International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

Machine Learning Based Non Live Finger Print Detection

Mrs.S.Subhashini , Research Scholar, Anna university, Regional campus, Madurai ,

Dr.P.Umamaheswari, Asst.Professor, Anna university , Regionalcampus, Madurai

Abstract— **In recent days, liveness detection of finger print image has become very essential in finger print recognition systems because fake finger prints are used in lieu of real finger prints. Many machine learning(ML) techniques have been widely used for non live finger print image detection because these techniques provide high accurate identification and also cost effective. These techniques also enhance the accuracy of classification of real and spoof finger print images. In this article , literature review is done about machine learning (ML) and its algorithms used for the detection of non live finger print. The main objective of this article is to compare and analyse various ML techniques used for spoof detection. It also provides an overview of performance merits and limitations of ML algorithms used in non live finger print detection .**

Index Terms— **Non live finger print, liveness detection , Machine learning, anti spoofing, spoof detection**

I. INTRODUCTION

A finger print is an impersonation of an individual finger which is unique and durable over the life of a human being . Finger prints are used for the identification of an individual . Any finger print consists of unique ridges and valleys pattern in it . Three common characteristics of finger print are loop ,whorl and arch . Loops are ridges that looks similar as thin lassos . In loops , ridge lines goes outward and loops again back to it . Whorls ridge pattern appears like a circular or spiral pattern of ridge lines . Arch are ridge line which start low at one end, rise in the middle, and then go back down again on the other end. Three common characteristics of finger print are loop ,whorl and arch . Loops are ridges that looks similar as thin lassos . In loops , ridge lines goes outward and loops again back to it . Whorls ridge pattern appears like a circular or spiral pattern of ridge lines . Arch are ridge line which start low at one end, rise in the middle, and then go back down again on the other end. Features of a finger print are very essential for detection of fake finger print . The three general features of fingerprint are (i) global level feature (ii)Local level feature (iii) Detail level feature. Global ridge lines of a finger print are global level feature. This feature is mostly used for finger print image classification.

.

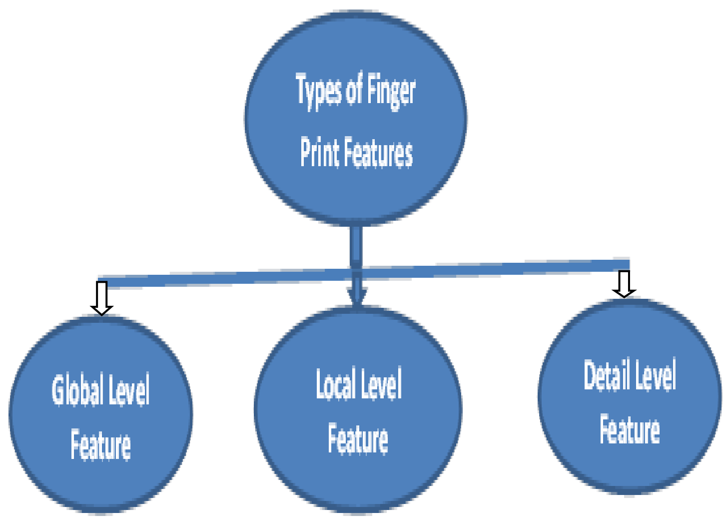


Fig .1. Three levels of features

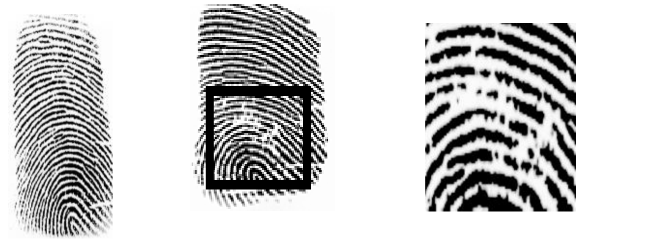
Minutiae details of ridges are local level features .These features are used for finger print recognition. Intra ridge details such as shape, pores , ridgecontours ,width etc., are detail level features. These features are used for finger print matching .

