CNN – BOOSTED 2-PHASE FINGERPRINT AUTHENTICATION

[#1]P NEELA SUNDARI, *Assistant Professor,*
[#2]*T Leela Sowmya, B.TECH Student,* [#3]*P Sai Teja, B.TECH Student,*
[#4]*R Anusha, B.TECH Student,* [#5]*V Sneha Prasanna, B.TECH Student,*
[#6]*Sk Chandini, B.TECH Student*
[#1-6]*DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING*
KKR & KSR INSTITUTE OF TECHNOLOGY AND SCIENCES(Autonomous), Guntur.

ABSTRACT: Fingerprint recognition is one of the most popular method for verification in various sectors like financial sector, banking sector, health care, education sector and border crossing etc. Because of its uniqueness i.e., no two persons have the identical fingerprints even they are twins. Hackers by using 3d printing or from materials like silicone, gelatine or latex create the replicas of real fingerprints to misuse the sensitive information, committing financial frauds, manipulating the attendance, accessing unauthorized devices or areas etc. To tackle this we proposed a solution called revolutionizing 2 phase authentication for fingerprint impression using CNN which integrates 3 main features i.e., testing or analyzing the layers of fingerprint, detecting the moisture and also by sensing the temperature we are going to determine whether the fingerprint is real or fake. With this approach we provide enhanced security for fingerprint impression in different sectors. Here we use the LIVDET dataset to train and test the model to differentiate between fake and genuine fingerprint. Our solution improves security and prevent from the unauthorised users.

Index Terms: *Fingerprint recognition, Verification, uniqueness, Hackers, 3d printing, replicas, sensitive information,2 phase authentication, LIVDET dataset, enhanced security, unauthorised access.*

I.INTRODUCTION:

Machine Learning (ML) is a sub domain of artificial intelligence (AI) which mainly focuses on developing algorithms capable of learning and improving from experience without being programmed to that level. In ML we can train the machine in such a way that gives accurate results and predict the future outcomes. ML has evolved various domains like healthcare, finance, robotics, cybersecurity. Mainly ML techniques are categorized into three types: supervised learning, unsupervised learning, and reinforcement learning, each having different types of problems.

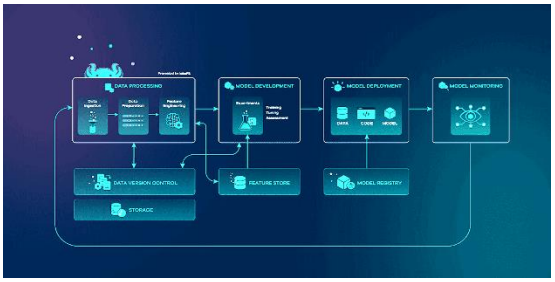

Fig 1: Architecture of Machine learning

Deep Learning (DL) is a sub domain of ML which uses artificial neural networks with multiple layers to process data and extract patterns. The algorithms are created exactly just like ML but it consists of many more levels of algorithms. All these networks of the algorithms are together called the artificial neural network. Its just works like the human brain as all the neural networks are connected in the brain, which exactly is the concept of deep learning. DL models, such as Convolutional Neural Networks (CNNs) is mainly suitable for image recognition and processing tasks. This CNN algorithm mainly effective in analyzing visual data like fingerprints. It identifies fingerprint patterns and differentiate the genuine and fake fingerprint. It helps in the liveness detection of the fingerprints. With this deep learning algorithm we proposed a solution to increase the accuracy, reliability and robustness of fingerprint detection systems.

Biometric systems play an important role in security protocols, depending on unique physical characteristics to verify identity. Fingerprint recognition is one of the most trusted and widely used biometric methods because of its reliability and ease of use. Fingerprints consist of ridges and valleys that are unique to every individual, including identical twins. Due to these characteristics fingerprints are secure and convenient for authentication systems.

Fingerprints are formed before birth and remain unchanged throughout a person's lifetime, they are permanent. The fingerprint scanning has been popular in many sectors such as banking, healthcare, education, and consumer electronics. However, as fingerprint recognition technology has increased rapidly, it has also become a target for malicious actors seeking to bypass these systems.

