# Survey on Fingerprint Spoofing, Detection Techniques and Databases

Samruddhi S Kulkarni
ME Student (Dept of E &TC)
R. H. Sapat COE,Nashik
Maharashtra

Hemprasad Y Patil
Assistant Professor (Dept of E &TC)
R H Sapat COE, Nashik,
Maharashtra

## ABSTRACT
In biometrics, Fingerprint is widely used in identification of individual's identity. Biometric recognition is leading technology for identification and security systems. Fingerprint has unique identification among all other biometric modalities.Use of the fingerprints as biometric characteristics is extensively used and developed for fingerprint recognition in forensic, civilian and commercial applications.This paper presents the brief data about fingerprint spoofing which encompasses misuse caused by the attackers. Fingerprint spoofing detection attributes to the investigation of the finger characteristics to ensure whether the finger is spoofed or live. The various spoofing types are explained and there detection techniques are introduced with three commonly used databases.

## General Terms
Image processing, Machinelearning, Fingerprint Recognition.

## Keywords
Biometrics, Fingerprint spoofing, Detection, databases.

## 1. INTRODUCTION
Biometrics technology is an automated recognition system which enables the authentication of individual based on biological and behavioral characteristics such as face ,iris ,gait ,voice ,fingerprints etc. Biometric methods are supposed to be a set of secure methods for identification and authentication of an individual as it has makeable advantages as compared with other methods. But at the same time biometric systems may be vulnerable to attacks, at each level such as biometric sensor level, data communication, database etc. These systems are not totally spoof proof. Recently, some studies summarized the possibility of spoofing recognition systems by artificial biometric samples such as fake fingerprints, artificial iris, facemask etc. Fingerprint Identification system is becoming a commonlyused biometric technique with authentication, security, safety and many other vigilance system. Unlike other biometric traits such as iris, face, palm, etc., fingerprint identification is a most commonly used technique due to unique characteristics of fingerprint of every individual. This feature makes it most reliable and preferred method amongst othertechniques [6].Due to its wide spread use, researchers have analyzed, the competitive attacks on the fingerprint identification systems including fingerprint "Impersonation". What is Impersonation?-It is a duplicate artificial fingerprint known as "Spoof artifacts" and ispresented to a fingerprint sensor to fool the recognition system.Spoofing is a method of attacking biometric systems where artificial objects are presented to biometric acqition system that imitates biological and behavioral characteristics; the system is designed tomeasure. This paper focuses on Fingerprint Spoofing, its types and its identification techniques.

## 2. FINGERPRINT SPOOFING
Fingerprints cannot lie, but liars can make fingerprints", this quote is attributed to "Mark Twain", which is proving right in many occasions[7].Technology is growing years after years and people are also becoming user friendly with the upgraded technology. It results in weakness of security of fingerprint sensor. It is not difficult now a day to find detailed guidelines on how to create spoofed fingerprint on biometric systems. Due to these reasons, fingerprint stands out biometric traits regarding its vulnerabilities to spoofing attacks. Differentiating a live fingerprint from a person with some other source is called as "Spoof Detection" [7].

### 2.1 Spoofing attacks in Fingerprint System Security

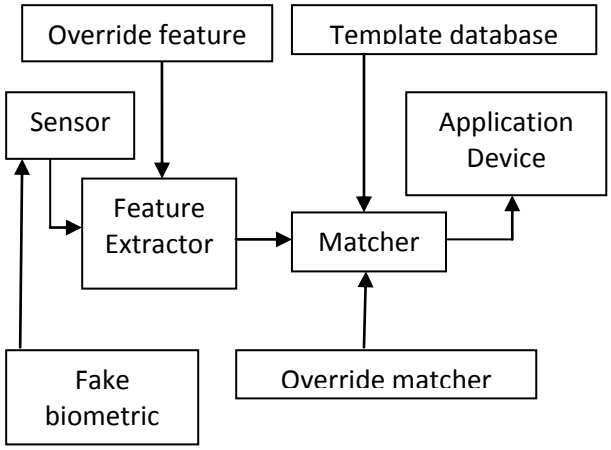


**Fig 1:The figure shows vulnerable points of attacks in fingerprint system security. The points represent various attacks which occur in the system by the attacker.**

These attacks do not require much or typical knowledge about the system operation.

