IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Detection of Artificially Molded Fingerprints using Machine Learning

Dr.V.Keerthika+[1] Rithika Bhargav K*[1], Monika Rani*[2], Pramodhini K S*[3], Arpitha K*[4]

*Student,4th year, Dept of Computer Science and Engineering

+Associate professor, Dept of Computer Science and Engineering

Dayanand Sagar Academy of Technology and Management

Abstract— Building a solution for biometric authentication, such as the one available on some smartphones, that can determine whether the fingerprint applied is real or artificially molded. Fake fingerprint detection refers to recognizing a fingerprint image created by using a fake fingerprint . These situations are causing the most reliable biometric technology which is fingerprint recognition vulnerable. The main objective of this project is about fingerprint spoofing which encompasses misuse caused by the attackers. Fingerprint morphing or techniques like spoofing detection is attributed to the investigation of the finger characteristics to ensure whether the finger is spoofed. The primary objective of this problem statement is to determine if the fingerprint is applied as part of biometric authentication is real or artificially molded. This paper aims to achieve the detection of fake fingerprints using CNN (Convolution Neural Networks) algorithm as the classifier, to classify and map the features of the fingerprints accordingly.

Keywords— Fingerprints, CNN algorithm, detection, feature mapping, anti-spoofing, Machine Learning, LivDet.

1. INTRODUCTION

Nowadays, biometric recognition systems are being 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 behavioral attributes of individuals. The fingerprint is one of the most frequently used authentication systems since they guarantee high identification accuracy, are 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 aloof 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, play-dough, wood glue, etc... In contrast, an indirect attack imposes deep information about the system's module. With the increased amount of attack tools, researchers have been attracted to develop a system that can assess and provide a solution for the liveness detection of fingerprint systems. Figure 1 shows the researches documents proposed in fingerprint biometrics which

has rapidly grown and attracted researchers in the last years.
This type of identification of fingerprints can reduce any type of attacks and helps to keep a safer system comparatively.

This system of detection and storing of fingerprints in a database can be replaced for other regularly used systems to reduce the morphing of even other import documents and make the proofs more private and hence increasing security.

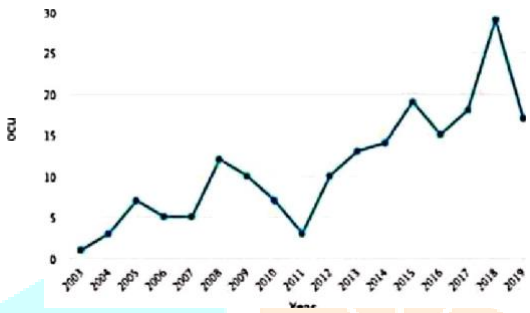

Fig. 1. Graph of documents published per year in the period 2003-2019 matching keywords including biometrics and fingerprint. From Scopus (https://www.scopus.com)

Our purpose is to review the different studies proposed in fingerprint detection systems that can classify real fingerprint images and fake ones.

The remaining sections of this paper are structured as follows:
Section 1 is the introduction, and a background is given in section 2. In section 3, the proposed methodology is presented. Section 4 is the system architecture for the proposed system. Conclusion and fixture work are discussed in section 5. section 6 deals with acknowledgment and section 7 contains the references which is the bibliography.

2. LITERATURE REVIEW

[1], Biometrics technology is an automated recognition system that enables the authentication of an individual based on biological and behavioral characteristics such as the face, iris, gait, voice, fingerprints, etc. Biometric methods are supposed to be a set of secure methods for the identification and authentication of an individual as it has makeable advantages as compared with other methods. But at the same time, biometric systems may be vulnerable to attacks, at each level such as biometric sensor level, data communication, database, etc. These systems are not spoof proof. Recently, some studies summarized the possibility of spoofing recognition systems by artificial biometric samples such as fake fingerprints, artificial iris, facemask, etc.