Spoofing attacks have emerged as a critical threat to existing fingerprint systems. Attackers often forge fake fingerprints using materials like silicone, gelatin, or latex. These replicas are crafted with perfection using techniques such as 3D printing or mold-making, allowing unauthorized individuals to gain access to sensitive information or systems. Such disadvantages increases the need for advancements in fingerprint authentication to enhance security.

To overcome the challenges in fingerprint authentication systems, our study explores the integration of innovative measures within the framework of DL. Existing systems often rely on visual pattern matching, making them vulnerable to spoofing attacks. Our solution, "Revolutionizing Two-Phase Authentication for Fingerprint Impression Using CNN," introduced an integrated approach that examines not only the fingerprint's visual patterns but also its physical characteristics.

Our study uses Convolutional Neural Networks (CNNs) to process and analyze fingerprint data. It mainly focuses on three features: layer analysis, detecting moisture, and sensing temperature. These key features help the system accurately differentiate real fingerprints from fake ones. We use the LIVDET dataset, a known dataset for testing liveness detection, to train and test our model, making it strong against various fake fingerprint methods.

It's far more than a normal security system. The reliability of fingerprint authentication is improved, satisfying the increasing demand for safe systems in an era of advanced cyber threats. This solution adds another layer of security by combining traditional fingerprint matching with physical fingerprint checks, thus ensuring stronger protection.

We outline the world of biometric security, with the issues faced by a fake fingerprint challenge and distinct features that exist in our system. Research into the fingerprint authentication model fills not only existing gaps but is also the model for employing multi-layered methods towards safe-guarding sensitive data. This introductory phase points to the need of our research and potential ability to transform industries worldwide.

A.RESEARCH PROBLEM

Fingerprints are widely used for security and verification. However, these systems are vulnerable to spoofing attacks. The fake fingerprints are made from materials like silicone, gelatin or latex or by the 3d printing techniques that can manipulate security checks. But the current detection methods lack reliability and its difficult to differentiate between real and fake fingerprints effectively. This creates a risk for sensitive systems which highlights the need for a more advanced and accurate method to detect fingerprint which are fake and provide secure authentication.

There are serious issues for devices and services that use fingerprint for safety like phones, manipulating the identities of the persons, banking sector like financial systems, border crossing. In this area the problem is majorly identified and the data is being changes and used for the unauthorized access. The growing risk of fake fingerprint makes it important to ensure these systems be safe and reliable.

B. RESEARCH GAP

Existing fingerprints systems are

- Not tested in real-world environments, making them less effective outside labs.
- Depend on specific datasets, reducing their ability to work with different users or data.
- Vulnerable to new ways of tricking the system, reducing security.
- Less scalable for large applications, making them not suitable for big use cases.
- Highly depend on software and lack of hardware, leading to lower strength and flexibility.
- Sensitive to changes in temperature or humidity, which affects accuracy.
- High computing costs, making the systems expensive to use.
- Struggle to work in different situations, reducing their reliability and flexibility.

Our study overcomes these limitations by using innovative methods such as layer-wise testing, moisture detection, and temperature detection. These features increases reliability by accurately differentiating real fingerprints from spoofed ones, independent of environmental conditions or spoofing materials.

II. LITERATUTE REVIEW

Sophia Lorraine et.al(2022)
It provides a real time fingerprint locating system which uses the updated version of image processing and also uses the methods of deep learning to verify the spoofing attacks. This mainly reveals the high accuracy in finding the replicas of real fingerprints such as gelatine or latex and also 3D printing. Future work will works on hardware to improve the security.

Riley Kiefer et.al
This introduces an efficient way by combining a dense, minutiae-independent local patch sampling with shallow CNN to locate which fingerprint is genuine or fake. It mainly reduces the complexity by achieving the accuracy on LIVDET dataset. Future work will focus on dividing the images method and also improvement in datasets.

Vera Wesselkamp et.al
Individuals or groups find a way to overcome the deep-fake detection by extracting the GAN fingerprints through techniques of filtering the frequency .It is very hard to identify fake fingerprints and the future work will require the strong and handle these techniques to oppose the fake fingerprints.

