ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Preventing Mobility Device Intrusion And Theft Using Biometric Fingerprint Recognition

Vanitha.M[1], Vidhya Gandhi.P[2], Rajkumar.M[3], Rajkumar.S[4]

Final year students, B.E-CSE, K.S.Rangasamy College of Technology, Tiruchengode, Tamilnadu, India[1, 2, 3]

Assistant Professor, K.S.Rangasamy College of Technology, Tiruchengode, Tamilnadu, India [4]

ABSTRACT: Fingerprint based authentication system project is used to more secure your system compare to all other security device which uses biometric reader. In the project data from the finger print is send to the system through port and fingerprint reader is used to read the data from port and validate the data with your data (what ever entered). If the validation output success then the user would be allowed else it blocks the user to allow. The system has to use third party component to read or send the data through the serial port. In the project implementation you have to enter your data (user id and password) after register finger print, so data for the validation could be catch directly from finger print through the serial port. After read the data from serial port using third party component in biometric database FVC2004, it checks whether the entered by the user and reading data's are match or not. After your successful validation (match) you can move ahead for further works else you can't. In an existing system we secure the system through check whether the user id and password match with data's in database or not, but it's possible to steal the data from the database. So it's not highly secured so go for the implementation of fingerprint based authentication system project. Fingerprint based authentication system project is more secured compare to all other securities, because you can't stole any user information due to high security. Information stored in fingerprint is only known by the user so even through unknown person uses the fingerprint they can't enter the correct data while we checking. If the third person uses fake finger print to access the system, which is also recognized and block the user to use. Finally we conclude no way to steal the user's data and we can maintain the user's information safely and securely, so fingerprint based authentication system is more secured compare to all other security device or system.

I. INTRODUCTION

1.1 INTRODUCTION TO BIOMETRIC RECOGNITION

A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition, or simply biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics.

Humans have used body characteristics such as face, voice, gait, etc. for thousands of years to recognize each other. Alphonse Bertillon, chief of the criminal identification division of the police department in Paris, developed and then practiced the idea of using a number of body measurements to identify criminals in the 19th century. What biological measurements qualify to be a biometric? Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- Universality: each person should have the characteristic;
- Distinctiveness: any two persons should be sufficiently different in terms of the characteristic;
- Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.

II. EXISTING SYSTEM

Recently, due to the increasing demands of the fast-growing consumer electronics market, more powerful mobile consumer devices are being introduced continuously. With this evolution of consumer electronics technologies, personal information in consumer devices also becomes increasingly rich and valuable. For example, cell phones are now used for the payment of goods, bank transfer, stock dealing, and e-mail checking. This convenience also means that it can be a disaster if the cell phone is lost or stolen. To address this problem, secure user identification technologies for consumer devices are being introduced. Specifically, a variety of biometric sensor technologies are studied. Compared to key and password methods, these biometric sensor technologies are more convenient and accurate as well as do not have the danger of password exposure.

(b) Consumer electronics devices for secure user identification.

Fig. 2.1 Fingerprint-based secure user identification systems.

IMPLEMENTATION STEPS OF EXISTING SYSTEM

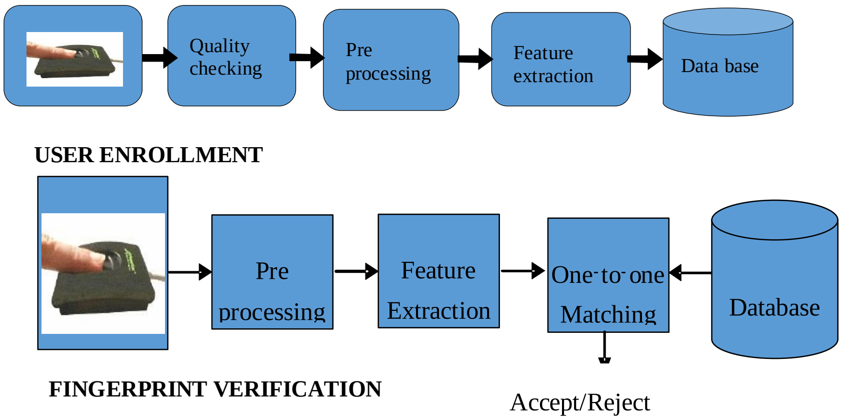


Fig. 2.2 User enrollment and fingerprint verification phases of the fingerprint-based user identification system.

