Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 4 (2023)

Fingerprint Recognition System Using Machine Learning

Upendra Reddy[1], Ragi Raghava[2], Lohitha Sreya[3], Raparla Varshitha[4], Rani Medidha[5]

Department of Computer Science and Engineering,

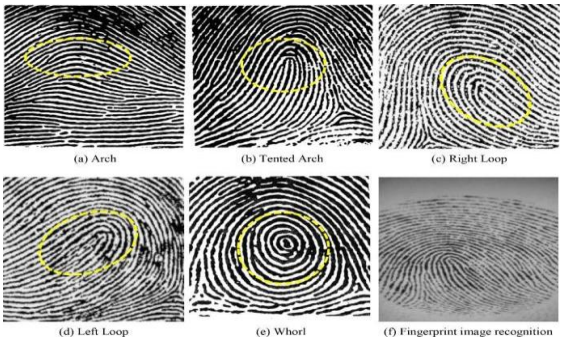
Koneru Lakshmaiah Education Foundation, Guntur, India.

***Abstract:* -**

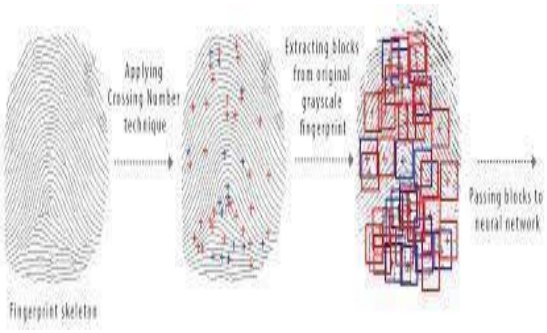
Fingerprints can be considered a crucial and dominant trait in the field of biometrics because of their high-security prominence, reliability, low cost, and acceptability. As fingerprint identification systems and fingerprint systems deployments are highly in demand, numerous challenges are rising in every phase of the system which includes feature extraction, matching of features, classification of fingerprints, and enhancements of the fingerprint image. Several ML (Machine Learning) techniques introduce several not-so-traditional techniques and solutions to the identification challenges. This research study gives us a keen understanding of the emphasis with the help of fundamental machine learning techniques and their implementation for the sake of compensating for the major complications regarding fingerprint identification**.**

Introduction: -

The Internet of Things can be considered a highly impactful aspect of our daily lives and our daily technologies start from surfing the Internet to the nation's defense mechanism. IoT can be considered as the network of things because of its specially generated infrastructure which helps the people in accomplishing the tasks in a large number. Such infrastructure of the Internet of Structure can be interrupted by aiming the networks from the miscellaneous sources that lead to the clogging of the network traffic and insane interruptions when it comes to the functioning. Such harmful and impactful ways of interrupting the networks can be caused using false biometrics, and that will certainly be a great loss. The main motive for Fingerprint recognition is to undermine the organization's web server or the country's defense mechanisms. A false biometric can be defined as an attempt to use an individual's fingerprint or any other biometric data to penetrate their data and cause a loss to them. These attacks usually take place using a process named Smurf attacks, which can be considered as the sum of the target's processing, memory usage, and bandwidth. Generally, the servers cannot handle the server crash or the ending in the collapse of the service because it will not be able to respond to the user request. So, it is mandatory to develop new prototypes and new techniques that can detect the fraudulent attacks of repetitive requests efficiently and effectively. It is also necessary to prevent the economic losses of the organizations and the unavailability of services to the users. In recent days, the main complication that recognition systems are facing is differentiating the legitimate users and false biometrics. The actions that will help the organizations prevent the response to Fingerprint recognition can show a positive impact on the services and the legitimate users present in the network.



