International Journal of Scientific Engineering and Science
Volume 4, Issue 5, pp. 22-28, 2020. ISSN (Online): 2456-7361

Biometric Authentication by Using Fingerprint Recognition System

Abdullah Saud[1], Nazar Elfadil[2]
[1]College of Postgraduate Study, Fahad Bin Sultan University, Tabuk, KSA
[2]College of Computing, Fahad Bin Sultan University, Tabuk, KSA

Abstract— *The fingerprints in the human being are unique and do not repeat. It has features that vary from person to person. There are two popular techniques for making matches between the two fingerprints to recognize them: Minute-based and correlating-based techniques. Minute-Based technology is widely used but has some difficulty in extracting features if the fingerprint images are of low quality. The purpose of this project is to examine how features of fingerprint can be derived. In addition, the two main techniques for matching (Minute-based and correlating-based) will be studied.*

Keywords— *Fingerprint, Feature Extraction, Minute based, correlating based, Fingerprint Matching*.

I. INTRODUCTION

Biometrics can be defined as "Use the biological and behavioural characteristics of individuals to automatically identify them" [1]. Fingerprint is considered a biometric identifier that dependent on biometric data for individuals. The discovery of fingerprints can be used in a various application like authentication method, criminal search, and various security issues. Each fingerprint is a unique pattern that distinguishes a specific person, and thus represents a secure means of identifying the allowed and disallowed persons. This uniqueness can be detected from the shape and defining marks as illustrated in figure 1.

Fig. 1: Defining marks in fingerprint.

There are three types of fingerprint pattern, the arches, the loops, and the Whorls as illustrated in figure 2. To a lesser extent, there can be a type that combines previous types (Composite).This categorization is based on the diversity of ridges found in the fingerprint from person to person.

Fig. 2: Types of Fingerprint.

Detection the fingerprint is consists of five main steps, image acquisition, image pre-processing, feature extraction, classification, and decision making. Classification process is the main step to detect fingerprint. The temperature, humidity affects the temperature of the skin, which causes the images of fingerprints to be blurred. Also, the position of the finger when it is placed on a scanner and the way it is pressed also leads to changes in the fingerprints image that taken. Image pre-processing is used to reduce noise, enhance contrast, and so on [2], and [3]. Features extraction step [4].

The importance of this paper stems from the need for it to be used in all sectors for security purposes. It can be used in banking systems, education, and business this method for authentication can be used to login to devices and application without having to remember passwords.

Also, this method is very cheap, reliability, high secure, and accurate. Besides that, this method requires only small size of memory to save the fingerprint image which save the memory requirement.

The main aim for this research paper is to explore how the fingerprint can be detected for the purpose of identifying individuals. Authors concentrate on the minutiae-based and correlation-based that are used to matching fingerprint. Based on the previous research questions can define the following objectives:

- Review the biometrics concepts
- Review and analysis fingerprint features that are unique for person.
- Review and analysis the matching techniques to identify fingerprint.

While the remainder of this paper is organized as follows. The related works is thoroughly discussed in section II. Section III discusses the research methodology. Nevertheless, proposed solution is thoroughly elaborated in section IV. Section V emphasis on experimental results findings' discussion. The research conclusion and limitations were mainly discussed in section VI.

International Journal of Scientific Engineering and Science
Volume 4, Issue 5, pp. 22-28, 2020. ISSN (Online): 2456-7361

II. RELATED WORKS

In this section authors will provide a quick review of biometric fingerprint concepts and authors will provide a comparison of the overall fingerprint matching techniques. Also, a comparison of the overall machine learning approaches to apply these matching techniques.

Fingerprint is one of the most common authentication methods for its low accuracy and cost [5].Many applications use fingerprint to identify persons. Fingerprint identification system stores a set of fingerprints in a database, then it tries to identify a fingerprint by Matches it with the fingerprints already in the database. All applicable methods for fingerprint recognition attempt to reach the proper accuracy and speed.

