A SURVEY ON MACHINE AND DEEP LEARNING FOR FINGER KNUCKLE PRINT AUTHENTICATION

Abstract

Beneficially, biometric personal authentication is very important for the research community due to its broad applicability to several security applications. In terms of precision and computational complexity, manual biometric frameworks are considered to be more fruitful. In hand-based biometrics, finger knuckle prints are one of the biometric surface features that can be used to ensure personal authentication. The result is the fact that the external surface of the finger back knuckle region shows fluctuating and exclusive patterns. The existing analysis of FKP authentication system such as Geometrical, statistical, transform and texture-based methods are usually a time-consuming and difficult task. With advanced machine learning techniques and profound learning concepts, it can be made easy and fast and can be very useful for society. So, the essential place of this paper is to consider a survey of the different machine learning and deep learning-based Finger Knuckle Print verification system. This survey will assist aspiring researchers in the area of finger knuckle print authentication systems.

Keywords: Finger Knuckle Print; Deep Learning; Machine Learning; Performance Measures.

Authors

Sathiya Lakshmanan
Department of Computer Applications
Alagappa University
Karaikudi, India

Palanisamy Velliyan
Department of Computer Applications
Alagappa University
Karaikudi, India

Abdelouahab Attia
Computer Science Department
Mohamed El Bachir El Ibrahimi University of Bordj Bou
Arreridj, 34000, Algeria

LMSE Laboratory
Mohamed El Bachir El Ibrahimi University of Bordj Bou
Arreridj, 34000, Algeria

I. INTRODUCTION

In pattern recognition framework that coverts the collected biometric information from the people into pattern these system called biometric framework. Furthermore, the extracted pattern data must be quantified to authenticate an individual in a simple and automated manner. Biometric characteristics are well suited for use in human identification because they are invariant, observable, appropriate, and permanent. When a biometric trait is easily scanned or read by the machine, it is said to be highly accepted by the consumer [1]. Physical traits are determined by human morphological features, while behavioral traits are based on the subject's unique actions. Biometric checks are a method of determining an individual's personality based on physiological or behavioral characteristics. Ears, hand geometry, iris, retina fingerprints, palms, and other features are often seen as the characteristics of the physiological system. In addition, biometric behavioral attributes are often perceived [2] as voices, gaits, signatures, and keystroke dynamics. In both the verification and identification mode, a biometric authentication system can work based on the utility context. One person is identified by one matching system between the selected biometric characteristics and a template already stored in check mode. Within the identity mode, a person is authenticated through a single process that matches all the system pattern templates with the extracted pattern information. Biometric systems are divided into two groups in the range used to produce biometric authentication: unimodal biometrics and multimodal biometrics. Single biometric feature for unimodal system recognition. However, the unimodal system has some disadvantages, Like the lack of biometric exclusivity, spoof attacks sometimes influence system precision, errors came in sensor captured data so maybe accuracy will affect. So, these problems are solved easily by the multimodal system. That's why a multimodal-based recognition system is a very trending concept in biometrics. Multimodal system in the sense to use a combination of different traits such as faces, iris, fingerprint, retina, palm print, and hand geometry. The benefit of multimodal biometrics is highly resistant to noise, improves fitting precision, and offers high strength for attacks.[3]. Since hand-based applications are low-cost capture devices, the high potentiality for recognizing individuals, a high acceptance rate of users, and speed efficiency that's why most access control applications are used hand-based biometric authentication systems. Individual recognition is made from fingerprints, palm prints, hand-related features, hand-vein patterns, and fingerprint knuckled patterns. The researchers suggested broad models of personal recognition using well-established methodologies to use the highly specific patterns found on the inner and exterior surfaces of the hands for biometric properties, and the literature also pointed to the performance and usability of these technology booming. Among the different patterns of the hands [4] are fingerprints, Prints of palm and hand shape, structures of the palm of the hand, and surfaces of the finger knuckle. In modern times, fingertip images constitute one of the growing biometric features of hand-based identification. These specific finger knuckle surface designs are more able to identify individuals, thus contributing to a highly precise and computationally economical biometric system. Individuals can be distinguished more easily using these distinct patterns on the finger knuckle surface, resulting in a highly accurate and computationally efficient biometric process [5]. The Following Fig.1. Illustrates the overall architecture of the FKP Authentication framework.