Some of the attacks are,

1. Presentation attacks: Reproduction of biometric modality is presented at the inputs.

2. Sensor is bypassed and previously stored data is hacked and used.

3. The set of extracted features are replaced with the false sets.

4. The matcher is corrupted and sample is matched with the false set.

5. The final match is altered by an attacker.

## 2.2 Spoofing methods

There are two main methods [5]:

1. Co-operative spoofing

2. Non-Cooperative spoofing

### *2.2.1 Co-operative spoofing:*

In co-operative spoofing, we have "Direct mold spoofing method".In this method, the spoof is formed using a live finger mold.We can use plastic material to obtain the mold and gelatin for the cast.The spoof fingerprints are usually made up of materials (like play-doh, clay, and gelatin) which are easy to scan by commercial fingerprint scanner. This duplication of fingerprint is a co-operative process as the real owner participates in creation as spoof fingerprints.

In Direct mold, the finger is pressed on a surface and negative impression of fingerprint is fixed and mold is taken. The mold is then filled with moisture based material and spoof is formed[5].

### *2.2.2 Non Co-operative spoofing*

There are four types of non cooperative spoofing,

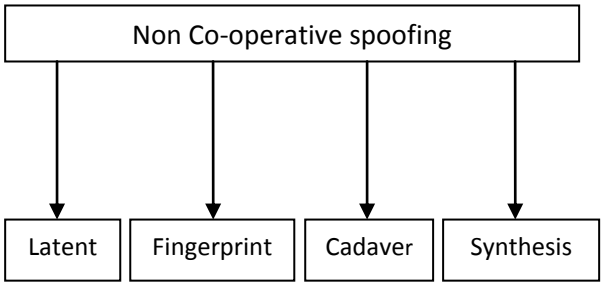


**Fig 2:Types of Non co-operative spoofing [6]**

#### 2.2.2.1 *LatentFingerprint*

These are the impressions which are produced by the rigid skin known as friction ridges on human finger. They are the marks left at the area and may not be visible with the naked eyes. To flash them, the surface on which the fingerprint is left is powdered with the brush. The background powder is removed and the lifted print is placed on the sensor and exposed to UV Light[9].

#### 2.2.2.2 *FingerprintReactivation*

Inthis method, graphite powder is brushed on the sensor, where the latent fingerprint is deposited on the sensor is reactivated [6].

#### 2.2.2.3 *Cadaver*

This method uses dead finger for spoofing [6].

#### 2.2.2.4 *Fingerprintsynthesis*

In this method, the fingerprint image is reconstructed using templates like minutiae points on the fingerprint and a digital image is captured which can be transferred to the spoofing artifact [6].

## 2.3 Spoofing detection

Characterizing a live fingerprint from an individual with some other sources is known as "Spoof Detection". The detection techniques address the issues of liveliness and can be based on two major types [13];

1. Hardware based

2. Software based.

### *2.3.1 Hardware based spoof detection [5][6]:*

These techniques accomplish the individuality of vitality such as temperature, electrical conductivity, pulse oximetry, skin resistance etc.But these methods require additional hardware and make the device expensive .The limitation of the above methods are tabulated below,

**Table 1: Limitations of hardware based spoof detection methods [5].**

| Liveness Detection Technique | Limitation |
|---|---|
| Temperature | Lack of ability to detect the wafer thin silicon rubbers. |
| Electrical Conductivity | Can be fooled by some saliva on the silicon artificial fingerprint. |
| Pulse Oximetry | Can be deterred by using translucent spoofing fingerprint. |
| Skin resistance | Can be fooled by artificial fingerprint with same type of requirements for original fingerprints. |

### *2.3.2 Software based spoof detection*

These methods are based on two mains techniques [6]:

1. Dynamic based

2. Static based

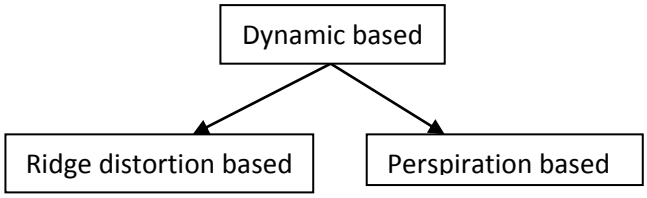


**Fig 3: Types of Dynamic based spoofing methods**

These are derived by processing multiframe of same fingerprint in two successive images which are captured within a finite time interval.