Some optimizations must be inserted on the image especially when using the minute-based techniques. The first process is BINARIZATION process, in which the image becomes gray to binary (black and white). There are a number of ways to implement BINARIZATION that you mentioned in [6].

Another process that improves the image is thinning, in which the digital shape of the image is converted into a clear skeleton from which authors can extract features [7]. The binarization of the image is illustrated in figure 3, and the thinning of the image is illustrated in figure 4.

Fig. 3: (a) Original, and (b) binarization image of fingerprint.

Fig. 4: Original and thinning image of fingerprint.

A fingerprint is identified by comparing it with the fingerprints in the database according to their bifurcation and minutiae points as illustrated in figure 5. There are various techniques to apply the recognition process, minutiae-based and correlation-based [8], [9], and [10].Minute based Technique selects minute points in the fingerprint image and then compare them to the ones in the database as illustrated in figure 6. The Correlation based Techniques compares the Global pattern of edges and valleys database as illustrated in figure 7. This type of methods depends mainly on comparing pixel values in fingerprint images. These methods do not require prior image processing.

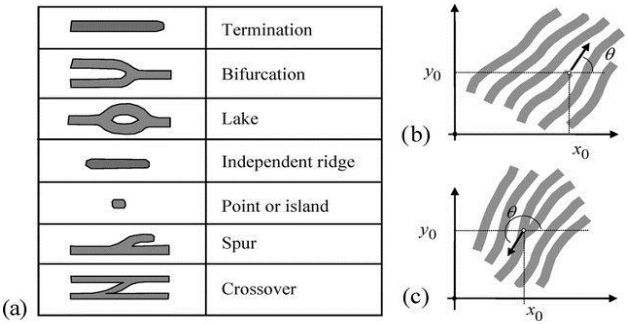

Fig. 5: (a) The common fingerprint minutiae types: (b) ridge ending, and (c) ridge bifurcation [11].

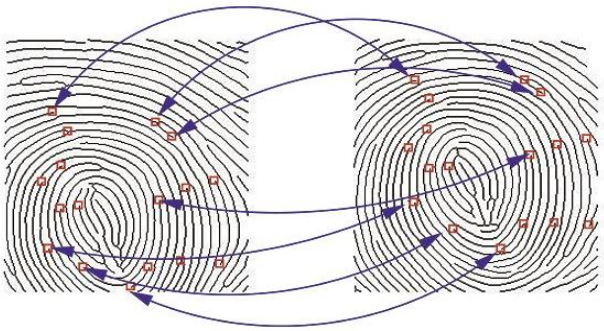

Fig. 6: Minutiae-Based fingerprint matching.

Fig. 7: Correlation-Based fingerprint matching.

To apply the previous two techniques; Minute-based and Correlation-based, authors use many algorithms such as machine learning. Machine learning is learning from previous experiences based on pre-collected data. This data is collected based on the features to be defined according to the existing system.

There are many machine learning algorithms [12].The types of these algorithms are classified according to the learning style to supervised learning, unsupervised learning and reinforcement learning. And according to similarity (how it works) to the following types:

- Linear Regression
- Decision Tree: This type of algorithm is classified as supervised learning, usually used for classification.
- SVM
- Naive Bayes
- KNN

- K-Means
- Dimensionality Reduction Algorithms
- Genetic Algorithms
- Deep Learning algorithms

The common tasks that machine learning can perform are regression, classification or clustering. Regression is a supervised machine learning technique. This type is used to predict by studying a set of dependent and independent variables. Simple Linear Regression is one of the regression algorithms [13].The linear regression model provides a sloped straight line representing the relationship between the variables as illustrated in figure 8. Linear regression algorithm attempts to adjust the X inputs to produce the Y output.

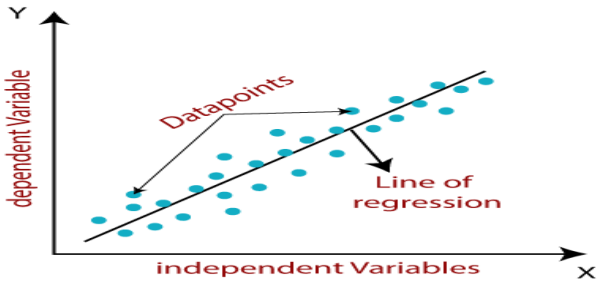

Fig. 8: Relationship between dependent and independent.

