ISSN:0975-9646

Efficient Biometric Authentication Technique using Fingerprint

Vishal Vishwas Jadhav[#1], Rahul Ratnakar Patil[*2], Rohit Chandrashekar Jadhav[#3],Adwait Niranjan Magikar[#4]

Department of Computer Engineering, PES's Modern College of Engineering
Shivajinagar, Pune – 411005, India

Abstract— **In this paper we have to explain about Fingerprint Recognition System and Finger-Print pattern, Features, as well as its algorithm.**

We mainly, emphasis on the problem facing due to system which uses conventional characteristics like username and password or security PIN Number and Which solution is better for such problem.

The purpose of this work is to make automated system based on biometric fingerprint authentication. In this case, finger-print that are useful for the various services of government or organization or business.

Keywords— **finger-print, patterns, minutiae features, biometrics, verification, enrolment, identification**

I. INTRODUCTION

The most of the authentication systems use User-name – Password, Security Pin, One Time Password, Photo ID etc., and each system faces common problem of to identify/verify authorized person. The system may give chance to any dishonest person if he/she knows your password or Security PIN.

From the above paragraph, we can make conclusion that the Password is not suitable for our authentication system. Due to this, we have to explore new authentication system i.e., biometric authentication system. Biometric uses human's physiological and behavioural characteristics.

The Biometric characteristics have good extent of uniqueness, availability, collectability. If we use this characteristics in our daily authentication system, the system gives good performance and throughput.

In this paper, we mentioned about finger-print authentication system based on biometric finger-print recognition.[1]

In all biometric techniques, fingerprint recognition is considered the most prominent and reliable one.

II. FINGER-PRINT PROPERTIES

Finger-Print has some properties as follows :[2]

1) Universality: Each person has its own Finger-Print characteristic.
2) Distinctiveness: No two persons have same Finger-Print i.e., It is distinct characteristic.
3) Permanence: The Finger-Print characteristic cannot change with respect to time and place. It is invariant over a period of time.
4) Collectability: the characteristic can be measured quantitatively. In India, the finger-print database can be collected UID (ADHAR Project) Database.
5) Performance: It gives achievable recognition accuracy in less amount of time, as well as reduces the operational and environmental factors that affect the accuracy and speed.
6) Acceptability: It gives acceptance of people in their daily use.
7) Circumvention: It reflects how easily the system can be trapped by fraudulent person.

III. FINGER-PRINT ANALYSIS

The analysis of fingerprints for matching purposes can be done using the several features of the Finger-print pattern.

These includes:
1. Patterns
2. Minutiae Feature

It is also necessary to know the structure and properties of human skin, for successfully applying some of the image processing technologies.

A. Patterns

The three basic patterns of fingerprint ridges:

1. Arch: The ridges or valleys enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.
2. Loop: The ridges or valleys enter from one side of a finger, form a curve, and then exit on that same one.
3. Whorl: Ridges or valleys form circular ring around a central point of the finger.

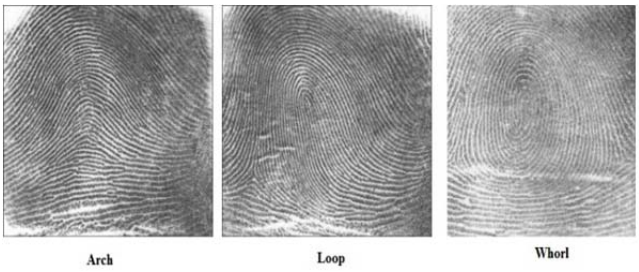

Fig. 1 : Finger-Print Patterns

B. Minutiae Features

There are three basic types of Minutiae Features:

1. Ridge Ending: The Point at which ridge is ended.
2. Bifurcation: The Point at which two ridges are bifurcated. Or they meeting with each other.
3. Dot: This is a short ridge also called as Dot.
4.

