International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

TRIVIAL FINGERPRINT: GENERATING A DEEP 'MASTER' PRINT TO EXPOSE FINGERPRINT VULNERABILITIES

Sagar Kotian[1], Hrushikesh Patil[2], Shrivatsa Kulkarni[3]

[1,2,3]*Student, Department of Computer Engineering, Pillai HOC College of Engineering and Technology*

Abstract - *Presently, the most widely used biometric identification system is the fingerprint system. The conventional fingerprint systems have been proven to be one of the most reliable systems today, but with such wide usage, there come issues and errors associated with it which can prove to be threats. In this paper, we propose a system that tackles these vulnerabilities by using an alternate method of scanning. Conventional fingerprint systems use absolute scanning for matching and verification. In our system, we create a deep master print which is a kind of fingerprint that can be used to attack a fingerprint system. By attacking, we mean to ethically hack into the current fingerprint systems such that such partial prints cannot be used against fingerprint systems. By using AI, we train our agent to generate deep master print through datasets to create a neural network that generates near trivial print which results in decreased further fingerprint hacks. We will also be generating a physical synthetic model of the trivial master print. This system is expected to reduce imposter fingerprints on a large scale.*

Key Words*: *biometric, fingerprint, neural networks, ethical, masterprint, imposter, synthetic.

1. INTRODUCTION

In this digital era, fingerprints are considered the most secure means of authentication. It is considered to be secure, fast, and reliable due to the unique property of fingerprints. Currently, the fingerprints taken by the scanners, say, phones, have scanners small enough to just take a small part of a finger. The partial fingerprints have fewer changes of uniqueness than a full fingerprint. Fingerprints have proven to be crucial and vital due to its unique and consistent property, but more recently due to advancement in computing capabilities, it has become automated i.e. Biometric. Currently, the system uses absolute fingerprints for authentication. Hence, it could be using more time. To make it effective, a system is proposed which takes a fingerprint as input by extracting the minutiae and compares it with the database. It provides the facility to match fingerprints and also identify the identity of an individual in less amount of time. To achieve good minutiae extraction in fingerprints with a varying quality external hardware fingerprint scanner is used.

1.1 OVERVIEW

The System is divided into 2 Stages:-

Stage 1:-

1. Fingerprint Extraction using external hardware.

Fig 1. *Extracted Fingerprint from Hardware.*

2. Extract Minutiae using Minutiae based extracting technique.

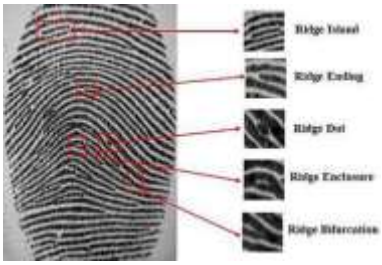


Fig 2. *Minutiae Based Extraction Features.*

3. Calculate the parameters to display results.

Stage 2:-

4. Generating a Trivial-Fingerprint using GAN (Generative Adversarial Network).

2. EXISTING SYSTEM

In most of the systems, the main focus was on the extraction process only. It is somewhat successful in giving an efficient result but the matching process was not considered and the collected data i.e., partial fingerprints remained inconsistent. Wherever the matching process was considered it was time-consuming providing the best case as well as the worst-case due to the use of algorithms like linear search. Also, using synthetic fingerprints partial fingerprints can be generated that can be used to mimic an individual. Other than this, if

the fingerprint is of low quality or distorted due to some reason, then the authorized person doesn't authorize.

Malicious users try to make the quality poor on purpose so that the identification and verification process gets difficult. For the past two decades, the study of the security of biometrics is trending. Even though the biometric system has so many advantages, it is still victimized to vulnerability attacks. Attacks can be on the user interface, between a module's interface, on modules or the database. Interface attacks prove to be somewhat successful as spoofing of fingerprints was done and the spoofed one is presented. It requires a mirror image like a biometric sample being unknown to the target image that is to be matched with, specifications related to image or permission for accessing the database, the vulnerability of this attack is higher when compared with other attacks.

Protection mechanisms like encryption, digital signature, hashing, etc. may not be easily applicable when an attack occurs, causing a serious and realistic threat for fingerprint verification systems especially that of mobile devices.

3. PROPOSED SYSTEM

The Authentication system input fingerprint is verified by matching its extracted minutiae feature with the fingerprints present in the database and the result is displayed based on the verification details and the matching percentage. After extracting the minutiae features of the input fingerprint, it is then verified in the database by matching the features with the fingerprints already stored in it. If the match is found, then the details of that individual are displayed along with matching percentage and the time it took for verification.