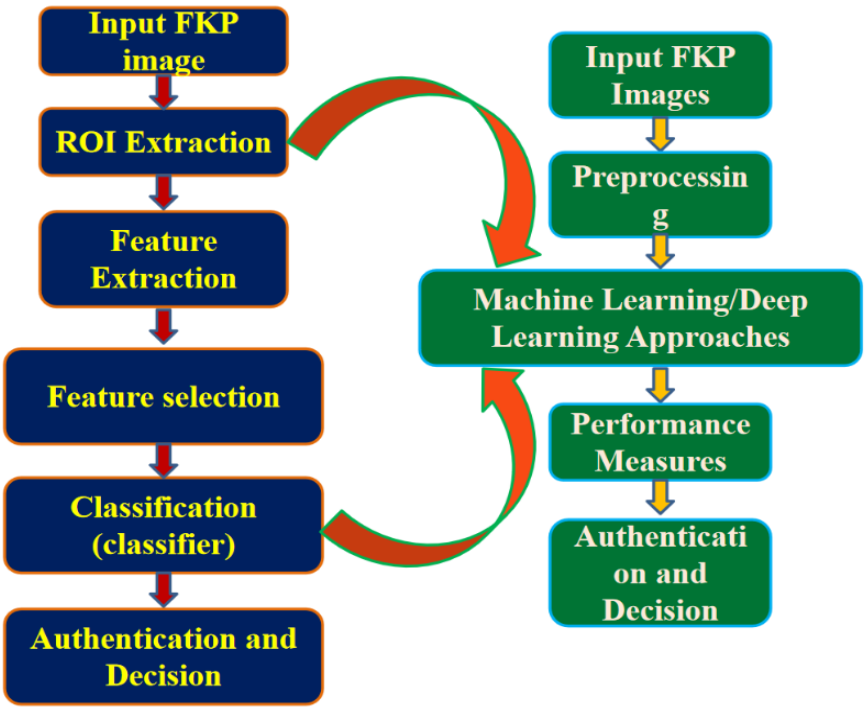

Figure 1: Block diagram of machine or deep learning system for FKP Authentication

This paper focuses mainly on the review of the current situation of machine learning and deep learning-based methodologies for finger knuckle print authentication as well as the accuracy and performance evaluation of the existing machine learning and deep learning method-based information are reported and summarized in the following sections. In general, we focus on recent research based on those two disciplines that give the readers more information and the challenges faced in developing a more effective Finger knuckle print authentication process. We have chosen publications that were written between 2017 and 2020 for this report.

The paper is reminded like this. Section 2 shows the authentication data sets published by finger knuckle. Performance measures are outlined in section 3. Section 4 and section 5 discuss traditional machine learning and deep learning methods for print authentication. Lastly, Section 6 provides for conclusions.

II. PUBLICLY AVAILABLE FKP DATABASES

Finger knuckle prints are portrayed as skin patterns on the backside of the hand. This includes three phalangeal articulations: such as finger connection to the finger's hand surface, finger center articulation is called Inter Phalangeal(PIP), and the fingertip joint connection is called a distal connection. [6] This series of joints within the back of the finger is known in Fig.2 as lines, wrinkles, curves, etc.

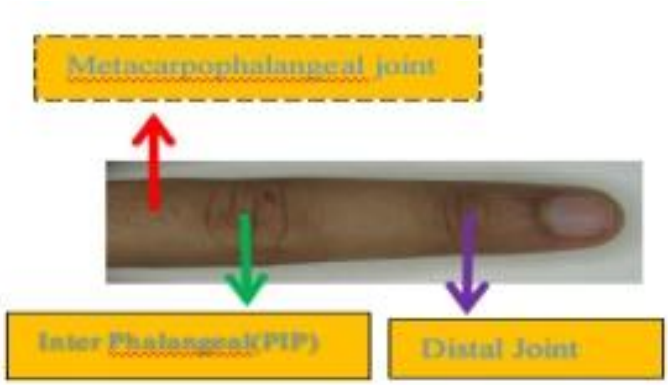

Figure 2: Description of the Finger Knuckle prints Image

The image acquiring device to collect the back of the finger and the captured image is shown in **Figure 2 (a) and (b).**

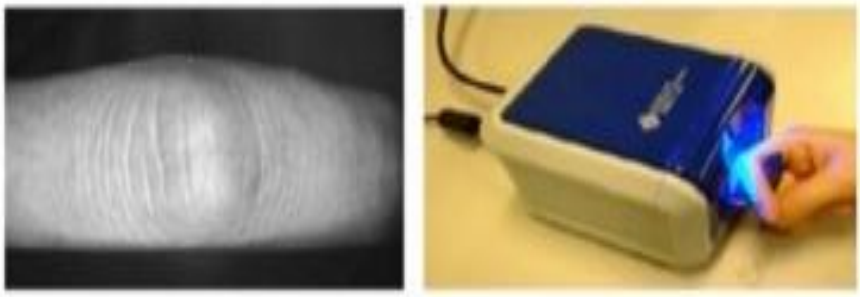

Figure 2(a) and 2(b): Captured ROI image and Input device

In Figure 2: The complete, unique skin patterns on knuckle surfaces provide rich texture information for the reliable identification of a person.

1. **Polyufkp Database:** In this PolyUFKP database, 165 people were acquired using the automatic low-resolution digital cameras in a stuck-free environment, including a hundred and twenty-five men and forty women. This image capture system with finger knuckles collects images of men and women in two different classes. Each session presents 6 pictures of the 4 separate surfaces of the finger knuckle. The four-finger knuckles were taken from the left index knocking finger (LI), the left-center knuckle (LM), the right center finger knuckle(RI), and the right-center finger (RM). Thus, in a single session, 24 images of each person were gathered. In total, 48 images were presented in two periods with the help of all people. In the finger knuckle surface images database, there are 7,900 images. The pictures were taken from 660 knuckle surfaces. For each session, they have taken 25 days time interval for capturing the FKP image as well as these databases also provide the ROI FKP image. The ROI sub figure in the FKP image contains the highlights ideal for personal authentication. Table 1 shows the following contours of finger knuckle printing information [7]. The database related to one of the images shows in the following **Figure 3.**

Figure 3: PolyUFKP Database image

2. **Iit Delhi Finger Knuckle Database:** The complete database and all the images are captured via a contactless low-resolution digital camera. This database consists of images from finger knuckles of 158 users aged sixteen to fifty-five years. In the database, there are completely 790 finger-knuckle photos. For each person in the database for identification purposes, they gave the sequential integer number to all the images. The edge and line detection process of the reason the full finger knuckle print image, as well as ROI images, has been available in the database for the user [8]. In the following Fig.4. Shows IIT Delhi FKP Database image.

