International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

INTEGRATION OF PHYSICAL SYSTEM MONITORING, CRIME POSTING & ALERTING DANGEROUS ZONE

A. Priyanka GAndhi[1], S. Madhushree[2], A. Nandhini[3], V.ANITHA MOSES[4]

[1, 2, 3] B.E., Department of CSE, Panimalar Engineering College, Chennai, Tamilnadu, India.
[4] M.E., Department of CSE, Panimalar Engineering College, Chennai, Tamilnadu, India.

Abstract - *We introduced an android application for people security on their way. Android user can post dangerous location based on the event happened in that particular place. User can post photo or crime activity happened in that place. The crime data is updated in the server only when more than 3 people have posted the same event in that place. Once the event is posted, automatic alert is displayed to all the general users who cross that area. Similarly in finding criminals their finger prints are automatically checked with criminal records. By using above two processes we can easily find the criminal who are all involved in crime. And also we will get precaution about travelling place.*

***Key Words*: Biometric sensors, Automatic alert, Android application, Precaution.**

1. INTRODUCTION

In this paper, we will examine how Aadhaar biometric database can be used for crime investigation and how it can be integrated with the existing system in India, the challenges of integration, and possible solutions. Paper also highlights some of the technical and legal challenges for its implementation which is a policy matter. The whole system is designed in such a way that it can be easily verified by Government and Non-Government services. The system has been promoted as a tool for reducing fraud in many private and public distribution systems and enabling the government to better deliver public benefits. These systems generally stores citizen's basic information as well as their biometric information and normally its built in such a way that it can be used for multiple purposes. In many countries, such systems are used for identifying the forgery, tax evasion and crime investigation. Our objective is to explore, how such system can be used for law enforcement and crime investigation.

1.1 USE OF BIOMETRIC DATABASE FOR CRIME INVESTIGATION

Today a massive computing power and well written pattern matching algorithms have made it possible to automatically search and detect the patterns of similarity in many different kind of digital database of patterns which may include fingerprints, faces, and irises. Effectiveness and accuracy of such system are very promising even for very large databases.

Fingerprints analysis is one of the most vital and integral process in crime investigation. Fingerprint databases are commonly used worldwide by almost all the police department and law enforcement agencies for the purposes of forensics, crime investigation and identifying the criminal's involvements in various crimes. In India, it's a challenging task for investigators to fish out fingerprints of criminals which often get lost or lay hidden in piles of files in police stations because no attempt has been made to put them in one database. For the country like India, having world second largest population, it's really a very difficult to architect a separate biometric or identity database for different-different purposes individually. As 90% of Indian population has enrolled in Aadhaar, It becomes a standard biometric database which can be used for various purposes including the crime investigation.

1.2 UNIQUE IDENTIFICATION AUTHORITY OF INDIA

The Unique Identification Authority of India (UIDAI) was created with the objective to issue Unique Identification numbers (UID), named as "Aadhaar", to all residents of India. Aadhaar system is built purely as an "Identity Platform". The main purpose of Aadhaar is to provide a biometric attached identity that is verifiable online. The whole system is designed in such a way that it can be easily verified by Government and Non-Government services. The system has been promoted as a tool for reducing fraud in much private and public distribution system and enabling the government to better deliver public benefits.

2. PERFORMANCE MEASUREMENT OF BIOMETRIC IDENTIFICATION SYSTEM

The main aspect to evaluate a biometric system is its accuracy. From the user's point of view, an error of accuracy occurs when the system fails to authenticate the identity of a registered person or when the system erroneously authenticates the identity of an intruder

A biometric matching system's response is typically a matching score (s) that quantifies the similarity between the input and the database template representations. The highest percentage gives the accurate results that shows the two biometric measurements come from the same person. A threshold regulates the system decision. The system infers that pairs of biometric samples generating scores higher than or equal to are mate pairs (that is, they belong to the same person). Consequently, pairs of biometric samples generating scores lower than are non-match pairs (that is,

they belong to different persons). The distribution of scores generated from pairs of samples from different persons is called an impostor distribution; the score distribution generated from pairs of samples from the same person is called a genuine distribution. (see Chart -1).

