e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604028 |

Detecting Passive Attacks in Fingerprint Spoofing Using Convolutional Neural Network

Maryam Jameela[1], Mohammed Affnan[2], Mohammed Sadiqulla[3], Pooja K C[4], Prof. Shilpa K C[5], Prof. Anu C S[6]

UG Student, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[1]

UG Student, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[2]

UG Student, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[3]

UG Student, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[4]

Assistant Professor, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[5]

Assistant Professor, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[6]

ABSTRACT:A self-learning, secure and independent open-set solution is essential to explore the characterise the liveness of fingerprint presentation. Fingerprint spoof presentation is classified as live (a Type-I error) is a major problem in a high-security establishment. Type-I error are manifestation of small number of spoof sample. The proposed work uses only live sample to overcome above challenge. In this work an adaptive 'fingerprint presentation attack detection' (FPAD) scheme using interpretation of live sample. It requires initial high-quality live fingerprint sample of the concerned person. It uses six different image quality metrics as a transient attribute from each live sample and record it as 'Transient Liveness Factor' (TLF). Study for the work also proposes to apply fusion rule to validate scheme with three outlier detection algorithms, one-class Convolutional Neural Network (CNN), isolation forest and local outlier factor. This work results in phenomenal accuracy of 100% in terms of spoof detection, which is an open-set method. Further, this study proposes and discuss open issues on person specific spoof detection on cloud-based solutions.

I.INTRODUCTION

Nowadays, biometric recognition systems have used in a variety of identification sectors,due to their convenience and robustness compared with conventional techniques such as a password. Biometrics recognition systems rely on the physiological and behavioural attributes of individuals. The fingerprint is one of the most frequently used authentication systems since they guarantee high identification accuracy, cost-effective, and can be applied to huge datasets of images. Those characteristics make fingerprint recognition systems deployed in many applications, such as attendance, smartphone identification, forensics, health-care systems, banks, etc. However, those systems are not immune from malicious attacks. There are two types of attacks that biometric are vulnerable from direct, and indirect attacks. Direct attack is the most common since there is no knowledge is required to conduct the attack. For the fingerprint recognition system, it can be performed in the sensor device with simple and handy tools like silicon, wood glue, etc.

In contrast, indirect attack imposes deep information about the system's module. With the increased amount of attack tools, researchers have attracted to develop a system that can assess and provide a solution for liveness detection of fingerprint. In many developed countries turns into fully automated with smart home and lifestyle. Biometric authentication is one of the effective methods for unlocking or running any smart devices in the environment. Also, many spoofing fingerprints are happening in developed countries. So, the liveness detection is the only solution for anti-spoofing. The living moment of the individual or any functional information will be detected by the addition of liveness detection.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604028 |

II.LITERATURE REVIEW

No.	Paper Title	Author Name	Year	Summary
1	Evaluation of Fingerprint Liveness Detection by Machine Learning Approach	Dr.Edriss Eisa Babikir Adam	2021	This article focuses on the implementation and evaluation of suitable machine learning algorithms to detect fingerprint liveness
2	Robust anti-spoofing techniques for fingerprint liveness detection	Habib & Selwal	2021	The paper discusses the various fingerprint artifacts, state-of-threat ML and DL based PAD algorithms, and publicly available benchmark datasets
3	Fingerprint Spoofing Detection Using Machine Learning	Faizah Hasan Alqahtani & Rachid Zagrouba	2020	A comparison between datasets used in the literature was made based on specific metrics
4	Anti-spoofing method for fingerprint recognition using patch based deep learning machine	D. M. Uliyan, S.Sadeghi, and H.A.Jalab,	2019	Improve the interoperability of fingerprint templates generated by different combinations of sensors and algorithms.
5	Authentication of area fingerprint scanners	V.I. Ivanova, and J.S. Baras	2019	With the help of advanced machine learning algorithms, the accuracy of spoofing detection can be increased

Existing systems typically rely on traditional fingerprint scanners or biometric authentication systems that are designed to detect fake or fabricated fingerprints. These systems may use techniques such as liveness detection, which involves analyzing the characteristics of a fingerprint to determine whether it is from a live finger or a replica. However, these systems can be misled by sophisticated spoof fingerprints that are difficult to distinguish from genuine fingerprints and it is not very practical for all forms of spoof fingerprinting materials. The two types of materials as Gelatin and wood glue were obtained and tested in real-time.