With the help of machine learning techniques, one can deduce a pattern amongst the user behaviours and their input biometrics. Algorithms that are driven by such data, and machine learning can be taken into consideration as one of the accurate and impactful ways of detecting the patterns amongst biometrics the constantly changing users, and their input requests. Machine learning techniques can detect malicious attempts that will be used for the sake of false biometrics. In recent years many organizations that provide privacy internet services like personal data protection, banking, economic transactions to the public domain and defense, and so on are facing the urge to maintain an accurate biometric recognition system and safe network or the IoT environment. Most of the existing systems that are used for security are not at all capable of preventing false biometric recognition, these tools do not possess the accessibility or the power to identify whether the incoming input requests are a false packet or the normal user packet. This research study has been conducted with the results that we have obtained through examining 4 distinct machine learning algorithms namely Random Forests, SVM, KNN, and ANN to determine the attacks by utilizing the classification models that are considered to be best in detecting the fraudulent IP addresses.



Literature Survey: -

Numerous researchers are trying to develop new and promising techniques to detect Fingerprint recognition using ML and deep learning. Some of such recent works regarding this domain are discussed below.

[R. Amrish1, K. Bavapriyan2, V. Gopinaath3, A. Jawahar4, C. Vinoth Kumar]

ML can be considered as the data of AI (Artificial Intelligence), that uses several algorithms to uncover the patterns present in the data, which are usually utilized for the sake of creating the models that are driven by the data. Due to its adaptability, ML is an ideal choice in situations where the data is always changing, and the work becomes challenging when it inevitably shifts. ML methods can help organizations detect the false biometrical data packets that are utilized to combat different sorts of Data breaches. In terms of accuracy, deep learning, which involves multiplelayer abstraction and machine learning techniques, provides more accurate results generated. Deep learning is improved noticeably by elevating the device capabilities and making it very appropriate for the sake of IoT devices.

[Boyang Zhang; Tao Zhang; Zhijian Yu]

The daily evolving society, which has been mostly dependent on communication and data technology in recent decades has maintained it with much more exposure and vulnerability to a huge variety of personal data breaches. Using false Fingerprints or overriding fingerprint recognition can ruin the potentiality of privacy and sometimes can cause great loss both economically and professionally and shows its impact on information-providing services and online sites that mostly produce revenue, resulting in a noticeable decline in the losses thereby impacting the services provided to the legitimate clients. The research study of fingerprint recognition is a highly particular area of research that includes there is a huge number of techniques that are being proposed and have also been proposed in previous research one such infamous technique is artificial intelligence which uses an evolutionary algorithm for detecting the attempts made in the time of Data breach. The schemes that are known for detecting Fingerprint recognition are deteriorating to support the main motive of Fingerprint recognition and its prior recognition. To severely mitigate the threats, in this research paper, the researchers organized and utilized the grasshopper optimization algorithm (GOA) with the help of a deep learning algorithm named GOIDS. This certain approach is dependent on the monitored software ambiance and will be able to distinguish and differentiate between fake and normal traffic. The GOIDS chooses the most relevant and efficient features from the raw dataset named as IDS dataset that helps to differentiate complicated lower-speed Cyber threats and that is the point when the selected features are further carried forward to the classifiers that is decision tree, SVM (Support Vector Machine), multilayer perceptron that helps in identification of data breach and naïve bayes. The publicly available datasets which are called CIC-IDS 2017 and KDD Cup 99 were utilized regarding the experimental study of the researchers for their experimental studies. From the results of the experimental simulation, we can clearly understand that GOIDS with the help of a decision tree performs with higher accuracy and functions with much higher detection with a low false-positive rate.

[Raidi, imam; Sunardi; mahumad, arif wirwan et al 2018]

Overriding the biometric recognition systems with fake biometrical data is a kind of cyber-attack with the number both in intensity and in volume accelerated in recent days. Fake biometric data mainly fake fingerprint data can be considered as the major complication when it comes to the secrecy, availability, and integrity of the resources that are owned by the reputed internet organizations that are performing remarkably in the public domain. This experiment has proved that the quasi-newton training function will show us the highest accuracy value of 0.992 against the resilient propagation training function resulting in an accuracy of 0.989 and the scale conjugate training function which leads to the accuracy of 0.988.

[G. Wang, J. Hao, J. Ma, and L. Huang, “A new approach to intrusion detection using artificial neural networks and fuzzy clustering,” Expert Systems with Applications, vol. 37, pp. 6225V6232, 2010.]

