since real-world data may be very noisy.
(3) Beyond bag-of-words features: With the resurgence of RNNs, the temporal aspects from data are being captured efficiently as compared to bag-of-word features.

Figure 5 shows the use of deep learning approaches applied to various traits:

4.2.1. Face

The face is the most common biometric trait used to recognize humans in biometric systems. It can be used for various activities like crime prevention, surveillance, and forensic applications as well as in social networks. Automatic face recognition has various challenges associated with it due to image quality and other factors such as variations in pose, expression, style, age etc. Various deep learning approaches have been proposed for the detection and alignment of faces. These can be classified into feature-based approaches which make use of local features, as well as appearance-based approaches making use of global features.

Face recognition using a deep-learning approach combines both local and global factors. The use of CNN-based approaches has made a significant impact on the process. During authentication, the similarity between the two faces should be taken care of and cost function should be minimized. Using deep learning, face recognition becomes a multi-class classification problem where the prediction of a label can be done using cross-entropy loss (with softmax activation) in its layer. A series of CNN architectures with varying objectives has been proposed by authors (Sun et al., 2014) for authentication. The extracted features are used along with Joint Bayesian learning for matching faces (Chen et al., 2012) Authors make the following observations while using this approach: i) if more training data is fed as input, it would help improve the accuracy of the system (ii) use of different color channels and scales for the representation of faces is effective iii) Use of deep learning can help to extract features and make the system robust to occlusion.

4.2.2. Fingerprint

Fingerprint has been used in various applications such as forensics, cellphone unlocking, banking applications, etc. (Amira et al., 2011). Many algorithms used for authentication of fingerprints are based on the matching of minutiae (Ratha et al., 2001). The major features of these minutiae are ridge endings and

bifurcations. Various studies involve the extraction of handcrafted features followed by classification. Recently, deep learning has found its way in this domain. Authors (Barrett, 2013) made use of multi-scattering convolutional networks, which segmented fingerprint images into different orientations using wavelets.

In recent years, there have been a lot of studies which focus on preprocessing followed by feature extraction using deep networks, and prediction using classifiers. In this direction, CNNs have been successful due to availability of large-scale labeled datasets, availability of GPUs and good regularization techniques used in these networks.

The vast majority of feature extraction methods extensively peruse textural properties or configuration of image pixels. A robust feature extractor should have the capability of dealing with rotation, translation and skin distortion.

Figure 1 shows the process of authentication in biometric systems.

4.2.3. Iris

Authors (J Liu et al., 2015) used CNNs to learn filters from iris images from visible and infrared sources. Authors (Gangwar & Joshi,) used two very deep CNN architectures for authentication of iris and demonstrated the robustness of this approach. Authors (Silva et al., 2015) proposed the classification of the iris, based on the characteristics of contact lenses. Authors (Nguyen, Pham, et al., 2018) used a three-layer CNN to identify left and right iris images that have been incorrectly labeled.

Input images need to undergo a lot of preprocessing and segmentation before they can be taken up for feature extraction (Zhao and Kumar, 2017). This is important to improve the classification performance. Other factors like translation; rotation, etc., can be handled well by these networks (Kuo, 2016).

Tables 1, Tables 2, Tables 3 give an overview of some studies which involve the use of deep learning approaches for authentication using popular traits

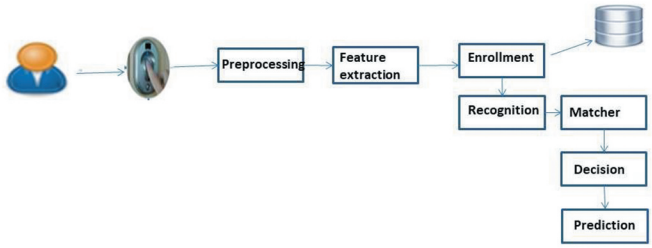

Figure 1. Authentication process in biometric systems.

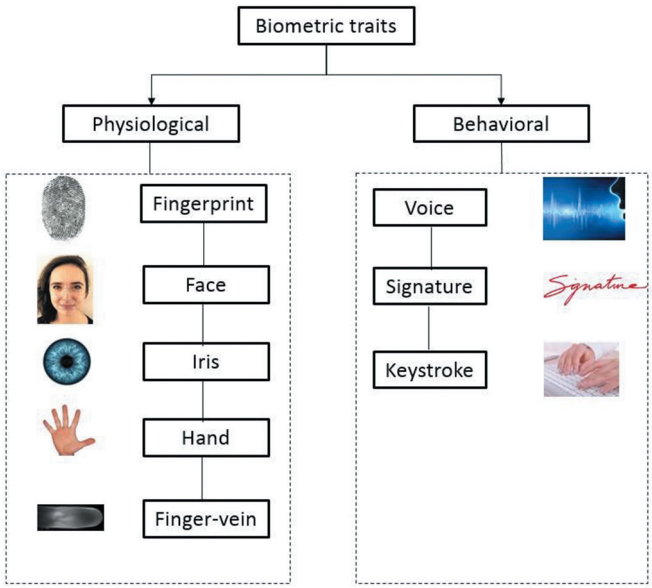

Figure 2. Commonly used traits for biometric authentication.

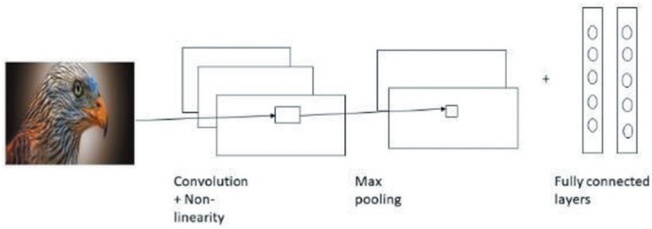

Figure 3. Architecture of CNN.

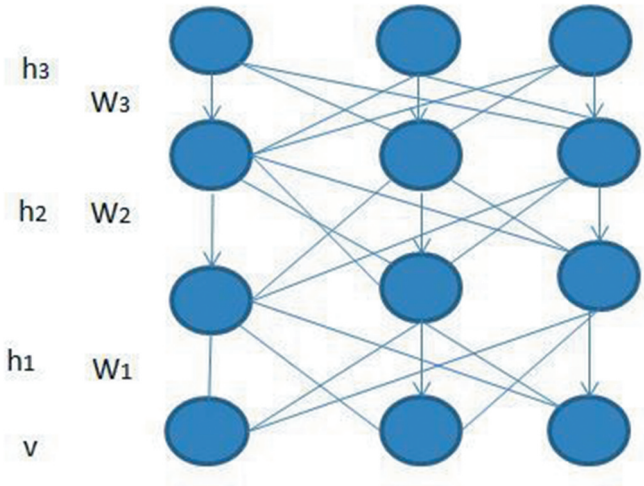

Figure 4. Architecture of a deep belief network.

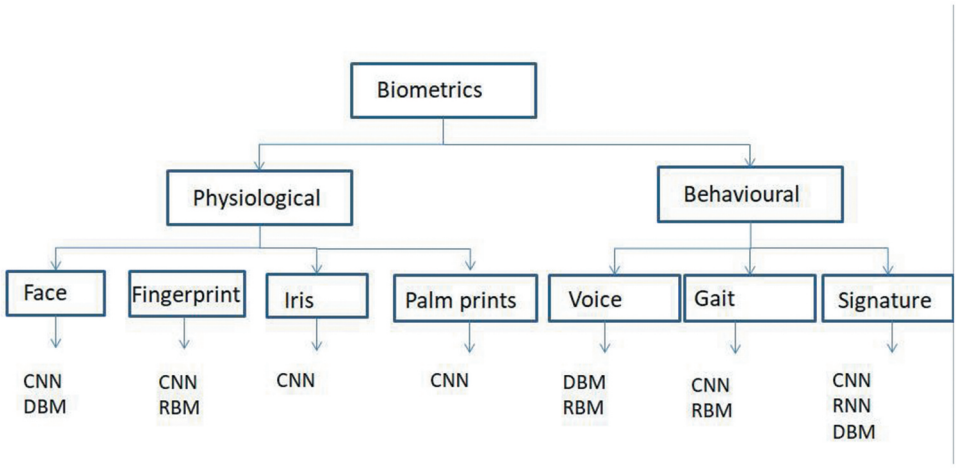

Figure 5. Use of deep learning to recognize biometric traits.

like face, fingerprint and iris, respectively. We also study the performance achieved using such approaches on more traits – fingervein (Liu and Xie et al., 2013, Matthias et al., 2014) voice and palmprints. This can be observed in Tables 4, Tables 5.

The common performance metrics used in these tables to evaluate the performance of biometric systems are:

(1) False accept rate (FAR) denotes the ability of a non-authorized user to access the system.

Table 1. Performance of deep learning methods on authentication using face.