In proposed system, the first stage requires the person to enter several correct and spoofed fingerprints as a training dataset, while in the testing stage, a new fingerprint is being tested for its liveliness. Based on that, the spoofness score is being found, and this spoofness score determines whether the Fingerprint is spoofed or live.

III.METHODOLOGY OF PROPOSED SURVEY

Data Collection:

Data collection in fingerprint spoofing is typically done using an image acquisition system to capture high- resolution images of the fingerprint. This data can then be processed using specialized algorithms to identify unique features in the fingerprint, such as minutiae points, ridge patterns, and other characteristics. Once the data has been collected and analyzed, it can be used to create a digital representation of the fingerprint, which can then be used to compare the original image to other potential spoofed images.

Data processing:

Data processing in fingerprint spoofing involves collecting, analyzing, and storing fingerprint data. This data is used to create a spoofed fingerprint for a user. The process begins with collecting biometric data from the user, such as a picture of

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604028 |

their fingerprint or a scan of their fingerprint taken with a specialized device. This data is then analyzed to create a unique digital representation of the fingerprint. This representation can be used to create a spoofed fingerprint that can be used to gain access to secure systems. Finally, the data is stored in a secure manner to ensure that the spoofed fingerprint remains secure.

Training and Testing:

Fingerprint spoofing is the act of creating a fake fingerprint to fool a biometric system. Training and testing for fingerprint spoofing involves creating a dataset of both real and spoofed fingerprints, and then using machine learning algorithms to determine which fingerprints are authentic and which are spoofed. Additionally, cross-validation techniques should be employed to ensure that the model is performing well. Testing should be done using a variety of different spoofs so that the system is robust to different types of spoofs. Finally, the system should be tested on a variety of different biometric systems to ensure that the model is able to detect spoofs across different systems.

Modeling:

Fingerprint spoofing is the practice of creating a fake fingerprint that is designed to fool biometric security systems. To accurately model this process, researchers use a variety of machine learning algorithms such as support vector machines, random forests, and deep learning networks. These models are used to identify patterns in the spoofed fingerprints, as well as classify them as genuine or not. Additionally, researchers have also used data augmentation techniques to improve the performance of the models. For example, they may add noise or blur to the image to create a more realistic spoof. Finally, the models are tested against real- world samples to ensure their accuracy.

Prediction:

Fingerprint spoofing involves using a fake fingerprint to gain access to a device or system. To predict if a fingerprint is a spoof or real, machine learning algorithms can be used to analyze the features of the fingerprint, such as its shape, size, and texture. These algorithms can be trained to recognize patterns that indicate a spoof fingerprint and flag it as a potential risk. Additionally, the use of biometric authentication systems can also help to ensure that only legitimate fingerprints are used for authentication.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604028 |

