MACHINE LEARNING FOR DETECTING FINGERPRINT SPOOFING

Prof. Liya Naiju[1], Tejas M[2], Shourya Gowda K V[3], Yadav S G[4], Swathi M K[5], Vaidhyanath A V[6]

Article History: Received: 15.08.2022 **Revised:** 16.10.2022 **Accepted:** 22.12.2022

Abstract

Numerous investigations have given liveness finger impression discovery programmes using a variety of strategies. Our study will analyse numerous tests that are suggested in liveness finger impression location frameworks that may distinguish between real and fake unique mark images utilising AI techniques. Considering certain measures, The datasets utilised in the literature were compared. The findings imply that BSIF and LPQ are the most noteworthy highlights. Support vector machine (SVM) calculations were frequently used as a classifier. Fingerprint, liveness discovery, biometrics that are resistant to parodying, security, and machine learning are all watchwords.

[1]Asst. Professor, Department of MCA, The Oxford College of Engineering, Bengaluru, Karnataka, India – 560068
[2,3,4,5,6]MCA Final Year, Department of MCA, The Oxford College of Engineering, Bengaluru, Karnataka, India – 560068

Email: [1]liyawilsonk@gmail.com

DOI: 10.31838/ecb/2022.11.12.58

1. Introduction

Frameworks for biometric recognition are already being used in the variety of industries for differentiating proof.due to its effectiveness and simplicity when compared to earlier strategies like a secret phrase. In biometrics recognition frameworks, social and physiological credits are taken into account [1The finger imprint is one of the most often used verification frameworks because it ensures high exactness of the distinguishing proof, is cost-effective, and can be used on large datasets of photographs. Due to these characteristics, finger impression recognition frameworks can be used for a variety of purposes, such as participation.. Examples of recognisable proof include the legal sciences, healthcare systems, banking, and so forth. On the other hand, those frameworks are not immune to malicious attacks.

The two sorts of attacks that biometrics are susceptible to are direct and indirect assaults.
[2]. Since no information is expected to direct the attack, direct assault is the most often identifiable sort of assault. For the specific mark recognition framework, the sensor device can be manipulated with the help of straightforward and useful objects as silicon, play-doh, wood sticks, and others. Unexpectedly, a diversionary attack uncovers a lot of information concerning the framework's module. Scientists have worked to develop a framework that can evaluate and provide a solution for liveness identification of finger imprints as the number of assault devices has expanded.

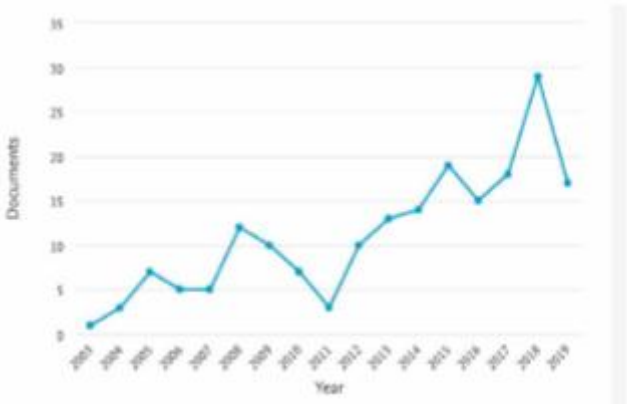

Fig. 1. Graph of documents published each year from 2003 to 2019 that contain the terms "biometrics" and "fingerprint." originating from Scopus (www.scopus.com)

Figure 2 classifies the many suggested study types for fingerprint liveness detection. As may be seen, survey papers have no published research.

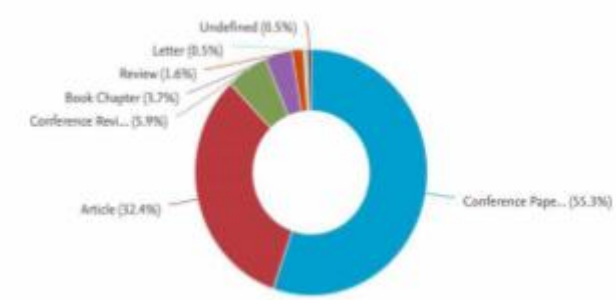

Fig. 2 shows a classification of published publications from 2003 to 2019 that contain the keywords "biometrics," "liveness," and "fingerprint." Scopus (https://www.scopus.com) claimsFoundation

