IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907210 |

# A New Data-Driven Semantic Approach for Detecting Attack on Finger Geometric

**Gurusai G, Sachin S, Varun M, Dr.P.Visu**

UG Student, Dept. of CSE., Velammal Engineering College, Chennai, India

UG Student, Dept. of CSE., Velammal Engineering College, Chennai, India

UG Student, Dept. of CSE., Velammal Engineering College, Chennai, India

Professor, Dept. of CSE., Velammal Engineering College, Chennai, India

**ABSTRACT:** Biometric Signature refers to the process of incorporating the handwritten signatures or fingerprints in watermarking technology.

The attack consists in interpolating a smoothed connected version of the forged signature and selecting the most relevant salient points, skipping those that belong to tremor or indecisive movements due to the faking procedure. The Sigma Lognormal model is then used to synthetize the new on-line signature in the hope of obtaining an improved imitation.
All the data for performing this procedure will be taken from a set of sample data which is got from available open sources from internet.
We create the fingerprint-based authentication system based on four stages; the first stage is the pre-processing where image is enhanced using histogram equalization, Fourier transform, binarization and then segmentation to extract the important information in the fingerprint image. In the second stage, minutiae are extracted based on ridge highlighting and minutiae marking. The third stage is the post-processing where the H-breaks isolate points and false minutiae are removed. Finally, in the matching stage, minutiae are matched if they have almost identical direction and position.

**KEYWORDS:** Deep learning, Finger geometric, Python, Image processing, IDE's (Eclipse), Matplotlib, bio-metric, Vector, Dataframes, ndarray, NumPy.

## I. INTRODUCTION

We create the fingerprint-based authentication system based on four stages; the first stage is the pre-processing where image is enhanced using histogram equalization, Fourier transform, binarization and then segmentation to extract the important information in the fingerprint image. In the second stage, minutiae are extracted based on ridge highlighting and minutiae marking. The third stage is the post-processing where the H-breaks isolate points and false minutiae are removed. Finally, in the matching stage, minutiae are matched if they have almost identical direction and position.

The obliteration can be done on friction ridge patterns by abrading, cutting, burning, applying strong chemicals, and transplanting smooth skin. While the distortion can be done by turned the friction ridge patterns into unnatural ridge patterns using plastic surgery when portions of skin are removed and inserted in different positions, the imitation is a surgical process where a large area friction skin can be transplanted from other parts of the body, or cutting and then mosaicking several portions of friction skin. In the case of face-based authentication systems, the alterations can be applied on face via plastic surgery or prosthetic make-up.

## II. RELATED WORK

1. **"Biometrics Evaluation Under Spoofing Attacks",**
   **Authors: Ivana Chingovska, AndréRabello dos Anjos, and SébastienMarcel**
   **Published Year: 2017.**

While more accurate and reliable than ever, the trustworthiness of biometric verification systems is compromised by the emergenceof spoofing attacks. Responding to this threat, numerous research publications address isolated spoofing detection, resulting in efficient counter-measures for many biometric modes. However, an important, but often

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907210 |

overlooked issue regards their engagement into a verification task and how to measure their impact on the verification systems themselves. A novel evaluation framework for verification systems under spoofing attacks, called expected performance and spoof ability framework, is the major contribution of this paper. Its purpose is to serve for an objective comparison of different verification systems with regards to their verification performance and vulnerability to spoofing, taking into account the system's application-dependent susceptibility to spoofing attacks and cost of the errors. The convenience of the proposed open-source framework is demonstrated for the face mode, by comparing the security guarantee of four baseline face verification systems before and after they are secured with anti-spoofing algorithms.

Finger rings are assumed to present high intensity structures in hand radiographs, and cover the finger span. In order to locate finger rings, no manual indication is required except that the algorithm needs to know in advance whether one or more rings occur in the hand radiograph. To detect a finger ring, the region around each pixel on the finger midlines is examined. To determine the actual joint locations, a 10 mm × 5 mm block, which is adequate to cover the joint region, is shifted along each midline curve. For each point on a midline curve, the sum of the absolute directional second order derivatives within the block is calculated. The joint locations of DIP, PIP, MCP and IP are set as the locations where the responses in the indicated intervals are maximum. The size of the local neighbourhood is not critical, and is empirically set to 5 mm × 5 mm. The underlying assumption is that the local entropy is higher inside the hand and at the hand border, whereas the value is lower in the homogeneous background.

## III. PROPOSED WORK

One of the biggest challenges in on-line signature verification is the detection of malicious and skilled attacks. This paper proposes a new conceivable attack for an on-line signature biometric scheme.