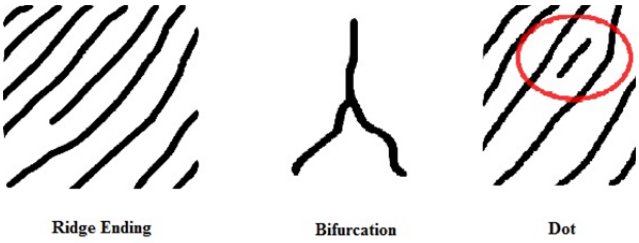

Fig. 2 : Finger-Print Minutiae Feature

IV. FINGER-PRINT MATCHING ALGORITHM

Fingerprint Matching algorithms are used for comparison of previously stored templates of fingerprints with user fingerprints for authentication process. In order to do this either the original image must be directly compared with the user's fingerprint image or certain features must be compared.

Geometry based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) and minutiae features between a previously stored template and a user fingerprint. The requirement is that the images can be aligned in the same orientation. To do this, the algorithm finds a central point in the user's fingerprint image and centers on that. In a geometry-based algorithm, the template contains the type, size, and orientation of patterns and features within the aligned fingerprint image. The user's fingerprint image is graphically compared with the stored template to determine at what extent they match.

V. FINGER-PRINT RECOGNITION[5]

The basic blocks of Finger-print recognition system are as follows:

1. User Input: The user input is an input to recognition system which takes the biometric input or Identification number in case of verification.

2. Pre-processing: In this block, the data which is accepted by the user input block will be converted into a 2D matrix and is then forwarded to the feature extractor block.
   Pre-Processing Consists of various types image processing techniques:
   a. Alignment
   b. Local Ridge Orientation
   c. Local Ridge Frequency
   d. Enhancement

3. Quality Checker: It checks the quality of the given finger-print input before feature extraction.

4. Feature Extractor: The work of the feature extractor is to extract the unique feature (i.e., patterns and minutiae features) of the data and pass it to the template generator block.
   The Fingerprint Patterns are Arch, Loop and Whorl. The Minutiae Features are Ridge Ending, Bifurcation and Dot

5. Template Generator: The template generator is generated by the features extracted by the feature extractor.
   During enrolment phase the template of the new user is added in the System database. During verification/identification phase the user template is passed to the Matcher.

6. System Database: The use of System Database is to store the user's fingerprint template and provide the same whenever requested by the System or Matcher Mechanism.

7. Matcher: It plays an important role of the matching during the verification or identification phase.

   When the template is sent by the Template generator needs to be verified or identified, the matcher requests the data from the System Database and compares the template which is received by the user. If the stored template matches, user will be provided access to the application else access is denied.

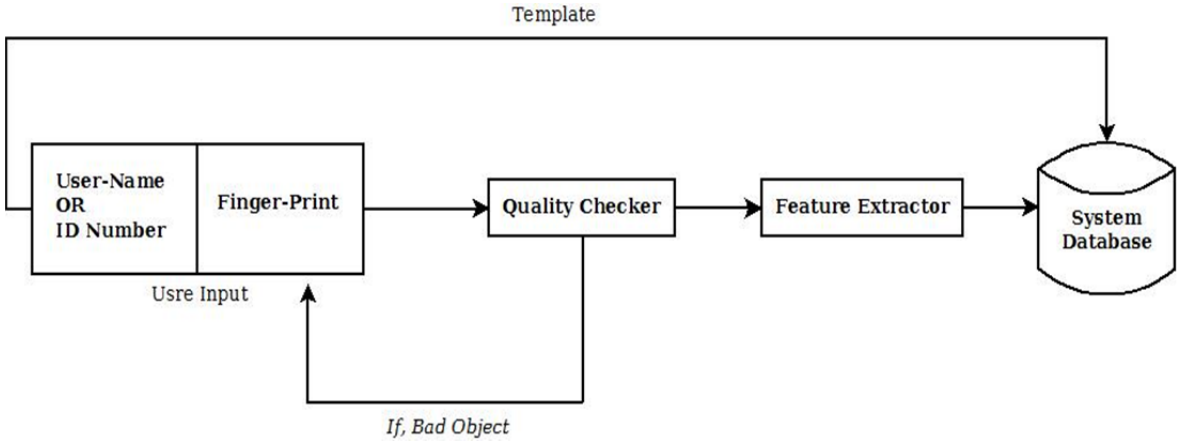

Fig. 3 : Enrolment of Finger-Print[8]

