Analysis and Detection of Altered Human Fingerprints using Minutiae Technique

Asst Prof. Ranjeet Suryawanshi¹, Tushar Kamble², Nikhil Joshi³, Abhijit Nikam⁴, Amol Khedkar⁵

¹Professor, Dept. of Computer Engineering, Trinity College of Engineering, Pune, India
²B.E. Dept. of Computer Engineering, Trinity College of Engineering, Pune, India

Abstract—Now a day’s biometric security is popularly used for unique authentication. Biometric authentication system provides more benefits than traditional id and passwords. Fingerprints of a person are unique throughout his/her life. Fingerprint biometric system is cheaper as compared to another biometric such as retina, DNA, face etc. altered fingerprint detection was an issue in existing systems, so we have proposed a system that will overcome it and detect the altered fingerprints. For analysis and detection of altered fingerprints we are using minutiae algorithm to detect fake users and altered fingerprints. Minutiae algorithm also categorized the fingerprints on the bases different patterns. We have proposed a system to that will automatically detect the altered fingerprints and produce the match count. We have also proposed that we will provide an alternative security to the users.

Keywords—Fingerprints, Minutia Distribution, AFIS, Ridge pattern, alteration.

I. INTRODUCTION

Developments in biometric recognition have provided strong mechanism for an authentication. The biometric recognition is based on face, retina, DNA, Voice, Fingerprint etc. Fingerprints is a unique identity of person. Fingerprints of person do not change in his/her entire life. It is easy to identified person with their fingerprints. Generally fingerprint recognization has been used by law enforcement agencies to identified victims [1] [2]. But today’s criminal history shows that people can changed their fingerprints by using abrasive materials such as acid, latex, plastic surgery etc. It can evade the fingerprint identification system. Thus fingerprint alternation is serious threat since this system is used by several law enforcement agencies to identified criminal records. Integrated Automated Fingerprint Identification System (IAFIS) is used to detect fingerprints, but it cannot detect the altered or fake fingerprints [4].

The important Moto behind introducing this paper is to build a system that is able of finding fake or Altered Finger prints and if a percentage value is found to be less than assume value than alternative security technique such as One Time Password (OTP), e-mail recovery, captcha will be provided.

A. Fingerprints

There are different pattern of Fingerprints like tiny ridges, whorl, double loop, Simple loop and valley on the tip of each finger. Fingerprints of two people are not same, they are an unique identity of person. The probability that your fingerprints will match with someone else’s is one out of 64 billion peoples [5] [10].

Fingerprints are more unique than DNA. The identical twins may have same DNA but their fingerprints will still differ. Fingerprints never change with people age also they are inexpensive to collect and analyze, so they are considered as ideal measure for security purpose. Fingerprints are an arrangement of ridges, known as friction ridges.

There are mainly 3 types of fingerprints pattern such as loop, whorl or arches:
Fig. 2 Fingerprint Patterns

a) Loops: Loops start on one side and exit on other side of the finger. Ulnar loop and Radial loop are two types of loops: The slope of ulnar loops is toward the little finger, while the slope of Radial loops is toward the thumb. About 60-70% loop occurs in fingerprint pattern.
b) Whorls: Whorls form a circular or spiral pattern, 25-35% whorls are seen in fingerprint pattern.
c) Arches: Arches are like narrow mountains that slope upward and then downward.

B. Detection of fingerprints

Occurrence of opening on the exterior part of the fingers, the outcome in the gathering of perspiration on the fingertips. This wetness remains on the object that is been touched by the person, which leaves the print on that object that is been touched by the individual. The prints of the individual can be visible by the eyes of a person which depends upon the surface of the object that is been touched. The visible surfaces could me glass, polished stone etc and invisible surfaces like wood, water, paper etc. The finger Prints left on the visible surface like polished stone can visualize with the help of powder & lifted with tape [6]. But the non-visible surfaces like wood requires special processing with help of lighting like X-rays and lasers to make it visible to our naked eyes.

