IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96124

Fingerprint spoofing detection using convolution neural network

Pooja Wadageri[1], Vidya S[2]

[*1]Dept. of MCA, Bangalore Institute of Technology, Bengaluru, India.

[2]Dept. of MCA, Assistant Professor, Bangalore Institute of Technology, Bengaluru, India.

Abstract: Various tactics had been used in many studies to give liveness finger impression discovery programmes. This paper will examine the various tests proposed in liveness finger impression location frameworks that are capable of separating genuine and phoney unique mark photographs using AI procedures, as well as dissect various plans. In light of explicit measurements, a contrast of produced the datasets used in the literature. The outcomes suggest that the most notable highlights are LPQ and BSIF. back-end vector machine computations (BVM) were extensively employed as a classifier.

Keywords: Fingerprint, liveness discovery, biometrics that are resistant to parodying,security, and machine learning are all watchwords

1. INTRODUCTION

Biometric recognition frameworks are already being applied in a range of distinguishing proof fields Because of its simplicity and strength when compared to previous approaches such as a secret word. People's physiological and social credits are used in biometrics recognition frameworks.[1] One of the most often employed verification frameworks is the finger impression. because it ensures high distinguishing proof exactness, is economical, and could be used on large images from datasets. These characteristics allow finger impression recognition frameworks to be used in a variety of applications, such as participation. Legal sciences, medical care frameworks, banks, and so on are all examples of identifiable proof. Those frameworks, on the other hand, are not impervious to spiteful attacks. Direct and indirect attacks are the two types of assaults against which biometrics are vulnerable.[2] Because No data is anticipated to guide the attack, direct assault is the most commonly recognised. It is possible to act in the sensor device using simple and convenient instruments such as Play-doh, wood, silicon, and other materials for the unique mark recognition framework... Surprisingly, roundabout assault elicits extensive information regarding the framework's module. Scientists have tried to create a system that can evaluate and supply a remedy for determining a finger's liveness impressions as the number of assault instruments has grown.

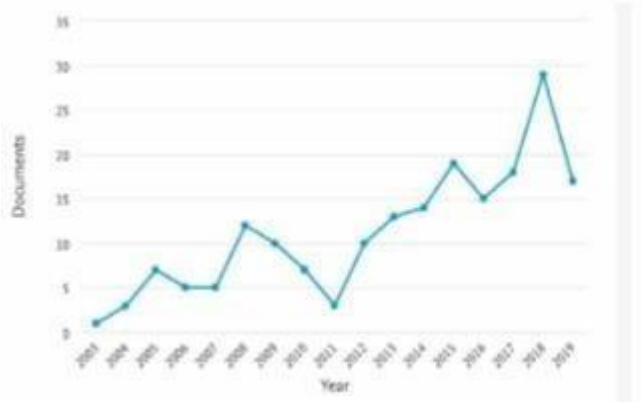


Fig. 1 shows a graph of the number of documents published each year between 2003 and 2019 that had the keywords "Fingerprint" and "biometrics." originating Through Scopus (www.scopus.com).

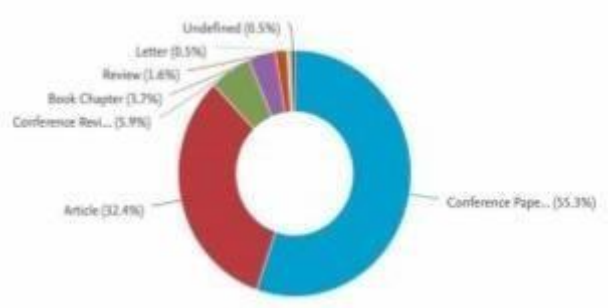
IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96124

Figure 2 identifies the various proposed research projects in the field of Liveness detection forfingerprints, where it is



apparent not been published research projects have been done for survey papers.

Fig. 2The classification of published publications from 2003 to 2019 is shown in a pie chart using terms like "biometrics," "fingerprint" and "liveness." The Scopus website (https://www.scopus.com) claims.

1.Foundation

In order to arrange real and fake unique mark images, liveness finger impression location frameworks offer a wide range of tests.

The rest of sections to this piece of work are as follows: The presentation is in section I, while the basis is in section II. A writing audit is put into practise in Region III. Study and association make up the fourth category. The discourse is in Area V. Area VI discusses the work's completion and its goals going forward.