Non live finger prints are artificial finger print images which are created using inexpensive, soft flexible material and they are used as in lieu of real finger print image in biometric systems. Such fake finger print image is known as non live finger print image . They are constructed artificially by the fraudulent imposters . These imposters need representation of original fingerprint to create the artificial finger print image . They use casting material like latex , ecoflex , malleable material like plastic, or wax and other materials like play-doh, silicone, paper , Glue, clay, film, gelatin, rubber, dental impression etc for constructing the spoof finger print image. In general, artificial finger prints are not moist in nature. But nowadays fake finger print that carries the optical, electrical, and mechanical properties of a live finger are also created using highly sophisticated technologies. Characteristics of real and fake finger prints are different due to skin conditions, operating environment , fabricated material used for creating spoof finger print etc., Some of the differences between real and non live finger (Spoof) print images are as follows :

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

1. Fake finger print may contain broken ridges and blow holes due to deficiencies at casting where as its corresponding real print contain no broken ridges and blow holes .
2. Persipiration characteristics of real and fake fingerprint are different . Fake finger contains no sweat pores where as real finger print contains sweat pores.
3. Pores of real fnger print can not be imitated in fake finger print.
4. Though Fake images have similar geometrical structures as live images , ridge and valley shapes are not perfectly imitable in fake finger print.
5. Materials used for making spoof finger print consists of large organic molecules. Thus, miniature features such as pores cannot be imitated in real finger print .
6. Fake finger contains thick ridges because ridge widths can be altered due to amount of pressure the user exerts.
7. Fake print contains noise in its valleys due to incomplete stamping of fake finger print .
8. Real and spoof finger print visually look different because non live fingerprints look more darker than real finger print and have less contrast than live fingerprints.
9. Live fingerprint have higher energy concentrations in ridge-and-valley frequencies. But Fake images have more diffused energy distribution because of broken ridges and valley noise .
10. High-frequency components of the fake images had more energy than those of the live images because the noise components were distributed in fake images.
11. Some times pores can be detected in fake fingerprints though the pores of live fingerprint images are invisible.
12. Pores spacing in real and fake finger print are distinct due to sensor characteristics.
13. Finger print sensors cannot accept low quality fake fingers it accepts only when it is of high quality and match as same as real finger print.

Live finger print fake **Non live finger (f ake)** **Very minute details in finger print**



(A) BROKEN RIDGES IN FAKE FINGER

(b)Noise components in fake finger

(c) Non clarity of ridges,valleys of fake finger

(d) Thick ridges in fake finger

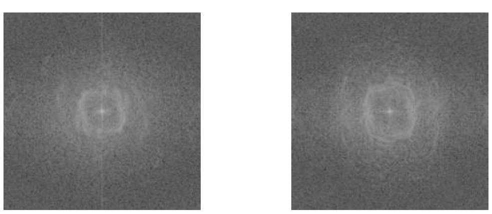
Fig. 2. Live finger print (left) and Non live finger print (right)

II. NON LIVE FINGER PRINT DETECTION METHODS

Finger print scanners have been widely used for personal identification in personal computers, automated teller machines, credit card transactions, electronic transactions to access control for airports, nuclear facilities and border control. It provides more security than traditional security methods such as passwords, keys, signatures, picture identification, etc. Though finger print scanners provide more secutity but it is more vulnerable to be spoofed with fake finger print images . Fake finger print recognition systems detect whether given finger print is real or fake . Finger print

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

anti spoofing techniques have been developed to prevent and detect spoofing attack in finger print scanners. Characteristics of real and fake finger prints are different due to skin conditions, operating environment , fabricated material used for creating spoof finger print etc., Two types of fake finger print detection methods are (i) Hardware based methods (ii) Software based methods. Hardware based methods use additional hardware for detecting liveness of finger print . Explicit characteristics of real finger print such as temperature, odor, pulse oximetry, blood flow ,heart beat, electrical and spectral characteristics .etc, are used for detection because these explicit charcteristics are not present in non live finger print. Hardware based detection methods are bulky and very expensive .But software based detection methods need no additional hardware thus very cost effective .These methods work with finger print image captured by sensors . Two approaches of software based detection methods are (i) static approach (ii) Dynamic approach . Dynamic approaches analyse skin persipiration and skin distortion for liveness detection .In static approaches, multiple static features of fingerprint are extracted , analysed and converted to vectors for classifictaion of real and fake finegr print. Static approaches uses features such as pores, surface coarseness , power spectrum, morphological characteristics , statistical properties etc., Also image based features such broken ridges ,blow holes , noise components, thick ridges etc., which are present in fake finger are analysed for finger print fake detection . Power spectrum analysis is used for finger print enhancement, finger print quality analysis , finger print matching etc.,. Ridges and valleys with specific frequencies are present in real and non live finger print images. Frequency bands of real and spoof finger print are distinct . Though power spectra of real and live finger print contains same ring patterns but have distinct energy changes due to minute changes present in fake finger print.