Liveness finger impression location frameworks provide a comprehensive range of tests to organise real and false unique mark images.
The following are the remaining sections of this work: Section I has the presentation, and Section II contains the foundation. In Region III, a writing audit is in use. The fourth category includes research and affiliation. Area V contains the conversation. The work's conclusion and future objectives are covered in Area VI.
1. Take into account the global ridgeline. In a hierarchy where classes can gain from global highlights, this level is the one that is most frequently employed.
2. Nearby level: references to ostensibly unimportant information gathered from the edge At

this level, the matching mechanism is frequently employed.
3. Detailedness: Form, porosity, edge shapes, and width are intra-edge characteristics that need to be taken into account. Additionally, level is frequently used to coordinate finger impressions. public datasets on liveliness (a). The provided acknowledgment mechanism is validated using numerous public datasets because the finger imprint is the most widely employed biometricSeveral publicly available datasets with fraudulent photographs (CASIA) include LivDet 2009, LiveDet 2011, LivDet 2015, ATVS, and the Chinese Academy of Science Institution of Automation. A part of these datasets are supported by an itemised basis in the accompanying text.
2015's LivDet: Dataset The Battle for Liveness Detection in Fingerprints An initiative called LiveDet 2015 attempts to give students and the wider public the tools they need to combat mocking software and hardware [6]. Live photos and false pictures are two sub-datasets of the dataset obtained from four sensors. exam restrictions
Wood glue with Ecoflex Samples of actual and false photographs from the ATVS dataset are shown in Figure 3.

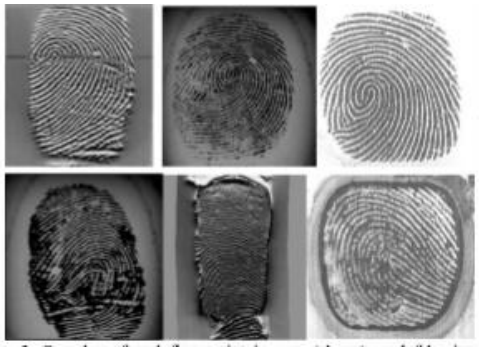

Fig. 3. Examples of phoney fingerprint images (below) and real fingerprint images (above) from the ATVS dataset.

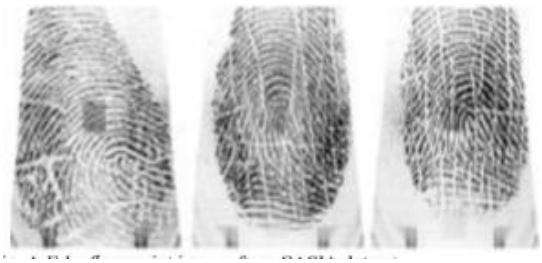

Fig. 4. Images of fake fingerprints from the CASIA dataset

Figure 5: An illustration of a fingerprint scan from LivDet 2015, with authentic samples at the top and fake ones at the bottom. The following Biometrika samples are available: Crossmatch, Digital Persona, Green Bit, and Devices.

Literature

A .Unique finger impression

Structures for recognising Numerous research have examined the validity of fingerprint differentiation. In addition, the model can be used to improve the security of finger impression scanners by identifying attacks on scanners brought on by replacing the scanner hardware or the product; this problem has become widely prevalent on mobile devices and personal computers. The developers of

[8,] developed a model that can extract an instance of a distinctive mark and compare it to an instance. 22 distinct mark scanners produced identical results.The rate of error in these model approval findings is considerable. [9] suggested a unique convolutional brain network (CNN) model based on a convolutional brain networks (CNN) with four convolutional layers, three maxpooling layers, and three totally associated layers. The prototype had prepared and trained. A finger imprint recognisable proof calculation was directed in light of the wave iotas strategy for highlight extraction, which does not rely on the image quality measurement or picture upgrading to lessen the misleading choice. The datasets employed FCV2002 unique mark datasets, dividing each image into groups of 16 images to account for wave particle variation. Different finger imprint images were arranged using SVM computations. The model presented herself beautifully. [13] suggested revising the pre-handling procedure's use of images to enhance the photographs.Binarization is the division of an image into a foundation and a frame. employing a thresholding method, a closer look. They performed a comparative examination of local and global thresholding and offered an adaptable approach to nearby thresholding in this review. The datasets that were used were FVC2000 and FingerDOS. Both the time usage and image quality of the outcomes of the computation are better. According to [14], a calculation known as idle finger impression division foresees dividing elements from local approaches of the distinctive finger impression picture, allowing the spotlights to examine frontal edge and foundation commotion. These elements include saliency, image force, inclination, edge, and others. quality. Random Choice The layout was done using the AI algorithm called Forest. the preparation and testing of the IIIT-D CLF, the model NIST SD-4 inked print dataset, and the NIST SD-27 Using the inactive dataset, the expression state and computation outputs of the idle model were calculated and compared. Scaling the unique mark image to 60*60 pixels in the component extraction stage allowed [15] to use a straightforward parallel example. After being resized, the photos were binarized with a limit esteem and split into nine equal halves. For, it is found that the straight paired design the squares. The order is the subsequent phase, and for this step, two AI systems—neural organisation and nearest neighbour classifiers—were employed. They built and tested the model using the datasets FVC200214 and FVC200415. The accuracy of the brain network's performance was higher than that of the closest neighbour classifier, according to the results.