Training Dataset	Strength of technique	Performance
LFW	Use of deep CNN on large scale dataset, discussion of trade-off between data purity and time (Parkhi et al., 2015)	Accuracy: 98.95%
Yale facial images dataset	Symmetry of faces explored using CNN to improve performance (Ramaiah et al., 2015)	Accuracy: 94.01% Misclassification error: 23.05%
Cox Face DB)	Use of autoencoders along with deep CNN (Bashbaghi et al., .	Accuracy: 91.20%
SFC	3D face modeling and use of nine layer deep network to improve performance(Taigman et al., 2014)	Accuracy: 97.35 ± 0.25%
LFW dataset	Multi patch deep CNN to extract low dimensional features (J Liu et al., 2015)	Accuracy:99.41%
CASIA Webface	Explores the variations in poses using deep CNN (Masi et al., 2016)	Accuracy:94.6%
CASIA Webface	Use of pre-trained LeNet CNN network and patch based triplet network(Peng et al., 2016)	Accuracy: 96.60%
Celebfaces+WDRef	Use of deep CNN to optimize the face embeddings(Schroff et al.,2015)	Accuracy: 99.30%
LFW	CNN (Sun et al., 2016)	Accuracy: 99.63%
CASIA Replay	Use of pre-trained VGGNet architecture (Lakshminarayana et al., 2017)	HTER(CASIA):1.1 HTER(Replay-Attack) 0.8
LFW	Performance improvement using triplet networks by splitting spaces into subspaces with similar faces (Wang et al.,)	Accuracy:98%
YTF (Youtube Faces dataset	Use of deep CNN along with SVM for classification(Wen et al.,)	Accuracy: 94.72%
Youtube faces dataset	Recognition in unconstrained environments on large data (Kulkarni, 2018)	Accuracy: 84.3 ± 6.8%
LFW	Feature normalization in CNN architecture (Hasnat et al.,)	Accuracy:99.62%
CASIA Webface	Shared parameters of CNN for face detection, pose estimation etc. (Ranjan et al., 2017)	Accuracy:92.2%

Table 2. Performance of deep learning methods on authentication using fingerprints.

Training Dataset	Strengths of the technique	Performance
FVC 2002	Two continuous Restricted Boltzmann machines on clean fingerprint images(Sahasrabudhe & Namboodiri, 2013)	EER: 22.95
FVC 2002, 2004,2006	CNN combined with ensemble methods and batch normalization (Wang-Su & Sang-Yong, 2017)	Accuracy – 98.3%
Finger vein dataset	Seven layers of CNN (Y Liu et al., 2017)	Accuracy:99.53%
Fingervein	Use of deep CNN on large fingervein datasets(H Huang et al., 2017)	EER = 0.42
Finger vein Developed In-house	4 layer CNN with reduced complexity and subsampling(Radzi, 2016)	Accuracy = 99.38%
WVU DB	Latent fingerprint recognition using CNN(Cao & Jain, 2019)	Rank 1:70.8

Table 3. Performance of deep learning methods on authentication using iris.

Training Dataset	Strengths of the technique	Performance
LG2200	Deep CNN to study microstructures in iris(Gangwar & Joshi,)	EER:2.40
CASIA	Use of pre-trained ResNet model and classification using SVM (DT Nguyen et al., 2018)	Accuracy:98.5%
CASIA	Deep CNN to determine iris boundaries even in inferior quality images(Kim et al., 2018)	EER:0.99
IITD	Deep CNN to determine iris boundaries even in inferior quality images (Kim et al., 2018)	EER:0.64
NICE	Image capturing using new segmentation techniques in unconstrained environments and classification using ResNet Raja, Raghavendra, Vemuri et al., 2015)	EER:13.98
IITD iris dataset	Use of pre-trained VGGNet and classification using SVM (Garcia-Romero et al., 2014)	Accuracy:99.4%
Free dataset	Use of pre-trained LeNet and classification using SVM (Maram & Lamiaa, 2018)	Accuracy:93.5%
IITD	Use of pre-trained AlexNet and classification using SVM (Maram & Lamiaa, 2018)	Accuracy:98.33%

Table 4. Performance of deep learning methods on authentication using voice.

Training Dataset	Strengths of the technique	Performance
SRE 2012	Extract Baum-Welch statistics to train a vector extractor using deep neural networks (Kenny et al., 2014)	EER:2.16
SRE 2004,2005,2006	Use of deep belief network to learn utterances of inputs (Vasilakakis et al.,)	EER:2.18
SRE 2012	Use of Convolutional Neural Networks to extract features from voice signals (Saleem & Hansen, 2016)	EER:0.45

Table 5. Performance of deep learning methods on authentication using palmprint.

Training Dataset	Strengths of the technique	Performance
PolyU	Contactless palmprint recognition using Convolutional Neural Networks(Jalali et al., 2015)	Accuracy:99.98%
PolyU	Use of pretrained AlexNet model to capture palm ROIs (Dian & Dongmei, 2016)	EER:0.0443%

(2) False Reject rate (FRR) describes the number of authentic users falsely rejected by the system.
(3) Equal Error Rate (EER) is the value where FAR and FRR become equal.
(4) Accuracy is an important performance metric, which denotes the percentage of profiles correctly matched to available templates.
(5) The Half Total Error Rate (HTER) or Average Classification Error (ACE) is calculated as the average of FAR and FRR.

4.3. Potential improvements in these approaches

Based on the gaps in existing research works, the potential improvements and future directions can be analyzed from the points below:

- Most of the approaches used in the tables use robust deep learning frameworks, however, authentication becomes challenging in real-world situations such as unconstrained environments.
- These frameworks can be improved to enhance the security of biometric systems, thus ensuring protection from spoofing and other attacks.
- Massive data: The availability of large amounts of data makes it challenging for deep learning frameworks in terms of network complexity. To get large number of features from these data instances, complex models are required. The use of parallel processing on distributed frameworks can help to solve this problem.
- Hyperparameter tuning: Various factors can be optimized for deep learning frameworks so that they are able to run on mobile phone applications.
- Data pre-processing: It is very important to preprocess the input images efficiently. For example, over-segmentation or unclear pupil images can lead to errors in case of iris images.

5. Applications of deep learning to enhance security of biometric system

A biometric system can be secured against various listed vulnerabilities with the help of deep learning approaches:

5.1. Spoofing detection

Spoofing attacks can take place if a fake trait is presented to the sensor of the biometric system. As these traits can be compromised, it is easy for an intruder to use this stolen trait to bypass the sensor. Thus the system will not be able to distinguish between the real and forged trait. With some prior knowledge of the input, an intruder can succeed in breaching a biometric system. This threatens the security and privacy of an individual. Thus detection of spoofing attacks is one of the important challenges while designing a biometric system. Figure 6 shows the various kinds of materials used for spoofing fingerprints:

5.1.1. Face

Face presentation attack detection (PAD) has become an important issue in recognition of faces since the technology has been applied in various authentication systems and mobile devices. Four kinds of presentation attacks are possible in such a system: printed photo, displayed image attack, replayed video attack and 3D mask. The first three kinds of attacks usually print or display a forged face image in a 2D medium (e.g., paper and LCD screen). In case of a 3D face mask scenario, the attacker wears a 3D mask to deceive face recognition system. (Gotardo et al., 2018).

Authors used a CNN network was used to detect spoofing for all traits like face, iris and fingerprint (Peng et al., 2016). Authors combined the 2 layers of CNN with LSTM to detect spoofing in faces (Masi et al., 2016). Authors proposed a shallow CNN network to distinguish between genuine and

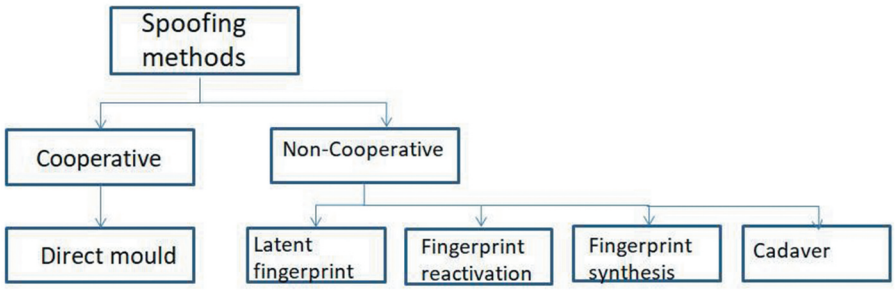

Figure 6. Methods of spoofing attacks on fingerprints.

spoofed faces (Sun et al., 2016). They used non-linear diffusion along with the additive operator and the diffused image was given as input to CNN to classify the image as real or spoofed. In another work, Li et al. tackled the 3D mask attacks by detecting the pulse from videos, which may be sensitive to camera settings and light conditions. Besides, it becomes easier to obtain 3D masks by attackers with the development of 3D printing (Roomi et al., 2015).

The most widely used approach is the use of Convolutional Neural Networks (CNN). Most of the studies work on faces as a whole, or small patches taken from faces. Thus they do not learn local cues from each facial region. Authors used transfer learning with the help of pre-trained VGG16 for feature extraction from faces (Zhou et al., 2006). Other important works in the literature make use of global features by using other pre-trained architectures (Wang et al.,)

The authors explore random patches for face spoofing detection (Wen et al.,). Such an approach can especially be used for augmentation of data. Despite giving good results, it can distract the network from learning spoofing cues. Rather, it would only learn the structural information available from facial regions (Kollreider et al., 2009). Figure 7 shows the process of detection of spoofed faces in a biometric system(Shiranthika,, 2019).