(a) (b)

Fig .3. The power spectra of (a)live (b) fake fingerprint

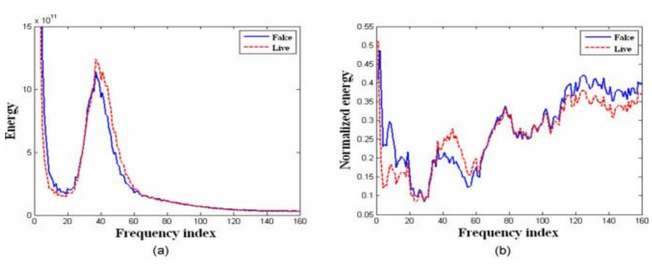


Fig. 4 .Energy concentration of live and fake fingerprint images. (a)Energy concentration of live and fake images. (b) Normalized energy concentration.

III. **MACHINE LEARNING (ML) AND ITS CLASSIFICATION**

Artificial intelligence is the branch of computer sciences which simulates the human intelligence by computers. Machine learning is a subfield of artificial intelligence which makes the computer to learn from past data with out being explicitly programmed and improve performances from past experiences. Deep learning(DL) is a sub field of ML and Neural network is a subfield of deep learning. Machine learning depends more on intervention of human to learn where as deep learning does not depends on manual intervention.

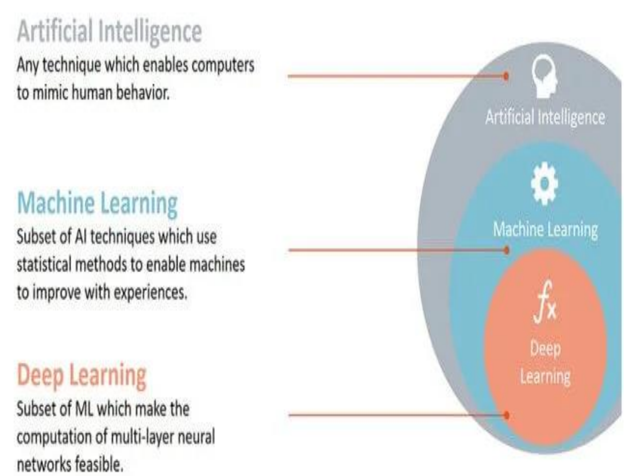


Fig. 5 . Artificial Intelligence and its subsets

Machine learning algorithms are used for classification or predictions, regression, clustering , association etc., It accepts past data , learns from given input data and build logical models. When new data is received from the built models , output is predicted.