In this paper, we present a new alteration attack on biometric authentication systems. We suppose that the impostor has altered image of the real user and he presents it as request in order to gain unlawful access to the system. Altered image can be recuperated from a fingerprint trace in case of fingerprint-based systems or user photograph for attacking face-based authentication systems. Next, we study the impact of alteration level on the matching score for fingerprint and face based biometric systems. Our analysis shows that both systems are vulnerable to the proposed attack and the alteration level has serious impact on the security of biometric systems.

Alteration attack is also considered a serious threat. However, the problem of altered biometric trait underwent limited studies in the literature and the available research works are interested in alteration of impostor biometric trait in order to hide his identity during the authentication process. For example, in the case of fingerprints, the proposed alterations are the obliteration of ridge, distortion and imitation of fingerprint.

### ADVANTAGES OF PROPOSED SYSTEM:

- Supports a method for synthesizing the results of the components of themodel
- Filters are adjusted automatically to extract the most usefulinformation
- Equalization ensures that the resulting histogram issmooth
- Improved with the histogram equalizationtechnique
- Stages can be applied to theimage

## IV. HARDWARE AND SOFTWARE SPECIFICATION:

### HARDWARE SPECIFICATION:

Hardware Requirements:

| Hardware | Minimum Requirements |
|---|---|
| Disk Space | 32 GB or more,10 GB or more for Foundation Edition |
| Processor | 1.4 GHz 64 bit |
| Memory | 2 GB |

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907210 |

Display (800 × 600) Capable video adapter and monitor

**SOFTWARE SPECIFICATION:**

Backend Technologies:

- Python
- Numpy
- Sci-learn
- Eclipse IDE

## V. PSEUDO CODE

Step 1: Importing all the necessary packages needed for performing this process.

Step 2: Collecting fingerprint data in the form of images.

Step 3: Converting the images to Gray scale then to binary scale images and finally finding out the ridges and edges present in it.

Step 4: Plotting a graph from the images gathered.

Step 5: Finding the differences between the new fingerprint and the old fingerprint images using the plotted graphs

Step 6: Display the result containing the images which encompass the places where the ridges and patterns are similar and where they are not.

## VI. MODULES WITH EXPLANATION

**Module 1:** Exploratory Data Analysis is generally cross-classified in two ways. First, each method is either non-graphical or graphical. And second, each method is either univariate or multivariate (usually just bivariate). Non-graphical methods generally involve calculation of summary statistics, while graphical methods obviously summarize the data in a diagrammatic or pictorial way. Univariate methods look at one variable (data column) at a time, while multivariate methods look at two or more variables at a time to explore relationships.

**Module 2:** Dataset Processing File Handling Package is one of the more comprehensive packages for progress bars with python and is handy for those instances you want to build scripts that keep the users informed on the status of your application. Package works on any platform (Linux, Windows, Mac, FreeBSD, NetBSD, Solaris/SunOS) in any console or in a GUI, and is also friendly with IPython/Jupyter notebooks.

**Module 3:** Feature Selection The number of pixels in an image is the same as the size of the image for grayscale images we can find the pixel features by reshaping the shape of the image and returning the array form of the image. Edges in an image are the corners where the pixel change drastically, as the images are stored in array form, we can visualize different values and see where the change in pixel value is higher but doing it manually takes time.

**Module 4:**Prediction ImageDataGenerator class allows allow rotation of up to 90 degrees, horizontal flip, horizontal and vertical shift of the data. We need to apply the training standardization over the test set. ImageDataGenerator will generate a stream of augmented images during training. We will define Exponential Linear Unit (ELU) activation functions A single fully-connected layer after the last max pooling. The padding='same' parameter. This simply means that the output volume slices will have the same dimensions as the input ones.