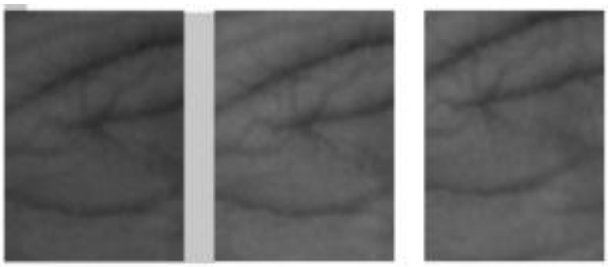

Figure 4: IIT Delhi FKP database image

3. **Polyu Mobile Phone Database:** The images were collected from the PolyU FKP database and also it contains 561 images for further processing [9]. The complete description of all the images is depicted in the following **Table 1**.

Table 1: Various FKP Databases and their Descriptions

Database Name	Image Description	Pixel Resolution	Subjects	Age group	Cropped image	Types of finger
PolyUFKP	7920 images(4 fingers*12 sample* 165 identities)	110*220	(125-Male and 40 - Female)	143 subjects - 20-30 years and others - 30-50	18 subjects - 147 images	Right index, Right Middle, Left index, Left

				years, 2 session		Middle
IIT Delhi	790	100*80	158 subjects with 5 images	16-55 years	790	Middle finger
PolyU Mobile	561 from 187 fingers with 3 images per finger	100*80	109 subjects	-----	18 subjects	Index finger

III. PERFORMANCE MEASURES FOR FINGER KNUCKLE BIOMETRICS

The performance of the authentication system based on the knuckle is carried out in two modes of verification and identification.

The system is assessed by verification mode for the receiver operating properties (ROC), which is a maneuver of false acceptance rate(FAR) against false rejection rate(FRR) for disparate threshold values as well as in another way to expound the equal error rate(EER) that is delineated as where the value of FAR and FRR are indistinguishable.

For identification mode, the system is appraised through the cumulative match curves(CMC) which is a maneuver of a probability of identification against the size of the enrolled users and also appraised by the recognition rate(Rank-1) that is given by,

$$Rank-1=\frac{S}{T}*100\% \quad (1)$$

Where S is the number of images to which the right identity is accredited, T is the total number of identification images used[10].

Moreover, Receiver Operating characteristic (ROC) and Area under the curve (AUC) are used to plot the graphs regarding the above performance measure values. These graphs are very informative and helpful to analyze the performance of our model and proposed algorithm.

I.

IV. FINGER KNUCKLE BIOMETRICS RECOGNITION METHODS BASED ON THE APPROACH OF GEOMETRIC, CODING, SUBSPACE, and TEXTURES

The following Table 2. shows the traditional Approaches for the FKP image Recognition such as Geometric, Coding, Subspace and Texture analysis methods.

Table 2: Description of the Existing Methods for FKP Authentication

Publication Detail	Feature extraction	Classifier	Accuracy
[8]	Canny edge detector	Euclidean distance	EER-1.39%
[11]	Haar wavelet, Randon transform	Parzen window distance	EER-0.3,0.9%
[12]	Ridge feature-based algorithm	SVM	VFR-0.023%
[13]	Fourier transform	BLOPC	EER-0.31%
[14]	Gabor wavelet transform	Matching distance	EER-0.13%
[15]	Randon transform	Correlation	EER-0.53%
[16]	Kekre's wavelet transform	ANN	EER-80%(TAR)
[17]	2D-DFT	BLPOC	EER-6.352%, 0.748%, 0.556%
[18]	2D-BDCT, 2D-DCT mod2	Matching	EER-2.09%
[19]	HAAR	K-means, Bayesian classifier	CRR-100%
[17]	DCT	SVM	CRR-98%
[20]	2D block DCT	GMM, log-likelihood	EER-0.37%
[21]	KWT	Euclidean Distance	TAR-TRR 80%, 89.99% FAR-FRR 20%, 10.01%
[22]	SIFT	Kmeans Clustering	GAR-99.4%
[23]	Contourlet transform	PCA	CRR-98.72%, EER-0.82%
[24]	Probabilistic Hough Transform (PHT).	KNN	EER-1.02%
[25]	Elliptical Hough Transform	Correlation coefficient	EER-0.78%
[26]	Gabour filter	KNN	ACC=99%

The comparison of the existing methods has some limitations such as:

- The texture schemes achieved satisfactory results, albeit at the expense of computational time. The image is converted into a particular domain that reflects the features of the original texture in transformation methods.
- Coding-based methods are commonly used to extract orientation or edge details, but they do not retain all of the orientation features when the image is rotated.
- In the subspace method, the subspace coefficients do not have the equal level of discrimination as knuckle prints and it is used in lower-dimensional subspace coordinates only.
- The Line-based approach takes lines to form the images with less accuracy and more computational time.

V. TRADITIONAL MACHINE LEARNING BASED METHODS

Machine learning (ML) can learn the data and anticipate results. It's a bunch of strategies for the machine to work without the requirement for human association. There have been a variety of fields of AI processes, such as language recognition, computer vision, robot control, experimental science acceleration, bio-monitoring, and product proposals, and computer-assisted design.