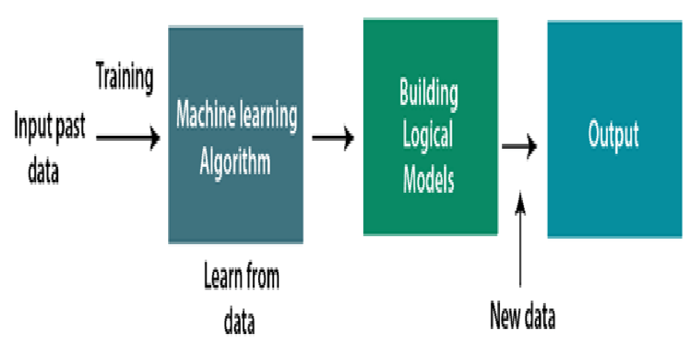


Fig .6 .Machine learning Model

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

Machine learning (ML) algorithms are used to perform very complex tasks that handles large amount of data. It saves time and money . Now a days machine learning is used for **self-**driving cars**,** cyber fraud detection**,** face recognition**,** image classification**,** friend suggestion by Facebook **,** Amazon virtual assistant "Alexa"etc ., Machine learning is classified in to four categories (i)Supervised learning (ii)Unsupervised learning (iii) Semisupervised (iv) Reinforcement learning . In supervised machine learning , algorithms are trained with labeled data sets to predict outcomes or classify given data set. Some of the supervised machine learning methods are Gaussian naïve bayes classifier, linear regression, logistic regression, decision tree , random forest, support vector machine (SVM), neural networks etc., In unsupervised machine learning , unlabeled data sets are analysed and clustered. Some of the unsupervised learning methods are principal component analysis (PCA) , singular value decomposition (SVD), neural networks, k-means clustering, probabilistic clustering methods, Hierarchical clustering, Self-organizing maps, Hidden Markov models etc., Semi-Supervised learning is a kind of Machine Learning which has ground between Supervised and Unsupervised learning algorithms. In semisupervised learning combination of labeled and unlabeled datasets are used as trainng data set . semisupervised learning is used to over come the limitations of supervised and unsupervised learning methods. *clustering and* classification algorithms can be combined for semisupervised learning. *Google expander is a semisupervised method* . Reinforcement learning is a kind of ML method and it makes a computer program to interact and learns to act within the environment . Some of the reinforcement learning algorithms are Q-Learning, *SARSA* **(** State Action Reward State action**),** Deep Q Neural Network (DQN), Markov Decision Process etc.,

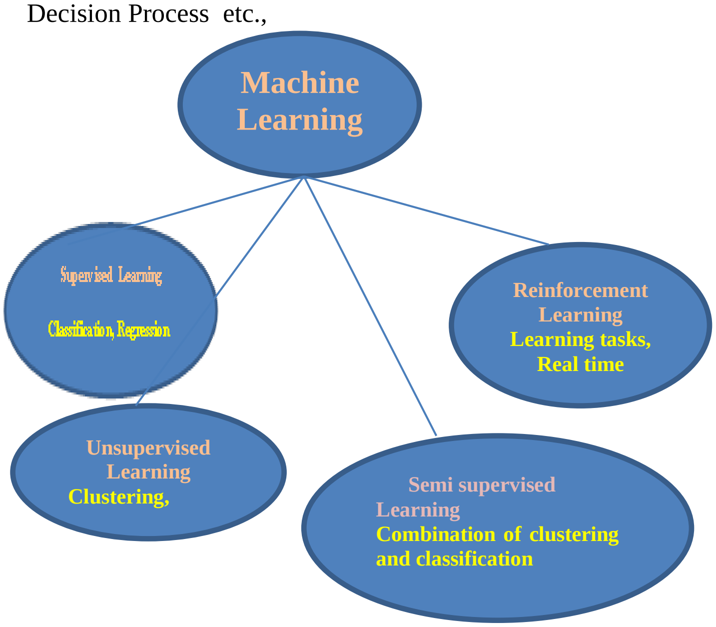


Fig. 7.Types of Machine Learning

IV. MACHINE LEARNING FOR NON LIVE FINGER PRINT DETECTION

Machine learning technique enhance the accuracy of classification system that distinguish between lives and non live finger print images . Supervised machine learning can be used for finger print image classification . Software-based anti-spoofing techniques extract salient features from the fingerprint images to distinguish live and non live finger print image . Some of the feature extraction methods are hand-crafted features (Weber local binary descriptor), scale-invariant feature transform (SIFT), convolutional neural networks (CNN) etc., to learn feature representation of fingerprints. The Gray Level Co Occurrence Matrix (GLCM) method is the most effective method to extract texture-based feature. Texture characteristics can also be extracted using the Gabor filter and used for fake fingerprint detection. But Weber Local Descriptor(WLD) and LPQ method that extracts features of finger print images is used to achieve better fake fingerprint detection. Extraction of texture data using LBP or Gabor filters produce favorable performance in fake fingerprint detection. When feature extraction is to be done with human interaction, machine learning algorithms can be used for finger print spoof detection. Machine learning algorithms works mostly on structured data . Three basic components of ML are datasets, features and algorithms.