5.1.2. Fingerprints

Most of the smartphone vendors are taking care that fingerprint templates remain protected within the smart device. Several fingerprint sensors were tested to check if they accepted fake fingerprints. It was observed that around 11 fingerprint-based authentication systems were exposed to fake fingerprints, and these were accepted with a probability of around 67%. With the increasing number of iPhones, the possibility of fingerprint spoofing on TouchID is being explored.

Attacks involving dummy fingers are successful in Apple iPhone 5S and Samsung Galaxy S5.

Detection of spoofing in fingerprints has been studied using deep learning in recent years (Yang and Wang, 2019). These approaches work effectively against fake fingerprint materials (Kuo, 2016). Authors made use of CNNs and Local Binary patterns to extract features from fingerprints and classification is performed using SVM (Sahasrabudhe & Namboodiri, 2013).

Leakage of such information is a threat and stolen traits can be used by malicious users to impersonate another person. Therefore, there is a need to detect whether the fingerprint presented to the biometric system is real or forged .The sensor of a biometric system detects the ridges and valleys of a fingerprint input to it. Further, the template is matched against the stored templates of individuals. Depending on the extent to which these

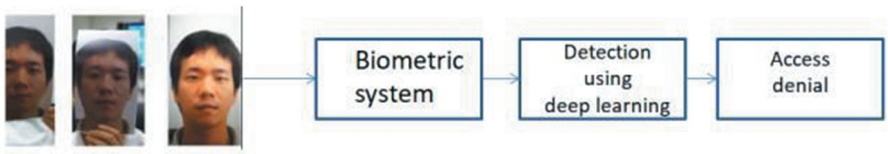

Figure 7. Spoofing in biometric systems.

templates match and the system threshold, the individual would be authenticated or denied access.

For creating an artificial or spoofed fingerprint, the following materials could be used:

- Direct mold comprising silicone or gelatin.
- Latent fingerprinting using a powder or a mask exposed to UV light.
- A synthetic fingerprint template could be reconstructed
- A viscous material could be deposited on the sensor.

Figure 8 shows the images of spoofed fingerprints obtained with user cooperation in the ATVS-FFp dataset (Galbally et al., 2012)).

5.1.3. Iris

In the case of spoofing in biometric systems involving authentication using iris, impostor accesses the images and enrolls his template in place of the targeted individual. An attacker can obscure useful information in the texture of images using various techniques. Or he can enroll a template that does not belong to any real person and use it for further purposes. They can also generate synthetic iris patterns (Bowyer & Doyle, 2014). To accomplish such an attack, impostor presents an input which is processed by a system and matched to an existing template. This could be in the form of print attacks, in which a photograph of the iris is taken and presented to the sensor. Presentation attacks are generally successful for input images acquired in near-infrared light as compared to those captured in visible-light images. Authors (Rathgeb & Busch, 2017) show how to generate a single iris code which can act as the starting point for the preparation of morphed iris codes to match with the identity of more than one individual. Authors (Rathgeb et al., 2013) used a hill-climbing approach to create iris images that could be used for false enrollment. This includes training of systems using real and forged samples of different types of spoofing attacks. In another technique, authors (Lefohn et al., 2013) worked on generating artificial irises that match the patterns of live irises, by using multiple layers. The various possible threats and security issues are as follows:

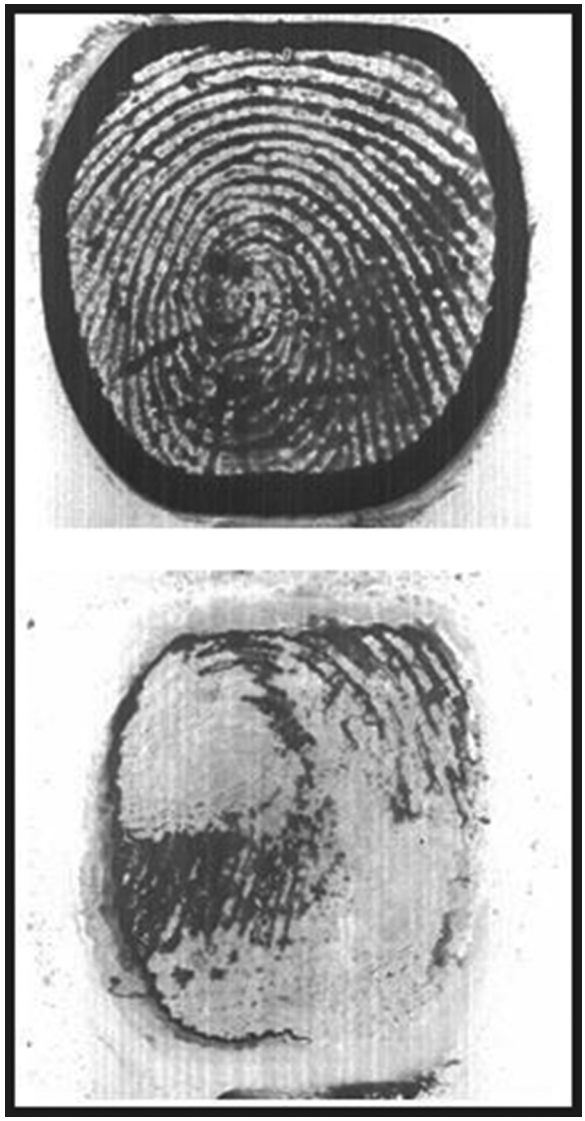

Figure 8. Spoofed fingerprints from the ATVS-FFp dataset.

- Presenting forged data to the sensor
- Exploit similarity between individuals, e.g., faces of identical twins
- Destruction of biometric sensor
- Intercept a biometric signal and replay it
- Alter the information from the channel to prevent a genuine user from being authenticated
- Modify the input image
- Inject Trojan horse in the system
- Obtain access to biometric templates, add or modify information

5.1.4. Results achieved using deep learning to detect spoofing

Table 6 explores the various approaches used for detection of spoofing in different traits. The

performance shown by deep learning techniques surpasses the results of state-of-the-art techniques, in terms of various metrics.

5.1.5. Open issues and future directions in spoofing detection

Authors (Marasco & Ross, 2014) observed that the performance of spoofing detection algorithms can decrease if different materials are used during training and testing. Therefore, there is a need to develop general countermeasures which do not get impacted by the material used to create the spoofs. Human factors such as pressure, humidity and temperature, etc., can affect the performance of the deep learning framework. Developing interoperable spoofing detection algorithms is effective while integrating them in biometric systems. A robust fusion scheme can make use of the liveness scores and match scores to get a final decision. It is important to develop methods that can certify the level of security of the biometric system. The advent of mobile biometrics has highlighted the need for designing robust techniques which can be optimized to detect spoofing in mobile phones.

5.2. Template protection using deep learning

The main motivation of using biometric systems is to prevent unauthorized users. However, it is possible that the biometric templates might not be secure. This might lead to a number of security vulnerabilities like denial of service and breach of privacy of users. One of the important steps making biometric systems secure is to protect the templates in the database. These templates are the features extracted from the biometric trait of an individual and stored as records. In the stage of verification, the query input is matched with template data and a verdict is given after the result of comparison. Figure 9 shows the use of image and key to create a biometric template.

To reduce the impact of distortions and global registration, authors proposed local structure based methods to store biometric templates. Authors (Yang et al., 2018) proposed a cancelable template design to protect templates. Each structure is local triangle based and it is transformed with the help of transformation matrices. These features are further converted to binary format. Further, a specific key is used to permute it into a feature representation scheme. To slow down the global registration process and lower the impact of nonlinear distortion in another work (Sadhya & Singh, 2018), authors proposed registration-free local structure-based methods.

Authors (Wang et al., 2014) applied geometrical properties, e.g., local relation, from minutiae triplets (Wang, C. et al., 2017) to perform hashing on fingerprints. The emerging homomorphic encryption technology seems to be another solution for enhancing security as it helps to match traits in an encrypted domain. Some of these techniques are visual Cryptography and Privacy-preserving Photo Sharing (Hashim & Saleh, 2018). The security of biometric templates continues to be an important area of research.

Table 8 shows the results achieved in the domain of template protection using deep learning approaches. The performances achieved indicate that such approaches are robust in enhancing the security of a biometric system.

5.2.1. Results

We analyze a few deep learning approaches that have been used to secure biometric templates enrolled in a system. The results have been tabulated in Table 7.

5.2.2. Open challenges and future directions in protection of templates

One of the main challenges in a biometric system is the generation of non-invertible and non-linkable templates without reducing the accuracy of authentication. In case a biometric template gets revoked, it should be possible to generate the original template. Furthermore, the performance of the biometric system should not get deteriorated. Robust frameworks are needed when can prevent any kind of correlation between the protected templates. For template protection in biometric systems which fuse information from two or more traits, storage of multiple templates is another open challenge. This is because more data needs to be stored for a single individual in case of such systems.

Table 6. Performance of deep learning methods to detect spoofing vs state-of-the art methods denotes deep learning approach.

