IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 4, April 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204207 |

Spoof Detection for Fingerprint Recognition Based on Deep Learning

M Sujitha[1], R Ayyappa[2], V Parthasaradi[3]

PG Student, Department of Electronics and Communication Engineering, E.G.S Pillay Engineering College, Nagapattinam, India[1].

Assistant Professor, Department of Electronics and Communication Engineering, E.G.S Pillay Engineering College, Nagapattinam, India [2].

Assistant Professor and Head , Department of Electronics And Communication Engineering, E.G.S Pillay Engineering College, Nagapattinam, India [3]

ABSTRACT: Nowadays the identity theft is increased. The Fingerprint Based Biometric System is have a great importance in secured system The Forgets violate them by Presenting Fabricated attempts For example. Artificial Fingerprint s are made by silicone molds, gelatin and play-doh these materials are may be illegally used for identity frauds by malicious users This process is called spoofing. Some of the existing Methods using Handcrafted descriptors have been implemented for assuring user presence it gives the low accuracy rate in recognition. The proposed method used Discriminative Restricted Boltzmann machine to recognize Fingerprint accurately against Fabricated materials for spoofing

KEYWORDS – Fingerprint, patch based deep learning, spoofing, Restricted Boltzmann machine

I. INTRODUCTION

The continuous development of information technology, biometric technology has become an important part of safety-related applications, such as public security crime investigations, access control systems, government identity certification, and terrorism prevention or detection. The most widely used biometric technology today is fingerprint identification

one of major challenges confronting biometric systems isthe rapid threat of malicious actions. The most of malicious actorsuse a common type of presentation attack, known as ‘‘spoofing” todefeat biometric systems. The main goal of presentation attackis impersonating target victims that have the desired authorization. It happens when intermediate spoofing forgers intentionallyguess that identity of unsuspecting individuals via steal victim’sfingerprints, tampering them with a certain legal material todefraud fingerprint recognition based systems Failure to prevent fingerprint spoofing forgeries on devicesmay compromise confidential information in many applicationssuch as video surveillance biometric identification and faceindexing in social media . This issue motivates researchers toemploy countermeasure techniques and combined them into thebiometric based systems to beat such forgery.

II .OBJECTIVE

The main contributions ofour method are attempts to distinguish real fingerprint images from fake Ones and analyzes the image consistency based on scaled androtated ROIs. Based on these ROIs features, we propose adeep discriminative model for training detection. We introduce two main techniques: DRBM and DBM used in the proposed method identify representation of real and forged fingerprints.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204207 |

III. LITERATURE SURVEY

This project presents Biometrics is the automated recognition of individuals based on their biological and behavioral characteristics such as fingerprints, face, iris, gait, and voice. The use of fingerprints as a biometric attribute has been extensively discussed in the scientific literature, and a variety of techniques have been developed for performingfingerprint recognition. Fingerprint recognition systems have been incorporated into an umber of forensic, civilian, and commercial applications .Given its widespread usage, researchers have analyzed the vulnerability of these systems to different types of adversary attacks, including finger-print obfuscation and impersonation. Fingerprint obfuscation refers to the deliberate alteration of the fingerprint pattern (e.g., cutting or burning the fingertips) by an individual who wants to avoid being recognized by the system. For example, a person on a watch list may attempt to modify his or herfingerprint pattern to prevent being matched against his or her entry on the watch list

IV. METHODOLOGY

The propose method to determine fake fingerprintsregarding spoof forgeries were used in authentication based systems, we adapt multiple features called deep features whichextracted from images such as, Deep Boltzmann Machine (DBM). The main benefit of DMB is that its layered architecture helpsto investigate a complex relationships between features andenables deep learning of high detailed features of data. Extractingfeatures from the input image based on Deep Neural Networks aidsto understand data in depth. DBMs are probabilistic deep learningthat copes with complex patterns impressively by extractinghighly detailed features from the image. It is suitable for tasks inwhich the patterns might not be easily detected or forged. Resultson the Cross Match dataset show that our technique achievesgood results with comparison to handcrafted based methods, theresults show high detection rate regarding spoofing attack. Themotivation of using deep learning features includes:

1) Restricted Boltzmann Machines (RBMs) adapted in manyapplications such as image classification and medical imageinvestigation and pattern analysis to solve various learningproblems.

2) Restricted Boltzmann Machines typically developed toextract features and build a self-contained framework forgenerating competitive non-linear classifiers.

3) We introduce RBM algorithm that introduces a discriminantfactor to RBM training.

V.APPLICATIONS

The system provides a secure and hassle free way to start and stop vehicle engine user just need to scan finger to start the vehicle. No need to carry any key. The system only allow authorized users to start the vehicle. users can first register into the system by scanning fingerprint recognition

VI. RESULTS

To achieve a perception of these three fingerprint benchmarks, various parameters in our method have been adjusted to give agood results

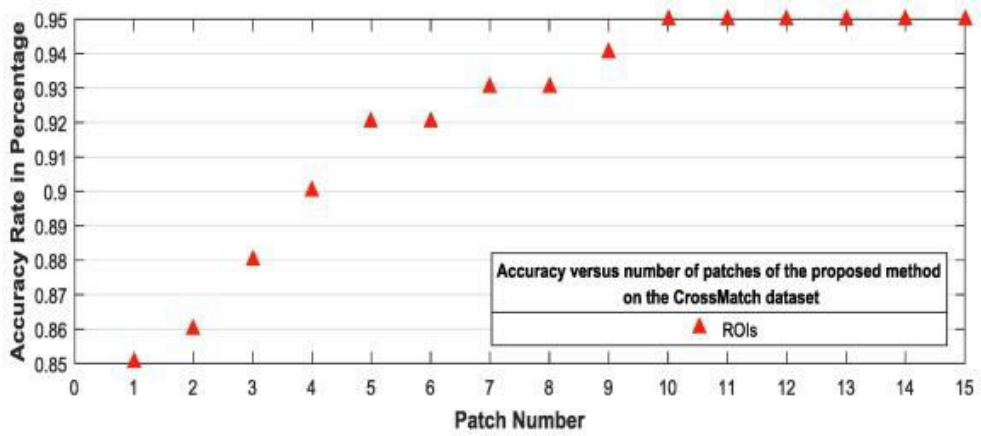
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204207 |