[2], The Fingerprint Identification system is becoming a commonly used biometric technique with authentication, security, safety, and many other vigilance systems. Unlike other biometric traits such as iris, face, palm, etc., fingerprint identification is the most commonly used technique due to the unique use characteristics of the fingerprint of every individual. This feature makes it the most reliable and preferred method amongst other techniques. Due to its widespread use, researchers have analyzed, the competitive attacks on the fingerprint identification systems including fingerprint ,“Impersonation”. What is Impersonation? - It is a duplicate artificial fingerprint known as “Spoof artifacts” and is presented to a fingerprint sensor to fool the recognition system

[3], Spoofing is a method of attacking biometric systems where artificial objects are presented to a biometric acquisition system that imitates biological and behavioral characteristics; the system is designed the main objective of this project about fingerprint spoofing which encompasses misuse caused by the attackers. Fingerprint spoofing detection is attributed to the investigation of the finger characteristics to ensure whether the finger

is spoofed or live. The various spoofing types are explained and their detection techniques are introduced.

[4] , In this paper the authors have proposed a method wherein: fingerprint spoofing detection and identification have followed the traditional CNN model. A CNN model requires a huge dataset to learn from the training dataset. The fingerprint database used in the proposed work has fingerprint images of just many individuals. Hence, the proposed work has been implemented based on the transfer learning model. Transfer learning is an approach where the model is pre-trained on a huge database of images and the knowledge gained by the model through those images is used for training another set of images. One of the major transfer learning models is ResNet-50CNN's network design consists of multiple layers. Convolutional neural networks are made up of different layers between the layers of input and output. These layers, known as the hidden layers, consist mainly of the Convolutional layer, Pooling layer, and Fully connected layer. In our model, we used the Convolutional layer, pooling layer, fully connected layer, and activation functions.

3. BACKGROUND

In this section, fingerprint image characteristics, the most important features of fake images, and the public liveness datasets are presented.

a. Fingerprint image features

The main step in designing the anti-spoofing fingerprint identification system is to understand the images' features. There are many characteristics of each feature that were proposed hy various studies. Fingerprint general features can be divided into three levels:

1. *Global level:* include global ridgefine. This level is the most used in a classification where the classes can derive from global features.

2. *Local-level:* refers to detail's minutiae derived from the ridge. This level is widely used for the matching process.

3. *Detail level*: consider the intra-ridge details characteristics include: shape, pore, ridge contours, and width. Also, this level is commonly used for fñigerprint matching.

b. Public liveness datasets

The fingerprint is the most widespread biometric; therefore, many public datasets are published to validate the produced recognition system. A few numbers of public datasets containing fake images are available such as LivDet 2009, LiveDet 2011, LivDet 2015, ATVs, and the Chinese Academy of 5cience Institution of Automation (CASIA). A detaded background of some of these datasets is in the next paragraph. LivDet 2015 dataset The Fingerprint Liveness Detection Competition LiveDet 2015 is established to encourage the academic and industrial community to develop anti-spoofing software or hardware. The dataset forms two sub datasets live images, and fake images collected from four sensors. Limited studies had used LivDet 2015 in their system. The figure shows various samples of LivDet 2015 fingerprint images.

Fig 2.For an example of fingerprint images from LivDet 2015, the top row includes live samples; the bottom row includes fake samples. Samples are from Biometric (a) Cross match, (b) Digital Persona, (c) Green Bit, (d) Devices.

c. Convolution Neural Networks (CNN Algorithm)-Working

A Convolutional Neural Network (ConvNet/CNN) is a Deep Learning algorithm that can take in an input image, assign importance (learnable weights and biases) to various aspects/objects in the image, and be able to differentiate onefrom the other. The pre-processing required in a ConvNet is much lower as compared to other classification algorithms. While in primitive methods filters are hand-engineered, with enough training, ConvNets can learn these features/characteristics. The architecture of a ConvNet is analogous to that of the connectivity pattern of Neurons in the Human Brain and was inspired by the organization of the Visual Cortex. Individual neurons respond to stimuli only in a restricted visual field region known as the Receptive Field. Acollection of such fields overlaps to cover the entire visual area.