Database & Trait	Method	Performance
LivDet 2013 (Fingerprint)	Optimization of CNN architecture and learning of weights (Menotti, 2015)*	Accuracy:99.08%
Biometrika 2013 (Fingerprint)	Optimization of CNN architecture and learning of weights (Menotti, 2015)*	Accuracy: 99.85%
LivDet 2013 (Fingerprint)	Local binary descriptor wth SVM classifier(Xia et al., 2019)	Accuracy: 93.22%
Warsaw database (Iris)	Optimization of CNN architecture and learning of weights Menotti, 2015)*	Accuracy:99.84%
Biosec (Iris)	CNN (Menotti, 2015)*	Accuracy: 98.93%
Replay-attack database (Face)	Optimization of CNN architecture and learning of weights (Menotti *	HTER: 0.75
MobBioFake (Iris)	Optimization of CNN architecture and learning of weights (Menotti, 2015)*	Accuracy: 100%
3DMAD (Face)	Optimization of CNN architecture and learning of weights (Menotti, 2015)*	HTER: 0.0
CASIA (Face)	Two stream CNN for detection of local features and holistic depths(Atoum et al., 2017)*	EER:4.5%
Replay attack database (Face)	Two stream CNN for detection of local features and holistic depths (Atoum et al., 2017)*	EER: 2.9%
Replay attack database (Face)	Use of pre-trained VGGNet for detection(Lei et al., 2018)*	HTER: 16.62%
Replay attack database (Face)	Use of LSTM along with CNN for detection of temporal features (De Souza et al., 2018)*	EER:0.33% HTER:2.50%
Replay-attack database (Face)	Local discriminant analysis followed by SVM classification(Wen et al., 2015)	TPR @ FAR = 0.1 92.2 TPR @ FAR = 0.01 87.9
CASIA (Face)	Hyperspectral feature extraction followed by SVM classification(Wen et al., 2015)	Printed photo: 84.58 Replay attack: 94.82
MSU gummy Finger database (Fingerprint)	Use of Wavelet transform for (Tan & Schuckers, 2006)	Accuracy:80–100%
Private fingerprint database (Fingerprint)	Static and dynamic features*(Yang et al., 2018)	Accuracy: 75.35%
LivDet 2011 (Fingerprint)	Complete Local Binary pattern feature extraction for contrast enhancement(Wen et al., 2015)	Accuracy: 91.7%
MSU face database (Face)	Local Binary Pattern for feature extraction and SVM for classification(Wen et al., 2015)	Printed photo: 93.88 Replay attack: 96.19
IIITD CLI (Iris)	Detection using Cogent and Vista sensor(Gupta et al., 2014)	Accuracy: 94.30 (Cogent) 95.50 (Vista)
Biosec (Iris)	Classification using SVM(Sequeira et al.,)	Classification error: 0.5%
Clarkson database (Iris)	Classification using SVM(Sequeira et al.,)	Classification error: 6.2%
CASIA-FAS (Face)	Methods involving Image Quality Assessment and deep learning (Galbally & Sébastien, 2014)*	HTER: 32.4%
Replay attack (Face)	Methods involving Image Quality Assessment and deep learning(Galbally & Sébastien, 2014)*	HTER: 15.2%
Fake facial database (Face)	Calibration and comparison against lighting(Cho & Jeong, 2014)	Accuracy: 98.15%
CASIA (Face)	Patch based handicraft approach(Zahid & Foresti, 2016)	EER:4.65%
Warsaw 2017 (Iris)	Use of CNN and MLBP (Nguyen, Pham, et al., 2018)*	ACER: 0.016%
LivDet15 (Iris)	CNN (Hoffman et al., 2018)*	Accuracy:99.97%
ATVS-FFp (Fingerprint)	Use of pre-trained Inception model(Adik et al., 2019)*	Accuracy:99.2%
FVC-2002 (Fingerprint)	Use of pre-trained ResNet50 model(Chugh et al., 2018)*	ACE: 1.49%
LivDet 2013 (Fingerprint)	CNN with image scale equalization (Yuan et al., 2019)*	Average accuracy:95.30%

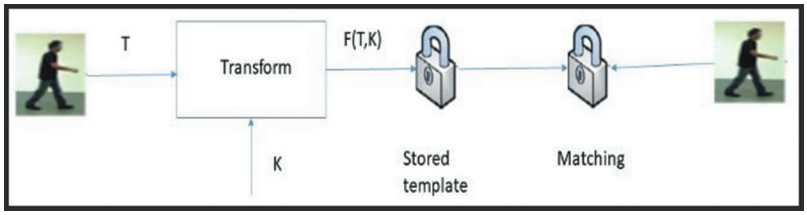

Figure 9. Protection of biometric templates.

Table 7. Deep learning approaches used for template protection.

Database	Method	Performance
CMU-PIE face dataset	CNN and Maximum Entropy Binary(MEB) encoding (Pandey et al., 2016)	Genuine Accept Rate (GAR): 97.59% at 0 FAR EER: 1.14%
CMU-PIE	Binary discrimminant analysis (Pandey et al., 2016)	GAR: 96.38% at 0FAR
Yale face dataset	CNN and MEB encoding (Pandey et al., 2016)	GAR:96.74 ± 1.35% at 0 FAR EER: 0.93 ± 0.18%
Finger vein	CNN and random projections(Kumar et al., 2019)	GAR:95.3% at 1.5% FAR
Finger vein	Principal Component Analysis (Kumar et al., 2019)	GAR:95% at 4.3% FAR
Finger vein	Deep belief network(Kumar et al., 2019)	GAR:96.9% at 1.5% FAR
CMU-PIE	CNN and random projections(Y Liu et al., 2017)	GAR: 99.98% ± 0.02%
FEI	CNN and random projections(Y Liu et al., 2017)	GAR:99.98% ± 0.03%
Color-FERET	CNN and random projections(Y Liu et al., 2017)	GAR: 99.24% ± 0.10%

Table 8. CNN architecture used.

Operation	Hyperparameter	Values
Convolution	Filters	32,64,128,256,512
	Number	5,5,5,5,5
	Fully connected layers	1024,2
Activation	Applied	ReLu,Softmax(Last layer)
Pooling size	Max Pooling	2,2,2

5.3. Identification in unconstrained environments such as video surveillance

Some applications might impose constraints on how a trait is acquired. Example, lifting of latent fingerprints from a crime scene, or iris sensors requiring iris to be close till the process gets over (Garris et al. 2000). User acceptance of iris authentication technology can be greatly enhanced if iris patters can be captured from a distance by iris sensors, while the subject is in motion.

But it might not be very reliable due to large intra-class variations. Therefore, robust algorithms are required for this process. Another example of an unconstrained environment is video surveillance, in which CCTVs are used to capture faces in public places. It is estimated that there are more than 1 million CCTV cameras in London and around 5 million cameras in the UK itself (Barrett, 2013) The captured videos are analyzed by human operators and any incident is reported. Real-time video processing can be used to detect such incidents. However, it might be subjected to replay attacks where intruders might impersonate the person-of-interest.

5.3.1. Open issues and future directions

Face recognition in surveillance applications is a very challenging problem because images captured might be of poor quality. This may be due to low resolution of camera or large distance between camera and individual, or the speed at which he is moving, illumination and occlusion problems. There might be changes in pose and expressions as the subject is not getting captured with his due cooperation (Yin & Liu, 2018). He might be wearing accessories or caps or glasses. A subject may try to hide. Moreover, in video surveillance, a sequence of face images is matched against a gallery of still images.

Generally, it cannot be estimated that which order of images in the video sequence would give a correct result. Thus, authentication of faces from the video introduces an additional layer of complexity because of the various evidence given by multiple images that can be merged. Authors (Klontz & Jain, 2013) simulated the recognition of faces to identify the suspects of a bomb attack. They achieved this by adding the images of two suspects against a database of around 1 million images. The image obtained from surveillance cameras and FBI was matched against the images in their gallery using two state-of-the-art COTS face matchers. As a result, the image of one of the suspects matched with his high school photograph. Due to variation in pose, the image of the other suspect could not be matched. Even in case

of the suspect being caught, it might be argued that the match was obtained due to the same pose. This highlights the limitations of existing matchers and the need for automatic face detection systems.

Thus a large improvement is needed in case of the accuracy achieved during unconstrained face recognition. It needs to be made fully automated so that it can be deployed successfully in real-world applications like surveillance.

6. Information fusion to enhance security

In the last few years, research has been going on for the use of multimodal biometric systems in both government and private sectors. Multimodal biometric systems help to overcome the limitations of individual classifiers and unimodal biometric systems. This is done by fusing scores from different traits. Therefore, these systems improve recognition performance and also add several other advantages to the security and privacy of individuals (Nanni, 2017)

Although they help to obtain a better accuracy as compared to normal biometric systems, some gaps and challenges are relevant for discussion.

Firstly, many works on multimodal biometric systems involve the combination of two or more traits from different unimodal databases. However, this does not reflect well in real-world approaches as features from a single person are necessary to be correlated (Al Waisy et al., 2017). Secondly, most of the techniques used are based on traditional state-of-the-art approaches or shallow machine learning models to decipher biometric traits. The use of deep learning models in multimodal biometric systems is being explored and can give a real boost in performance. Thirdly, most of these systems lack flexibility as accuracy would decrease if one of the biometric traits is unavailable or missed. Therefore, these gaps need to be worked upon to make multimodal biometric systems robust and efficient.

