# Face Spoofing Detection using Texture Analysis

Ms. P. Devi[1], Dr. S. Anila[2]

[1] *Assistant Professor (Sr. Gr.), Department of Electronics and Communication Engineering, Sri Ramakrishna Institute of Technology, Tamilnadu, India*
[2] *Professor, Department of Electronics and Communication Engineering, Sri Ramakrishna Institute of Technology, Tamilnadu, India*

## ABSTRACT

*Forensic agencies are the backbone in identifying the suspect behind the theft incident or the crime scene that has occurred. Although we have CCTV cameras placed at our home, these agents are called only if there is no absolute evidence about the suspect obtained through these cameras. The identification of the anonymous guy fails often by viewing the recorded data without any processing techniques. Also CCTV forensics is a very difficult task as the data procured from a CCTV can be in a damaged state with bad lighting ambience, noise, blurring due to optical settings.Hence forth through some efficient image processing techniques with a predefined image database, we will be able to reveal the suspect. This paper focuses on the recognition of the suspect automatically mainly through textures.*

**Keyword:** - *Face recognition, spoofing detection, texture analysis*

## 1. INTRODUCTION

Introduction With many terrifying news warning us of burglars and robbers, it may seem like no one can be safe these days. Thefts and crime scenes happen everywhere around the globe. Thievery has always existed in all cultures. Throughout historical evolution, property owners have tried to protect their possessions using personal guards or some sort of locking mechanisms. For a long time, locks and keys provided protection but it is not the case today. In the modern world, theft, robbery and crime scenes happen often at major public places and even at zones where there is tight security. Hence forth security also needed modification .This advancement is provided by technology. No one can completely stop a crime scene from being occurred everywhere, but suspects can be narrowed down in crime scenes using some of the techniques. Currently forensic agents are the boss in figuring out a criminal through some evidences and clues which are left behind the suspects at the spot they trace the suspect using fingerprints that are left behind by the criminals inadvertently in the objects that are used by them at the crime scene. There are many examples of unsolved theft cases throughout history. Let us look at one recent attack at Germany.

Among the world's largest gold coins is a 100 Kg treasure from Canada which is called the Big Maple Leaf. The coin is an inch thick and 21-inches wide. It was secured in Berlin's Bode Museum. It was stolen on March 27, 2017 — and police have no idea about the incident and how the thieves had managed to loot such a treasure. The coin had the head of Queen Elizabeth II on one side and a maple leaf on the other. It was worth nearly 500 Lakhs (INR).

Police reports say that the thieves used a ladder and broke in through a window and no facial data were clearly visible through the obtained CCTV surveillance cameras.Such is the drawback. Although the museum had cameras, detection of the faces became difficult due to the earlier described factors. Henceforth processing of DVR data is highly required in today's world.

This paper is about the identification of the suspect at the crime scene from the video/image acquired. The image acquired is processed based on the body textures such as the face, color, shape and many such attributes. The details acquired are processed and then compared with the database of criminals who are involved in frequent robbery and theft. This technique will bring to light the true burglar.

## 2. SURVEY AND STATISTICAL REPORTS

Introduction The following is the statistical report of 2018 from the central ministry giving us the number of cases filed.

**CRIME STATISTICS**
**Table37.1 (A)-INCIDENCE OF COGNIZABLE CRIME UNDER IPC**

| Year | Murder | Dacoity | Robbery | Burglary | Theft | Riots | Other | Total |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 2001 | 36202 | 6154 | 19901 | 101182 | 252803 | 76222 | 1276844 | 1769308 |
| 2002 | 35290 | 6101 | 18764 | 96461 | 247462 | 68945 | 1307307 | 1780330 |
| 2003 | 32716 | 5303 | 17512 | 92827 | 245237 | 57334 | 1265191 | 1716120 |
| 2004 | 33608 | 5311 | 18458 | 92490 | 273045 | 59971 | 1349132 | 1832015 |
| 2005 | 32719 | 5141 | 17673 | 90108 | 273111 | 56235 | 1347615 | 1822602 |
| 2006 | 32481 | 4747 | 18456 | 91666 | 274354 | 56641 | 1399948 | 1878293 |
| 2007 | 32318 | 4579 | 19136 | 91218 | 285043 | 59915 | 1497464 | 1989673 |
| 2008 | 32766 | 4530 | 20522 | 93742 | 316761 | 66018 | 1559040 | 2093379 |
| 2009 | 32369 | 4586 | 22409 | 92070 | 324195 | 62942 | 1582774 | 2121345 |
| 2010 | 33335 | 4358 | 23393 | 90179 | 330312 | 67571 | 1675683 | 2224831 |
| 2011 | 34305 | 4285 | 24700 | 92504 | 340800 | 68500 | 1760481 | 2325575 |
| 2012 | 34434 | 4314 | 27343 | 92892 | 337407 | 74633 | 1816165 | 2387188 |
| 2013 | 33201 | 4539 | 31927 | 104401 | 372622 | 72126 | 2028906 | 2647722 |
| 2014 | 33981 | 4395 | 38071 | 114646 | 440915 | 66042 | 2153513 | 2851563 |
| 2015 | 32127 | 3972 | 36188 | 114123 | 467833 | 65255 | 2229902 | 2949400 |

