Research Paper Engineering

Criminal Action Surveillance System

*Bhavesh Lonkar

* Department of Computer Engineering, Sinhgad Academy of Engineering, University of Pune.

ABSTRACT

The proposed system is automated system to reduce paperwork in the criminal investigation. It is a stand-alone application keeping in mind the security issues. Following are the key features of the software to be implemented,
1. It basically involves storing the records of the criminals along with the images, medical details, finger-prints, crime conducted, punishments, officers' involved in short the case-file.
2. Verification of criminals on the basis of finger-print matching.
3. It also stores the details of the officers' within the jurisdiction of the main jail where the software is installed.
4. It will also be able to store FIRs' along with the scanned image of the written FIR (hard copy image).
5. It will take into account the attendance of the individuals using the biometric system.
6. It also involves the instant messaging facility over the mobile which can inform all the main centres in the country about some emergency.
7.The system will also take into account the passport-verification data required to be done for every citizen for passport issue.

Keywords :

I.INTRODUCTION

Now a days all the processes right from the registration of the case to the result of the Honorable court are carried out through paper work. Definitely it is desired but includes more manpower and time. Also the existing systems like CCTNS(Crime and Criminal Tracking Network System) is suffered from a lot of difficulties and flaws. CCTNS is almost a Rs.2000 Cr project launched by Ministry of Home Affairs, Govt. of India. So it's a costlier project than estimated. It is padded with the corruption issues and dispute between State governments. So we are going to develop a stand alone application that will be installed in a police station. It will keep all the criminal records happened within that area. It's a cheaper system than the existing ones as well as very handful to the police staff to operate.

This is about the surveillance security provided to the criminal actions within the jurisdiction of the particular police station. Adaptation of this system in police stations will not only improve the efficiency of the police enquiry process but also reduce the paper work and time. It will able to keep all the criminal records at a central station securely.

It includes a criminal database with a physical details of the criminal and a Biometric finger-print module that will cover verification for both criminal and attendance of the police staff. Scope of this system is to maintain all the types of crimes, involved criminals, police officers, evidences, eye-witnesses and other supporting documents. Therefore it's a kind of automation made in the criminal catching actions.

Use of these application will surely improve the reputation of Police department as the criminal actions affects the society and their well beings. By using these strategies police will find themselves as a rapid action police forces to identify criminals and to suppress the crime in society providing security to the people

II.SYSTEM ARCHITECTUE

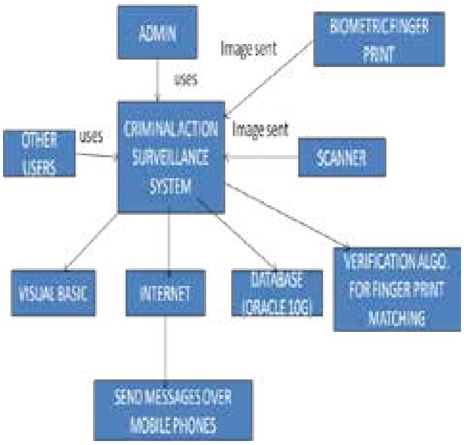


Fig 1. SYSTEM ARCHITECTURE

User Characteristics

The intended users are general computer users with a general knowledge of the basic functionalities of the computer machine like the users are expected to know how to install the application, how to search for something required etc.

The interface of the application will be very user-friendly. The features will be simplified and interactive thus the technical knowledge of the user finds least importance. The user linked with their respective criminal case should be keen enough to avail himself the offers and schemes launched by the government authorities.

General Constraints, Assumption, Dependence, Guideline

There are two different users who will be using this product:

- Administrator who will manage the entire system.

- Police staff will maintain everyday work of the police station right from criminal records to the log files.

These features are available to the Administrator are:

- They can register to the system.
- They have the power to manage the system.
- They can add officer database to the system.
- They can confirm/validate the criminal information.
- They can keep track of the crime and its evidences.

The features available to the police staff are:

- Register into the system. After registration he/she has the right to login and use the features of this system. User can use following features:

1. Add/update/delete criminal and official records
2. Document scanning
3. Fingerprint scanning
4. Instant messaging service
5. Maintenance of case files

SYSTEM FEATURES

As we have already mentioned above that the system will have provisions for the admin and user respectively. Now the administrator has all the access rights to manage the entire system.

A user can have access to all facilities except the attendance records with the help of a username and a password. After logging in he/she can view home page along with the all the facilities.

The back end of the system will have a database which is intended to store, retrieve, update and manipulate information related to the system which includes:

- Administrator/User information
- Criminal records and their case history
- Officer records within the jurisdiction
- Scanned documents and images

The administrator can Login and Logout. When the Administrator logs into the system, the system will check for validity of login.