In literature, the main focus of this section has been the use of machine learning methods for the authentication of print finger knuckles.

Amraoui et.al [27] identifies an efficient unimodal finger knuckle print recognition system with the help of a compound local binary pattern (CLBP) for extraction of features and classifies the results using Euclidean distance, city-block, and Jeffery divergence. The most important recognition rates for the Left Index finger, Left Middle, Right index, and Right Middle finger, were 98.18 percent, 99.29 percent, 98.48 percent, and 98.89 percent.

Gabour Vector Machine (SVM) based Finger Knuckle Recognition System presented by Muthukumar et. al[28]. The short and long features of gabour are extracted and the distances calculated with the hammer distance (HD). Finally, classification is done by the concept of support vector machine and score level fusion. In this work, a new combination of dual instances has been found, and also better results have been achieved, such as 96,01% for MAX and 92,33% for MIN than 89,11% for a single instance.

Devi et.al [29] introduced a remarkable methodology for finger knuckle print authentication with the utilization of multi-measurement binary patterns (MMBP). This work performed well against the LBP descriptor. This work produces 98.1%, 93%, 98.4%, 98.8% for the left index, the center-left, the right, and the right-center respectively.

The biometric authentication system based on the phase compliance with the Gabor filters was proposed by hammouche et. al[30]. In this paper, the entire FKP image is first extracted with Region of Interest (ROI), then only the Gabor filters and phase conformity are used to extract the feature from the ROI image. Finally, the extracted feature lengths are reduced by the PCA+LDA method and matching distance calculated using cosine Mahalanobis distance. This work produced recognition rate of LIF - 93.64%, EER - 2.83%,

RIF - 97.23% with EER - 3.10%, LMF - 95.66%, 2.12% EER and RMF gave 93.43% with 3.03% EER value.

The concept of Gabor with exception - Maximisation (EM) and SIFT techniques - has been considered by Vidhyapriya, etc. [31] to be a safe biometric finger knuckle authentication system. The acquired features are classified by using the support vector machine (SVM) algorithm. In these works, they focus mainly on reducing the rate of false refusal without increasing the rate of false acceptance. This work tests the results using PolyUFKP and Real-time database. The GAR value of the PolyUFKP database is 98% and FRR value is 0.20 and the GAR value of the Real-time database is 99% with a 0.001 EER value.

Altair et.al [32] developed a personal authentication system for finger knuckle print. In this work preprocessing, feature extraction, and classification were done. Mainly the classification was prepared by using an improved version of neural networks such as quantum neural network (QNN), wavelet neural network (WNN), and quantum wavelet neural network (QWNN). In this work, LI gave 0.0198 MSE value, 98.84% ACC and time is 0.0292, RI is 0.0430 MSE value, 96.5203 ACC and time is 0.0290, LM is 0.1027 MSE value, 90.5461 ACC and time is 0.0297 and RM value is 0.0584 MSE, 94.983 ACC and 0.0290 times. The quantum computing-based FKP authentication system produced low inexactness with high speed.

Heidari et. al[33] have developed a new method of classifying and authenticating texture for FKP images using a weighted mean-based pattern (WEM). The proposed work used a weighted mean measure for feature selection and an SVM classifier used to classify the results. This work was evaluated with various databases such as brodatz, vistex, and stex, and the accuracy of this work 97.14%.

Hana. F.M et.al [34] developed a strong and new reliable system for FKP authentication. In this work, to enhance the image with the help of limited contrast adaptive histogram equalization (CLAHE). In this work accuracy of the authentication system is dynamic by changing the region size and clip limit. The features are extracted by using speeded-up robust features (SURF) and principal component analysis (PCA). The greatest precision of this work is 97% using the SURF method.

Jaswal gaurav et.al [35] have proposed an efficient FKP authentication system using a novel ROI segmentation algorithm and classifier. Novel ROI images are created using a watershed transformation algorithm (WTA) and random forest classifier used for classifying the extracted features. This work tested using the PolyUFKP database with 99.68% CRR and 0.78% EER value.

Muthukumar et.al [36] introduced a novel personal identification system with efficient data storage. This authentication process includes a 2D log Gabor filter, multi-manifold discriminant analysis (MMDA) with K-Means clustering. Fuzzy vault-based chaff pointers are used for storing the FKP template. The overall accuracy of the LI is 97.11% with a 0.23 EER value, RI is 96.14% with 0.2 EER value, LM is 98.01% and 0.16 EER and RM is 94% with a 0.28 EER value.

Jaswal et.al [37] presented a non-decimated quaternion wavelet and 2D2 LDA-based FKP authentication. The architecture is carried out using the uncontrolled fusion rank level by the borda counting method. The presented method accomplished LI is 98.38% accuracy and 2.96% EER, LM is 98.78% accuracy and 3.11% EER, RI is 99.31% accuracy and 2.36% EER and RM is 99.33% accuracy and 2.56% EER value.

Haouam et.al [38] developed an LBP and codebook-based FKP recognition system. However, local binary pattern and codebook used for feature extraction from FKP image and calculated the histograms regarding that features. Finally, the SVM classification is used for the identification of the person. The scheme was evaluated on the PolyUFKP database that achieved the results of LI-0.8960%, LM-0.8770%, RI- 0.6629%, and RM - 0.9725% accuracy.