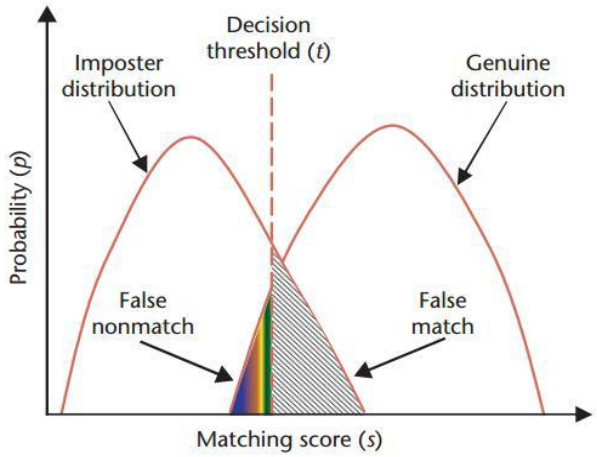

Chart -1: Biometric system error rates

There are several factors that can provoke accuracy errors. Biometrical Error rates are quantitative metrics of the accuracy of biometrical systems. They help biometric researchers and industry providers to improve their solutions and help system users to evaluate and choose the appropriate solutions for their applications. There are two types of error metrics: (a) to evaluate capture devices. (b) To evaluate biometric algorithms. The Failure to Capture Rate (FCR) evaluates the capacity of a capture device to properly read a biometrical record in several environmental and human conditions. The failure of capture device is known as "Capture Error". For biometric algorithms evaluation there are metrics associated to each phase of the recognizing process

The Failure to Enroll Rate (FER) measures the capacity of Enroll Component of the algorithm to detect, extract and compose the template from the biometric record read by the capture device, i.e., the FER is computed only for biometric record properly read. In the case of matching algorithm we have two important error rates: The False Matching Error Rate (FMR) measures the rate of actual impostor comparisons that are erroneously considered genuine. On the contrary the False Non matching Error Rate (FNMR) measures the rate of actual genuine comparisons that are erroneously considered impostors. In the case of ranking algorithm the main ranking error rate is the Rank (n) that measures the rate of genuine comparisons is included among the n most similar comparisons from a database

An operational biometric system makes a trade-off between false match rate (FMR) and false non-match rate (FNMR). In fact, both FMR and FNMR are functions of the system threshold t: If the system's designers decrease to make the system more tolerant to input variations and noise, FMR increases [6]. On the other hand, if they raise t to make the system more secure, then FNMR increases accordingly. System performance can be depicted at all operating points (thresholds) in the form of a receiver operating characteristic (ROC) curve. An ROC curve plots FMR against (1 – FNMR) or FNMR for various values of threshold. (see Chart 2).

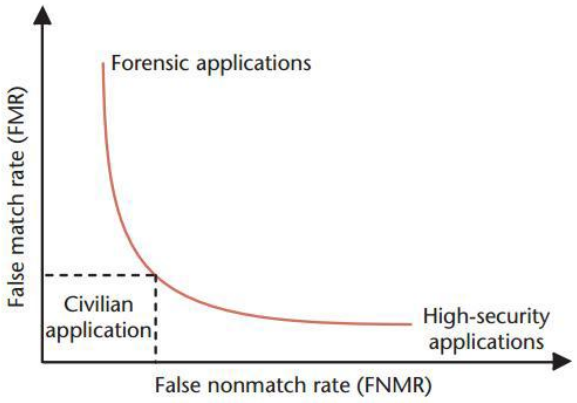

Chart -2: Receiver operating characteristic curve

3. PERFORMANCE OF AADHAAR BIOMETRIC SYSTEM

As fingerprints alone will not be sufficient for achieving higher accuracy in biometric identification, Aadhaar has used multi-model biometric fusion techniques. UIDAI has achieved accuracy as high as 99% de-duplication due to the fusion of fingerprint and iris scores. A Proof of Concept (PoC) study was carried out by UIDAI to assess the feasibility of using iris for on-line biometric authentication in the Indian context (Table 1). The findings of this study are presented in the report. This report covers the design framework, field implementation, data collection and analysis. It interprets empirical results to assess effectiveness of iris technology, authentication processes and devices.

Table -1: FEASIBILITY OF IRIS BASED ON-LINE AUTHENTICATION

Findings	% of Residents	
	Single-Eye Cameras	Dual-Eye Cameras
Authenticated in first try	95.89	99.29
Authenticated in multiple tries	99.21	99.40
Failed authentication (FRR+FTC)	0.79	0.60

If we study the UIDAI's own technical report, the system has approximately a chance of 0.5 per cent occurrence of false identification. In Indian context this fractional values could possibly make Lakhs of people as Suspect. We can narrow

down this number but still chances are there that innocent may suffer, if the investigative agency solely depends on the system identification process.