Although existing multimodal biometric systems have been shown to improve the accuracy of existing systems, it is important to address the stated problems (Harjoko et al., 2009)

In the next section, we highlight our contribution in this field of research. Our proposed framework is based on deep learning to detect spoofed fingerprints using input images from various popular datasets.

7. Case study: application of deep learning to detect spoofing in fingerprints

Our contribution (Arora & Bhatia, 2020) highlights the role of preprocessing and hyper-parameter tuning in the detection of spoofing in fingerprints. We use histogram equalization to increase the contrast of input fingerprint images. This process helps to make the probability of a fingerprint's histogram uniform. Thus histogram equalization extends the histogram of a given fingerprint image to either ends. For a given image, the gradient of cumulative density function at any point is equal to probability density at that point. The probability density of pixel intensity level is calculated by the following equation:

$p_r r_k = \frac{n_k}{n}$ $0 < p_r(r) r_k < 1$ (6)

$0 < k < 255$ (7)

k is the pixel intensity level,n_k is the number of pixels and k represents the gray level.

Table 8 gives a summary of the layers used.

Figure 10 gives the flow of our proposed framework:

The main merits of this framework are the use of the preprocessing improves the rate of detection of spoofed fingerprints. The CNN architecture deployed has a lower number of model parameters as compared to pre-trained models. Thus it is robust and suitable to be deployed in mobile-based applications involving authentication using fingerprints.

The model has been evaluated on popular fingerprint benchmarks like FVC2006, ATVSFFp, Ghiani et al. 2013, LivDet 2015 and Spoofing-Attack Finger Vein Database.

The results achieved using the proposed framework on the LivDet 2013 dataset have been compared with some of the studies reviewed in Table 7. This has been depicted in Figure 11.

It is observed that our proposed framework achieves a better performance by improving the accuracy of detection. Thus, various factors like preprocessing and hyper-parameter tuning play an important role in enhancing the security of biometric systems.

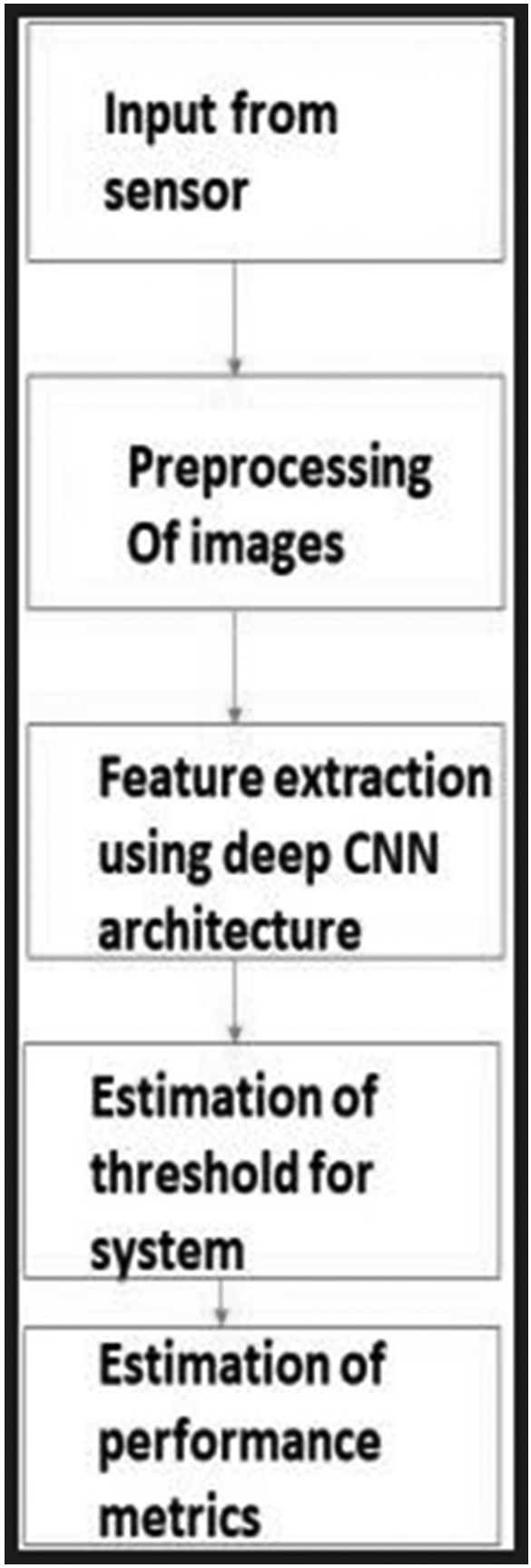

Figure 10. Proposed approach for detection of spoofed fingerprints.

In the next section, we review some popular datasets used in studies conducted in the field of biometric research.

8. Popular datasets used

Some popular datasets which are being used for detection of faces in various research works are as follows:

- **YouTube Faces (YTF)** (Lior et al., 2011): This dataset comprises 3,425 YouTube videos of 1,595 celebrities. These are divided into 5000 pairs of videos.
- **Labeled Faces in the Wild (LFW)** (GB Huang et al., 2007): It comprises 13,323 photos of 5,749 celebrities taken under unconstrained settings. Further, these pictures are divided into 6000 pairs.
- **CASIA Face Image database**: There are images of students, volunteers in this database which has images in BMP format. Also, it has many various intra-class variations like pose, illumination, distance, etc.
- **MORPH** (Ricanek & Tesafaye, 2006): This dataset is mostly used for estimation of soft biometric traits like age, gender, ethnicity etc. The first part pf the database has 1,724 images of 515 people while the second has 55,134 images of 13,000 individuals.
- **IDIAP Replay attack database** (Maio et al., 2002): It comprises 1200 videos of 5 subjects. These videos were captured using a MacBook and have a resolution of 320 × 480.These were captured in a controlled environment with uniform background as well as uncontrolled environment with reflections in the background.

Some popular datasets which are being used for detection of fingerprints in various research works are as follows:

- **Fingerprint Verification Competition (FVC 2002)** (Garris et al.): The FVC 2002 dataset consists of three fingerprint datasets (DB1, DB2, and DB3) collected using different sensors. Each dataset consists of two sets.

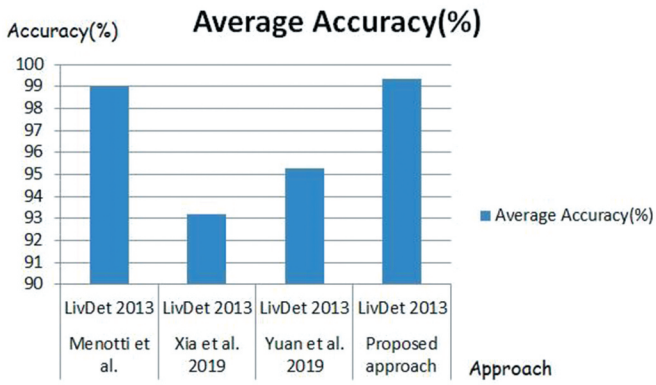

Figure 11. Comparison of studies involving spoofing detection in LivDet 2013 dataset.

- **WVU DB** dataset (Cao & Jain, 2019): This consists of 449 latent fingerprints and corresponding reference fingerprints.
- **ATVS ff-p** (Galbally & Sébastien, 2014) contains real as well as fake fingerprint samples of the index and middle fingers of 17 users. These were captured using Biometrika Fx2000 sensor, thermal sensor and a flat capacitive sensor. Thus there are 816 total samples in the database.
- **VERA fingervein database** (Tome et al., 2014). The VERA Fingervein Database is used for recognition of fingerveins instead of fingerprints. It consists of 440 samples from 110 users. The database also has fake images for detection of spoofing attacks in biometric systems.
- **LivDet** (Ghiani et al., 2013): The LivDet datasets (2011, 2013, 2015 and 2017) consist of live and fake samples of fingerprints. For instance, LivDet 2013 has more than 16000 images acquired from four different sensors, with equal number of real and fake fingerprints. The data is split into training and testing sets. The different sensors are Biometrika, Italdata, Swipe and Crossmatch. However, the Crossmatch and Swipe datasets were not utilized for evaluation due to some anomalies present in the datasets. that are equally split between training and testing sets. However, the CrossMatch and Swipe readers from LivDet 2013 dataset were not utilized for evaluation purposes because the organizers found some anomalies in these datasets. Also, Biometrika and Italdata sensors were used to capture fake fingerprints from users without their cooperation.
- **MSU Fingerprint Presentation Attack Dataset** (Chugh et al., 2018): The MSU dataset has real and spoof images captured using the Crossmatch sensor and Lumidigm Venus sensor. There are 9000 live images and 10,500 forged image sin this database.