There are two Approaches of detection of Fingerprints

a) Comparison of lifted Fingerprints
b) Live Scanning

In First Approach is mainly applicable in Forensics & Second approach is applicable in Security application & for identification of the authorized user, also used criminal cases to catch the thief.

C. Analysis and classification of fingerprints

The classification is done on the basis of patterns they form on the fingers. The key features are ridge endings and split. These features are called minutiae. There are various patterns formed the fingers that are single loop, double loops, whorl.

D. Types of Altered Fingerprints:

a) Obliteration,
b) Distortion,
c) Imitation

a) Obliteration: Obliteration is an one of the form alteration, which completely destroys ridge pattern on fingertips. Fingertips are obliterated due to cutting, burning, chemical reaction, abrading. Skin disease such as leprosy and side effect of cancer drug can also obliterate fingerprints [1].

b) Distortion : Distortion create unnatural ridged pattern on fingertip by removing portion of skin for fingertip and grafting them back in different positions. In distortion their local ridge structure remain similar to natural fingerprints but global ridge pattern is abnormal [1].
c) Imitation:

In Imitation friction ridge pattern is preserved by an elaborate a procedure of fingerprint alteration. In this area of skin is removed and the remaining skin twitched and seamed together [1].

II. RELATED WORKS

Soweon Yoon, Jianjiang Feng, and Anil K. Jain [1] have proposed a system that analyze and detect the altered fingerprints. They have developed an algorithm for automated detection of altered fingerprints based on characteristics of fingerprint orientation and minutiae distribution. They have also evaluated the capability of fingerprint image quality assessment software for detecting altered fingerprints. Since the software was found to have limited ability, the proposed system was developing.

Chandrakanth Biradar, Vijeth Rao [4] have combined various techniques to build a minutiae extraction and minutiae matcher algorithm. It have help to understand the procedure of altered fingerprint recognition.

Sonam Shukla, Pradeep Mishra [3] have proposed and optimized algorithm for fingerprint identification. The proposed system detects the set of minutiae iteratively in the inputted image. In proposed system the minutiae of only the template image need to estimated. The system is capable of differentiating fingerprints by setting appropriate threshold value.

Abhishek Rawat [5] has proposed a Hierarchical Fingerprint Matching System. They have proposed system that overcome challenges like template images, error introduced in registration due to problem like wrinkle, pruning.

III. EXISTING SYSTEM

In Existing System fingerprints quality assessment algorithms are designed. This algorithm checks if an image contains sufficient information say Finger Point for matching. It had a potential of checking whether an image is an original fingerprint or Fake fingerprint is restricted. Fingerprint quality control software can be evaded by obliterated fingertips depending on the area of the injury. If the area of injury is small the fake fingerprint is not detected by the existing System. In existing altered fingerprint recognition system, it gives only the acknowledgement that the inputted fingerprint image is altered or not.

Consider the following example

The Existing system is used in organization for providing authentication to the user. It uses the biometric device for scan the fingerprints. The image from biometric device is compared with the image already stored in database and provides the authentication accordingly. If the fingerprints are altered the system fails to recognize it.

Disadvantages of existing system:

- a) If damage area is small hard to detect
- b) More time required.
- c) Verified security is less.

IV. PROPOSED SYSTEM

In this paper we propose a system for altered fingerprint analysis and detection for real time authentication of user. This system will calculate the percentage of pre-match score and post-match score by using minutiae matching algorithm. Providing authentication is based on the output produced by the algorithm. If the percentage result is greater than or equal to certain assume value then the system directly authorizes the user. Else if the result is less than assume value the system will provide a One Time Password (OTP) facility.

We have provided a new feature in the proposed system that is in case if the person finger causes pruning or wrinkles the system does not provide access to the system due to less match count, so we have provided an alternative security to that person to get the access to the system.