Classification is a type of supervised machine learning, in which the computer is trained with labelled data. This task is used to make a match between input data and the corresponding class. K-Nearest Neighbours is one of the most common classification algorithm [12]. This algorithm classifies an object by bringing it closer to its closest neighbours by certain measures as illustrated in figure 9.

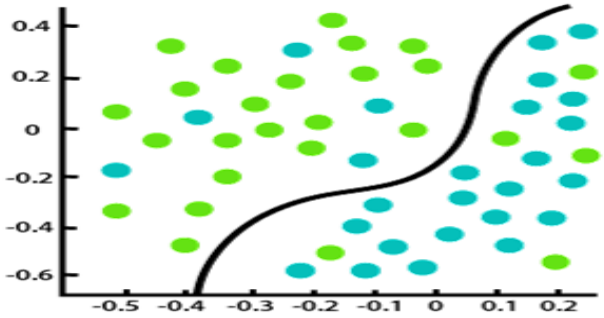

Fig. 9: Classification algorithm.

In addition to, support vector machine (SVM) can classify the fingerprint complicated data by using features vector to train the classifier and adjust the result according some rules [12].Neural networks and deep learning are also considered to be a good and accurate methods to recognize the fingerprint [13], [14], and [15].

Finally, clustering is unsupervised machine learning task. Clustering is a type of unsupervised, automated learning in which unlabelled data is used. This type is used primarily to detect data similarity, group similar data together, and then authors can enter data inputs and see which group this entry will belong to. K-MEANS cluster algorithm is used to group similar data into a single group as illustrated in figure 10. The idea of K-MEANS cluster algorithm is illustrated firstly in [16], the inputs are placed in the cluster closer to its centre, with cluster centres recursively adjusted and inputs reassigned to appropriate groups in an iterative method.

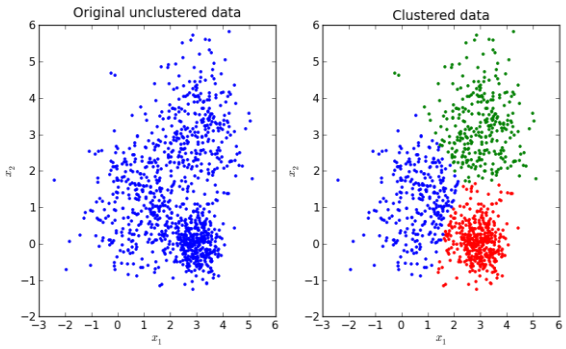

Fig. 10: Cluster K-Mean algorithm.

Fingerprint detection is considered as a classification problem. There are several factors that affect fingerprint recognition and capture [17]. For example, the position of the fingerprint on scanner device moves the captured fingerprint image. Also, the oblique fingerprint mode multiform the fingerprint images. The difference in the click through force tapping on the fingerprint device, causing the ridges to be muddled in the fingerprint, causing the captured images to be noisy. Finally, the changed skin condition due to moisture or changes in blood pressure, for example, affects the images acquired for the fingerprint.

Machine learning approaches are used today to fingerprint recognition. To design a classifier, training first based on the data collected and then test the classifier by using the same training data or other data.

Early on, many researches try to accurately identify the fingerprint, for example two machine learning approaches, support vector machines (SVMs), and recursive neural networks (RNNs), are used in [18] to give a fingerprint classification algorithm. RNNs is used to extract distributed features from fingerprint, this features then can be integrated in the SVMs to classify fingerprint.

A mathematical framework is designed in [19] to recognize fingerprint. This framework is divided into two parts, the first part is based on the person's biometric measurements like fingerprint and the second part is based on information, soft biometric measurements, such as age, length, and so on. The Bayesian decision theory is used by this framework to integrate the soft biometric information with the output of the primary biometric system. Finally, this research concluded that the soft biometric improves the fingerprint configuration process.