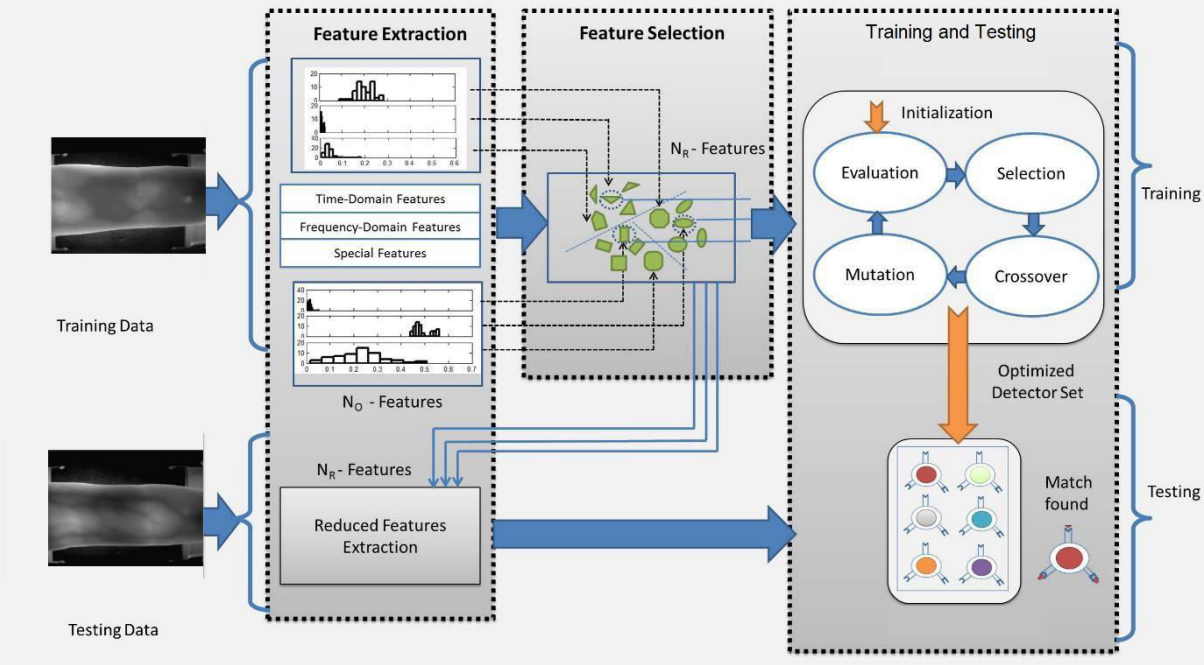
International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907210 |

**ARCHITECTURE DIAGRAM:**




**Algorithm used:**

**DEEP NEURAL NETWORK**

- Deep learning algorithms learn progressively more about the image as it goes through each neural network layer.
- Early layers learn how to detect low-level features like edges, and subsequent layers combine features from earlier layers into a more holistic representation

## VII. SIMULATION RESULTS

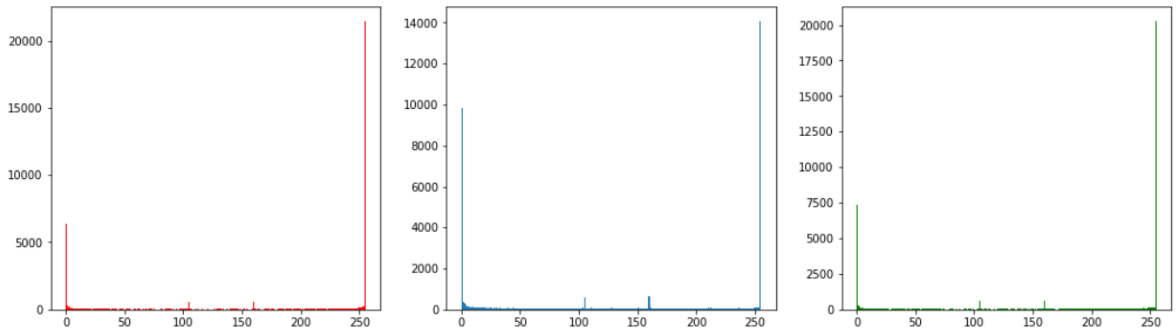


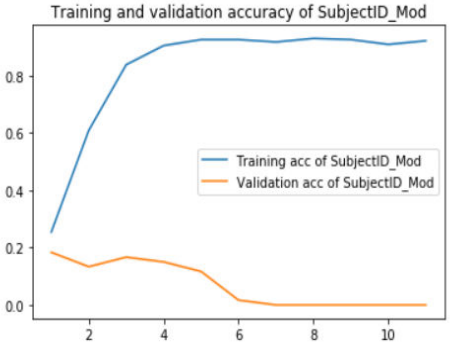
**Fig: Histogram plot to compare**

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907210 |

```
Id recognition accuracy:  0.0 %
Finger Attack Detection accuracy:  10.000000149011612 %
```



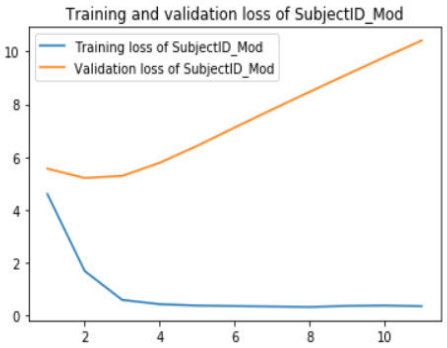
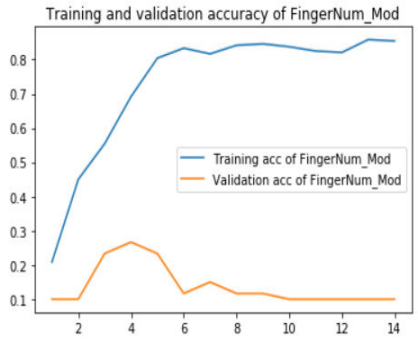