Attia et.al [39] introduced binarized statistical image features and Gabor filter with DRB classifier-based FKP authentication system. The features based on the BSIF and Gabor filters are directly fed into the DRB classification to determine if the user is genuine or impressive. The proposed work has been evaluated on the PolyUFKP database. The reported results of all FKP modalities with BSIF and DRB classifier yields 0.19% EER value and 99.65% accuracy.

Attia et.al [40] designed an approach to classifying FKP based authentication systems for both verification and identification using Log Gabor, TPLBP with cosine Mahalanobis distance. Both methods are extracted the real and imaginary based features from the ROI images and both features are combined to calculate the matching distance using the cosine Mahalanobis method. Here LDA method used for feature reduction and the framework was tested on the PolyUFKP database and achieved 96.16%, 94.65%, 95.05%, and 94.34% of accuracy for all LMF, RMF, LIF, and RIF respectively.

LR, karlmarx [41] et.al have proposed fractional cuckoo search algorithm (FCS) and HOG method based FKP identification with SVM classifier. In this work, the FKP features are extracted using the HOG method, and the weights are calculated to the corresponding features using a fractional cuckoo search algorithm. The algorithm has been extensively evaluated using the PolyUFKP database. The achieved result of the work is 98.97% accuracy respectively.

Anbari et.al [42] designed an effective FKP authentication system using a relaxed local ternary pattern (RLTP). For experimental analysis, the PolyUFKP database has been used. The reported accuracy and EER values were 96.43% and 0.91%.

Fei et.al [43] suggested FKP recognition with the help of discriminative direction binary feature learning (DDBFL). In this work, DDBFL and K hash function is used to extract the feature vector. The cascaded framework yields an accuracy of 92.2%. A brief description of representative traditional machine learning based methods is presented in Table.3.

A concise description of typical traditional machine learning-based methods is presented in Table.3.

Table 3: Description of the Machine Learning Methods

Ref	Database	Methods/Approach	Performance
[27]	PolyUFKP	Compound local binary pattern, Euclidean distance	Accuracy LI-98.18%, LM-99.29%, RI-98.48%, RM-98.89%
[28]	PolyUFKP	Gabor filter, Hamming distance, Support vector machine	Accuracy Double instance for MAX rule-96.01% , MIN rule-92.33% and single instance-89.11%
[29]	PolyUFKP	Multi Measurement Binary Pattern(MMBP)	Accuracy LI-98.1%, LM-93%, RI-98.4%, RM-98.8%
[30]	PolyUFKP	Phase Concurengy and Gabour filter, PCA+LDA	Accuracy LIF-93.64%, RIF-97.23%, LMF-95.66%, RMF-93.43% EER LIF-2.83%, RIF-3.10%, LMF-2.12% and RMF-3.03
[31]	PolyUFKP, Real time Database	Gabor filter, Exception-Maximization algorithm, SIFT	PolyUFKP database GAR value is-98%, FRR-0.20%, and Real-time database is -99% GAR value and EER-0.001.
[32]	PolyUFKP	Quantum neural network(QNN), wavelet neural network(WNN), quantum wavelet neural network(QWNN)	LI- ACC-98.8400, MSE-0.0198% and time-0.0292 RI- ACC-96.5203%, MSE-0.0430, time-0.0290 LM- ACC-90.5461, MSE-0.1027, time-0.0297 RM- ACC-90.5461, MSE- 0.0584 and time is - 0.0290

[33]	PolyUFKP, brodatz, vistex and stex	Weighted mean based pattern and SVM	Accuracy-97.14%
[34]	PolyUFKP	CLAHE, SURF and PCA	Accuracy-97%
[35]	PolyUFKP	Watershed transformation and Random forest classifier	CRR-99.68% and EER-0.78%
[36]	PolyUFKP	Gabor filter, MMDA and K-Means clustering	Accuracy LI-97.11%, RI-96.14%, LM-98.01%, RM-94%. EER value LI-0.23%, RI-0.2%, LM-0.16% and RM-0.28%
[37]	PolyUFKP	Non decimated quaternion wavelet, backtracking search algorithm, 2D2 LDA	Accuracy LI-98.38%, LM-98.78%, RI-99.31%, RM-99.33% EER value LI-2.96%, LM- 3.11%, RI- 2.36% and RM-2.56%
[38]	PolyUFKP	Local binary pattern, Codebook, and SVM	Accuracy LI-0.8960, LM-0.8770, RI-0.6620, and RM-0.9765.
[39]	PolyUFKP	BSIF+DRB classifier	Accuracy - 99.65% and EER - 0.19%.
[40]	PolyUFKP	Log Gabor filter, TPLBP, LDA, and Cosine Mahalanobis distance	Accuracy LMF-96.16%, RMF-94.65%, LIF-95.05% and RIF-94.34%.
[41]	PolyUFKP	Fractional cuckoo search algorithm, HOG method and SVM	Accuracy -98.97%
[42]	PolyUFKP	Relaxed local ternary pattern	Accuracy - 96.43% and EER - 0.91%
[43]	PolyUFKP	Discriminative direction binary feature learning(DDBFL) and K hash function	Accuracy-92.21%
[51]	PolyUFKP	Monogenic with LPQ descriptor + PCA and LDA	LMF-96.26%, LIF-94.55% RIF-92.73% RMF-96.46%

VI. DEEP LEARNING BASED METHODS

Li, shuyi et.al [44] introduced the multi-modal finger-recognition discriminant local coding-based neural convolution network (LC-CNN). The modality of the LC-CNN for deeper trimodal fingers and their modalities are given to the input of the SVM classifier to classifying a person. The scheme has been evaluated using the various database with 99.98% of accuracy.