Some popular datasets which are being used for detection of iris in various research works are as follows:

- **IITD iris dataset** (Kumar and Passi, 2010): The IIT Delhi Iris Database comprises iris images collected from the college staff and students. The images have been captured using JIRIS, JPC1000 and CMOS camera. The 1120 images have been divided into 224 different classes associated with each subject. The images have a resolution of 320x240, comprising 176 males and 48 females.
- **CASIA v4 iris dataset** (Tan et al., 2010): CASIA-IrisV4 has around 55000 images captured from 1800 live subjects and 1000 virtual users. These are collected under infrared illumination and are stored in 8-bit gray-level JPEG format. The different datasets synthesized were CASIA-Iris-Interval, CASIA-Iris-Lamp, CASIA-Iris- Distance, and CASIA-Iris-Thousand.
- **VSSIRIS** (Raja et al., 2015): This database consists of iris images acquired using iPhone 5S and Lumia 1020 under unconstrained conditions.

- **Q-FIRE** (Johnson et al., 2010): The Q-FIRE dataset consists of 3,123 high-resolution images acquired at 5 ft and 2,902 low-resolution images acquired at 11 ft from 160 subjects each.
- **LG2200 and LG4000** (CVRL,2013):The ND-CrossSensor-Iris-2013 dataset consists of iris images taken with two iris sensors: LG2200 and LG4000. The LG2200 dataset comprises 116,564 iris images, and LG4000 consists of 29,986 iris images of 676 subjects.
- **WVU** dataset (Shah & Ross,): The synthetic iris images are generated using many approaches which were model-based, anatomy-based and making use of many parameters like iris thickness, pupil size, fiber size, eye angle etc. The images are divided into 10000 classes, with each class having 16 images. Out of these, 15 images are of poor quality and 1 is of good quality, with effects of noise, blur, contrast and reflection in combination.

Some popular datasets which are being used for detection of voice in various research works are as follows:

- The NIST SRE series (NIST SRE Series, 2012) is divided into various datasets. For instance, **SRE 2012** consists of nine distinct tests. The benchmark uses 1,918 target speakers from speech corpora used in previous SREs.

9. Conclusion and future work

In this paper, we have described the application of deep learning for authentication of various traits in biometric systems. It is observed that deep learning techniques have outperformed the traditional state-of-the-art methods due to their capability of learning features efficiently. While authentication is the main focus of biometric systems, various vulnerabilities such as attacks on enrolled templates and attacks using forged identities are some of the biggest challenges faced. The paper reviews the studies that employ the use of robust deep learning frameworks to deal with these challenges. We summarize the strengths and drawbacks of various frameworks which explore the role of deep learning. We also highlight future directions such as the role of information fusion in enhancing the security of biometric systems. We list the various datasets available in this domain and highlight our contribution in this domain with the help of a case study.

In the future, we would focus on the various aspects of research which are in a nascent stage. One of them is large scale identification using deep learning, where millions of identities need to be authenticated. This has received little attention so far as it requires complex models and faster resources. Deep learning in biometrics has been explored very little beyond common traits like face, fingerprints,iris and voice. We would explore its use by gathering data for less common traits.

Behavioral biometrics would be useful in scenarios where sequential data needs to be analyzed. However, very few behavioral biometric traits have been explored using deep learning approaches. We would explore more such applications of deep learning, which hold a lot of potential in the field of biometrics to secure real-world applications.

ORCID

Shefali Arora http://orcid.org/0000-0002-8839-749X

References

Adik, C., Waze, A., & Tendulkar, S. (2019). Fingerprint and face spoof detection using deep learning. *International Journal of Innovative Research in Technology*, *5*(6), 187–189. http://ijirt.org/Article?manuscript=147256

Al Waisy, A. S., Qahwaji, R., Ipson, S., & Al-Fahdawi, S. A multimodal biometric system for personal identification based on deep learning approaches .*In 2017 seventh international conference on emerging security technologies (EST)*, Canterbury,UK,2017,pp. 163–168.

Amira, M., Eldin, A., & Wahdan, A. (2011). Fingerprint recognition. *Advanced biometric technologies*, 210–224. https://doi.org/10.5772/23476

Arora, S., & Bhatia, M. P. S. (2020). Fingerprint spoofing detection to improve customer security in mobile financial applications using deep learning. *Arabian journal for science and engineering*, *45*(10), 2847–2863. https://doi.org/10.1007/s13369-019-04190-1

Atoum, Y., Liu, Y., Jourabloo, A., & Liu, X. Faceanti-spoofing using patch and depth-based CNNs. *In 2017 IEEE International joint conference on biometrics (IJCB)*, Denver, CO, 2017, pp. 319–328.

Barrett, D. One surveillance camera for every 11 people in Britain, says cctv survey, (The Telegraph),2013. telegraph.co.uk. http://www.telegraph.co.uk/technology/10172298/One- surveillance- camera- for- every- 11- people- in-Britain- says-CCTV-survey.html (accessed 24.03.16).

Bashbaghi, S., Granger, E., Sabourin, R., & Parchami, A. Deep Learning Architectures for Face Recognition in Video Surveillance. *arXiv:1802.09990*,2018

Bowyer, K. W., & Doyle, J. S. (2014). Cosmetic contact lenses and iris recognition spoofing. *Computer*, *47*(5), 96–98.

Cao, K., & Jain, A. K. Automated latent fingerprint recognition. in ieee transactions on pattern analysis and machine intelligence. *IEEE transactions on pattern analysis and machine intelligence*. *41*4:1 April 788–800 2019;https://doi.org/10.1109/TPAMI.2018.2818162.

Chen, D., Cao, X., Wang, L., Wen, F., & Jian, S. (2012). *Bayesian face revisited: A joint formulation*. European Conference on Computer Vision, Springer, 7574, pp 566-579.

Cho, M., & Jeong, Y. (2014). Face recognition performance comparison of fake faces with real faces in relation to lighting. *J. Internet Serv. Inf. Security.*, *4*(4), 82:90. https://doi.org/10.22667/JISIS.2014.11.31.082

Chugh, T., Cao, K., & Jain, A. (2018). Fingerprint spoof buster: Use of minutiae-centered patches. *IEEE, Trans. Inf. Forensics Security*, *13*(9), 2190–2202. https://doi.org/10.1109/TIFS.2018.2812193

CVRL.Cross-Sensor Iris, N. D. Dataset. Computer Vision Research Lab,University of Notre Dame. https://sites.google.com/a/nd.edu/public-cvrl/data-sets. 2013.

De Souza, G. B., Papa, J. P., & Marana, A. N. On the Learning of Deep Local Features for Robust Face Spoofing Detection. *arXiv:1806.07492v2 [cs.CV]*,11 Oct 2018. Proceedings of 31st Conference on Graphics, Patterns and Images (SIBGRAPI) 2018.

Dian, L., & Dongmei, S. Contactless palmprintrecognition based on convolutional neural network. *In Proceedings of the IEEE 13th international conference on signal processing (ICSP'16)*, 2016, pp.1363–1367. Chengdu, China.

Ding, S., Zhu, H., Jia, W., & Su, C. (.2011). A survey on feature extraction for pattern recognition. *Artificial Intelligence Review*, *37*(4), 169–180. https://doi.org/10.1007/s10462-011-9225-y

Galbally, J., Alonso-Fernandez, F., Fierrez, J., & Ortega-Garcia, J. (2012). A high performance fingerprint liveness detection method based on quality related features. *Future Generation Computer Systems.*, *28*(1), 311–321. https://doi.org/10.1016/j.future.2010.11.024

Galbally, J., & Sébastien, M. Face Anti-Spoofing Based on General Image Quality Assessment. In *Proceedings - International Conference on Pattern Recognition*. 2014, pp. 1173–1178. Stockholm, Sweden.

Gangwar, A., & Joshi, A. DeepIrisNet: Deep iris representation with application in iris recognition and cross-sensor iris recognition. *In Proceedings of the IEEE international conference on image processing*, Phoenix, AZ, USA, 25–18 September 2016; pp. 2301–2305.

Garcia-Romero, D., Zhang, X., McCree, A., & Povey, D. Improving speaker recognition performance in the domain adaptation challenge using deep neural networks. *In Proceedings of the IEEE spoken language technology workshop (SLT'14). IEEE*,2014, pp. 378–383

Garris, M. D., & McCabe, R. M. NIST Special Database 27: Fingerprint Minutiae from Latent and Matching Tenprint Images. Technical Report 6534. NIST,2000.

Geoffrey, H. A. (2010). Practical guide to training restricted Boltzmann machines. *Momentum*, *9*(1), 926. https://doi.org/10.1007/978-3-642-35289-8_32

Ghiani, L., Yambay, D., Mura, V., Tocco, S., Marcialis,G., Roli, F., Schuckcrs, S. (2013). LivDet 2013 Fingerprint Liveness Detection Competition 2013. In 2013 *International Conference on Biometrics (ICB)*, Madrid: IEEE, pp. 1-6. doi: 10.1109/ICB.2013.6613027.

Gotardo, P., Riviere, J., Bradley, D., Ghosh, A., & Beeler, T. (2018). Practical dynamic facial appearance modeling and acquisition. *ACM, Trans. Graph*, *37*(6), 1–13. https://doi.org/10.1145/3272127.3275073

Gupta, P., Behera, S., Vatsa, M., & Singh, R. On iris spoofing using print attack. *In 2014 22nd international conference on pattern recognition, stockholm*, 2014, pp. 1681–1686. Stockholm, Sweden.