**Fig: Histogram plots of accuracy and loss (SubjectID_Mod)**



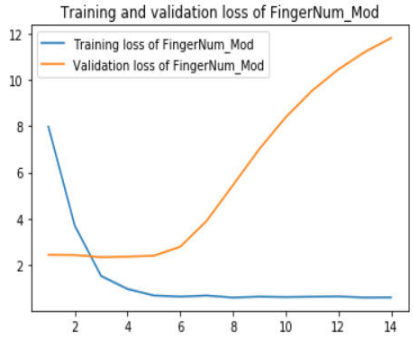




**Fig: Histogram plots of accuracy and loss (FingerNum_Mod)**

## VIII. CONCLUSION AND FUTURE WORK

Even though our way of approach has higher efficiency compared to previous methods like SIFT algorithms, the effectiveness of ours for trivial attacks is low. This is because of the amount of time it takes to come to a conclusion by the system to say that the fingerprint is a fake. But in case of complex attacks effectiveness and efficiency is more compared to the conventional ones.

In terms of future enhancement, this could be made available in the internet online so that it can be used by any organization or individual for security.

Also, if made online this could be taken a step further into making it an open-source biometric software detection, so that other developers can keep improving the software on a larger scale.

## REFERENCES

[1] D. de Santos-Sierra, M. F. Arriaga-Gómez, G. Bailador, and C. Sánchez-Ávila, "Low computational cost multilayer graph-based segmentation algorithms for hand recognition on mobile phones," in Proc. Int. Carnahan Conf. Security Technol. (ICCST), Rome, Italy, 2014, pp. 1–5.

[2] W. Kang and Q. Wu, "Pose-invariant hand shape recognition based on finger geometry," IEEE Trans. Syst., Man, Cybern., Syst., vol. 44, no. 11, pp. 1510–1521, Nov. 2014.

[3] B. P. Nguyen, W.-L. Tay, and C.-K. Chui, "Robust biometric recognition from palm depth images for gloved hands," IEEE Trans. Human–Mach. Syst., vol. 45, no. 6, pp. 799–804, Dec. 2015.

[4] Morales et al., "Synthesis of large-scale hand-shape databases for biometric applications," Pattern Recognit. Lett., vol. 68 , no. 1, pp. 183–189, 2015.

[5] R. M. Luque-Baena, D. Elizondo, E. López-Rubio, E. J. Palomo, and T. Watson, "Assessment of geometric features for individual identification and verification in biometric hand systems," Expert Syst. Appl., vol. 40, no. 9, pp. 3580–3594, 2013.

[6] S. Marcel, M. S. Nixon, and S. Z. Li, Handbook of Biometric Anti-Spoofing: Springer, 2014.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907210 |

[7] D. Gragnaniello, C. Sansone, and L. Verdoliva, "Iris liveness detection for mobile devices based on local descriptors," Pattern Recognition Letters, vol. 57, pp. 81-87, 2015.
[8] L. Yang, G. Yang, Y. Yin, and X. Xi, "Finger Vein Recognition with Anatomy Structure Analysis," IEEE Trans. Circuits Syst. Video. Technol., 2017.
[9] L. Yang, G. Yang, L. Zhou, and Y. Yin, "Super pixel-based finger vein roi extraction with sensor interoperability," in Proc. 8th Int. Conf. Biometrics (ICB), Phuket, May. 2015, pp. 444–451.
[10] L. Yang, G. Yang, Y. Yin, and R. Xiao, "Sliding window-based region of interest extraction for finger vein images," Sensors, vol. 13, no. 3, pp.3799–3815, 2013.
[11] F. Liu, Y. Yin, G. Yang, L. Dong, and X. Xi, "Finger vein recognition with super pixel- based features," in Proc. Int. Joint Conf. Biometrics (IJCB), Florida, USA, Sep./Oct. 2014, pp. 1–8.
[12] L. Dong, G. Yang, Y. Yin, F. Liu, and X. Xi, "Finger vein verification based on a personalized best patches map," in Proc. Int. Joint Conf. Biometrics (IJCB), Florida, USA, Sep./Oct. 2014, pp. 1–8.
[13] X. Xi, G. Yang, Y. Yin, and L. Yang, "Finger vein recognition based on the hyper information feature," Opt. Eng., vol. 53, no. 1, pp. 013108– 013108, 2014.
[14] K. B. Raja, R. Raghavendra, and C. Busch, "Video presentation attack detection in visible spectrum iris recognition using magnified phase information," IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2048-2056, 2015.
[15] R. F. Nogueira, R. D. A. Lotufo, and R. C. Machado, "Fingerprint Liveness Detection Using Convolutional Neural Networks," IEEE ransactions on Information Forensics & Security, vol. 11, no. 6, pp. 1-1, 2016

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details