Trabelsi et.al [45] proposed architecture with its convolution neural network CNN capable of structured prediction of unimodal and multimodal based FKP recognition. The architecture reached an accuracy of 96.88%, 98.44%, 97.77%, 97.72 for LIF, LMF, RIF, and RMF respectively.

Daas et.al [46] designed a convolution neural network for multimodal traits such as FKP and Finger vein with fusion level feature and fusion level score. In this work, features are extracted for both traits with the help of transfer learning CNN architectures which are Alexnet, VGG16, and ResNet50. finally, the combined extracted features are given as input to the SVM or Softmax classifier. A publicly available database was utilized for evaluation. The achieved result was 99.89% accuracy and 0.05% EER for multimodal.

Zhaiy et.al [47] have developed batch normalized FKP recognition CNNs. The experiment was conducted on the PolyUFKP database, which exhibited the accuracy of 99.1%, 98.9%, 99.4%, 98.3% for LI, LM, RI, and RM correspondingly.

The neural siamese convolution network for FKP recognition was presented by Joshi et. al[48]. Network training is also carried out based on the concept of the euclidean distance and various convolution layers used for personal authentication which are RELU activation function, batch normalization, and dropout. The reported accuracy is 99.24% using the siamese convolution neural network.

Daksh thapar et.al [49] have considered Major finger, Minor finger, and nail-based FKP recognition using CNN with 128-D Siamese network for feature extraction techniques. The method was evaluated on publicly available datasets PolyUFKP, PolyU contactless FKI which attained an accuracy of 97.01% and an EER value of 0.9%.

Racid chlaoua et.al [50] introduced FKP modalities identification based on PCANet, binary hashing, and Block histogram. The feature vectors are given as input to the linear multiclass support vector machine (SVM) for classifying a person. In this work, to increase the recognition rates by using Matching score level fusion. The reported accuracy and EER value is 100%, 0.0001%. A brief description of representative traditional machine learning based methods is presented in Table.4.

Table 4: Representative Deep Learning-Based Methods

Ref	Database	Method / approach	performance
[44]	PolyUFKP	local coding based convolution neural network(LC-CNN), SVM classifier	Accuracy - 99.98%.
[45]	PolyUFKP	Own convolution neural network CNN	Accuracy 96.88%, 98.44%, 97.77%, 97.72 for LIF, LMF, RIF and RMF
[46]	PolyUFKP	Transfer learning CNN, Alexnet, VGG16 and ResNet50, Softmax , SVM classifier.	Accuracy - 99.89% and EER - 0.05% .
[47]	PolyUFKP	batch-normalized CNN with deep learning	Accuracy LI - 99.1%, LM -98.9%, RI - 99.4%, RM- 98.3%
[48]	PolyUFKP	siamese convolution neural network, euclidean distance,	Accuracy - 99.24%
[49]	PolyUFKP, PolyU contactless FKI	CNN with 128-D Siamese network	Accuracy - 97.01% and EER value - 0.9%.
[50]	PolyUFKP	PCANet, binary hashing, Block histogram, linear multiclass support vector machine(SVM)	Accuracy - 100% EER - 0.0001%.

VII. CONCLUSION

In this article, an overview of recent methods and frameworks based on machine and deep learning methods for finger knuckle print authentication has been presented. Earlier finger knuckle print authentication and recognition by using traditional Geometrical, coding, texture, and line-based approaches are difficult to identifying a person whether he/she is genuine or an impostor at an earlier stage and also that results are shown in table3. It is hoped that this paper will facilitate the task of finger knuckle print authentication and classification research more interesting for budding application developers, researchers, and practitioners. This survey has outlined, in different sections, most publicly available databases, performance measures for Finger knuckle print authentication, finger knuckle print authentication methods used machine and deep learning, which have shown in the above survey contents. For brevity, we have summarized the existing methods, in Table.3, Table.4 and Table.5, to provide a clearer insight on the applied techniques and research progress. According to the findings of this survey, one can see that deep/machine learning is resourceful to finding a person whether he/she is a genuine/imposter with high performance. In Table 1 some of the most publicly known databases have been provided for researchers as they are a very important part of any experiment. All in all, we can say that the future promises to develop machine learning and finger knuckle print authentication schemes that

are profoundly based on learning and use in many security applications, sexual harassment, and civilizational problems. We plan to study a variety of engine and deep learning architectures for a hybrid scheme to authenticate fingerprints.

ACKNOWLEDGEMENTS

This research work has been supported by RUSA PHASE 2.0, Alagappa University, karaikudi. This research was supported by UGC-NFSC fellowship.