Harjoko, A., Hartati, S., & Dwiyasa, H. (2009). A method for iris recognition based on 1D coiflet wavelet. *World Acad. Sci. Eng. Technol.*, *56*(8), 126–129. https://doi.org/10.5281/zenodo.1079934

Hashim, A. T., & Saleh, Z. A. (2018). Visual Cryptography and CSK for biometric template security. *Journal of Engineering and Applied Sciences*, *13*(18), 7642:7647. https://doi.org/10.36478/jeasci.2018.7642.7647

Hasnat, A., Bohn, J., Milgram, J., Gentric, S., & Chen, L. DeepVisage:Making face recognition simple yet with powerful generalization skills. *arXiv:1703.08388v2*,2017.

Hassaballah, M., & Aly, S. (2015). Face recognition: Challenges, achievements and future directions. *IET Computer Vision*, *9*(4), 614–626. https://doi.org/10.1049/iet-cvi.2014.0084

Hoffman, S., Sharma, R., & Ross, A. Convolutional neural networks for iris presentation attack detection: Toward cross-dataset and cross-sensor generalization. *In The IEEE conference on computer vision and pattern recognition (CVPR) workshops*, 2018. Salt Lake City, UT, USA.

Huang, G. B., Ramesh, M., Berg, T., & Learned-Miller, E. Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments. Technical Report 07–49, University of Massachusetts 2007.

Huang, H., Liu, S., Zheng, H., Ni, L., Zhang, Y., & Li, W. Deepvein: Novel finger vein verification methods based on deep convolutional neural networks. In *IEEE international conference on identity, security and behavior analysis*, 2017. New Delhi, India.

Ilya, S. Training Recurrent Neural Networks. Ph.D. Dissertation.University of Toronto, 2013. University of Toronto Computer Center Toronto, Canada.

Jain, A., Hong, L., & Pankanti, S. (2001). Biometric Identification. *Information Systems Security*, *43*(2), 90–98. https://doi.org/10.1145/328236.328110

Jain, A., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, *79*, 80–105. https://doi.org/10.1016/j.patrec.2015.12.013

Jalali, A., Mallipeddi, R., & Lee, M. Deformation invariant and contactless palmprint recognition using convolutional neural network. *In proceedings of the 3rd international conference on human-agent interaction*. Korea: ACM, 2015, pp. 209–212.

Johnson, P. A., Lopez-Meyer, P., Sazonova, N., & Hua, F., Schuckers Quality in face and iris research ensemble (Q-FIRE). In *Proceedings of the IEEE 4th International Conference on Biometrics: Theory Applications and Systems* (BTAS'10). Washington, DC, USA: IEEE,2010,pp. 1–6.

Kenny, P., Gupta, V., Stafylakis, T., Ouellet, P., & Alam, J. Deep neural networks for extracting Baum-Welch statistics for speaker recognition. In *Proceedings of the Odyssey Conference*, 2014, pp 293–298. Finland.

Kim, R. A., Nguyen, D. S., Owais, P. H., Park, M., & Iris, K. R. (2018). DenseNet: Robust iris segmentation using densely connected fully convolutional networks in the images by visible light and near-infrared light camera sensors. *Sensors Basel*, *18*(5), 1501. https://doi.org/10.3390/s18051501

Klontz, J. C., & Jain, A. K., A Case Study on Unconstrained Facial Recognition Using the Boston Marathon Bombings Suspects, Technical Report MSU-CSE-13-4, Michigan State University, 2013.

Kollreider, K., Fronthaler, H., & Bigun, J. (2009). Non-intrusive liveness detection by face images. *Image and Vision Computing*, *27*(3), 233–244. https://doi.org/10.1016/j.imavis.2007.05.004

Krizhevsky, A., Sutskever, I., & Hinton, G. (2017). ImageNet classification with deep convolutional neural networks. *Communications of the ACM*, *60*(6), 84–90. https://doi.org/10.1145/3065386

Kulkarni, H. (2018). *Deep Learning for Facial*. Recognition, Ryerson University.

Kumar, A. and Passi, A. (2010). Comparison and combination of iris matchers for reliable personal authentication. *Pattern Recognition,*43(3),1016–1026.

Kumar, J., Arun,Chalamala, S., & Jami, S. Securing face templates using deep convolutional neural network and random projection. In *2019 IEEE international conference on consumer electronics (ICCE)*,2019, pp. 1–6. Las Vegas, NV, USA, USA.

Kuo, C. (2016). Understanding convolutional neural networks with a mathematical model. *J. Vis. Commun. Image, 41,*1–21 . https://doi.org/10.1016/j.jvcir.2016.11.003

Lakshminarayana, N. N., Narayan, N., Napp, N., Setlur, S., & Govindaraju, V. A discriminative spatio-temporal mapping of face for liveness detection. In *Proceedings of the 2017 IEEE international conference on identity, security and behavior analysis, ISBA* 2017, New Delhi, India, 22–24 February 2017.

Lefohn, A., Budge, B., Shirley, P., Caruso, R., & Reinhard, E. (2013). An Ocularist's Approach to Human Iris Synthesis. *Computer Graphics, 23*(6). https://doi.org/10.1109/MCG.2003.1242384

Lei, L., Zia, Z., Jiang, X., Roli, F., & Feng, X. Face Presentation Attack Detection in Learned Color-liked Space. *arXiv:1810.13170v2 [cs.CV]*,2018.

Lior, W., Hassner, T., & Itay, M. Face recognition in unconstrained videos with matched background similarity. *In proceedings of the IEEE conference on computer vision and pattern recognition (CVPR'11)*,2011, pp. 529–534. Providence, RI, USA.

Liu, J., Deng, Y., & Huang, C. (2015). *Targeting ultimate accuracy: Face recognition via deep embedding. arXiv:1506.07310.*

Liu, L., Xie, T., Yan, J. B., Li, W., & Lu, P. Q. (2013). HZ. An Algorithm for finger-vein segmentation based on modified repeated line tracking. *Imaging Sci. J*, *61*(6), 491–502. https://doi.org/10.1179/1743131X12Y.0000000013

Liu, Y., Ling, J., Liu, Z., Shen, J., & Gao, C. (2017). Finger vein secure biometric template generation based on deep learning. *Soft Computing*, *22,*2257–2265. https://doi.org/10.1007/s00500-017-2983-y

Maio, D., Maltoni, D., Cappelli, R., Wayman, J., & Jain, A. K. FVC2002: Second fingerprint verification competition. In *Proceedings of the 16th International Conference on Pattern Recognition*. 2002, pp. 811–814. Quebec City, Quebec, Canada.

Maram, A., & Lamiaa, E. (2018). Convolutional neural network based feature extraction for IRIS recognition. *International Journal of Computer Science and Information Technology*, *10*(2), 65–78. https://doi.org/10.5121/ijcsit.2018.10206

Marasco, E., & Ross, A. (2014). A survey on antispoofing schemes for fingerprint recognition systems. *ACM Computing Surveys*, *47*(2), 1–36. https://doi.org/10.1145/2617756

Masi, I., Rawls, S., Medioni, G., & Natarajan, P. Pose-aware face recognition in the wild. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp.4838–4846. Las Vegas, NV, USA.

Matthias, V., Pedro, T. E. L., & Marcel, S. Cross-Database evaluation with an open finger vein sensor. *In IEEE workshop on biometric measurements and systems for security and medical applications (BioMS)*,2014. Rome, Italy.

Menotti, D. (2015). DeepRepresentations for iris,face and fingerprint spoofing detection. *IEEE Transactions on Information Forensics and Security*, *10*(4), 864–879. https://doi.org/10.1109/TIFS.2015.2398817

Nanni, L. A. (2017). Overview of the combination of biometric matchers. *Inf. Fusion*, *33*, 71–85. https://doi.org/10.1016/j.inffus.2016.05.003

Nguyen, D. T., Pham, T. D., Lee, Y. W., & Park, K. R. (2018). Deep learning-based enhanced presentation attack

detection for iris recognition by combining features from local and global regions based on NIR camera sensor. *Sensors (Basel)*, *18*(8), 2601. https://doi.org/10.3390/s18082601

NIST SRE Series. Multimodal Information Group. http://www.nist.gov/itl/iad/mig/sre.cfm. 2012.

Pagnin, E., & Mitrokotsa, A. (2017). Privacy-Preserving biometric authentication: challenges and directions. *Security and Communication Networks*, 1–9. https://doi.org/10.1155/2017/7129505

Pandey, R. K., Zhou, Y., Kota, B. U., & Govindaraju, V. Deep secure encoding for face template protection. In *2016 IEEE conference on computer vision and pattern recognition workshops (CVPRW)*, Las Vegas, NV, 2016, pp. 77–83.

Parkhi, O. M., Vedaldi, A., & Zisserman, A. Deep face recognition. In *Proceedings of the british machine vision conference(BMVC)*,2015,pp. 41.1–41.12. Swansea ,UK.

Peng, X., Ratha, N., & Pankanti, S. Learning face recognition from limited training data using deep neural networks. In *Proceedings of the 23rd international conference on pattern recognition*,2016, pp. 1442–1447. Cancun, Mexico.