In [20] SVM and naive Bayes method were combined to improve fingerprint recognition by using fingerprint's core and delta. Reliance on some curve features in ridgelines used in [21] to recognize the fingerprint. Deep learning was applied using methods Deep Boltzmann Machin and Restricted Deep Boltzmann Machin to recognize the fingerprint by examining

complex texture patterns [22]. Finally, a comparison between SVM, and deep learning techniques are used.

III. Project Methodology

This research is dependent on literature review as a way to explore the various techniques of fingerprint detection. This reviews include the Biometrics fingerprint concept, feature extraction and different techniques that are commonly used to detect fingerprint.

Some experiments are designed to explore the most accurate machine learning technique. Various datasets are passed to various machine learning techniques to get the most accurate technique. The data is collected from the most common respiratory for fingerprint. Based on the results obtained, the results will be discussed to illustrate the features that can be extracted, the matching techniques to identify fingerprint.

The paper methodology will depend on the explanation fingerprint features that can be extracted to perform fingerprint classification. The classification process here will be the final stage by assigning the fingerprint entered to one of the fingerprints in the database. In working on this paper, authors compare the correlation-based and minutiae-based techniques that are used to matching fingerprint. The overall layout of the paper is explained in figure 11.

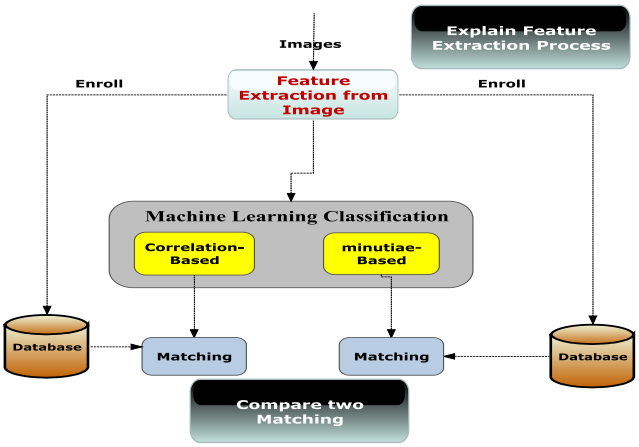

Fig. 11: Project layout.

A. Pre-processing

There are two important pre-processing steps, the first is the binarization of the image and the second is thinning the image. Authors apply the two steps on a fingerprint images to explain the pre-processing steps to prepare the fingerprint images to feature extraction process.

B. Feature Extraction

Authors will now look at how to implement the feature extraction process, and the different methods that are used to carry out this process. The fingerprint is a collection of a sequences of lines, matching to ridges and valleys on the Surface of the fingertip. These fine details (minutiae) characterize every human being and are not repeated, as each fingerprint varies in these details. Fingerprint features can be classified into three levels as illustrated in figure 12 [22].

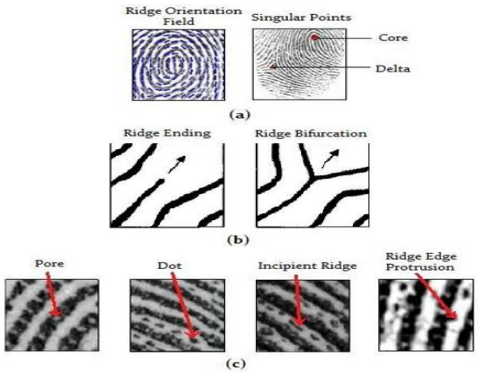

Fig. 12: Fingerprint features levels [23].

Features in level 1 are not unique but are used as additional rating features, are based on Core and Delta, and so on and it illustrated in figure 12(a). At the second level, feature has Minutiae points such as Ridge ending as shown in figure 12(b).