**A. Ridge Distortion based [6]**

This method was proposed by Antoneli et al. in 2006, where he found that the distortion produced by a real finger when pressing and moving on a scanner is more than a spoofed finger. These distortions are analyzed by processing a sequence of frames at a very high frame rate. The finger is assumed to be non-distorted at the beginning and its movements are analyzed using optical flow. The result and performance of this method depends on precision of minutiae extraction and pairing.

**B.Perspiration based**

One of the types in dynamic spoofing method is "Perspiration". It uses live finger. It is based on detecting perspiration between human skin and other material, as the sweat starts from pores and diffuses along the ridges; it makes the region between pores darker.The resultant moisture pattern can be captured. Live fingerprints exhibit non-uniformity due to perspiration, where as spoof fingerprints show high uniformity. Derakhshari [10]. has worked in this

field and introduced a method to provide fingerprint authentication. More investigation of accuracy and environmental conditions are required to increase its efficiency [5].

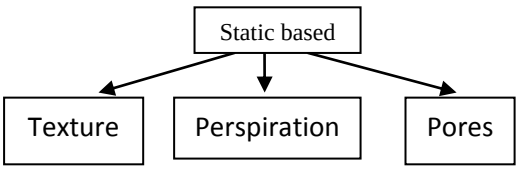


**Fig 4: Types of Static based spoofing methods**

These are analyzed using single fingerprint impression and compared with others. These methods are cheaper and fast than compared with dynamic features. These features consider textural characteristics, skinelasticity, perspiration based or combination of these features.

**A. Poresbased**

This method uses very high resolution sensor to acquire the image. Manivanan in 2010 has proposed this method by applying two filters [11],

1. High pass filter

2. Correlation

The high pass filter extracts the active sweat pores while the correlation filter is used for locating the pores position. In 2011, Espinoza [12] worked on spoof detection which compared the pores quantity between spoof fingerprint and live fingerprint.

# 3. DATABASES

In this section, we will review several databases that are used for research purpose. The commonly used and recommended fingerprint databases are,

1. LivDet

2. ATVS

3. FVC (Fingerprint Verification Competition)

## 3.1 LivDet

This is Liveness Detection Competition(LivDet)which was first held in the year 2009 organized by University Of Cagliari,Italy,in cooperation with Clarkson University ,USA [2].

The goal of this competition was to compare different technologies and methods for software based liveness detection with common experimental methods.This database contain three subsets;

a. Live Fingerprint

b. Fake Fingerprint

c. Three different optical sensors: Biometrica, Identix, Cross match.

Fingerprints are collected from various material for spoof fingerprints [2].

**Table 3: Dataset collection for LivDet 2009 [4];**

| Dataset | Sensor | No. of Persons | Live Fingerprint | Fake fingerprint |
|---|---|---|---|---|
| #1 | Biometrica | 500 | 2000 | 2000 |
| #2 | Identix | 160 | 1500 | 1500 |
| #3 | Crossmatch | 254 | 2000 | 2000 |

**Table 4: Dataset collection for LivDet 2011 [3];**

| Dataset | Sensor | No. of Persons | Live Fingerprint | Fake fingerprint |
|---|---|---|---|---|
| #1 | Biometrica | 50 | 400 | 81 fingers<br>22 subjects |
| #2 | Italdata | 50 | 400 | 81 fingers<br>22 subjects |
| #3 | Digital Persona | 100 | 200 | 100 fingers<br>50 subjects |

**Table 5: Dataset collection for LivDet 2013 [1];**

| Dataset | Sensor | No. of Persons | Live Fingerprint | Fake fingerprint |
|---|---|---|---|---|
| #1 | Biometrica | 30 | 300 | 100 fingers<br>15 subjects |
| #2 | Italdata | 30 | 300 | 100 fingers<br>15 subjects |

## 3.2 ATVS

This database is obtained from Biometric Recognition Group ATVS Madrid, Spain.In this database spoofed fingerprints are taken from real replicas. In this database, two sets were considered#1 and #2 [2].

In first dataset, samples of middle and index finger of both hands were considered.

Seventeen individuals were considered ,which included ,Sixty-eight fingers that were captured using three sensors; Biometrica, Yubee with ATMEL, Precise 100.In total 816 real images were captured and same number of spoofed images.