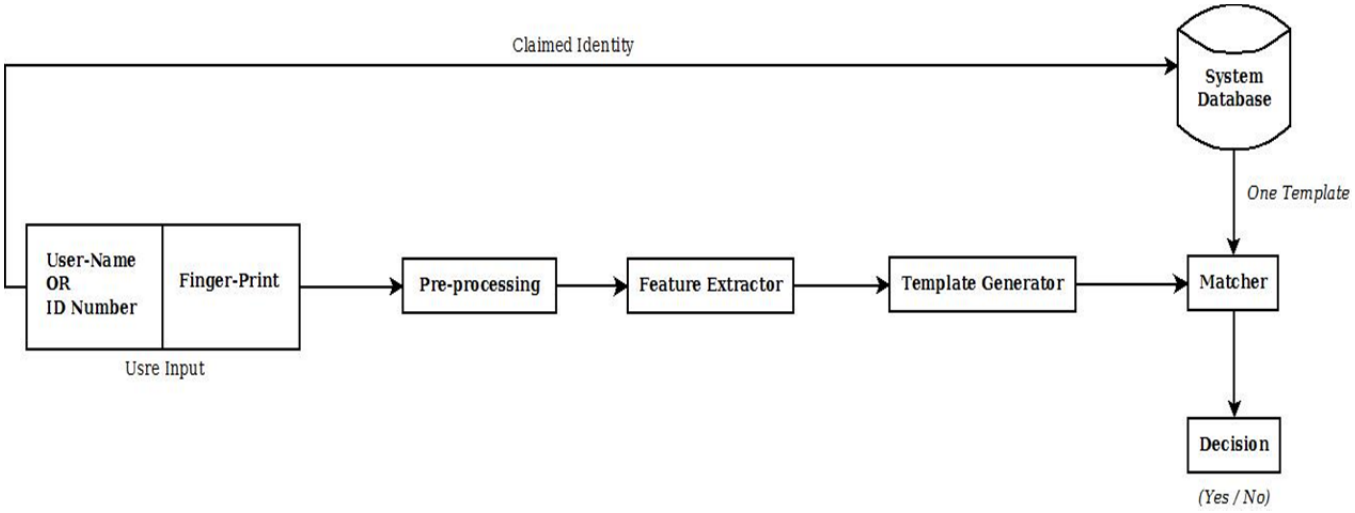

Fig. 4 : Verification of Finger-Print[8]