In the user enrollment phase, the quality of a fingerprint image is first checked and then preprocessing is performed. Then, features of the fingerprint such as minutiae are extracted and stored on the database. In the fingerprint verification phase, preprocessing and feature extraction of input data are first performed similar to the user enrollment phase. Then one-to-one matching between the input data and the template data enrolled in the database is performed.

DRAWBACKS OF EXISTING SYSTEM

While our implementation is successfully able to decide whether 2 fingerprint images belong to the same finger or not, it is by no means perfect. As shown by the results, there are erroneous results produced sometimes. Also, the computation time of the algorithm is still too high for a seamless real-time application.

In order to make our implementation more efficient, there is scope for improvement in the image enhancement step and minutiae matching algorithm. Image enhancement is generally the most crucial step as thinning and minutiae-extraction simply cannot proceed to give any useful results as long as the quality of the image is very high. We have tested out algorithm on online images of a reasonably high quality.

III. PROPOSED SYSTEM

The proposed system is to computerize for various purposes and maintained client process. The latest technology will be used in the proposed system. this system allows valid user to access otherwise gives alert message to the owner , this message easy find the theft using Orientation Extraction Algorithm(OEA).

ADVANTAGES

The required information can be retrieved easily.

- People can get drives and download files from remote system.
- Time will not be wasted in the process.
- Corrections can be made easily.
- High speed.
- Wastage of manpower is reduced.
- Less Time

3.1 STEPS INVOLVED IN FINGERPRINT RECOGNITION

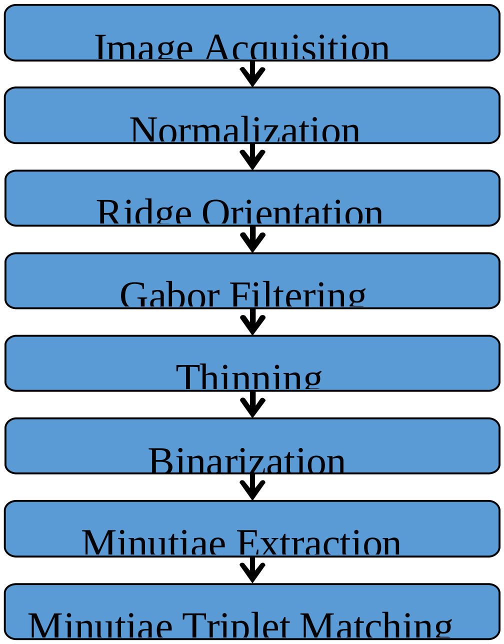


Figure: 3.1.1 Steps For Fingerprint Recognition

FINGERPRINT DATABASE USED

In order to test the validity of our implementation, we have used the FVC2004 fingerprint image database. FVC2004 was the Second International Competition for Fingerprint Verification Algorithms and we acquired the database that was provided to the participants of this competition. The images used were online images of a reasonably good quality. Most parts of most of the fingerprint images were recoverable and did not produce too many spurious minutiae after enhancement and thinning.

RIDGE ORIENTATION

Ridge orientation is the process of obtaining the angle of the ridges throughout the image. Ridge orientations are calculated on a block-basis for a WxW block. W is generally equal to 16.

IMAGE ENHANCEMENT

Implications of poor quality image:

- A significant number of spurious minutiae may be created
- A large percent of genuine minutiae may be ignored, and
- Large errors in their localization (position and orientation) may be introduced.

NORMALIZATION

For normalization we have done simple histogram equalization, which enhances the contrast of images by transforming the values in the fingerprint image.