REFERENCES

[1] G. Jaswal, A. Kaul, and R. Nath, "Knuckle Print Biometrics and Fusion Schemes--Overview, Challenges, and Solutions," *ACM Comput. Surv.*, vol. 49, no. 2, pp. 1–46, 2016.
[2] L. Zhang, L. Zhang, D. Zhang, and H. Zhu, "Online finger-knuckle-print verification for personal authentication," *Pattern Recognit.*, vol. 43, no. 7, pp. 2560–2571, 2010.
[3] K. Usha and M. Ezhilarasan, "Robust personal authentication using finger knuckle geometric and texture features," *Ain Shams Eng. J.*, vol. 9, no. 4, pp. 549–565, 2018.
[4] K. Usha and M. Ezhilarasan, "Finger knuckle biometrics--A review," *Comput. \& Electr. Eng.*, vol. 45, pp. 249–259, 2015.
[5] A. Kumar, "Importance of being unique from finger dorsal patterns: Exploring minor finger knuckle patterns in verifying human identities," *IEEE Trans. Inf. forensics Secure.*, vol. 9, no. 8, pp. 1288–1298, 2014.
[6] A. Kumar, "Can we use minor finger knuckle images to identify humans?," in *2012 IEEE fifth international conference on biometrics: theory, applications, and systems (BTAS)*, 2012, pp. 55–60.
[7] L. Zhang, L. Zhang, and D. Zhang, "Finger-knuckle-print: a new biometric identifier," in *2009 16th IEEE International Conference on Image Processing (ICIP)*, 2009, pp. 1981–1984.
[8] A. Kumar and C. Ravikanth, "Personal authentication using finger knuckle surface," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 1, pp. 98–110, 2009.
[9] K. Cheng and A. Kumar, "Contactless finger knuckle identification using smartphones," in *2012 BIOSIG-Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG)*, 2012, pp. 1–6.
[10] N. E. Chalabi, A. Attia, and A. Bouziane, "Multimodal finger dorsal knuckle major and minor print recognition system based on PCANET deep learning," *ICTACT J Image Video Process*, vol. 10, no. 3, pp. 2153–2158, 2020.
[11] L. Nanni and A. Lumini, "A multi-matcher system based on knuckle-based features," *Neural Comput. Appl.*, vol. 18, no. 1, pp. 87–91, 2009.
[12] M. A. Ferrer, C. M. Travieso, and J. B. Alonso, "Multimodal biometric system based on hand geometry and palm print texture," in *Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology*, 2006, pp. 92–97.
[13] L. Zhang, L. Zhang, and D. Zhang, "Finger-knuckle-print verification based on band-limited phase-only correlation," in *International Conference on Computer Analysis of Images and Patterns*, 2009, pp. 141–148.
[14] C. Hegde, P. D. Shenoy, K. R. Venugopal, and L. M. Patnaik, "FKP biometrics for human authentication using Gabor wavelets," in *TENCON 2011-2011 IEEE Region 10 Conference*, 2011, pp. 1149–1153.
[15] C. Hegde, P. D. Shenoy, K. R. Venugopal, and L. M. Patnaik, "Authentication using finger knuckle prints," *signal, image video Process.*, vol. 7, no. 4, pp. 633–645, 2013.
[16] H. B. Kekre and V. A. Bharadi, "Finger-Knuckle-Print verification using Kekre's wavelet transform," in *Proceedings of the International Conference \& Workshop on Emerging Trends in Technology*, 2011, pp. 32–37.
[17] S. Aoyama, K. Ito, and T. Aoki, "A finger-knuckle-print recognition algorithm using phase-based local block matching," *Inf. Sci. (Ny).*, vol. 268, pp. 53–64, 2014.
[18] M. Saigaa, A. Meraoumia, S. Chitroub, and A. Bouridane, "Efficient person recognition by finger-knuckle-print based on 2D discrete cosine transform," in *2012 International Conference on Information Technology and e-Services*, 2012, pp. 1–6.
[19] I. A. Gomaa, G. I. Salama, and I. F. Imam, "Biometric OAuth service based on finger-knuckles," in *2012*