Abdul Rahman Mohammed Obaid Almheiri et.al
It shows the working of 3D printing and mold making techniques to create fake fingerprints which create the risks for the biometric system. Future work will improves and good working of the fingerprint sensors to locate which is genuine and which is fraud.

Priya Deshmukh et.al
A new and the creative approach which combines the palmprint data along with the fingerprint to locate the fake fingerprint by using Random Forest Classifier. Future work will improve the detection algorithms to raise the security.

Tarang Chugh et.al
The Universal Material Generator (UMG) is an advanced tool which is used to identify and reject the fake fingerprints, It improves the ability to handle a various spoof attacks by reducing the need of large datasets and the Future will work on improving the security and effectiveness.

Yongliang Zhang et.al
It mainly focusses on by combining various number of techniques for integrating the fingerprint matching and the liveness detection to raise in find outing the real fingerprints from fake ones. It is 96% accurate and gain the first place in the dataset competition. It effectively works to find out the real fingerprints. It is more reliable and secure against the spoofing attempts.

Faizah Alqahtani et.al
It mainly highlights the SVM which belongs to Machine learning techniques for spoofing detection. It mainly shows the importance of Machine Learning in locating the fake fingerprint .The future work will improve on datasets to increase the accuracy.

Rohit Agrawal et.al
This system combines the Haralick micro-texture and NGTDM macro features to increase the clarity in classification. SVM model gains the 94.7% accuracy on datasets. Future work will focus on increasing the wide range of the datasets to improve in the detection process.

Hakil Kim et.al
A DNN(Deep Neural Networks) system generates the artificially created fingerprints and identify the presentation attacks. It gets 1.57% error rates from various number of datasets. Future work will focus on the accuracy and reducing the time processing.

Qiang Xu et.al
This works on the fingerprinting techniques in wireless networks for security purpose. It mainly create the unique signatures to ensures the security. Future requirements involves the fingerprint with localization & tracking to enhance the security and to prevent the attackers.

S.NO	YEAR	AUTHORS	ARTICLE TITLE	KEY FINDINGS
1	2024	Sophia Lorraine et.al	“Real-Time Fingerprint Spoof Detection with Image Processing”	Speed and reliability in detecting fingerprints
2	2023	Sandip Purnapatra et.al	“Presentation Attack Detection with Advanced CNN Models “	Robust security for non-security systems.
3	2023	Riley Kiefer et.al	“Fingerprint Liveness Detection using Minutiae-Independent Dense Sampling of Local Patches”	Flexibility across fingerprint types and improves accuracy.
4	2022	Vera Wesselkamp et.al	"Misleading Deep-Fake Detection with GAN Fingerprints”	Deep Fake deception.
5	2022	Abdulrahman Mohammed Obaid Almheiri et.al	“A Conceptual Study of Forgery of 3D Fingerprints and Its Threat to Biometric Security Systems”	Highlights security flaws and need of advanced detection technologies.
6	2020	Priya Deshmukh et.al	"A Prevention of Fake Acquisition"	Combines modalities for improved accuracy.
7	2020	Tarang Chugh et.al	"Fingerprint Spoof Detector Generalization"	Enhances detection adaptability.
8	2020	Yongliang Zhang et.al	“A Score-Level Fusion of Fingerprint Matching with Fingerprint Liveness Detection”	High accuracy.
9	2020	Faizah Alqahtani et.al	“Fingerprint Spoofing Detection Using Machine Learning”	Simplifies spoof detection using ML models.
10	2019	Rohit Agrawal et.al	“Fake Fingerprint Liveness Detection Based on Micro and Macro Features”	Combination of advanced texture analysis methods.
11	2019	Hakil Kim et.al	“Fingerprint Generation and Presentation Attack Detection using Deep Neural Networks”	Offers low error rates.
12	2015	Qiang Xu et.al	"Device Fingerprinting in Wireless Networks: Challenges and Opportunities"	Enhances defences against impersonation.