III.HISTORY OF FINGERPRINT IDENTIFICATION

The history of using fingerprints as a scientific method for identification traces back to the 1880s, when Faulds suggested that latent fingerprints obtained at crime scenes could provide knowledge about the identity of offenders. In 1892, Galton published the well-known book entitled Fingerprints, in which he discussed the basis of contemporary fingerprint science, including persistence, uniqueness, and classification of fingerprints. Galton introduced Level 2 features by defining minutia points as either ridge endings or ridge bifurcations on a local ridge. He also developed a probabilistic model using minutia points to quantify the uniqueness of fingerprints. Although Galton discovered that sweat pores can also be observed on the ridges, no method was proposed to utilize pores for identification. In 1912, Locard introduced the science of poroscopy, the comparison of sweat pores for the purpose of personal identification. Locard stated that like the ridge characteristics, the pores are also permanent, immutable, and unique, and are useful for establishing the identity, especially when a sufficient number of ridges is not available. Locard further studied the variation of sweat pores and proposed four criteria that can be used for pore based identification: the size of the pores, the form of the pores, the position of the pores on the ridges, and the number or frequency of the pores. It was observed that the number of pores along a centimeter of ridge varies from 9 to 18, or 23 to 45 pores per inch and 20 to 40 pores should be sufficient to determine the identity of a person. In particular, pores provide essential information for fragmentary latent print examination since the number of minutia points in latent fragment prints is often too few. One such example is given in Fig. 2, where only one minutia is present in each fragmentary fingerprint, yet the attributes of about 20 pores in these images are sufficient to successfully determine a disagreement (non match) between the two prints. In 1962, Chatterjee proposed the use of ridge edges in combination with other friction ridge formations to establish individualization, which is referred to as edgeoscopy".

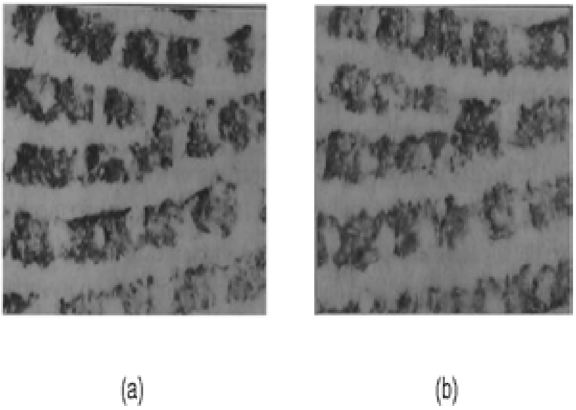


Fig.2. Role of pores in fragmentary latent print examination. (a) and (b) are fingerprint segments from different fingers. The two figures show a bifurcation at the same location on similar patterns. Normal examination would find them in agreement, but their relative pore locations differ

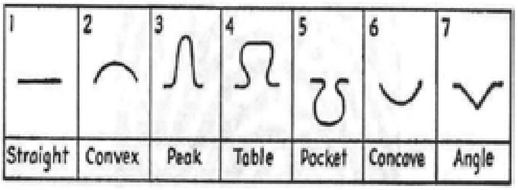


Fig. 3. Characteristic features of friction ridges.

Chatterjee discovered that some shapes on the friction ridge edges tend to reappear frequently and classified them into eight categories, namely, straight, convex, peak, table, pocket, concave, angle, and others (see Fig. 3). Subsequent research established that all the edge characteristics along friction ridges can be placed into one of these categories. It is believed that the differences in edge shapes are caused by the effects of differential growth on the ridge itself or a pore that is located near the edge of the friction ridge. In theory, the density of ridge edge features can be very large, e.g., given the average width of a ridge to be approximately 0.48 mm, a ridge 5 mmlong would contain approximately 20 edge characteristics. However, in practice, the flexibility of the friction skin tends to mask all but the largest edge shapes. Over the last 10 years, poroscopy and edgeoscopy have received growing attention and have been widely studied by scientists of ridgeology, a fundamental and essential resource for latent print examiners. It has been claimed that shapes and relative positions of sweat pores and shapes of ridge edges are as permanent and unique as traditional minutia points. And when understood, they add considerable weight to the conclusion of identification.

IV.BIOMETRIC SYSTEMS

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode.

- In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored in the system database. In such a system, an individual who desires to be recognized claims an identity, usually via a personal identification number (PIN), a user name, or a smart card, and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., "Does this biometric data belong to Bob?"). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

- In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database)

without the subject having to claim an identity (e.g.,"Whose biometric data is this?"). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

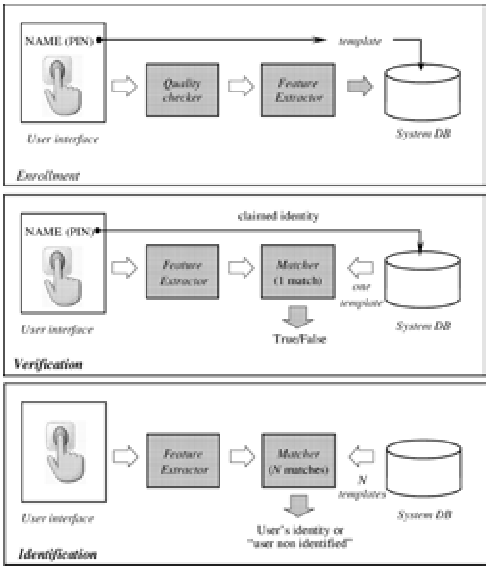
The block diagrams of a verification system and an identification system are depicted in Fig. 4; user enrollment, which is common to both of the tasks, is also graphically illustrated.