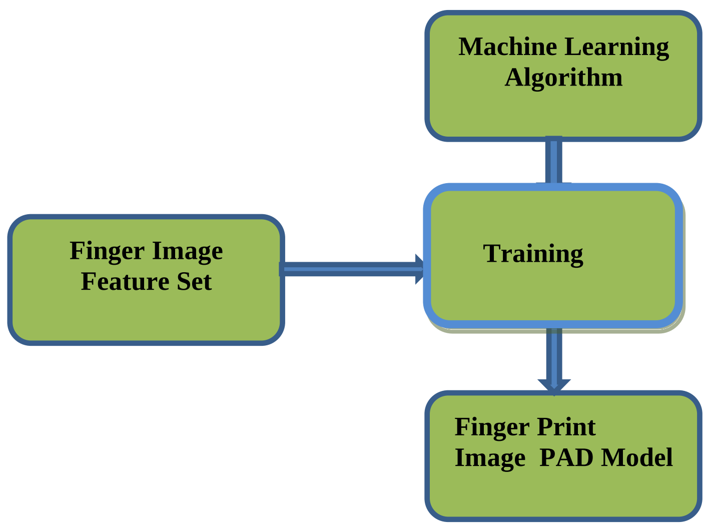


Fig. 8 . The generic architecture of a Machine Learning based finger print detection Model.

When no intervention of human is needed, deep earning can be used for spoof detection. Machine learning algorithms for spoof detection are less complex and easier to implement . Computational time of machine learning algorithm is less and produce effective result.Some of the differences between machine learning and deep learning based nonlive finger print detection are given below

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

S.No	Machine Learning based Non live Finger Print Detection	Deep Learning based Non Live Finger Print Detection
1.	Uses automated algorithms for output prediction and its model functions based on input finger print	Structures algorithms in layers to create an artificial neural network that learns and make decisions on its own for spoof detection
2.	Works efficiently on a lesser amount of data	Works efficiently on a huge amount of data
3.	Works on low-end machines	Requires high-end machines
4.	Less training time and more testing time	More training time and less testing
5.	Output is numerical value, score or classification	Can be anything like score, sound, text, etc
6.	Human Intervention is required to some extent for extraction of finger print image .	Human Intervention is not required for feature extraction.

Table 1: Difference between ML and DL for spoof detection

SVM machine learning algorithm is used to classify fingerprint images. It obtain good performance in relation with time consumption and image quality. SVM is widely used for two class classification problems. It is dataset specific because SVM algorithm that extracts Spatial domain, detailed ridge,fourier spectrum provides 99% accuracy for the dataset Livdet 2013 and 100% for ATVS dataset. Random Decision Forest is also used for finger print classification. Many machine learning algorithms was used for classification of two datasets ATVS and FVC2000, but only random forest algorithm had obtained better accuracy. Neural network over performed the nearest neighbor classifier in terms of accuracy.

V. SVM CLASSIFIER FOR SPOOF DETECTION:

In literature studies, though other ML algorithms are used for spoof detection, SVM classifier is widely used and provide better results than other ML algorithms. With trending AI, Kho et al[7] proposed a machine learning-based model for spoof detection which gives excellent results compared to existing methods. Kumar et al [8] also used machine learning with multi-feature method and carried out experiments on FVC 2000-2004. This experiment gave accuracy of 98% on the FVC 2000-2004 databases.

S. No	Feature Extraction Used	Data set	Machine learning algorithms	Performance metrics
1.	Spatial Domain Detailed Ridge Fourier spectrum	LivDet 2013 ATVS CASIA	SVM Classifier	• Accuracy for Livdet Det 2013 is 99% • Accuracy for ATVS is 99%
2.	Gray level Co-occurrence matrix	FO FC	SVM Classifier	• Accuracy for PO is 93.21% • Accuracy for PO is 84.93%
3.	WT LPQ PCA	LivDet 2011	SVM Classifier	• Average Classification error is 8.625%
4.	Binarizedfactual picture characteristics LPQ LBP BSIF	LivDet 2011	SVM Classifier	Total Error rate is 5.20 %
5.	Deviation,Variance Skewness,kurtosis, Hyperskewness , Hyper flatness	ATVS-FFp	SVM Classifier	Accuracy is 99.03% FAR=0.794% FRR=0.176%
6.	Feature set combined of residual noise , first order statistics, the intensity distribution and individual pore spacing	LivDet 2009	SVM Classifier	Average classification error is 12.5%
7.	wavelet-Markov local descriptor	LivDet 2009	SVM classifier	Average classification error is 2.8%
8.	LBP	LivDet 2011 LivDet 2013.	SVM based on a polynomial kernel	Average classification error is 11.47% for LivDet 2011 and 11.02% for LivDet 2013.
9.	Co-Occurrence matrices	LivDet 2009 LivDet 2011	SVM	Average classification error is 6.8% for LivDet 2009 and 10.98% for LivDet 2011
10.	New local descriptor-Local contrast phase.	LivDet 2011	linear-kernel SVM classifier	Average classification error is 5.7% for LivDet 2011