The process of extraction is performed by capturing a fingerprint image and applying an edge detection method on it. For this, white and black points are detected on it for highlighting the matching edges. A hardware device fingerprint scanner is used for extraction and making it easy and fast. After extracting the source fingerprint is compared with all the fingerprints stored in the database for the matching process. The focus is to ensure that the verification process is done in a minimum amount of time.

Steps involved:

Step 1: Extract fingerprint using the physical fingerprint scanner.
Step 2: Store the extracted fingerprint in the database.
Step 3: Extracting the minutiae of fingerprint.
Step 4: Select source fingerprint.
Step 5: Verify with the fingerprints in the database.
Step 6: Calculate the matching percentage.

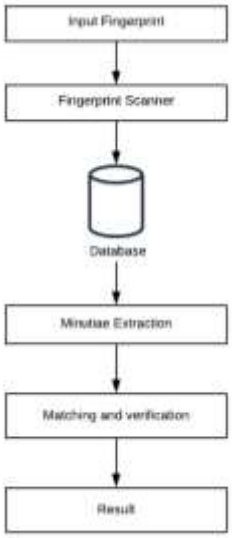


Fig -3: Stage 1 System Design

The Above Steps are used to perform all the preliminary work for stage 2 which involves the generation of Fake Samples using GAN (Generative Adversarial Network). A trivial fingerprint would mean a common fingerprint that could be used to unlock several different fingerprint inputs. This AI-based model will generate a single fingerprint out of a given number of fingerprints by a training method. The more inputs we feed it, the better it gets.

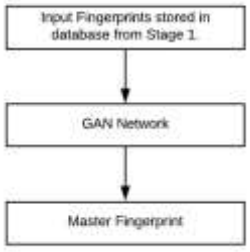


Fig -4: Stage 2 System Design

4. METHODOLOGY

A. Data Collection

The inputs are fingerprints that are obtained through a physical fingerprint scanner. The user gives his/her fingerprint input by placing their finger right on the surface of the hardware device.

B. Data Processing

The input fingerprints go through a procedure of analyzing. Edges in ridges of the fingerprints are detected as white and black points. This is known as edge detection. The edges are

considered as points on a graph that will be fed as an input to the next step.

D. Fingerprint Verification

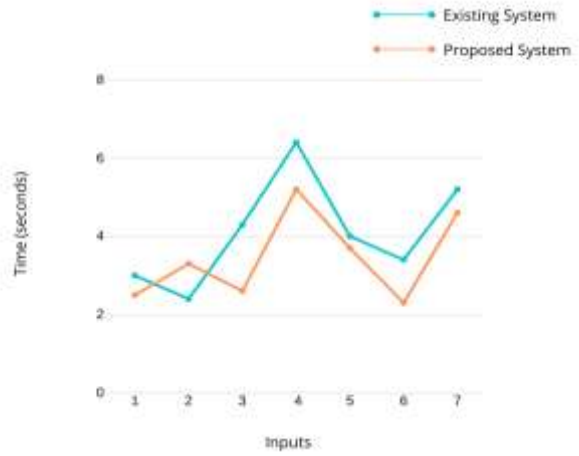
The input points are verified by comparing it with the fingerprint match in the database. If these edges are matched with the input fingerprint, it gets verified.

E. Master Print generation

The master-print or 'Trivial Fingerprint' is generated through a neural network algorithm GAN or Generative Adversarial Network. A GAN is a deep generative model that is essentially able to generate new content, in this case, a master-print.

5. RESULTS

We compared the results of the existing fingerprint scanning algorithm with our proposed algorithm by using the same fingerprint scanner in the same conditions to get precise results. The results were better in the case of our existing system by nearly 19% on average.



6. CONCLUSIONS AND FUTURE SCOPE

In the digital era, fingerprints have been an important part of our lives which also leads to threats to authorization and important data. The system is a way to tackle the vulnerabilities of the fingerprint scanning verification technique. It can counter potential threats of fake fingerprints and also increase the efficiency of the system. This system could be seen as a potential upgrade to the current fingerprint scanning system.

Future work could be done on these systems by improving the network by training or even use alternative neural networks or machine learning techniques.

7. REFERENCES

[1] Aditi Roy, Nasir Memon and Arun Ross, "MasterPrint: Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems" DOI 10.1109/ TIFS.2017.2691658.

[2] Jiexin Zhang, Alastair R. Beresford, Ian Sheret "SENSORID: Sensor Calibration Fingerprinting for Smartphones" {jz448, arb33}@cl.cam.ac.uk, ian.sheret@polymathinsight.co.uk

[3] Philip Bontrager, Aditi Roy, Julian Togelius "DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution" IEEE-978-1-5386-7180-1/18

[4] Thetha Das, Ashish Mulgaonkar, Srijeet Nair, "REAL-TIME FINGERPRINT VERIFICATION USING MASTERPRINT" ijrar (E-ISSN 2348-1269, P- ISSN 2349-5138)