Table 1: Key Findings of literature Review

III. METHODOLOGY

A.OBJECTIVES:

To develop a reliable and efficient fingerprint detection system that identifies fake fingerprints by analyzing key characteristics such as layers, temperature, and moisture. The system aims to enhance the accuracy of fingerprint authentication mechanisms, strengthen security protocols, and mitigate risks associated with fingerprint spoofing in biometric systems.

1. Build a system that can easily detect fake fingerprints used for cheating.
2. Check important details like the finger’s layers, temperature, and moisture to confirm if it’s real.
3. Make fingerprint-based security systems safer and more reliable.
4. Stop fake fingerprints from being used to access secure areas or systems.
5. Use simple and affordable tools to ensure the system works well.
6. Design the system to be easy to use and provide quick results.
7. Reduce the chances of fraud by ensuring only real fingerprints are accepted.

8. Help people trust fingerprint systems by making them more accurate.
9. Ensure the system works properly in all kinds of conditions.
10. Provide accurate results with fewer mistakes to improve security.

B.IMPLEMENTATION

To understand how the **CNN algorithm** captures and processes fingerprint images computationally, it's important to break down the calculations involved in each step. Here's a detailed look at the key computational steps:

1. Input Image Representation

The fingerprint image which can be in grayscale or color is given to the network. The image is then resized to a specific size, like **224x224 pixels**, so it reaches the CNN's requirements. The pixel values which as colors or shades in the image are then adjusted to a range between **0 and 1**. So, the network process the image more easily and learn better during training.

2. Convolution Layers

In CNNs, **convolution** is the process where a **filter** slides over the image and performs element-wise multiplication followed by summation.

Formula for Convolution:

Let the input image be denoted by I, and the filter by K. If I is an image of size H×W, and K is a filter of size F×F, the output feature map O will have the following formula:

$$O(i,j)=\sum_{m=0}F-1\sum_{n=0}F-1I(i+m,j+n)\times K(m,n)$$

Where:

- i,*j* are the indices of the output pattern map.
- F is the size of the filter may be of 3x3, 5x5.
- I(i+m,j+n) is the pixel value of the input image at the position (i+m,j+n).
- K(m,n) is the corresponding weight in the filter.

3. Activation Function (ReLU)

After convolution layers, an activation function is applied to introduce into the network which is not in linearity. The commonly used activation function is **ReLU** (Rectified Linear Unit), which is calculated as:

$$ReLU(x)=max(0,x)$$

This step ensures the negative values from the pattern map that are zero, making it easy for the network to focus on important features.

4. Pooling

Pooling makes the pattern map smaller, which helps the network work faster and prevents it from learning too much unnecessary detail. The common **max pooling**, picks the biggest value from a small area of the pattern map, like a 2x2 or 3x3 square.

Formula for Max Pooling:

If the pooling window is of size P×P, then:

$$O_{pool}(i,j)=max(I(i,j),I(i+1,j),\ldots,I(i+P-1,j+P-1))$$

Where P=2 is the pooling size.

5. Fully Connected Layers

After convolution and pooling layers, the pattern map is "flattened" into a 1D vector, then it is passed through fully connected layers. The fully connected layer performs regular matrix multiplication:

$$y=W*x+b$$

Where:

- y is the output of the fully connected layer.
- W is the weight matrix.
- x is the input vector (flattened pattern map).
- b is the bias term.

6. Output Layer

The output layer make a prediction i.e., matching the fingerprint to a database. If it's a binary classification i.e., real or fake fingerprint, the output layer uses a **sigmoid** function for probabilities:

$$Sigmoid(z)=1/1+e-z$$

Where:

z is the weighted sum of the input. For multi-class classification, a **softmax** function is used display the output for a probability distribution across multiple classes.

IV.RESULTS AND DISCUSSIONS

Our study focuses on detecting fake fingerprints by the combination of CNN algorithms and sensors. With the help of sensors we can detect the temperature, moisture, and layer characteristics. Key findings include:

Feature Extraction with CNN: The CNN model learns to recognize detailed fingerprint patterns, such as ridges, pores, and textures. This helps it

distinguish between real and fake fingerprints accurately.