Finally, in level 3 where features determine uniqueness, all dimensions of hills such as ports and dots are relied upon. Features that help identify the fingerprint are extracted and then recorded for each fingerprint in a database, this reducing calculations and comparison time. There are multiple techniques to extract features that exist in the three levels in fingerprint images [24].These techniques vary from reliance on minutiae details, texture, or integration of them.

C. Enrolment

In this steps authors only enrol the fingerprint features and template into the database to be compared in the matching steps

D. Fingerprint Matching

A fingerprint is identified by comparing it with the fingerprints in the database according to their bifurcation and minutiae points. The paper apply the minutiae-based by comparing termination and Bifurcations. Also, apply the correlation techniques by comparing patterns of cores and valleys.

IV. Experimental Result

Three experiments were done on a computer (i7, 8 RAM) with the Matlab R2015a software, using 10 fingerprint images. The first experiment is intended to demonstrate how to improve fingerprint image and the steps to prepare it for feature extraction, and also what features are being extracted will be shown. The second experiment explains Correlation-Based Fingerprint Matching and the third experiment explains Minutiae-based system. Authors need to explain the output of the two techniques in the second experiment and third experiment. The function of a fingerprint matching algorithms is to compare the fingerprint input with the fingerprints registered in the database and give a score that expresses the degree of similarity.

A. First Experiment

In this experiment authors apply the following steps, Binarize, Thinking, and finally extract the features. The results

of this steps are illustrated in figure 13, figure 14, figure 15, and figure 16.

Fig. 13: The original fingerprint image.

Fig. 14: Image after binarize.

Fig. 15: Thinning the binarize image.

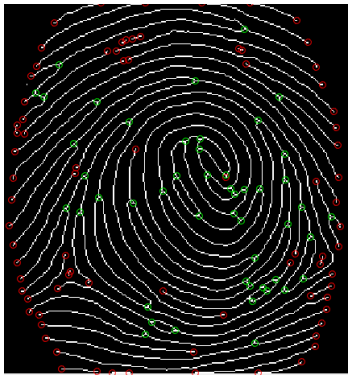

Fig. 16: Minutia data.

Now the Termination and Bifurcation on the original image can be illustrated in Figure 17.

Fig. 17: Termination and bifurcation on the original fingerprint Image.

The number of Terminations and Number of Bifurcations with their angles that exist in the previous fingerprint image are illustrated in figure 18.

Terminations :

X	Y	Angle
18	181	20.00
160	21	143.00
21	197	22.00
121	24	100.00
24	106	24.00
211	27	224.00
28	234	29.00
95	30	81.00
30	107	33.00
240	34	251.00
35	60	40.00
52	42	253.00
44	37	44.00
261	47	272.00
54	17	56.00
283	57	232.00
60	297	63.00
205	66	221.00
67	218	71.00
139	72	134.00

Bifurcations :

X	Y	Angle 1	Angle 2	Angle 3
39	74	46.00	77.00	58.00
51	64	167.00	70.00	115.00
75	170	79.00	141.00	89.00
81	90	158.00	115.00	97.00
118	163	128.00	269.00	130.00
247	133	259.00	142.00	153.00
152	266	153.00	141.00	160.00
113	168	64.00	171.00	173.00
172	111	171.00	119.00	178.00
140	193	140.00	197.00	151.00
199	171	200.00	156.00	205.00
177	208	22.00	208.00	152.00
209	226	212.00	230.00	214.00
242	216	207.00	216.00	276.00
219	96	220.00	151.00	223.00
231	226	234.00	233.00	225.00
236	77	240.00	123.00	240.00
233	241	144.00	243.00	180.00
254	166	255.00	224.00	261.00
190	278	174.00		

Fig. 18: Extracted termination and bifurcations data.

The first experiment is conducted 10 times on different fingerprint images to ensure quality of results

B. Second Experiment

A correlation-based matching is conducting by using a MATLAB code. Firstly, authors enrol 10 fingerprint for 5 persons, two image for each person as illustrated in figure 19.

In the second step authors pass a fingerprint to test the matching between it and the others in the database, authors pass another fingerprint for the second person as illustrated in figure 20.