The researchers have proposed that the ANN technology will be helpful to the researchers and the networks in tackling and handling the impacts of the Data breach. In this research paper, the data breach is considered one of the most common and familiar attacks in the field of defense and public safety with the maximum harm to the infrastructure. We can observe maximum number of research and approaches were conducted to elevate the performance of Fingerprint recognition systems such as there is no valid process or scheme that can completely prevent Data breaches. A system that can estimate the originality of fingerprint data will be of great help in real time to suppress the pessimistic impact by limiting the most suspicious and malicious attack sources. In this work, the authors have suggested a system that works with artificial neural networks (ANN) that helps in estimating the false biometrical data used at the time of the Data breach.

Methodology: -

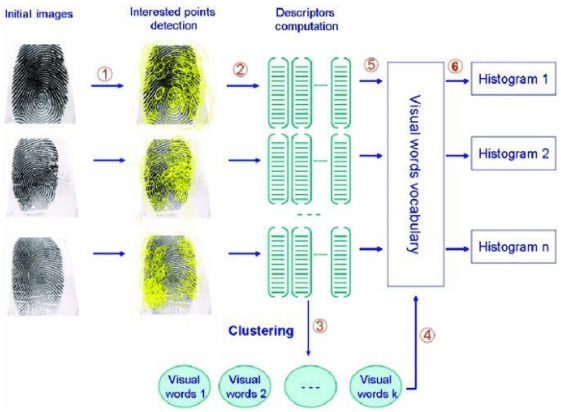
Our methodology defines our approach toward an understanding of different ML methods demands the study of several existing machine learning models that performs the detection of Data breach or false biometrics involvement. Through such analysis, it helps us to obtain a very clear vision regarding the Data breach. As a very first step, we have discussed several existing ways that are available for the attackers to perform the data breach. A few of such existing identification or recognition ways are:

- Retinal scanning
- Fingerprint scanning
- Voice analysis and
- Facial recognition

Due to the above-mentioned identification processes and by gaining the required amount of data for these processes any individual can perform overriding the recognition and can fake the identity of the targeted individual. The primary motive behind such actions is to steal the identity, create economic losses for the organizations, or breach the nation's defense. Sometimes the Fingerprint recognition systems are dependent on the persona of the attackers.

The most effective process of performing fingerprint recognition is by using the methods of machine learning with the help of algorithms to showcase the patterns in the biometrical data, which will be used to create a data-driven model. The versatility of ML made it an important way for the data this is an unpredictable and completely inconsistent dataset and the complexity of detecting false fingerprint attempts is continuously increasing. Although we can find minimal ways of detecting such attempts, there is no particular or named method that is perfectly suitable, effective, and accurate. Defending and reacting or tackling the attempts of false fingerprint recognition is highly a complicated task to handle. Where the pessimistic outcomes can prevent discomfort for the legitimate users. Even deep learning has remarkably evolved as a way to detect Fingerprint recognition in the field of IoT.

Coming to fingerprint recognition through machine learning techniques we have started our research study with a machine learning technique named the random forest (RF) method. Random Forest is one most known ML methods which is well known for its performance in the aspects of separations and classifications. The random forests generate different types of decision trees. Every tree of the decision tree will generate an alternate bootstrap test from the biometrical data that utilizes the tree classification algorithm.



The NSL-KDD dataset has been utilized in this research study. The experiment was conducted with the help of a Windows 10 device with a 64-bit OS, the testing model is 1,2s, and the frequency of the attack instances on the classes will be identified accurately.

$$\text{Accuracy} = \frac{TN + TP}{FN + TP + TN + FP}$$

The technique of RF is noticeably accurate with the reading when it comes to recognizing the fingerprint and differentiating the false fingerprints from the legitimate ones. Random Forests algorithm was utilized to train the

attack recognition and classification models which resulted in the accuracy percentage of 99.76% in the classified instances.

Another machine learning technique is SVM. SVM is one of the most crucial ML methods and it can surely be considered for the sake of fingerprint recognition. The variables of SVM are namely rate of classification, rate of false negatives, rate of false positives and then it sends the data that it has collected to the corresponding SVM, to its training and testing sets.