**Fig -1:** Crimes filed year wise

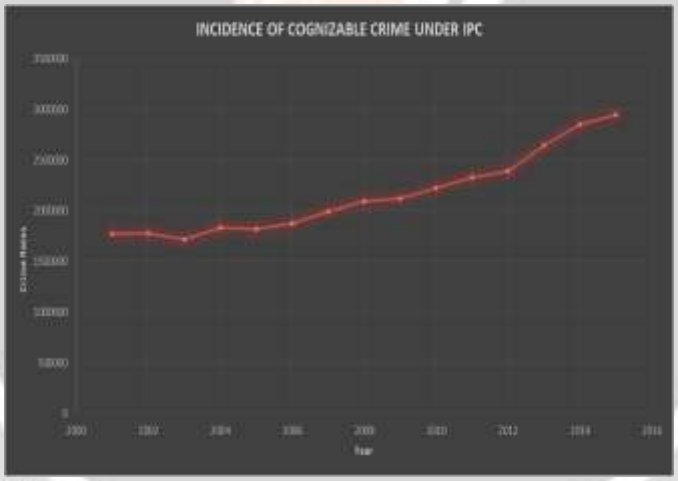


**Fig -2:** Column Chart of the crimes filed

As we can see there is a steady increase in the crime rates that take place. The solution of identifying the robber is through texture identifications. Texture in this case means the facial attributes such as eyes, nose, ears, walking gesture. These properties are identified initially which is taken as the input data for solving crimes.

## 3. METHODOLOGY

- Initially the database is filled with suspects in the neighborhood.
- The suspect's facial data is scanned at different angles

**Fig -3:** Suspect database

- The image of the suspect is taken from the CCTV footage at the crime scene

- It is then processed and facial data is obtained

- The facial data obtained is then split into different properties as per the database. For e.g., if the eye data is perfectly visible through CCTV footage then it is compared with the database for iris matching.

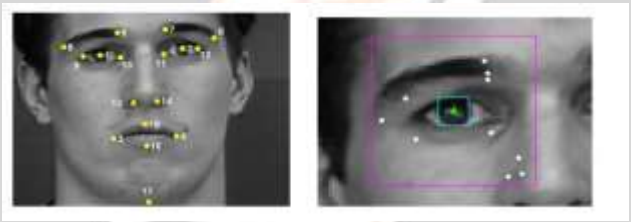

**Fig -4:** Iris is zoomed and processed

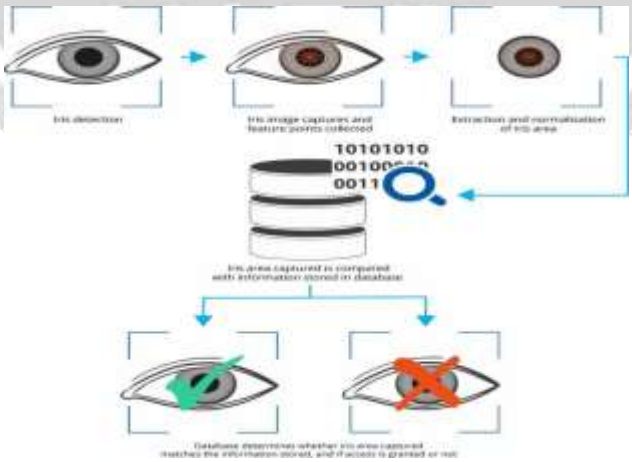


**Fig -4:** Comparison with database for nearest match

## 4. CONCLUSIONS

Thus the facial data obtained through the CCTV is processed based on the texture. The different properties of the obtained data are store under separate tags and are cross referenced with the available database to find the burglar.

## 5. REFERENCES

[1]. S. R. Arashloo, J. Kittler and W. Christmas, "An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol," in IEEE Access, vol. 5, pp. 13868-13882, 2017. doi: 10.1109/ACCESS.2017.2729161

[2]. A. Toosi, A. Bottino, S. Cumani, P. Negri and P. L. Sottile, "Feature Fusion for Fingerprint Liveness Detection: a Comparative Study," in IEEE Access, vol. 5, pp. 23695-23709, 2017. doi: 10.1109/ACCESS.2017.2763419

[3]. Z. Boulkenafet, J. Komulainen and A. Hadid, "Face Spoofing Detection Using Colour Texture Analysis," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1818-1830, Aug. 2016. doi: 10.1109/TIFS.2016.2555286

[4]. D. Wen, H. Han and A. K. Jain, "Face Spoof Detection With Image Distortion Analysis," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 746-761, April 2015. doi: 10.1109/TIFS.2015.2400395

[5]. Ahmad Zamani, Nazri & Darus, Zaharudin & Abdullah, Siti & Nordin, Md Jan. (2011). Multiple-frames super-resolution for closed circuit television forensics. 10.1109/ICPAIR.2011.5976908.

[6]. D. C. Garcia and R. L. de Queiroz, "Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 778-786, April 2015. doi: 10.1109/TIFS.2015.2411394

[7]. N. Erdogmus and S. Marcel, "Spoofing Face Recognition With 3D Masks," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, pp. 1084-1097, July 2014. doi: 10.1109/TIFS.2014.2322255

[8]. J. Galbally, S. Marcel and J. Fierrez, "Biometric Antispoofing Methods: A Survey in Face Recognition," in IEEE Access, vol. 2, pp. 1530-1552, 2014. doi: 10.1109/ACCESS.2014.2381273

[9]. A. d. S. Pinto, H. Pedrini, W. Schwartz and A. Rocha, "Video-Based Face Spoofing Detection through Visual Rhythm Analysis," 2012 25th SIBGRAPI Conference on Graphics, Patterns and Images, Ouro Preto, 2012, pp. 221-228.

[10]. A. K. Jain and B. Klare, "Matching Forensic Sketches and Mug Shots to Apprehend Criminals," in Computer, vol. 44, no. 5, pp. 94-96, May 2011. doi: 10.1109/MC.2011.153

[11]. J. Määttä, A. Hadid and M. Pietikäinen, "Face spoofing detection from single images using micro-texture analysis," 2011 International Joint Conference on Biometrics (IJCB), Washington, DC, 2011, pp. 1-7. doi: 10.1109/IJCB.2011.6117510