1. **On a global scale**: the global ridgeline,In a hierarchy where classes can be gain from aglobal highlights, this level is the one that is most frequently employed.
2. **The closest level**: allusions to trivial information gleaned from the edge At this level, thematching mechanism is frequently employed.
3. **Detailedness:** Form, porosity, edge shapes, and width are intra-edge characteristics that needto be taken into account. Additionally, level is frequently used to coordinate finger impressions.

public datasets on liveliness (a). Given that the finger imprint is the most widely used biometric, the provided acknowledgment system is validated using a number of public datasets. A few examples of publicly available datasets using fake images are LivDet 2009 ATVS, LiveDet 2011, LiveDet 2015, Chinese Academy of Science Automated Institute, and (CASAI)). The text that goes with these datasets provides an itemised foundation for a portion of them.

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 datasets that are subsets obtained using four sensors. exam restrictions Ecoflex and glueing wood Figure 3 display samples of the actual and false photos taken from the dataset for ATVS.

Figure 3. From the ATVS dataset, examples of authentic fingerprint photos (Above) and phoney pictures (below).

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96124

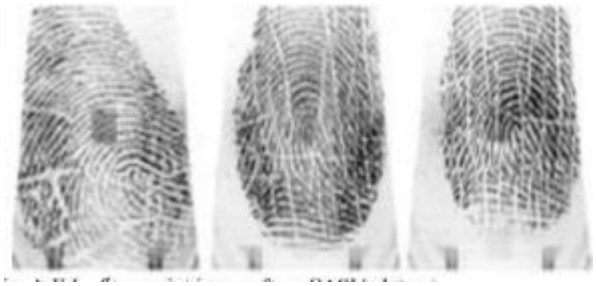


Fig. 4 shows counterfeit fingerprint pictures from the CASAI dataset.

Figure 5: A example of LivDet 2015 fingerprint scans, with real samples up top and fraudulent ones down below. (a) Crossmatch, (b) Digitized Persona, (c) Green Bit, and (d) Allof the Biometrika devices are samples.

2. LITERATURE SURVEY

A. A distinctive fingerprint

Frameworks for recognition the validation of fingerprint distinction has been the subject of several studies. In[8] a model was developed that can extract an instance of a distinctive mark and contrast it with an additional instance; Additionally, by identifying attacks on scanners brought on by swapping either the scanner's components or its product—a problem that has become widespread on PCs and mobile devices— The method can be utilised to increase the finger security imprint scanners. 22 distinct mark scanners produced identical results. The rate of error in these model approval findings is considerable. [9] developed a novel convolutional neural network (CNN) model based on convolutional brain networks that has three maxpooling layers, three completely associated layers, and four convolutional layers (CNN).

The prototype had prepared and trained. Given that the wave iotas approach to highlight extraction does not rely on image quality metrics or picture enhancement to lessen the likelihood of making a mistaken choice, [12] calculated with a fingerprint identification confirmation. 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] a review was advised to enhance the pre-handling procedure's utilisation of photos. Binarization is the thresholding-based separation of a picture into a foundation and a closer look. They performed a comparative examination of local and global thresholding and offered an adaptableapproach to nearby thresholding in this review. The datasets that were used were FingerDOS and FVC2000.

The calculation has produced better results with regard to timing usage and picture quality. In

[14] The highlights can investigate the forefront edge and foundation turmoil using a calculation known as division of idle finger impressions, which anticipates separating components from the neighbourhood methods of the distinctive finger impression image. Saliency, image force, inclination, edge, and quality are some of those components. Random Decision Forest was an AI algorithm that was used for layout. the model NIST SD-4 inked print dataset, NIST SD-27, and IIIT-D CLF preparation and testing The idle model's expression state and computation outputs were estimated and compared while using the inactive dataset. [15] scaled the image of the distinctive mark to 60*60 pixels in the component extraction stage to provide a clear parallel example. After being resized, the photos were binarized with a limit esteem and split into nineequal halves. For each square, the straight- paired pattern may be found. The order is the subsequent phase, and for during this stage, two AI systems—neural organisation and nearest local classifiers —were employed. They built and tested the model using the datasets FVC200214 and FVC200415. The accuracy of the brain network's

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96124

performance was higher than that of the closest neighbour classifier, according to the data.

B. Mocking Fingerprint

Recognition With the Aid of Machine Learning the framework for biometric recognition has used AI to increase their accuracy grouping frameworks between vibrant and mocking photos as a result of the rise in artificial reasoning, particularly AI. Analysts analyse the presentation accuracy for each study, for instance, and identify the most solid element for each dataset as well as the typical solid elements in [18]. They examine three separate datasets of fake

fingerprint images as well as a number of well-known materials used in fingerprint creation, and they arrange them using the AI classifier computation SVM. A different model built using deep learning [19], The sarcastic fingerprints made by different materials, such as play mixture, wood sticks, and gelatin, are identified. A patch-based deep learning machine and a Discriminative Specialized classifier were used to generate the model. Boltzmann machines come in the DRBM and DBM varieties. Utilizing, they enlisted KNN's assistance. Similarly, in [20] A review aims to dissect the effects of standardisation on two sensors from various finger impression photos in order to accurately recognise fake finger impression images..