11.	local image descriptor-convolution comparison pattern.	LivDet 2013	SVM	accuracy of 93% on the LivDet 2013 .
12.	local textural patterns	LivDet 2009 LivDet 2011	SVM classifier	Classification rate of 88.49% on the LivDet 2009 and 78.78% on the LivDet 2011 dataset.
13.	Local coherence patterns (LCP)	ATVS LivDet 2009 LivDet 2011 LivDet 2013	linear SVM	Accuracy of 93.49% on the ATVS and 78.02% on the LivDet 2009, 2011, 2013.
14.	LBP	LivDet 2009-2013 datasets	SVM classifier	Accuracy of 9.95% on the LivDet 2009-2013 datasets
15.	Second and third-order co-occurrence matrices	LivDet 2009 LivDet 2011	SVM classifier	Accuracy of 6.2% on the LivDet 2009 and 6.635% on the LivDet 2011.

Fig .8. Comparison of SVM Classifier performance used on different dataset

VI . CONCLUSION

Machine learning algorithms for fingerprint spoofing detection are well fitted for real-time processes but when large amount of data is to be processed, these algorithms show poor performance. Random forest algorithm of machine learning technique obtain better accuracy in spoof detection. But SVM classifier algorithm is the most widely used algorithm for classification of real and fake finger prints because it provides improvement accuracy rate. Even SVM algorithm that extracts features such a spatial domain, detailed ridge, fourier spectrum provides 99% accuracy on dataset Livdet 2013 and 100% on ATVS dataset. In literature studies, it is found that SVM classifier provides very good accuracy rate on some datasets only but not on all datasets. Thus it is concluded that though variety of machine learning based non live finger print detection models are available , there is still a requirement to develop a robust and efficient non live finger print detection algorithm.