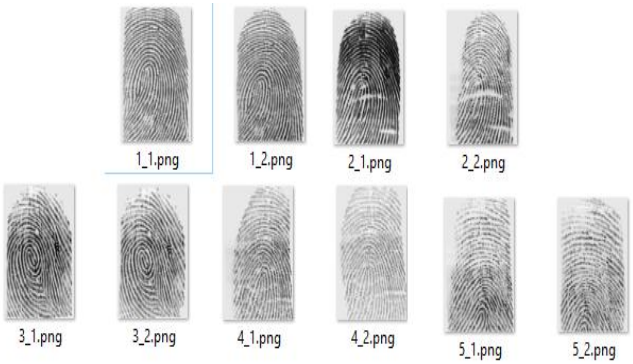

Fig. 19: 10 Fingerprint for 5 persons.

Fig. 20: Fingerprint for the second person.

The Correlation Filters computation gives the following results:

- PSNR value for class # 1 8.2635
- PSNR value for class # 2 12.6378
- PSNR value for class # 3 5.2825
- PSNR value for class # 4 6.7745
- PSNR value for class # 5 5.9525

Then these finger is belonging to class 2 which is true. This matching is applied for many times.

C. *Third Experiment*

The same processes that took place in the second experiment will be here where 10 fingerprints for five persons will be registered in the database to extract its features. Figure 21 illustrate the matching process.

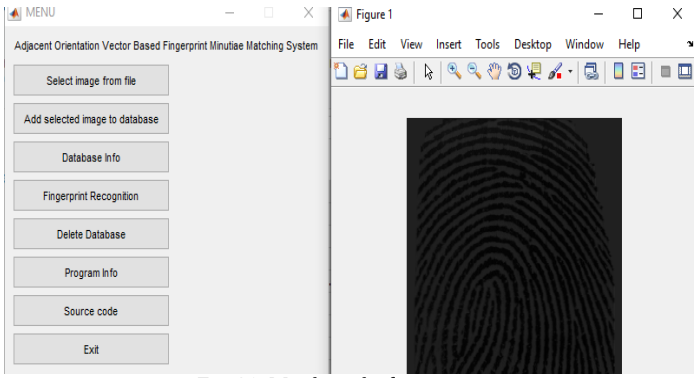

Fig. 21: Matching the fingerprint.

V. Conclusion and Future Work

In this paper, how to extract features from fingerprint images and what these features are described. An experiment using the Matlab software was performed on a number of fingerprints and the results of the experiment were displayed. Termination and Bifurcations are extracted and explained in the original image. Two another experiments have been conducted to make fingerprints matching, the first using the Correlation-Base Technique and the results of the experiment have been shown. The second is matching with Minutiae -based Technique.

Authors have explained how the two techniques (Minutiae -based, Correlation-Base) work, showing the results of the two experiences with the two techniques. It was noted that when the image quality was low, the features extracted could be distorted and untrue. The Correlation-based Technique has managed to address these situations because it compares general pattern of features.

In this study, authors found that minute-based technique is more widely used because of its speed to treat for Correlation-base. Also, minute-based has succeeded in dealing with the multiple rotation of the fingerprint image as it deals with specific features, unlike Correlation-Base.

In the future, authors aspire to study more of the speed and accuracy of the two techniques with the use of more than one algorithm for each technique. Also designing an integrated program to extract the fingerprint features and use it to verify the identity of internet users will be a good thing in the future.