A model of liveness presented by [21] to refrain from producing differentiating proof. The model had extracted the highlights using the multi-scale LPQ. They used PCA to mitigate thesedrawbacks due to the significant layering of the deleted parts, which increased complexity and demanded more memory. They created the model using the SVM classifier after reducing the extricated highlights vector, and then they put it to test to evaluate the exhibition. The results reveal an increase in precision. Another structure for mocking the enemy had been suggested by [22] to overcome the flaw in the standard frameworks that is a gap in the aim and cannot eliminate significant details from the captured picture. Two fresh methods for highlight extraction were added in their framework.

The first part, called intensity doublepeak, demonstrated that the 1D profundity signal should have just two summits., imitating the dual summit structure of actual fingernail skin. Assuming that there should be a peak in the 1D depth signal recorded prior to the biggest pinnacle, this acknowledges the additional layer that a real finger has covered., the following issubsingle-top. They test their methods using four datasets. The results of the inquiry show how precise and productive their paradigm is. To separate the mocking finger impression, it had used a different gradual learning process as opposed to the retraining method mentioned by [23]. SVM was used for the grouping process.

Table I: ANALYSIS OF FINGERPRINT RECOGNITION MODELS FORSPOOFING 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 ▪ Consistency from different rotation angles.	▪ LivDet 2013 ▪ LivDet 2015	▪ deep learning ▪ KNN	Equal Error Rate (ERR): 1e -7	Time complexity
[13]	GrayLevelCo-OccuranceMatrix (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 Neural Network (CNN-F)	LivDet 2009	SVM	ACC= 99.964%	No other metrics found
[18]	▪ Deviation ▪ Variance ▪ Skewness ▪ Kurtosis ▪ Hyperskewness ▪ Hyperflatness	ATVS-FFp	SVM	▪ ACC = 99.03% ▪ FAR = 0.794% ▪ FRR = 0.176%	Small Dataset

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96124

Table II: PUBLIC DATABASES USED IN THE LITERATUREREVIEW 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) 2000(Live
		Digital Persona	355×391	▪ Gelatine ▪ Play Doh ▪ Silicone ▪ Wood glue ▪ Latex	2004(Fake) 2000(Live
		Italdata	640×480	▪ Wood glue ▪ Latex ▪ Gelatine ▪ Ecoflex ▪ Silgum	2000(Fake) 2000(Live
		Sagem	352×384	▪ Wood glue ▪ Latex ▪ Gelatine ▪ Ecoflex ▪ Silicone	2008(Fake) 2000(Live
[11],[13],[21],[22]	LivDet 2013	Biometrika	312×372	▪ Wood glue ▪ Latex	2400 (Fake)

3. EXISTING SYSTEM

ID of a live finger impression picture is a significant test these days. Prior scientists proposed approaches on parody recognition utilizing close-set techniques. These techniques bound themto bomb under a specific condition. One of limit is presence of Type-I blunder, parody named live, which isn't really great for basic framework. In ongoing history, FPAD execution turned out in an assortment of the structure. Revealed examinations recommend a triple expansion in the mistake paces of unique finger impression parody finders while parodies utilizing the testing produces fresh materials or functional stage. This implies the speculation ability of existing finger impression parody finders is restricted across materials.

4. PROPOSED SYSTEM

Attacks increasingly come in "endless variety" and "realistic-looking" forms known as false fingerprint presentations as attack mechanisms continue to evolve. The work uses a person- specific live sample, in contrast to the existing techniques, to extract the liveness attribute. Thelive-sample has a built-in liveness feature, and several live samples that are enrolled or collected throughout time are put through tests to measure the liveness of each finger, which isreferred to as a "Transient Live Feature." Numerous live fingerprint samples will function better, proving the fingerprint PAD system's authenticity. The entire PAD community can benefit from this endeavour, which is essential and one of this work's most important contributions. With this gathered liveness data, referred to as the "Transient Liveness Factor" (TLF),It was demonstrated that a straightforward model could predict if an assault would occuron a test pictures. Here, the liveliness features of the various live samples of a particular person are drawn from the common data collection, numerous sets of independent characteristics are quantified, and then these characteristics are connected with conventional artificial intelligence techniques.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96124