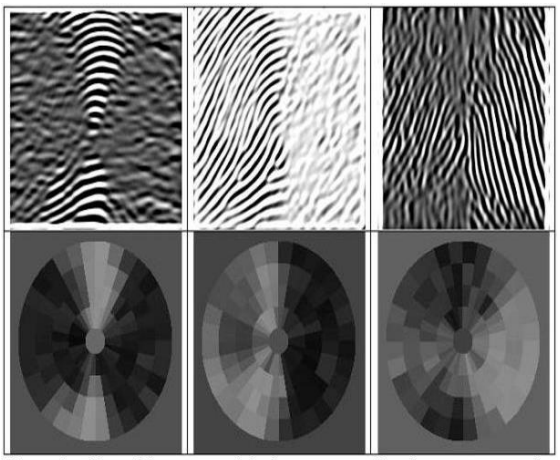
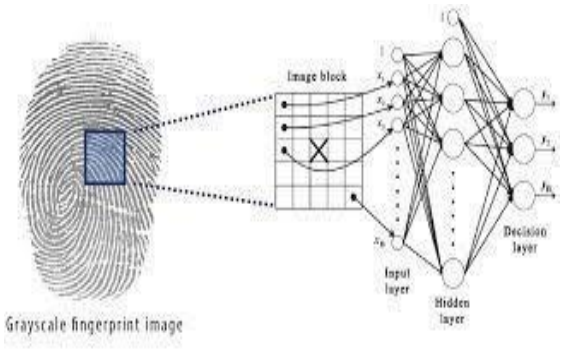


Figure 2. Filtered images and their corresponding feature vectors for orientations 0°, 5°, 22.5° and 45° are shown [11].

Though the SVM is made for the sake of both regression and classification complications it is used only for the sake of solving the classification complications. The primary motive behind utilizing SVM is to draw an ultimate decision over the limitations that can segregate “n” dimensional space into the different classes because of which insertion of fingerprint data becomes much easier.

This process permits the SVM module to detect the false Fingerprints with an accuracy rate of 99% and to minimize the false positive rates and the false negative rates when we compare it to the existing conventional models of attack detection.

We can categorically state from our research study that the ANN model can outperform all other classifier models with an accuracy rating of 99.95%.



A mechanism of fingerprint recognition was once described based on principles of artificial neural networks. SNN allows the biometrics that are legitimate and will be recorded in the database whereas the abnormal traffic will be flagged and tagged as suspicious. As ANN provides a noticeable analysis of the difference between fraudulent biometrical data and legitimate user fingerprints it can detect false fingerprints with a remarkable accuracy. Almost in the very same instances, the popular algorithm named KNN has an abundant number of reasons to tackle the obstacles on the classification basis of identification of legitimate fingerprints and false fingerprints. Euclidean distances are a suitable parameter for the KNN method for examining the distances

between two distant sites. The rate of information that is gained will be utilized to minimize the Euclidean distances. The algorithm's primary goal is to optimize the impact of a few crucial parameters and their supporting characteristics in relation to user categorization. GR-ADKNN algorithm and Traditional Average Distance-KNN algorithm can be utilized to measure the number of detection outcomes of numerous false fingerprint attempts. In order to make it easier to calculate the rate of accurate detection, we used a score indicator called the F1-Score indicator to denote the assessment parameters.

$$\text{F1-SCORE} = \frac{\text{Recall} * \text{Precision}}{\text{Recall} + \text{Precision}}$$

Results: -

According to our research study, we have obtained a clear understanding of various machine learning techniques for the sake of fingerprint recognition. An ML method known as SVM will be of great use in Fingerprint recognition with an utmost accuracy rate of 99.00%. SVM functions better than many other ML methods in the field of information security and pattern recognition.

Conclusion: -

In this research paper, we have gone over numerous existing techniques of fingerprint recognition. Fingerprint recognition can be considered one of the most dangerous and harmful threats to user privacy and the defense system of the nation. According to the observations that we have drawn throughout our research study we have understood that few of the machine learning techniques perform very well in the aspect of Fingerprint recognition with noticeable accuracies. Machine learning techniques like KNN, random forests, SVM, and so on are surely capable of detecting data breaches and identifying false fingerprints up to a great extent but still, a lot of research and development is needed in this particular domain as these machine learning techniques are constrained due to their limitations. The technology of biometrics can be considered as the mode of personal identification that utilizes both behavioral and psychological characteristics.