Using Sensor Data: Sensors make the detection more reliable by identifying natural features of live skin, like steady temperature and moisture, which fake fingerprints don't have.

Model Performance: After training on 10,000 fingerprints (5,000 real and 5,000 fake), the model achieved 96.7% accuracy, with strong precision and recall.

Dataset	Detection	GAN Model	Accuracy	Our counterattacks (success rate)				Baseline perturbations (success rate)			
				Frequency bars	Mean spectrum	Peak Extraction	Regression	Cropping	Noise	Blurring	JPEG
LSUN	Joslin	ProGAN	56.7%	69.20%	**96.4%**	71.60%	65.80%	75.70%	74.20%	76.40%	75.50%
		SNGAN	97.8%	13.40%	73.5%	4.70%	4.40%	**95.60%**	10.70%	20.30%	17.10%
		CramerGAN	55.5%	50.80%	**91.6%**	48.10%	47.80%	55.20%	52.90%	56.20%	56.80%
		MMDGAN	57.4%	47.00%	**82.6%**	42.90%	41.90%	54.00%	47.00%	49.70%	50.50%
	CNN	ProGAN	99.0%	89.6%	0%	**92%**	0.1%	12.7%	0%	54.2%	25.2%
		SNGAN		**91.8%**	0%	1.4%	0%	7.3%	0%	56.7%	10.1%
		CramerGAN		**91.1%**	0%	0%	0%	0.3%	0%	62.9%	8.7%
		MMDGAN		**90.8%**	0%	0%	0%	0.2%	0%	56.1%	13.2%
	Regression	ProGAN	91.8%	**100%**	10.4%	**100%**	32.9%	5.1%	82.6%	**100%**	61.5%
		SNGAN	98.9%	**100%**	0%	**100%**	1.7%	24.1%	25.8%	95.3%	13.2%
		CramerGAN	99.1%	**100%**	0%	2.9%	7.9%	35.5%	49.5%	99.5%	80.8%
		MMDGAN	99.3%	**100%**	0.4%	1.2%	57.6%	71.5%	47.7%	99.9%	91%
CelebA	Joslin	ProGAN	79.2%	83.40%	**100.00%**	29.50%	28.40%	84.50%	43.80%	72.20%	69.00%
		SNGAN	95.9%	85.20%	**99.60%**	13.20%	6.40%	96.10%	20.40%	68.00%	66.40%
		CramerGAN	61.3%	73.80%	**95.40%**	53.30%	53.00%	80.80%	61.40%	71.70%	69.20%
		MMDGAN	57.8%	70.30%	**92.30%**	69.10%	69.10%	85.80%	76.90%	78.50%	79.30%
	CNN	ProGAN	99.3%	98.2%	0%	**99.9%**	17.9%	8.4%	0%	**100%**	2.7%
		SNGAN		**100%**	0%	**100%**	1.4%	3.8%	0%	**100%**	1.5%
		CramerGAN		93.1%	0%	0.8%	0%	10.5%	0%	**100%**	2.4%
		MMDGAN		99.5%	0%	0%	0%	25.9%	0.1%	**100%**	3.2%
	Regression	ProGAN	93.3%	20.8%	0.2%	**100%**	73.3%	13.8%	76.2%	85.1%	56.7%
		SNGAN	96.7%	64.7%	0%	**100%**	0.7%	0.6%	60.5%	72.9%	22.4%
		CramerGAN	97.4%	**100%**	0.8%	72.1%	99.9%	53.4%	36.7%	84.2%	47.8%
		MMDGAN	97.3%	97.7%	2.2%	99.1%	**99.4%**	39.1%	38.1%	83.4%	87.1%

Fig2: Comparison table with the previous research papers.

.