B . Mocking Fingerprint

With the Help of Machine Learning, Recognition As a result of the rise in artificial reasoning, particularly AI, the biometric identification framework has employed AI to raise their accuracy grouping frameworks between liveness and mocking photographs. For instance, analysts evaluate each study's presentation accuracy, pinpoint the most reliable component in each dataset, and pinpoint the generally reliable elements in [18]. In addition to looking at three different datasets of fictitious fingerprint photos, they also look at a variety of well-known materials that are used to make fingerprints. They then arrange these using the AI classifier algorithm SVM. Another strategy that uses deep learning to identify the mocking fingerprints left by different materials [19] and includes: play mixture, wood stick, and gelatin. A patch-based deep learning system and a Discriminative Restrictedclassifier were used to generate the model. DRBM and DBM are two types of Boltzmann machines. They enlisted the help of KNN.utilization. Likewise, in [20] a review intends to identify counterfeit finger impression pictures, with a serious level of exactness, and break down the impact of standardization on two sensors from various finger impression pictures. A liveness location model was suggested by [21] as a means of avoiding the creation of differentiating evidence. The model had extracted the highlights using the multi-scale LPQ. Due to the extensive stacking of the removed bits, which increased complexity and required more memory, they employed PCA to mitigate these problems. After lowering the extricated highlights vector, they developed the model using the SVM classifier, and they tested it to assess the show. The findings show an increase in accuracy. Another demeaning framework was put up by [22] to fix the aim gap and incapacity of conventional frameworks to remove important data from the acquired image, which is a defect. Their strategy included two new The first section, profundity doublepeak, demonstrated that the 1D profundity signal should only have two summits to replicate the two-fold pinnacle structure of actual fingertip skin. The following is subsingle-top, assuming that there should be a peak in the 1D depth signal recorded before the largest pinnacle, acknowledging the additional layer covered on a genuine finger. They use four datasets to test their strategies. The investigation's findings demonstrate how accurate and useful their paradigm is.

Correlationand Analysis

The second dataset character uses a warm sensor in contrast to the first dataset character's optical sensor. The dataset was compiled using ATVS's open data. It is suggested to use a min-max standardisation technique to present fake unique mark pictures with different sensor settings. They

examine the effects of standardisation using the GLCM (Grey Level Co-Occurrence Matrix) image, which combines KNN (K-Nearest Neighbour), SVM (Support Vector Machine), and NN (Nearest Neighbour) (Neural Network) approaches. This review found increased

Conversation

The key conclusions and limitations of the audit are listed below. The binarized factual picture features BSIF and LPQ were employed by four models [14] [16] [27] [28] to extract the components from parodying frameworks. The GLCM include extraction strategy was used in one model [13]. The most often utilised datasets in the audited models are LiveDet 2011 and LiveDet 2013. [11] [12] [14] [16] [27] [28]. A phoney picture was delivered as a result of the use of several sensors and caricature materials. To improve precision, the preparation model makes use of several datasets. In [11], LivDet 13, ATVS, and CASIA were used. LivDet 09, integrated, [27] [28] 11 LivDet, and 12 LivDet

Table I: Comparison of Spoofing Fingerprint Recognition Models Using Machine Learning