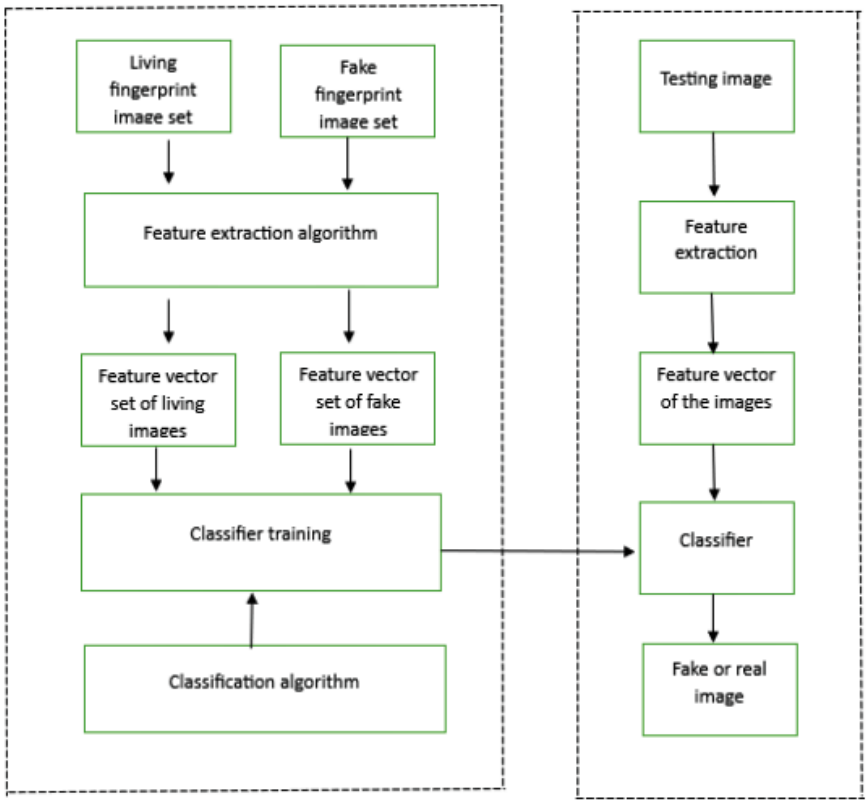

Figure 1: Methodology of the proposed work

Modules used:

- Preprocessing module – (image registration) is involving dimension reduction and filtering with the assistance of Region of Interest (ROI)
- Feature Extraction module –The CNN (Convolutional neural network) is used to capture high-level connections to input images. Thus, the process of CNN is viewed as a feature extractor. The higher the complexity of the problem to be solved, and greater the number of parameters and the amount of training data required.
- Classification module – Using SoftMax classifier the fingerprints were classified as genuine or forged**.**

The Preprocessing module involves image registration, which is the process of aligning multiple images of the same object or scene to a common coordinate system. This is typically done to remove any unwanted variation in the images due to differences in the way they were captured. The preprocessing module also involves dimension reduction and filtering using a Region of Interest (ROI) approach. This helps to reduce the dimensionality of the data and eliminate any irrelevant information, making it easier for the Feature Extraction module to identify important features.

The Feature Extraction module is where the CNN comes in. The CNN is used to extract relevant features from the preprocessed images. The CNN is a deep learning model that is capable of learning hierarchical representations of data by convolving input images with a set of learnable filters. These filters are used to detect low-level features such as edges and corners, which are then combined to form more complex features. The output of the CNN is a set of feature maps that are then used as input to the Classification module.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54|

| Volume 6, Issue 4, April 2023 |

| DOI:10.15680/IJMRSET.2023.0604028 |

The Classification module is responsible for classifying the preprocessed and feature-extracted images into one of two classes: real or fake. The classification is performed using a SoftMax function, which is a type of activation function commonly used in neural networks. The SoftMax function takes the output of the CNN as input and produces a probability distribution over the two classes. The class with the highest probability is then selected as the predicted class.

IV.CONCLUSION AND FUTURE WORK

Fingerprint spoofing detection is a critical security measure for any biometric system, as it can help protect against unauthorized access and fraud. Fortunately, there are a variety of techniques available for detecting spoofed fingerprints, such as active and passive anti-spoofing methods. These methods can be used together to provide an effective defense against spoofing attacks. With the proper implementation, biometric systems can be made much more secure and reliable. The purpose of this project is to implement the recent fingerprint recognition systems and anti-spoofing schemes based on the machine learning algorithm. A comparison between those models and between multiple datasets had presented. SVM is the most machine learning classifier used in the literature models. For the future work, a machine learning based model that helps in identification and classification fake fingerprints will propose using new public liveness fingerprint datasets.

REFERENCES

[1] Dr. Ediss EisaBasbikir Adam, “Evaluation of Fingerprint Liveness Detection by Machine Learning Approach-A”, in 2021
[2] Habib & Selwal, “Robust anti-spoofing techniques for fingerprint liveness detection”, in 2021
[3] Faizah Hasan Alqahtani & Rachid Zagrouba- “Fingerprint Spoofing Detection Using MachineLearning”-2020
[4] D.M Uliyan, S.Sadeghi, and H.A Jalab “Anti-spoofing method for fingerprint recognition using patch based deep learning machine” in 2019
[5] V.I Ivanova, and J.S. Baras “Authentication of area fingerprint scanners” in 2019
[6] R. P. Krish et al., "Improving automated latent fingerprint identification using extended minutia types", in 2019.
[7] X. Guo, F.Wu and X.Tang, “Fingerprint Pattern Identification And Classification” in 2018
[8] Nuraisha, and G. F. Shidik, "Evaluation of Normalization in Fake Fingerprint Detection with Heterogeneous Sensor", in 2018
[9] X. Guo, F. Wu, and X. Tang, "Fingerprint Pattern Identification and Classification", in 2018
[10] S. Fahman et al., "Classification of Live Scanned Fingerprints using Histogram of Gradient Descriptor", in 2018.

Impact Factor
7.54

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com