Seventh International Conference on Computer Engineering \& Systems (ICCES), 2012, pp. 170–175.
[20] A. Meraoumia, S. Chitroub, and A. Bouridane, "On-line finger-knuckle-print identification using Gaussian mixture models \& discrete cosine transform," 2013.
[21] R. D. Raut, S. Kulkarni, and N. N. Gharat, "Biometric authentication using kekre's wavelet transform," in *2014 International Conference on Electronic Systems, Signal Processing, and Computing Technologies*, 2014, pp. 99–104.
[22] A. Muthukumar and S. Kannan, "Finger knuckle print recognition with sift and k-means algorithm," *ICTACT J. Image Video Process.*, vol. 3, no. 03, p. 583, 2013.
[23] K. Usha and M. Ezhilarasan, "Contourlet transform based feature extraction method for finger knuckle recognition system," in *Computational Intelligence in Data Mining-Volume 3*, Springer, 2015, pp. 407–416.
[24] M. Choras and R. Kozik, "Knuckle biometrics based on texture features," in *2010 International Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics*, 2010, pp. 1–5.
[25] U. Kazhagamani and E. Murugasen, "A Hough transform based feature extraction algorithm for finger knuckle biometric recognition system," in *Advanced Computing, Networking and Informatics-Volume 1*, Springer, 2014, pp. 463–472.
[26] P. Jayapriya and R. Mani[1] P. Jayapriya and R. Manimegalai, "Finger Knuckle Biometric Authentication using Texture-Based Statistical Approach," in 2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW), 2018, pp. 170–174.megalai, "Finger Knuckle Biometric Authentication using Texture-Based Statistical Approach," in *2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW)*, 2018, pp. 170–174.
[27] A. Amraoui, Y. Fakhri, and M. A. Kerroum, "Finger knuckle print recognition system using compound local binary pattern," in *2017 International Conference on Electrical and Information Technologies (ICEIT)*, 2017, pp. 1–5.
[28] A. Muthukumar and A. Kavipriya, "A biometric system based on Gabor feature extraction with SVM classifier for Finger-Knuckle-Print," *Pattern Recognit. Lett.*, vol. 125, pp. 150–156, 2019.
[29] S. S. Devi and A. Suhasini, "FINGER KNUCKLE PRINT RECOGNITION USING MULTI MEASUREMENT BINARY PATTERN."
[30] R. Hammouche, A. Attia, and S. Akrouf, "A novel system based on phase congruency and gabor-filter bank for finger knuckle pattern authentication," *ICTACT J Image Video Process*, vol. 10, no. 3, pp. 2125–2131, 2020.
[31] R. Vidhyapriya and others, "Personal Authentication Mechanism Based on Finger Knuckle Print," *J. Med. Syst.*, vol. 43, no. 8, pp. 1–7, 2019.
[32] A. S. Altaher and S. M. R. Taha, "Personal authentication based on finger knuckle print using quantum computing," *Int. J. Biom.*, vol. 9, no. 2, pp. 129–142, 2017.
[33] H. Heidari and A. Chalechale, "New Weighted Mean-Based Patterns for Texture Analysis and Classification," *Appl. Artif. Intell.*, pp. 1–22, 2021.
[34] F. M. Hana and I. D. Maulida, "Analysis of contrast limited adaptive histogram equalization (CLAHE) parameters on finger knuckle print identification," in *Journal of Physics: Conference Series*, 2021, vol. 1764, no. 1, p. 12049.
[35] G. Jaswal, A. Kaul, R. Nath, and A. Nigam, "Finger knuckle image ROI extraction using watershed transformation for person recognition," in *2017 Fourth International Conference on Image Information Processing (ICIIP)*, 2017, pp. 1–6.
[36] M. Arunachalamand and K. Amuthan, "Finger Knuckle Print Recognition using MMDA with Fuzzy Vault," *Int. Arab J. Inf. Technol.*, vol. 17, no. 4, pp. 554–561, 2020.
[37] G. Jaswal and R. C. Poonia, "Selection of optimized features for fusion of palm print and finger knuckle-based person authentication," *Expert Syst.*, vol. 38, no. 1, p. e12523, 2021.
[38] M. Y. Haouam, A. Meraoumia, I. Bendib, and L. Laimeche, "Does the Learning Principle Help Us Improve Hand-Crafted Finger-Knuckle-Print Features?," in *020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP)*, 2020, pp. 229–234.
[39] A. Attia, Z. Akhtar, N. E. Chalabi, S. Maza, and Y. Chahir, "Deep rule-based classifier for finger knuckle pattern recognition system," *Evol. Syst.*, pp. 1–15, 2020.
[40] A. Attia, A. Moussaoui, M. Chaa, and Y. Chahir, "Finger-Knuckle-Print Recognition System based on Features-Level Fusion of Real and Imaginary Images," *J. Image Video Process.*, 2018.
[41] K. LR and others, "Development of High Recognition Rate FKP System using Fractional Cuckoo Search Optimization Method," 2019.
[42] M. Anbari and A. M. Fotouhi, "Finger knuckle print recognition for personal authentication based on

relaxed local ternary pattern in an effective learning framework," *Mach. Vis. Appl.*, vol. 32, no. 3, pp. 1–11, 2021.

[43] L. Fei, B. Zhang, S. Teng, A. Zeng, C. Tian, and W. Zhang, "Learning discriminative finger-knuckle-print descriptor," in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2019, pp. 2137–2141.

[44] S. Li, B. Zhang, S. Zhao, and J. Yang, "Local discriminant coding based convolutional feature representation for multimodal finger recognition," *Inf. Sci. (Ny).*, vol. 547, pp. 1170–1181, 2021.

[45] S. Trabelsi *et al.*, "Finger-Knuckle-Print Recognition Using Deep Convolutional Neural Network," in *020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP)*, 2020, pp. 163–168.

[46] S. Daas, A. Yahi, T. Bakir, M. Sedhane, M. Boughazi, and E.-B. Bourennane, "Multimodal biometric recognition systems using deep learning based on the finger vein and finger knuckle print fusion," *IET Image Process.*, vol. 14, no. 15, pp. 3859–3868, 2020.

[47] Y. Zhai *et al.*, "A novel finger-knuckle-print recognition based on batch-normalized CNN," in *Chinese conference on biometric recognition*, 2018, pp. 11–21.

[48] J. C. Joshi, S. A. Nangia, K. Tiwari, and K. K. Gupta, "Finger Knuckleprint based personal authentication using siamese network," in *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, 2019, pp. 282–286.

[49] D. Thapar, G. Jaswal, and A. Nigam, "Fkimnet: a finger dorsal image matching network comparing component (major, minor and nail) matching with holistic (finger dorsal) matching," in *2019 International Joint Conference on Neural Networks (IJCNN)*, 2019, pp. 1–8.

[50] R. Chlaoua, A. Meraoumia, K. E. Aiadi, and M. Korichi, "Deep learning for finger-knuckle-print identification system based on PCANet and SVM classifier," *Evol. Syst.*, vol. 10, no. 2, pp. 261–272, 2019.

[51] L.sathiya, V.palanisamy and Abdelouahab Attia, "Finger knuckle pattern person authentication system based on monogenic and LPQ features," Pattern analysis and Applications, vol. 25,issue no. 2, pp. 395–407, 2022.