Reference: -

[1] Jain, Anil K., Nandakumar Karthik, and Ross Arun. 2016. 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. *Pattern Recognition Letters* 79: 80– 105.

[2] Jain, Anil K., Arun A. Ross, and Karthik, Nandakumar. 2011. Introduction to Biometrics. Berlin: Springer.

[3] Zhao, Qijun, Jianjiang Feng, and Anil K. Jain. 2010. Latent Fingerprint Matching: Utility of Level 3 Features. MSU Technical Report, vol. 8, 1–30.

[4] Jain, Anil K., Yi Chen, and Meltem, Demirkus. 2007. Level 3 Features for Fingerprint Matching. U.S. Patent Application No. 11/692,524.

[5] Gupta, Dipalee, and Siddhartha Choubey. 2015. Discrete Wavelet Transform for Image Processing. *International Journal of Emerging Technology and Advanced Engineering* 4 (3): 598–602

[6] Byun, Hyeran, and Seong-Whan Lee. 2002. Applications of Support Vector Machines for Pattern Recognition: A Survey. *Pattern Recognition with Support Vector Machines*, 213– 236. Berlin, Heidelberg: Springer.

[7] Verlinde, Patrick, and G. Cholet. 1999. Comparing decision fusion paradigms using k-NN based classifiers, decision trees and logistic regression in a multi-modal identity verification application. In

Proceedings International Conference Audio and Video-Based Biometric Person Authentication (AVBPA).

[8] Kittler, Josef, et al. 1998. On Combining Classifiers. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 20 (3): 226–239.

[9] M. Barreno, B. Nelson, R. Sears, A. D. Joseph and J. D. Tygar, "Can machine learning be secure?", *Proc. ACM Symp. Information Computer and Communications Security (ASIACCS'06).*, pp. 16-25, 2006.

[10] L. Huang, A. D. Joseph, B. Nelson, B. Rubinstein and J. D. Tygar, "Adversarial machine learning", *Proc. 4th ACM Workshop Artificial Intelligence and Security Chicago IL*, pp. 43-57, 2011.

[11] B. Biggio, G. Fumera and F. Roli, "Pattern recognition systems under attack: Design issues and research challenges", *Int. J. Pattern Recogn. Artif. Intell.*, vol. 28, no. 7, pp. 1460002, 2014.

[12] B. Biggio, G. Fumera and F. Roli, "Security evaluation of pattern classifiers under attack", *IEEE Trans. Knowledge Data Eng.*, vol. 26, no. 4, pp. 984-996, 2014.

[13] P. Laskov and R. Lippmann, *NIPS Workshop on Machine Learning in Advances in Environments for Computer Security*, 2007.D. Joseph, P. Laskov, F. Roli and D. Tygar, *Dagstuhl Perspectives Workshop on Machine Learning Methods for Computer Security*, 2012.

[14] N. K. Ratha, J. H. Connell, R. M. Bolle, and , "An analysis of minutiae matching strength" in AVBPA ser. LNCS, Springer, vol. 2091, pp. 223-228, 2001.K. Jain, K. Nandakumar and A. Nagar, "Biometric template security", *J. Adv. Signal Process.*, vol. 2008, pp. 1-17, 2008.

[15] R. N. Rodrigues, L. L. Ling and V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks", *J. Vis. Lang. Comput.*, vol. 20, no. 3, pp. 169-179, 2009.Adler, A. Jain, N. K. Ratha and , "Vulnerabilities in biometric encryption systems", *Proc. 5th Int. Conf. Audio-and Video-Based Biometric Person Authentication ser. LNCS*, vol. 3546, pp. 1100-1109, 2005.

[16] J. Galbally, C. McCool, J. Fierrez, S. Marcel and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks", *Pattern Recogn.*, vol. 43, no. 3, pp. 1027-1038, 2010.