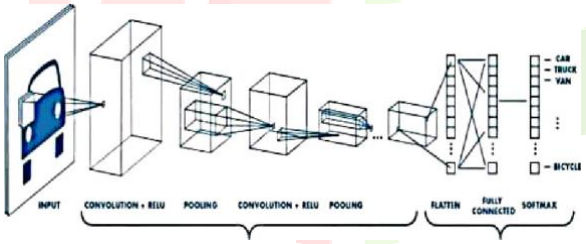

Fig 3: Working of CNN

4. METHODOLOGY

The proposed methodology has 4 basic components namely:

a. Image Acquisition
b. Pre-Processing
c. Feature Extraction and Detection
d. Verification

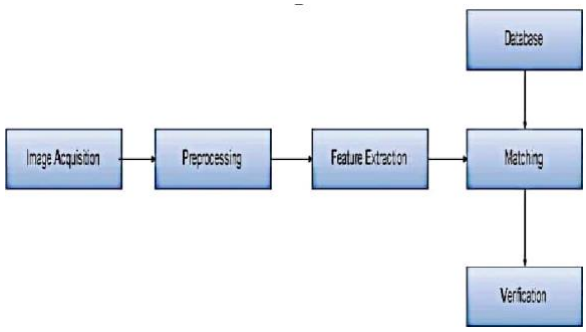

Fig 4: System Flow

4.1 IMAGE ACQUISITION

It is a process where a database is created for conducting experiments on the identification of real or fake fingerprints. In the database fingerprints, data is collected from different age groups which were chosen at random. The main purpose of creating a database is to check the robustness of fingerprint identification and recognition. The database contains various fingerprint images each of 10 fingers images. These are a combination of the original and fake fingerprints of each person respectively.

Fig 5: Real fingerprints(above) and Fake fingerprints (below) correspondingly

4.2.PRE-PROCESSING

Before performing actual operations on the fingerprint images, we must make sure that the images that are present in the database are noise-free images and are ready to undergo the feature extraction process. This can be done by applying noise removal filters. For this, we are using Normalised Box Filter. Let the kernel size be Kheight*Kwidth : If all the elements of a kernel are given unit values, convolving it with an image would mean replacing the pixel values with the sum of its neighbour in the Kheight*Kwidth window. If each element in the kernel is now divided by the kernel size, then the sum of all elements wd1 be 1, the normalized form. Such a convolution would result in pixel values being replaced by the mean or arithmetic average of neighboring pixels in the Kheight*Kwidth window. This effect can be used to achieve smoothness in images. Taking average would mean a reduction in sudden changes in intensity values between neighboring pixels.

Normalized box filter of size 3*3 =

1	1	1
1	1	1
1	1	1

4.3 FEATURE EXTRACTION AND DETECTION

This process is done using the help of the CNN (Convolution Neural Network) algorithm. This algorithm consists of 5 layers namely :

1. Convolution Layer
2. Pooling Layer
3. Fully Connected Layer
4. Activation Functions

4.3.1 Convolution Layer

This layer is the first layer that is used to extract the various features from the input images of fingerprints which are in RGB format. In this layer, the mathematical operation of convolution is performed between the input image and a filter of a particular size MxM. By sliding the filter over the input image, the dot product is taken between the filter and the parts of the input image concerning the size of the filtes (MxM). The output is termed as the Feature map which gives us information about the image such as the corners and edges. Later, this feature map is fed to other layers to learn several other input image features.

Fig 6: Real image (left) Convoluted image (right)

4.3.2 Pooling Layer

The primary aim of this layer is to decrease the size of the convolved feature map to reduce computational costs. This is performed by decreasing the connections between layers and independently operating on each feature map. Depending upon the method used, there are several types of Pooling operations. In Max Pooling, the largest element is taken from the feature map. Average Pooling calculates the average of the elements in a predefined sized Image section. The total sum of the elements in the predefined section is computed in Sum Pooling. The Pooling Layer usually serves as a bridge between the Convolutional Layer and the FC Layer

Fig 7: Original image versus pooled image

Fig 9: Final size of the image

4.3.3 Fully Connected Layer

The Fully Connected (FC) layer consists of the weights and biases along with the neurons and is use8 to connect the neurons between two different layers. These layers are usually placed before the output layer and form the last few layers of a CNN Architecture. In this, the input image from the previous layers is flattened and fed to the FC layer. The flattened vector then undergoes a few more FC layers where the operations of the mathematical function usually take place. In this stage, the classification process begins to take place.