**Table 6: Dataset collection for ATVS SET 1**

| Dataset | No.of fingers | No.of Persons | Live Fingerprint | Fake fingerprint |
|---|---|---|---|---|
| #1 | 68 | 17 | 816 | 816 |

In second dataset, replica fingers from which spoofed fingerprints images were collected were obtained without co-operation of the users. Here number of users were sixteen for sixty-four different fingers.

**Table 7: Dataset collection for ATVS SET 2**

| Dataset | No.of fingers | No.of Persons | Live Fingerprint | Fake fingerprint |
|---|---|---|---|---|
| #1 | 64 | 16 | 768 | 816 |

## 3.3 FVC

FVC is Fingerprint Verification Competition which was established for testing a

lgorithm of fingerprint extraction and matching.It comprised of four fingerprint databases DB1,DB2,DB3,DB4.Amongst these,DB1-DB3 were collected using optical ,capacitive and thermal sensors.DB4 was created using Synthetic Fingerprint Generator.(SFinGe).[2]

Each database is 150 fingers wide and 12 samples/finger in depth.Total 1800 fingerprint images.Databases are subdivided in two subsets A and B .

For subset A, it contains 140 fingers(1680 images)

For subset B, it contains ten fingers(120 images)

# 4. CONCLUSION AND FUTURE SCOPE

Spoofing is a substantial challenge in fingerprint recognition systems.This paper has presented different spoofing techniques along with variousstate-of-the-art databases.Spoofing detection and its types are also been reviewed with corresponding databases.

A fingerprint spoofing related algorithm needs a potent feature extractor which extracts the salient features from input images. A lot of algorithmic work is needs to be applied for fingerprint spoofing recognition system so as to derive generalized methods that are independent of specifications, requirements and results in increased spoofing recognition rate.

# 5. ACKNOLEDGEMENT

The authors are thankful to Prof. S. P. Agnihotri, Head of the Department, Dr. P. C. Kulkarni, Principal, Mr. P. M. Deshpande Project Director, Sir M. S. Gosavi, Director, and G.E.S. R.H.Sapat College of Enginnering, Nashik, and Maharashtra, India.

# 6. REFERENCES

[1] Luca G, Valerio M, Simona T, Gian M, Fabio R.2013,University of Cagliari - Department of Electrical and Electronic Engineering Italy.LivDet2013.

[2] Shahzad M, April 2012,Novel Active Sweat Pores Based Liveness Detection Techniques for Fingerprint Biometrics,Brunel University.School of Engineering and Design.

[3] David Y, Luca G, Paolo D, Gian Luca M, Fabio R,2011 S Schuckers,Clarkson University - Department of Electrical and Computer Engineering USA.

[4] Gian M, AaronT, Pietro C, Fabio R,Stephanie S, Dominic G, Alessandra Tand, LivDet 2009 Group.

[5] Mojtaba M, Wamadeva B, Jan 2010Liveness and Spoofing in Fingerprint Identification Issues and Challenges,School of Engineering & DesignBrunel UniversityUxbridge, Moddlesex.

[6] Emanuela M, Arun R, 2014. A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems ACM Comput. Surv.47, 2, Article A ,36 pages.

[7] Javier G,,Julian F,,Javier,,Raffaele C,2014,Fingerprint Anti-spoofing in Biometric Systems, Springer London.

[8] ManeeshS,July 2014Detection and Prevention of FingerprintAltering /Spoofing Based on Pores (Level-3) withthe Help ofMultimodal Biometrics,International Journal of Science and Research (IJSR).

[9] Annalisa F,Davide M ,2008,Fingerprint Synthesis and Spoof Detection,Springer London.

[10] R. Derakhshani, S. Schuckers, L. Hornak, L. O'Gorman, “Determination of vitality from a noninvasive biomedical measurement for use in fingerprint scanners”, Pattern Recognition.

[11] Maltoni D,Maio D, Jain A K, PrabhakarS,2003,Handbook of Fingerprint Recognitin,New York, Springer Verlog.

[12] Sousedik, C.; Busch, C., 12 2014 "Presentation attack detection methods for fingerprint recognition systems: a survey," in Biometrics, IET.

[13] Menotti, D.; Chiachia, G.; Pinto, A.; Robson Schwartz, W.; Pedrini, H.; Xavier Falcao, A.; Rocha, A., April 2015 "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection," in Information Forensics and Security, IEEE Transactions,vol.10, no.4, pp.864-879.