Reference	Feature extraction used	Dataset	Machine learning	Performance Metrics	Limitations
[11]	▪ Spatial domain ▪ Detailed ridge ▪ Fourier spectrum	▪ LivDet 2013 ▪ ATVS ▪ CASIA	SVM	The Accuracy (ACC) for: ▪ LivDet 2013: 99% ▪ ATVS: 100%	No other metrics found
[12]	▪ Shape ▪ Consistancy from different rotation angles.	▪ LivDet 2013 ▪ LivDet 2015	▪ deep learning ▪ KNN	Equal Error Rate (ERR): 1e -7	Time complexity
[13]	GrayLevelCo-OccurnceMatrix (GLCM)	▪ FO ▪ FC	▪ SVM ▪ KNN ▪ NN	SVM ACC for FO = 93.21% SVM ACC for FC = 84.93% KNN ACC for FO = 88.62% KNN ACC for FC = 80.89% NN ACC for FO = 98.54% NN ACC for FO = 88.05%	▪ No other metrics found ▪ Low Accuracy
[14]	▪ WT ▪ LPQ ▪ PCA	LivDet 2011	SVM	Average classification error (ACE) = 8.625 %	▪ No other metrics found
[16]	▪ LPQ ▪ LBP ▪ BSIF	LivDet 2011	SVM	Total Error Rate (TER)= 5.20%	▪ Misclassified live images with low quality and fake images with high quality ▪ No other metrics found
[17]	Convolutional Naural Network (CNN-F)	LivDet 2009	SVM	ACC= 99.964%	No other metrics found
[18]	▪ Deviation ▪ Varriance ▪ Skewness ▪ Kurtosis ▪ Hyperskewness ▪ Hyperflatness	ATVS-FFp	SVM	▪ ACC = 99.03% ▪ FAR = 0.794% ▪ FRR = 0.176%	Small Dataset

Table Ii: Public Databases Used In The Literature Review For Liveness Fingerprint Recognition

Study Reference	Dataset	Scanner	Image Size	Spoofing Materials	Samples Number
[17],[21], [22]	LivDet 2009	Biometrika	312×372	Silicone	1993(Fake) 2000(Live)
		CrossMatch	640×480	▪ Gelatine ▪ Play Doh ▪ Silicone	4000(Fake) 4000(Live)
		Identix	720×720	▪ Gelatine ▪ Play Doh ▪ Silicone	3000(Fake) 3000(Live)
[14], [16] , [21] , [22]	LivDet 2011	Biometrika	312×372	▪ Wood glue ▪ Latex ▪ Gelatine ▪ Ecoflex ▪ Silgum	2000(Fake) 2000Live
		Digital Persona	355×391	▪ Gelatine ▪ Play Doh ▪ Silicone ▪ Wood glue ▪ Latex	2004(Fake) 2000Live
		Italdata	640×480	▪ Wood glue ▪ Latex ▪ Gelatine ▪ Ecoflex ▪ Silgum	2000(Fake) 2000Live
		Sagem	352×384	▪ Wood glue ▪ Latex ▪ Gelatine ▪ Ecoflex ▪ Silicone	2008(Fake) 2000Live
[11],[13],[21],[22]	LivDet 2013	Biometrika	312×372	▪ Wood glue ▪ Latex	2400 (Fake)

2. Conclusion and Future Work

The purpose of this paper is to review current machine learning-based fingerprint identification techniques and anti-spoofing strategies. A number of datasets and these models has been compared. The machine learning classifier used most frequently in literary analysis models is the SVM. The LivDet2011 and LivDet2013 datasets were used more frequently throughout the training and testing phases than the other datasets examined in the literature research. Future suggestions for identifying and classifying false fingerprints will be based on machine learning and fresh public liveness fingerprint datasets.

3. References

1. Comp. Tech. Auto. Contr. Rad. Electro., Vol. 18, No. 1, pp. 140–147, "Survey of Primary Methods of Fingerprint Feature Extraction," 2018.

2. "Biometric System Attacks: An Overview," International Journal of Advanced Scientific Research, Vol. 1, No. 7, 2015, pp. 283-288. R. Jain and C. Kant.
3. M. Galar et al. (2015) Knowledge-Based Sys., Vol. 81, p. 76–97.
4. "RaspiReader: OpenSource Fingerprint Reader," page IEEE T Pattern Analytical Machine Intelligence, Vol. 41, No. 10, 2019; pp. 2511–2524.
5. V. Mura and colleagues, "LivDet 2015 fingerprint liveness detection competition 2015," IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2015, pp. 1-6.