Every part of this flattened image such as ridges, loops, spacing, etc. is compared with the original image and hence features are extracted and learned by the system.

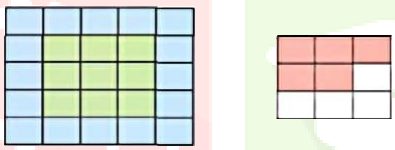

Fig 8: Feature Mapping

Finally, the convoluted image is given back as the output. This site is such that it is the right size for original and convoluted size.

4.3.4 Activation Functions

Finally, one of the most important parameters of the CNN model is the activation function. They are used to learn and approximate any kind of continuous and complex relationship between variables of the network. In simple words, it decides which information of the model should fire in the forward direction and which ones should not at the end of the network. It adds non-linearity to the network. There are several commonly used activation functions such as the ReLU, Sofimax, tanH, and the Sigmoid functions. Each of these functions has a specific usage. For a binary classification CNN model, sigmoid and softmax functions are preferred and for multi-class classification, generally, softmax is used.

5. SYSTEM ARCHITECTURE

Module 1:- The system should image process

Module 2:- The system should be Detecting the fingerprint

Module 3:- The system should recognize the fingerprint concerning the traded data

Module 4:- The system should automatically update to the database

How to process images: In which format the dataset should be entered and will be accepted and what corresponding output it will provide to us.

Detection of fake images using CNN (Convolution Neural Networks) by identification of features of fingerprints such as loops, grooves, ridges, spacing, line allocation, etc.

Recognizing Fake fingerprints using the above features as per the trained data to give desirable outputs.

Updating the databases.

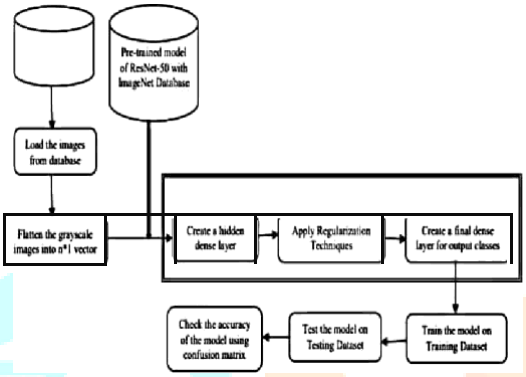

Fig 10: System Architecture

Increasing the accuracy to 91% and above helps in easy and clear distinguishing between the real and fake fingerprint analysis.

6.CONCLUSION

In this paper, a system that can detect artificially moulded fingerprints is proposed. This can be achieved using the CNN algorithm and its feature extraction mechanism. The image is magnified and each feature is carefully mapped and hence also increasing the accuracy to 90% and above for efficient and non-doubtable results.

7.ACKNOWLEDGEMENT

We would like to express our utmost gratitude to our respected principal Dr. Ravi Shankar M and HOD of the CSE Dr. C Nandini, extend our thanks to our beloved guide Dr. V Keerthika for allowing us to showcase our project and research work.

REFERENCES

[1] Diaa M. Uliyan, Somayeh Sadeghi, Hamid A. Jalab "Anti-spoofing method for fingerprint recognition using patch-based deep learning machine, 201S ELSEVIER paper"

[2] Shivanand Gornale, Abhijit Patil "Fingerprint based Gender Identification using Discrete Wavelet Transform and Gabor Filters , 2016 paper from INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS"

[3] H. I. Wahhab arid A.N. Alanssari "Fingerprint Spoofing Detection Using Machine Learning 2020 paper from IEEE"

[4] T. Chugh, K. Cao, and A. Jain "Fingerprint generation and presentation attack detection using deep neural networks 2019 IEEE paper"

[5] Anil K. Jain, Karthik Nandakumar, Xiaoguang Lu, "Integrating Faces, Fingerprints, and Soft Biometric Traits for user Recognition 2019 IEEE paper"

[6]https://towardsdatascience.com/acomprehensive-guide-to-convoliitional-neuraInetworks-the-eli5-way-3bd2b1164a53

[7]https://www.sciencedirect.com/science/article/pii/S2215B98619300527