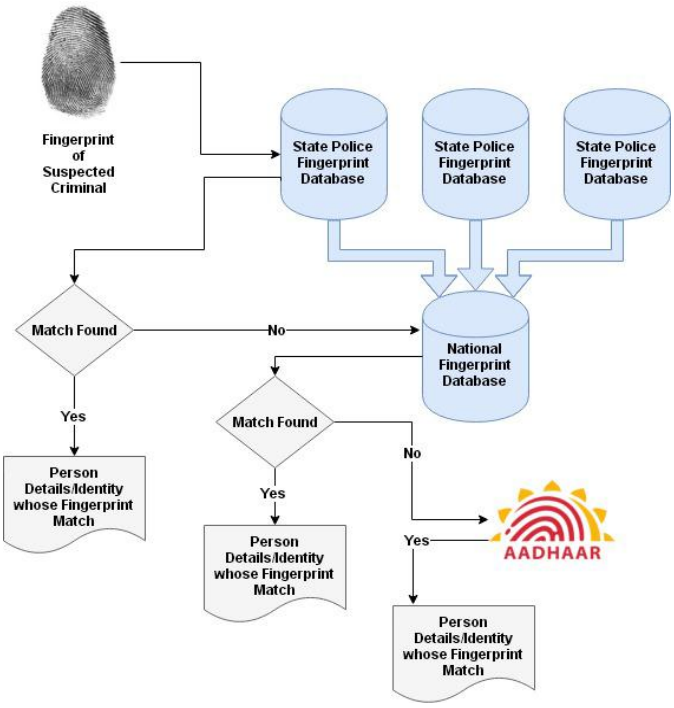

Fig -1: Architecture of Aadhaar Based Criminal Tracing System

3. ADVANTAGES

Aadhaar has highest number of citizen enrollment till today. It's one of the largest systems in the world storing such a huge number of Biometric information. The system is very reliable and scalable. Building similar type of system only for forensic and criminal investigation purpose may not be feasible and viable solution. Since Aadhaar is already well established system, its uses for the other purposes can be explored.

Aadhaar was never intended for Forensic purpose and thus it was not designed in that way. The citizens who enrolled for Aadhaar never gave his consent of using his information for such investigations.

4. CONCLUSION

Thus, the proposed new application will try to access Aadhar details via finger print sensors. This is to reduce the manual FIR system by making it automated. The databases of the existing criminal's record are used to find the criminals with the help of matching biometric sensors. In public point of view, we used time-based and location-based details to indicate the public, about the criminal activities in that area. This helps the public to know about the travelling place even though he/she is new to the particular place. The alert messages are also added by the public and it is updated to the database only if the same incident recorded for 3 times. This feature makes the crime evidently and also police comes to know about the particular crime and takes the steps accordingly. This application is try to help the public as well as police in such a way to improve the crime detection and analysis.

REFERENCES

[1] A. Sankaran, M. Vatsa and R. Singh, "Latent Fingerprint Matching: A Survey," in IEEE Access, vol. 2, no. , pp.9821004, 2014.

[2] Anil K Jain, Arun Ross, "Bridging the gap: From biometrics to forensics", Philosophical Transactions of The Royal Society B Biological Sciences 370(1674), August 2015.

[3] Anil K. Jain, Salil Prabhakar, and Sharath Pankanti. 2001. Twin Test: On Discriminability of Fingerprints. In Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '01), Josef BigÃ¼n and Fabrizio Smeraldi (Eds.). Springer-Verlag, London, UK, UK, 211-216.

[4] Bouchrika, I., Goffredo, M., Carter, J. and Nixon, M. (2011), On Using Gait in Forensic Biometrics. Journal of Forensic Sciences, 56: 882–889.

[5] D. Brown and K. Bradshaw, "A multi-biometric feature-fusion framework for improved uni-modal and multi-modal human identification," 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, 2016, pp. 1-6.

[6] D. Meuwly and R. Veldhuis, "Forensic biometrics: From two communities to one discipline," 2012 BIOSIG – Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG), Darmstadt, 2012, pp. 1-12.