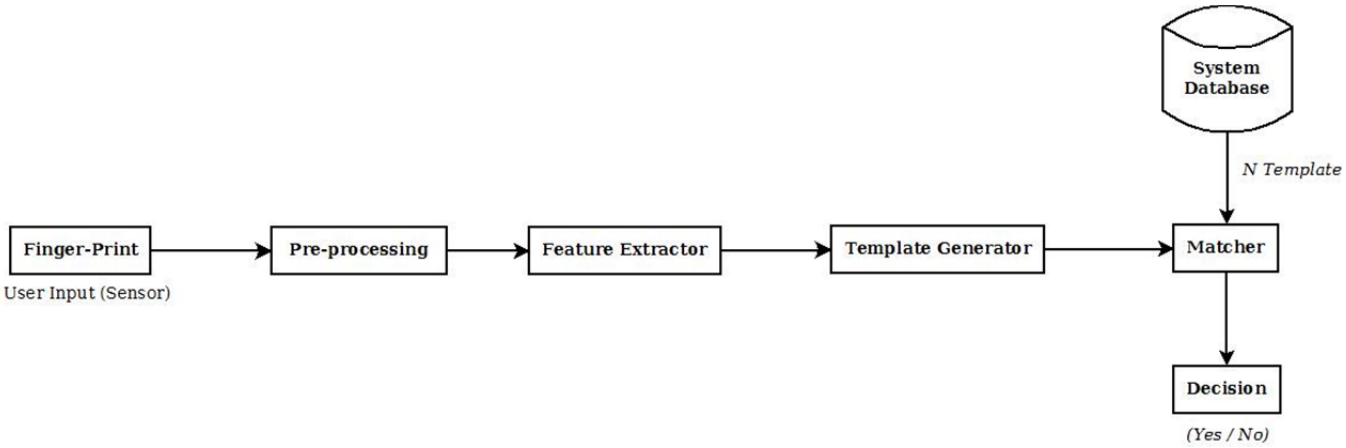

Figure 5 : Identification of Finger-Print[8]

VI. FINGER-PRINT PAYMENT SYSTEM

Biometric payment technology allows the user to pay with the touch of a finger or thumb on a fingerprint scanner linked to a payment database.

In 2009, report says Wal-Mart and Costco are investigating biometric payment systems that scan people's fingers to identify them and make payment process.[5]

The analyst report says a 20% cut in Wal-Mart's payment-processing costs could change to a 3-4% increase in earnings per share within three years

Pay-by-Touch and Bio-Pay state transaction times range from 5 to 15 seconds i.e., 70% faster than traditional forms of payment

VII. CONCLUSION

In this paper, we have discussed various fingerprint recognition patterns, features, algorithm and its analysis techniques. We have also discussed the implementation of Enrolment, Verification and Identification of Fingerprints.

The Proposed Fingerprint recognition system using Biometrics, the security and potential of existing system will be enhanced. This system will be generic and it can be used by multiple government services like payment of Electricity bill, Telephone bill, Income Tax returns, etc. Due to this, Government will be able to make fair and accurate decisions for Public Welfare. Optimized strategies extracted from this decisions can be developed to increase potential and profit of Organization.

Hence, this paper presented a type of this kind of Finger-print recognition system and this system that can be easily implemented. Meanwhile, the full implementation of such a model will help to achieve our objectives like security, efficiency, reliability and easy-to-use by many people in the world.

ACKNOWLEDGEMENT

Our thanks to the experts who have contributed towards survey of this paper.

REFERENCES

[1] Mangala Belkhede, Veena Gulhane, and Dr. Preeti Bajaj. Biometric mechanism for enhanced security of online transaction on android system: A design approach. International Conference on Advanced Communications Technology, February 2012.

[2] ANIL K. JAIN, LIN HONG, SHARATH PANKANTI, and RUUD BOLLE. An identity-authentication system using fingerprints. IEEE, 1997.

[3] Anil K. Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. IEEE, 2004.

[4] Karamjeet Kaur and Dr. Ashutosh Pathak. E-payment system on e-commerce in india. International Journal of Engineering Research and Applications, 2015.

[5] Dileep Kumar and Yeonseung Ryu. A brief introduction of biometrics and fingerprint payment technology. International Journal of Advanced Science and Technology, 2009.

[6] Ajeet Singh, Karan Singh, Shahazad, M. H. Khan, and Manik Chandra. A review: Secure payment system for electronic transaction. International Journal of Advanced Research in Computer Science and Software Engineering, 2012.

[7] Umut Uludag and Anil K. Jain. Attacks on biometric systems: A case study in fingerprints. The International Society for Optical Engineering, 2004.

[8] Prof.ShilpaP. Kodgire and Anju Mohan, Automatic Fingerprint Recognition Systems: A Review, International Journal of Electronics, Communication & Soft Computing Science and Engineering, 2014