LIMITATIONS OF (UNIMODAL) BIOMETRIC SYSTEM

The successful installation of biometric systems in various civilian applications does not imply that biometrics is a fully solved problem. It is clear that there is plenty of scope for improvement in biometrics. Researchers are not only addressing issues related to reducing error rates, but they are also looking at ways to enhance the usability of biometric systems.

Biometric systems that operate using any single biometric characteristic have the following limitations.

1) Noise in sensed data. The sensed data might be noisy or distorted. A fingerprint with a scar or a voice altered by cold is examples of noisy data. Noisy data could also be the result of defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor) orFig. 4. Block diagrams of enrollment, verification, and identification tasks are shown using the four main modules of a biometric system, i.e., sensor, feature extraction, matcher, and system database.



Unfavorable ambient conditions (e.g., poor illumination of a user's face in a face recognition system). Noisy biometric data may be incorrectly matched with templates in the database resulting in a user being incorrectly rejected.

2) Intra-class variations. The biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment, thereby affecting the matching process. This variation is typically caused by a user who is incorrectly interacting with the sensor or when sensor characteristics are modified (e.g., by changing sensors—the sensor interoperability problem) during the verification phase. As another example, the varying psychological makeup of an individual might result in vastly different behavioral traits at various time instances.

3) Distinctiveness. While a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these traits. This limitation restricts the discriminability provided by the biometric trait. Golfarelliet al. have shown that the information content (number of distinguishable patterns) in two of the most commonly used representations of hand geometry and face are only of the order of 10 5 and 10 3, respectively. Thus, every biometric trait has some theoretical upper bound in terms of its discrimination capability.

4) Non universality. While every user is expected to possess the biometric trait being acquired, in reality it is possible for a subset of the users to not possess a particular biometric. A fingerprint biometric system, for example, may be unable to extract features from the fingerprints of certainindividuals, due to the poor quality of the ridges. Thus, there is a failure to enroll (FTE) rate associated with using a single biometric trait. It has been empirically estimated that as much as 4% of the population may have poor quality fingerprint ridges that are difficult to image with the currently available fingerprint sensors and result in FTE errors. Den Os et al. report the FTEproblem in a speaker recognition system.

5) Spoof attacks. An impostor may attempt to spoof the biometric trait of a legitimate enrolled user in order to circumvent the system. This type of attack is especially relevant when behavioral traits such as signature and voice are used. However, physical traits are also susceptibleto spoof attacks. For example, it has been demonstrated that it is possible (although difficult and cumbersome and requires the help of a legitimate user) to construct artificial fingers/fingerprints in a reasonable amount of time to circumvent a fingerprint verification system.

V.FINGERPRINT MATCHING ALGORITHAM

```
1.  Let us consider the following variables,
    Boolean g_firstStep
    Boolean g_secondStep
    Boolean result
    Byte g_FirstMinData
    Byte g_SecondMinData
    Byte g_MatchingMinData
2.  Capture the finger print image 1 using fingerprint scanner.
3.  Extract the minutiae data from the finger print image and
    encrypt it as the byte g_FirstMinData.
4.  Let, g_FirstStep = True g_SecondStep = False
5.  If g_FirstStep = True then,
a)  Capture finger print image 2.
b)  Extract the minutae data and encrypt it as byte g_SecondMinData.
c)  result = Register (g_FirstMinData, g_SecondMinData)
i)  if result = True then,
A.  g_SecondStep = True.
B.  Display message "Finger print data registered".
ii) Else
A.  g_SecondStep = False.
B.  If ERROR then, Display message "Recapture the finger
    print".
C.  Else Display message "Finger print data not registered".
6.  If g_SecondStep = True then,
a)  Get the finger print minutae data of finger print image 1
    in g_matchingMinData.
b)  result = Verify (g_SecondMinData, g_MatchingMinData).
c)  If result = True then, Display message "Finger prints
    MATCHED".
```

d) Else
i) If ERROR then, Display message “Recapture the finger print”.
ii) Else Display message “Finger prints NOT MATCHED”.

VI. ADVANTAGES & DISADVANTAGES

ADVANTAGES

- It reduces paper work.
- High accuracy.
- Time required is less.
- It is automated system

DISADVANTAGES

- It is stand alone application

VII.CONCLUSION

Therefore keeping in mind the flaws of the existing system, the proposed system seems to be far better and efficient in terms of technology and integration point of view.

Crime deterrence has become an upheaval task, so with the implementation of this system there will be a possibility to curb criminal offences to some extent.

REFERENCES

[1]. Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and SalilPrabhakar, Member, IEEE | An Introduction to Biometric Recognition. | [2]. Anil K. Jain, Fellow, IEEE, Yi Chen, Student Member, IEEE, and MeltemDemirkus, Student Member, IEEE Pores and Ridges: High-Resolution Fingerprint Matching Using Level 3 Features