The techniques used to build system:

A. Automated Fingerprint Identification System(AFIS)
B. Minutiae Based Matching Algorithm

A. Automated Fingerprint Identification System

The AFIS is a biometric identification technique which is used to store, obtain, and analyze digital images of fingerprints. This technique is used for general identification and fraud prevention. AFIS has been used on large-scale in civil identification projects [11] [12]. The main purpose of AFIS is to prevent multiple enrollments in welfare, driving licensing etc.

B. Minutiae Based Matching Algorithm

Minutiae based matching technique is mostly used in biometric fingerprint detection and authentication system. In a process of finger scanning minutiae are specific point in finger images.
A Minutiae has two types which are ridge ending and bifurcation. If the ridge curve terminates or line is ending then that point known as ridge ending and if the ridge is split from one path to multipath or line separated in 2 branches then that point known as ridge bifurcation[10]. The location and numbers of minutiae differs from finger to finger for particular person as well as person to person for any fingerprints. The number of Finger points is recorded for each finger, when a set of fingerprint is scanned from a person.

Minutiae convert the image in 2D. Minutiae based algorithm depend on various ridge flow pattern and it also required the quality of fingers image to verify that system [1].

**Mathematical Model for Finger Print**

**a) Orientation Field Approximation:**

To signify the global orientation field, a set of polynomial functions is used, which is not only computationally efficient, but also provides a good approximation in orientation field modeling. In the below expression \( \theta(x, y) \) represents orientation field, and the cosine & sine components of the doubled orientation at \((x, y)\) is shown by the polynomials of order \( n \):

\[
\begin{align*}
g^c_n(x, y) & = \cos 2\theta (x, y) = \sum_{i=0}^{n} \sum_{j=0}^{n} a_{ij} x^i y^j, \quad (1) \\
g^s_n(x, y) & = \sin 2\theta (x, y) = \sum_{i=0}^{n} \sum_{j=0}^{n} b_{ij} x^i y^j, \quad (2)
\end{align*}
\]

Where \( a(i, j) \) and \( b(I, j) \) are the polynomial coefficients for \( g^n c (x, y) \) and \( g^n s (x, y) \) respectively. The model becomes flexible when the polynomials order increases, and also rapid changes in orientation field. When the polynomials order is too low, the orientation field approximated by the model is pretty unusual from the true orientation field [1] [3].

**b) Feature Extraction**

While the polynomial of Lower order model can sufficiently represent smooth (global) changes in the orientation field. The dissimilarity between the observed orientation field and the modeled orientation field indicates the locations and the amount of the rapid changes in the ridge flow [1] [3].

We define the error map \( \varepsilon(x, y) \) as

\[
\varepsilon(x, y) = \min(|\theta(x, y) - \hat{\theta}(x, y)|, \pi - |\theta(x, y) - \hat{\theta}(x, y)|)/(\pi/2)
\]
c) Analysis of Minutiae Distribution:

Let the set of minutiae of the fingerprint be denoted by $S_m$, i.e.

$S_m = \{x|x=(x, y)\}$ is the position of minutiae

System Architecture

![Fig. 6 System Architecture of Proposed System](image)

The above diagram represents the system architecture of our proposed system. In registration phase fingerprint images are scanned and provided as input, while scanning image preprocessing operation are performed. Here a quality is image is captured first and then it is converted in form of template. In feature extraction the images is classified according to different pattern. Minutiae points are determined from the image. The acquired data is stored in database.

In authentication phase the preprocessing operation and feature extraction is once again performed on inputted image. The gain image is searched in the database for its probable match. Depending on the result generated further action is performed. If the result is greater than or equal to the assume value then the user is authenticated else if image is altered then alternative security is provided.

V. CONCLUSION

Our proposed system deals with the problems encountered by traditional systems. We use the minutiae based matching algorithm to analyze and detect the altered fingerprint, if we detect the altered fingerprint the user will be blocked. We will provide an alternative security to the user if the match count is less. We are going to minimize the disadvantages of existing system.

REFERENCES