REFERENCES

1. Chugh, T.; Jain, A. Fingerprint Spoof Detector Generalization. IEEE Trans. Inf. Forensics Secur. (TIFS) 2020, 16, 42–55
2. Heeseung Choi, Raechoong Kang, Kyoungtaek Choi, Andrew Teoh Beng Jin, Jaihie Kim , "Fake-fingerprint detection using multiple static Features" , Optical Engineering vol 48 No 4,April 2009
3. NK Ratha, "Enhancing Security and Privacy in Biom etrics-Based Authentication Systems," IBM Systems Journal, v 40, n 3, 2001, p 614-634.
4. M. Galar et al., "A survey o f fingerprint classification Part I-Taxonomieson feature extraction methods and learning models", Knowledge-Based Sys., Vol.81, pp.76-97, 2015.
5. Gustavo Botelho de Souza, Daniel Felipe da Silva Santos,Rafael Gonc¸alves Pires, Aparecido Nilceu Marana, Joao Paulo Papa "Deep Features Extraction For Robust Fingerprint Spoofing Attack Detection" JAISCR, 2019, Vol. 9, No. 1, pp. 41 – 49
6. B. Tan and S. Schuckers, "New approach for liveness detection in fingerprint scanners based on valley noise analysis," J.Electron. Imaging, vol. 17, no. 1,p. 11009, 2008
7. J. Beom, W. Lee, H. Choi, and J. Kim, "An incremental learning method for spoof fingerprint detection," *Expert Syst. Appl.*, vol. 116, pp. 52–64, 2019, doi: 10.1016/j.eswa.2018.08.055.
8. M. Kumar and P. Singh, "FPR using machine learning with multi-feature method," vol. 12, pp. 1857–1865, 2018, doi: 10.1049/iet-ipr.2017.1406.
9. J. Galbally, S. Marcel, and J. Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition", IEEE T Imag. Proces., Vol.23, No.2, pp.710-724, 2014.
10. R. Jain, C. Kant, "Attacks on Biometric Systems: An Overview", Int. J Adva. Scient. Research, Vol.1, No.7, pp. 283-288, 2015.
11. L. Ghiani, et al., "Fingerprint liveness detection using local texture features", IET Biometrics, Vol.6, No.3, pp.224-231, 2017.
12. Toosi et al., "Feature Fusion for Fingerprint Liveness Detection: a Comparative Study", IEEE Access, Vol.5, pp.23695-23709, 2017.
13. D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Fingerprint liveness detection based on Weber Local image Descriptor," 2013 IEEE Work. Biometric Meas. Syst. Secur. Med. Appl. BioMS 2013 - Proc., 2013
14. R. Dubey, J. Goh, and V. Thing, "Fingerprint Liveness Detection From Single Image Using Low Level Features and Shape Analysis," IEEE Trans. Inf. Forensics Secur., vol. 6013, no. c, pp. 1–1, 2016.
15. Al-Ajlan, "Survey on fingerprint liveness detection," 2013 Int. Work. Biometrics Forensics, 2013, pp. 1–5, 2013.
16. E. Marasco and A. Ross, "A Survey on Antispoofing Schemes for Fingerprint Recognition Systems," ACM Comput. Surv., vol. 47, no. 2, pp. 1–36, 2014
17. G. Arunalatha and M. Ezhilarasan, "Fingerprint Spoof Detection Using Quality Features," Int. J. Secur. Its Appl., vol. 9, no. 10, pp. 83–94, 2015.
18. Y. S. Moon, J. S. Chen, K. C. Chan, K. So, and K. C. Woo, "Wavelet based fingerprint liveness detection," Trans. Korean Inst. Electr. Eng.,vol. 57, no. 6, pp. 982–984, 2008.
19. Kiefer, R.; Stevens, J.; Patel, A.; Patel, M." A Survey on Spoofing Detection Systems for Fake Fingerprint Presentation Attacks. In Proceedings of the International Conference on Information and Communication Technology for Intelligent Systems, Ahmedabad, India, 15–16 May 2020; pp. 315–334
20. Marcialis, G.M.; Lewicke, A.; Tan, B.; Coli, P.; Grimberg, D.; Congiu, A.; Tidu, A.; Roli, F.; Schuckers, S. First International Fingerprint Liveness Detection Competition—LivDet 2009. In Proceedings of the International Conference on Image Analysis and Processing, Vietri sul Mare, Italy, 8–11 September 2009; pp. 12–23.

21. Yambay, D.; Ghiani, L.; Denti, P.; Marcialis, G.L.; Roli, F.; Schuckers, S. LivDet 2011 Fingerprint Liveness Detection Competition 2011. In Proceedings of the International Conference on Biometrics (ICB), Washington, DC, USA, 11–13 October 2011; pp. 208–215.

22. Orrù, G.; Casula, R.; Tuveri, P.; Bazzoni, C.; Dessalvi, G.; Micheletto, M.; Ghiani, L.; Marcialis, G.L. LivDet in Action—Fingerprint Liveness Detection Competition 2019. In Proceedings of the International Conference on Biometrics (ICB), Crete, Greece, 4–7 June 2019; pp. 1–6.

23. Husseis, A.; Liu-Jimenez, J.; Sanchez-Reillo, R. Fingerprint Presentation Attack Detection Utilizing Spatio-Temporal Features. Sensors 2021, 21, 2059.

24. Hadid, N. Evans, S. Marcel, and J. Fierrez, "Biometrics Systems Under Spoofing Attack: An evaluation methodology and lessons learned," IEEE Signal Process. Mag., vol. 32, no. 5, pp. 20–30, 2015.
25. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion analysis," IEEE Trans. Inf. Forensics Secur., vol. 1, no. 3, pp. 360–373, 2006