Prabhakar, S., Pankanti, S., & Jain, A. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, *1*(2), 33–42. https://doi.org/10.1109/MSECP.2003.1193209

Radzi, R. (2016). F. User identification system based on finger-vein pattern using convolutional neural network. *ARPN Journal of Engineering and Applied Sciences*, *11*(5). http://www.arpnjournals.org/jeas/research_papers/rp_2016/jeas_0316_3805.pdf

Raja, K. B., Raghavendra, R., Vemuri, V. K., & Busch, C. (2015). Smartphone based visible iris recognition using deep sparse filtering. *Pattern Recognition Letters*, *57*(C), 33–42. https://doi.org/10.1016/j.patrec.2014.09.007

Ramaiah, N. P., Ijjina, E. P., & Mohan, C. K. Illumination invariant face recognition using convolutional neural networks. In *IEEE international conference on signal processing, informatics, communication and energy systems (SPICES)*, Kozhikode, 2015, pp. 1–4.

Ranjan, R., Sankaranarayanan, S., Castillo, C. D., & Chellppa, R. An all-in-one convolutional neural network for face analysis. In *Proceedings of the IEEE 12th international conference on automatic face and gesture recognition (FG'17)*. 2017, pp. 17–24. Washington, DC, USA.

Ratha, N. K., Connell, J. H., & Bolle, R. M. An analysis of minutiae matching strength. In *Proceedings of the 3rd international conference on audio-and video-based biometric person authentication*, Sweden, 6–8 June 2001, pp. 223–228.

Rathgeb, C., & Busch, C. Improvement of iris recognition based on iris-code bit-error pattern analysis. In *2017 international conference of the biometrics special interest group (BIOSIG)*, Darmstadt, 2017, pp. 1–6.

Rathgeb, C., Uhl, A., & Peter, W. (2013). *Iris biometrics*. Springer, .

Ricanek, K., & Tesafaye, T. Morph: A longitudinal image database of normal adult age-progression. In *Proceedings of the international conference on automatic face and gesture recognition (FGR'06). Southampton, UK: IEEE*, 2006, pp. 341–345.

Roomi, M., Beham, M. P., & Dharmalakshmi, D. (2015). Face spoofing detection based on depthmap and gradient binary pattern. *International Journal of Applied Engineering Research*, *9*(21), 4990–4996. https://www.researchgate.net/publication/274530129_Face_Spoofing_Detection_Based_on_Depthmap_and_Gradient_Binary_Pattern

Ross, A., Nandakumar, K., & Jain, A. K. (2006). Handbook of multibiometrics. *J. Chem. Inf. Model*, *53*(9), 1689–1699. https://doi.org/10.1007/0-387-33123-9

Sadhya, D., & Singh, S. (2018). Design of a cancelable biometric template protection scheme for fingerprints based on cryptographic hash functions. *Multimedia Tools and Applications*, *77*(12), 15113–15137. https://doi.org/10.1007/s11042-017-5095-x

Sahasrabudhe, S., & Namboodiri, A. M. Fingerprint enhancement using unsupervised hierarchical feature learning. In *Proceedings of the 2014 indian conference on computer vision graphics and image processing*. ACM, 2013.

Salakhutdinov, R., & Larochelle, H. *Efficient learning of deep boltzmann machines*. AISTATS,2010. Proceedings of Machine Learning Research, JMLR.

Saleem, M. M., & Hansen, J. H. L. A discriminative unsupervised method for speaker recognition using deep learning. In *Proceedings of the IEEE 26th international workshop on machine learning for signal processing (MLSP'16). Vietri sul Mare, Italy: IEEE*, 2016, pp.1–5.

Schroff, F., Kalenichenko, D., & Phibin:, J. FacenetA unified embedding for face recognition and clustering. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2015, pp. 815–823. Boston, MA, USA.

Sequeira, A., Juliano, M., & Jaime, C. Iris liveness detection methods in mobile applications. In *VISAPP 2014 - proceedings of the 9th international conference on computer vision theory and applications*, 2014. Lisbon, Portugal.

Shah, S., & Ross, A. Generating synthetic irises by feature agglomeration. In *Proc. of IEEE international conference on image processing (ICIP)*, Atlanta, USA, October 2006.

Shiranthika,, C. Face spoof detection. Data driven investor, Medium. https://medium.com/datadriveninvestor/face-spoof-detection-e0d08fb246ea,2019.

Silva, P., Luz, E., Baeta, R., Pedrini, H., Falcao, A. X., & Menotti, D. An approach to iris contact lens detection based on deep image representation. In *Proceedings of the IEEE conference on graphics, patterns and images, salvador*, Brazil, 26–29 August 2015, pp. 157–164.

Sun, Y., Chen, Y., Wang, X., & Tang, X. (2014). Deep learning face representation by joint identification verification. *Advances in Neural Information Processing Systems*, *2*, 1988–1996. https://doi.org/10.5555/2969033.2969049

Sun, Y., Wang, X., & Tang, X. Sparsifying neural network connections for face recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*,2016, pp.4856–4864. Las Vegas, Nevada, United States.

Sundararajan, K., & Woodard, D. (2018). Deep learning for biometrics. *ACM Computing Surveys*, *51*(3), 1–34. https://doi.org/10.1145/3190618

Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. Deepface: Closing the gap to human-level performance in face verification. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2014, pp. 1701–1708. Columbus, OH, USA.

Tan, B., & Schuckers, S. Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing. In *2006 conference on computer vision and pattern recognition workshop (CVPRW'06)*, New York, NY, USA, 2006, pp. 26–27.

Tan, T., He, Z., & Sun, Z. (2010). Efficient and robustsegmentation of noisy iris images for non-cooperative iris recognition. *Image and Vision Computing*, *28*(2), 223–230. https://doi.org/10.1016/j.imavis.2009.05.008

Tome, P., Vanoni, M., & Marcel, S. On the vulnerability of finger vein recognition to spoofing. In *IEEE international conference of the biometrics special interest group (BIOSIG), Darmstadt*, Germay,2014:1–10

Vasilakakis, V., Cumani, S., & Laface, P. SpeakerRecognition by means of deep belief networks. https://cls.ru.nl/staff/dvleeuwen/btfs-2013/vasilakakis-btfs2013.pdf

Wang, C., Zhang, X., & Lan, X. How to Train Triplet Networks with 100K Identities? *arXiv:1709.02940v1 [cs.CV]*,2017.

Wang, Y., Wang, L., Cheung, Y., & Yuen, P. C. Fingerprint geometric hashing based on binary minutiae cylinder codes. In *Proceedings of the 2014 22nd international conference on pattern recognition,2014*, pp.690–695. Stockholm, Sweden.

Wang-Su, J., & Sang-Yong, R. (2017). Fingerprint pattern classification using convolution neural network. *International Journal of Fuzzy Logic andIntelligent Systems*, *17(1)*, 170–176. https://doi.org/10.5391/IJFIS.2017.17.3.170

Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 746–761. https://doi.org/10.1109/TIFS.2015.2400395

Wen, Y., Zhang, K., Li, Z., & Qiao, Y. A discriminative feature learning approach for deep face recognition. *ECCV*. 2016, Springer.

Xia, Z., Yuan, C., Sun, X., Sun, D., & Lv, R. (2019). Combining wavelet transform and LBP related features for fingerprint liveness detection. *IAENG International Journal of Computer Science*, *43*(3), 290–298. http://www.iaeng.org/IJCS/issues_v43/issue_3/IJCS_43_3_04.pdf

Yang, W., Hu, J., Wang, S., & Wu, Q. (2018). Biometrics based privacy-preserving authentication and mobile template protection. *Wireless Communications and Mobile Computing*, 1–17. https://doi.org/10.1155/2018/7107295

Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. *Symmetry*, *11*(2), 141. https://doi.org/10.3390/sym11020141

Yin, X., & Liu, X. (2018). Multi-task convolutional neural network for pose-invariant face recognition. *IEEETransactions on Image Processing*, *27*(2), 964–975. https://doi.org/10.1109/TIP.2017.2765830

Yuan, C., Xia, Z., & Jiang, L. (2019). Fingerprint liveness detection using an improved CNN with image scale equalization. *IEEE Access*, *7*, 26953–26966. https://doi.org/10.1109/ACCESS.2019.2901235

Zahid, A., & Foresti, G. L. (2016). Face spoof attack recognition using discriminative image patches. *Journal of Electrical and Computer Engineering*, *1*, 14. https://doi.org/10.1155/2016/4721849

Zeng, M., Nguyen, L., Yu, B., Mengshoel, O., Zhu, J., Wu, P., & Zhang, J. Convolutional neural networks for human activity recognition using mobile sensors. In *6th international conference mobile computing, applications and services*, 2014, pp. 197–205. Austin, TX, USA.

Zhao, Z., & Kumar, A. (2017). *Towards more accurate iris recognition using deeply learned spatially corresponding features.in ICCV*

Zhou, K., Chellappa, R., Zhao, W (2006). Unconstrained Face recognition. *International Series on Biometrics, Springer,5* (1), 1–244.. 10.1007/978-0-387-29486-5