5. CONCLUSION

Reviewing current machine learning-based fingerprint recognition methods and anti-spoofing tactics is the aim of this work. These models and a variety of datasets had been compared. The SVM is the machine learning classifier that is most frequently employed in literary analysis models. Compared to comparable datasets discussed in the literature analysis, the LivDet2011 and LivDet2013 datasets were employed during the instruction and examination phases. The use of fresh public liveness fingerprint datasets will be made possible by an AI-based methodology that will be proposed in the future for detecting and classifying fake fingerprints**.**

REFERENCES:

1] H. I. Wahhab, and A.N. Alanssari, "Survey of Primary Methods of Fingerprint Feature Extraction", Comp. Tech. Auto. Contr. Rad. Electro., Vol.18, No.1, pp.140-147, 2018.
2] R. Jain, C. Kant, "Attacks on Biometric Systems: An Overview", Int. J Adva. Scient. Research, Vol.1, No.7, pp. 283-288, 2015
3] M. Galar et al., "A survey of fingerprint classification Part I- Taxonomies on feature extraction methods and learning models", Knowledge-Based Sys., Vol.81, pp.76-97, 2015.
4] J. J. Engelsma, K. Cao, and A. K. Jain, "RaspiReader: Open Source Fingerprint Reader", IEEE T Pattern Anal. Mach. Intell., Vol.41, No.10, pp.2511-2524, 2019.
5] V. Mura , "LivDet 2015 fingerprint liveness detection competition 2015", in 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp.1-6, 2015
6] J. Galbally, S. Marcel, and J. Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition", IEEE T Imag. Proces., Vol.23, No.2, pp.710-724, 2014.
7] X. Guo , F. Wu, and X. Tang, "Fingerprint Pattern Identification And Classification", 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), pp. 1045-1050, 2018.
8] X. Guo , F. Wu, and X. Tang, "Fingerprint Pattern Identification And Classification", 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), pp. 1045-1050, 2018.
9] S. R. Borra, G. J. Reddy, E. S. Reddy, "Classification of fingerprint images with the aid of morphological operation and AGNN classifier", Applied Computing and Informatics, Vol.14,No.2, pp.166-176, 2018.
10] S. Fahman , "Classification of Live Scanned Fingerprints using Histogram of Gradient Descriptor", 21st Saudi Computer Society National Computer Conference (NCC), pp.1-5, 2018.
11] L. Boutella, and A. Serir, "Fingerprint Identification by Wave atoms Transform and SVM",International Conference on Advanced Systems and Electric Technologies, pp.301-306, 2017.
12] M. B. Patel, "Performance Improvement in Binarization for Finger", IOSR J Comp. Eng.(IOSR-JCE), Vol.19, No.3, pp.68-74, 2017.
13] A. Sankaran, "Adaptive latent fingerprint segmentation using feature selection and random decision forest classification", Information Fusion, Vol.34, pp.1-15, 2017.
14] A. T. Gowthami, and H. R. Mamatha "Fingerprint Recognition Using Zone Based Linear Binary Patterns", Second International Symposium on Computer Vision and the Internet (VisionNet'15), Vol.58, pp.552-557, 2015.
15] R. P. Krish, "Improving automated latent fingerprint identification using extended minutia types", Information Fusion, Vol.50, pp.9-19, 2019.
16] S. Khade, S. D. Thepade, and A. Ambedkar, "Fingerprint Liveness Detection Using Directional Ridge Frequency with Machine Learning Classifiers", in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA).pp.1-5, 2018.
17] Q. Huang, S. Chang, C. Liu, B. Niu, M. Tang, and Z. Zhou, "An evaluation of fake fingerprint datasets utilizing SVM classification", Patt. Recogn. Lett., pp.1-7, 2015.
18] D. M. Uliyan, S. Sadeghi, and H. A. Jalab, "Anti-spoofing method for fingerprint recognitionusing patch based deep learning machine", Eng. Sci. Tech., an International Journal, 2019.
19] S. Nuraisha, and G. F. Shidik, "Evaluation of Normalization in Fake Fingerprint Detection with Heterogeneous Sensor", in 2018 International Seminar on Application for Technology of Information and Communication. pp.83-86, 2018.
20] Y. Chengsheng, X. Sun, and L. Rui, "Fingerprint liveness detection based on multi-scale LPQ and PCA", China Communications, Vol.13, No.7, pp.60-65, 2016.
21] F. Liu, G. Liu, and X. Wang, "High-accurate and robust fingerprint antispoofing system using Optical Coherence Tomography", Expe. Sys. Appl., Vol.130, pp.31-44, 2019.
22] J. B. Kho, "An incremental learning method for spoof fingerprint detection", Expe. Sys. Appl., Vol.116, pp.52-64, 2019.