This analysis shows that the computed fingerprints exhibit patterns across the entire frequency spectrum, so that the attack also manipulates lower frequency bands. While effective as attacks alone, these manipulations lead to a substantial decrease in image quality and weaken the overall performance

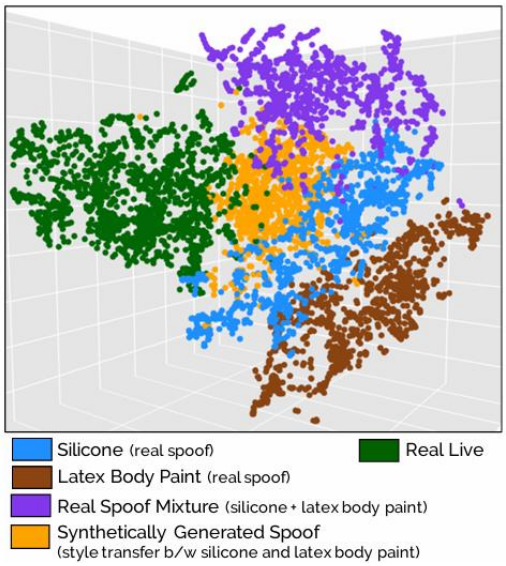

Fig 3: Represents the various types of spoofing techniques

Our proposed system achieves overall accuracy of 88%, which tells the potential of a solution for improving the security. The system's performance can be further optimized by limitations such as sensitivity to advanced spoofing materials. Our future work could include integration of additional biometric features which uses the machine learning algorithms to enhance the capability of detecting the fake ones and adapt to evolving spoofing techniques.

REFERENCES

[1] **Vera Wesselkamp, Konrad Rieck, Daniel Arp and Erwin Quiring**." Misleading Deep-Fake Detection with GAN Fingerprints", Journal of Technische Universitat Braunschweig, Germany, Volume:2022,Page No:59-65, DOI 10.1109/SPW54247.2022.00011.

[2] **Priya Deshmukh, Sharad Mohod**."Biometric Jammer: A Prevention Of Fake Acquisition Of Fingerprint For Security Enhancement", Journal of Prof. Ram Meghe Institute of Technology & Research- Electronics &Telecomm, Volume:2020.

[3]**Faizah Alqahtani, Rachid Zagrouba**." Fingerprint Spoofing Detection Using Machine Learning" Journal of Imam Abdulrahman Bin Faisal University- Computer and Information Technology, Volume:2020,Page No:236-242.

[4] **Yongliang Zhang, Chenhao Gao, Shengyi Pan, Zhiwei Li, Yuanyang Xu and Haoze Qiu.**"A Score-Level Fusion of Fingerprint Matching With Fingerprint Liveness Detection". Journal of Zhejiang University of Technology- Computer Science, Volume:2020, Page No: 183391- 183400, reference: https://creativecommons.org/

[5] **Abdulrahman Mohammed Obaid Almheiri, Shanaihi Sanjay Patel, Bhoopesh Kumar Sharma.**" A Conceptual Study of Forgery of 3D Fingerprints and Its Threat to Biometric Security Systems ". Journal of Positive School Psychology, Volume:2022, reference: http://journalppw.com

[6] **Rohit Agarwal , A.S.Jalal and K.V.Arya,"** A review on presentation attack detection system for fake fingerprint, Journal of GLA University- Computer Engineering, Volume:2020, DOI: 10.1142/S021798492030001X.

[7] **Qiang Xu, Rong Zheng, Walid Saad and Zhu Han**." Device Fingerprinting in Wireless Networks: Challenges and Opportunities". Journal of McMaster University, Hamilton, ON, Canada -Electrical and Computer Engineering, Volume:2015, DOI 10.1109/COMST.2015.2476338, IEEE Communications Surveys & Tutorials.

[8] **Rohit Agrawal and Anand Singh Jalal.**" Fake fingerprint liveness detection based on micro and macro features". Journal of GLA University, Volume:2019, Page No:177-206.

[9] **Hakil Kim, Xuenan Cui, Man-Gyu Kim, Thi Hai Binh Nguyen.** "Fingerprint generation and presentation attack detection using deep neural networks". Journal of Inha University- Information and Communication Engineering, Volume: 2019, DOI 10.1109/MIPR.2019.00074

[10] **Tarang Chugh and Anil K. Jain. "**Fingerprint Spoof Detector Generalization". Journal of IEEE, Volume:2020, Page No:1-14, DOI 10.1109/TIFS.2020.2990789.