References

[1] A.K. Jain, A. Ross, K. Nandakumar, Introduction to Biometrics, Springer, 2011.
[2] P. S. P. W. Jiajia Lei, Qinmu Peng, Xinge You, Hiyam Hatem Jabbar, "Fingerprint Enhancement Based on Wavelet and Anisotropic Filtering," International Journal of Pattern Recognition and Artificial Intelligence, vol. 26, no. 01, 2012.
[3] A. V Telore, "Study of Distortion Detection and Enhancement Methods for Fingerprint Images," 2016.
[4] R. Thai, "Fingerprint Image Enhancement and Minutiae Extraction", 2003.
[5] Jain, A.K., Bolle, R., Pankanti, S.: Biometrics Personal Identification in Networked Society. Springer (2009)
[6] P. Meenen, R. Adhami, "Approaches to Image Binarization in Current Automated Fingerprint Identification Systems", Department of Electrical and Computer Engineering, The University of Alabama in Huntsville, AL 35899 USA.
[7] E. V. Duro, "Fingerprints Thinning Algorithm", IEEE Aerospace and Electronic Systems Magazine, Vol. 18, Issue: 9, pp 28-30, 2003.
[8] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. Handbook of Fingerprint Recognition. Springer, New York, 2003.
[9] Mehmandoust S., Shahbahrami A. (2011) A Comparison between Different Fingerprint Matching Techniques. In: Cherifi H., Zain J.M., El-Qawasmeh E. (eds) Digital Information and Communication Technology and Its Applications. DICTAP 2011. Communications in Computer and Information Science, vol 166. Springer, Berlin, Heidelberg
[10] PP Bharti Nagpal, Manoj Kumar. (2015). Minutiae vs. Correlation: Analysis of Fingerprint Recognition Methods in Biometric Security System. International journal of engineering and technology (IJEAT) 5, 7
[11] A. K. Jain, A. Ross and S. Pankanti, "Biometrics: a tool for information security," in IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125-143, June 2006.
[12] Alpaydin, E. Introduction to Machine Learning; The MIT Press: London, UK, 2009; p. 584.
[13] Suzuki, K. Artificial Neural Networks-Architectures and Applications; IntechOpen Limited: London, UK, 2013.
[14] D. C. Ciresan, U. Meier, J. Schmidhuber. Multi-column Deep Neural Networks for Image Classification. IEEE Conf. on Computer Vision and Pattern Recognition CVPR 2012.
[15] Mosavi, A.; FaizollahzadehArdabili, S.R.; Várkonyi-Kóczy, A. List of Deep Learning Models. Preprints 2019, 2019080152.
[16] MacQueen, J. B. (1967). Some methods for classification and analysis of multivariate observations. In L. M. Le Cam & J. Neyman (Eds.), Proceedings of the fifth Berkeley symposium on mathematical statistics and probability (Vol. 1, pp. 281–297). California: University of California Press.
[17] D.Maltoni, D.Maio, A.K.Jain, and S.Prabhakar, Handbook of Finger print Recognition. Springer-Verlag, 2003.
[18] Yao Y., et. al., "A new machine learning approach to fingerprint classification," 7th Congress of the Italian Association for Artificial Intelligence, pp. 57- 63, 2001.
[19] Anil K. Jain, Sarat C. Dass, and KarthikNandakumar ,"Soft Biometric Traits for Personal Recognition Systems", Proceedings of International Conference on Biometric Authentication, LNCS 3072, pp. 731-738, Hong Kong, July 2004.
[20] Hong, J.H.; Min, J.K.; Cho, U.K.; Fingerprint classification using one-vs-all support vector machinesdynamically ordered with Bayes classifiers. Pattern Recognit. 2008, 41, 662–671.

[21] Wei L., Yonghui C., and Fang W., “Fingerprint Classification by Ridgeline and Singular Point Analysis," Congress on Image and Signal Processing, 2008.
[22] Uliyan, Diaa M., SomayehSadeghi, and Hamid A. Jalab. "Anti-spoofing method for fingerprint recognition using patch based deep learning machine." (2019).
[23] A. N. Mukunda, RaoSumitha S M. (2015). Multiple Features Based Fingerprint Identification System, International Journal of Research in Engineering and Technology 4 (9), 142-150.
[24] Tanmay Patil, Swati Nandusekar, "Different Techniques Used In The Process Of Feature Extraction From Fingerprint", IJIERT - International Journal of Innovations in Engineering Research and Technology, Volume 6, Issue 9, ISSN: 2394-3696, Page No. 6-15.