Parameter	Value
Size of input image	750 × 800
Patch size	40 × 40
Patch numbers	10 patches
GB- RBM	864 visible, 1000 hidden neurons
Maximum epochs	500
Meanfieldalgorithm	30 rounds
Learningrate	0.01
Momentum	0.5–0.92
Weight decay	10–4
Pooling size	1 × 3
Size of feature vector	128

Using the 10 ROIs from the original input fingerprint in the training DBM model, significantly makes the proposedmethod robust against missed or damaged ROIs of the inputimages. Furthermore, it gives a high accuracy detection rate when the size of the trained data is suitable in the dataset. The 10patches of input image show that, the size of trained data is increased to achieve about 0.95 accuracy rate.



Accuracy rate of the proposed method on cross match dataset computation cost of the proposedmethod for a single tested image is 45 s when we test images onItaldata dataset. Each step is given individually. Fingerprint preprocessing step for one image required 0.2 s and fingerprint deep features extraction required 10 s. The DBM training consumed 30 sand KNN classifier required 4.8 s. Similarly, the total computation time required to test one image on CrossMatch is 85 s, which isslower than Italdata and Biometrica due the large blank areas. We have tested three types of spoof materials: Wood Glue, gelatin,Play-Doh and 2D-printed ones on the proposed method Comparison shows performance evaluation of existing methods compared withour method

Reference Techniques used ACE

Nogueira Convolutional neural networks3.9%
Jiang and Xin Co-occurrence matrix11.00%
Gottschlich Histograms of gradients.6.7%
Zhang wavelet features and local binary pattern 2.1%
proposed method DRBM + DBM 3.6%

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204207 |

VII. CONCLUSION

In the proposed method, aftertraining a DBM, suchstructure has employed to extract deep features of the grayscale fingerprints. KNN classifier isapplied withthe feature vectors of the ROIs extracted by the DBM to examinespoof forgeries. The experiment results demonstrate that the Deep learning model is robust against different kindsof spoof forgeriessuch as wood glue, Gelatin and Play-Doh. Deep features are extracted from the real image of grayscale and Depth visual structure such as scaled and rotatedpatch ROIs. The performance evaluation of the DRBM + DBM method achieved state-of-the-artresults in three public fingerprint recognition benchmarks. However, our method still struggling to recognize fake fingerprints withunknown materials.

VIII. FUTURE SCOPE

we need to explore the capability of the proposed method in reducingthe time complexity of deep learning machine. We need to extend the method behavior to deal with spatio-temporal features of fingerprint images to explore the liveness properties.

REFERENCES

[1] E. Marasco, A. Ross, A survey on antispoofing schemes for fingerprintrecognition systems, ACM Comput. Surv. (CSUR) 47 (2) (2015) 28.
[2] G. Fumera, Multimodal anti-spoofing in biometric recognition systems, in: S.Marcel, M.S. Nixon, S.Z. Li (Eds.), Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks, Springer, London, 2014, pp. 165–184.
[3] C. Roberts, Biometric attack vectors and defences, Compute. Sec. 26 (1) (2007)14–25.
[4] K.W. Bowyer, Face recognition technology: security versus privacy, IEEETechnol. Soc. Mag. 23 (1) (2004) 9–19.
[5] D. Menotti et al., Deep representations for iris, face, and fingerprint spoofingdetection, IEEE Trans. Inform. Forensics Sec. 10 (4) (2015) 864–879.
[6] M. Sajjad et al., CNN-based anti-spoofing two-tier multi-factor authenticationsystem, Pattern Recogn. Lett. (2018).
[7] L. Ghiani et al., Livdet 2013 fingerprint liveness detection competition 2013,Biometrics (ICB), 2013 International Conference on, IEEE, 2013.
[8] Q. Huang et al., An evaluation of fake fingerprint databases utilizing SVMclassification, Pattern Recogn. Lett. 60 (2015) 1–7.
[9] T. Chugh, K. Cao, A.K. Jain, Fingerprint spoof detection using minutiae-basedlocal patches, Biometrics (IJCB), 2017 IEEE International Joint Conference on,IEEE, 2017.
[10] R.K. Dubey, J. Goh, V.L. Thing, Fingerprint liveness detection from single imageusing low-level features and shape analysis, IEEE Trans. Inf. Forensics Secur. 11(7) (2016) 1461–1475.
[11] C. Wang et al., A DCNN based fingerprint liveness detection algorithm withvoting strategy, Chinese Conference on Biometric Recognition, Springer, 2015.
[12] Y. Gao et al., Intermediate spoofing strategies and countermeasures, TsinghuaSci. Technol. 18 (6) (2013) 599–605.
[13] D. Baldisserra et al., Fake fingerprint detection by odor analysis, InternationalConference on Biometrics, Springer, 2006.
[14] Z. Akhtar et al., Evaluation of serial and parallel multibiometric systems underspoofing attacks, IEEE Fifth International Conference: Biometrics: Theory, Applications and Systems (BTAS), IEEE, 2012.
[15] J.J. Engelsma, K. Cao, A.K. Jain, Raspireader: open source fingerprint reader,IEEE Trans. Pattern Anal. Mach. Intell. (2018).

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details