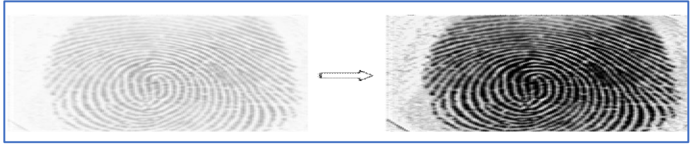


Figure 3.1.3 Fingerprint Normalization

FILTERING

The sinusoidal-shaped waves of ridges and valleys vary slowly in a local constant orientation. Therefore, a band-pass filter that is tuned to the corresponding frequency and orientation can efficiently remove the undesired noise and preserve the true ridge and valley structures. Gabor filters have both frequency-selective and orientation selective properties and have optimal joint resolution in both spatial and frequency domains. Therefore, it is appropriate to use Gabor filters as band-pass filters to remove the noise and preserve true ridge/valley structures.

THINNING

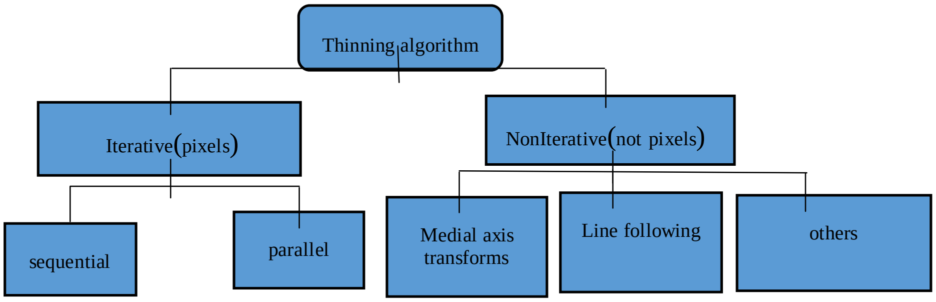


Figure 3.1.4 classification of common thinning

The above figure shows a classification of thinning algorithms. The second class of sequential thinning algorithms is parallel. In parallel thinning algorithms the decision for individual pixel deletion is based on the results of the previous iteration. Like sequential algorithms, parallel thinning usually considers a 3*3 neighborhood around the current pixel.

MINUTIA EXTRACTION

Our implementation of fingerprint identification and verification is based the topological structural matching of minutiae points. We only consider two kinds of minutiae; ridge endings and bifurcations as shown in the following figure: ridge endings and bifurcations as shown in the following figure:

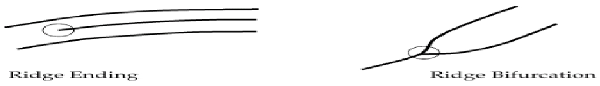


Figure 3.1.5 Minutiae structure

MINUTIAE MATCHING

Minutiae matching is the step which comes after minutiae extraction and it is here that match the minutiae obtained from two sample fingerprint images and test whether they are from the same fingerprint or not. However, a crucial step that needs to be carried out before they can use brute force and match minutiae on two images is alignment of the images. Alignment is necessary so that correctly match the images. They also need to take care of difference in positioning of minutiae due to plastic deformations in the finger.

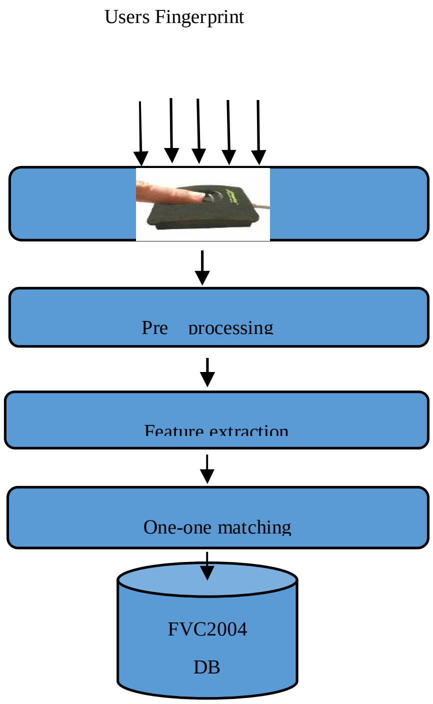
3.2 IMPLEMENTATION TECHNIQUES OF THE PROPOSED SYSTEM

IV. SYSTEM MODEL

MODULE

The below modules are used in project. They are

- Login
- Read Finger Print Image
- Verification of current user fingerprint
- Permitted to access
- Send alert message to the owner



USER ENROLLMENT

Figure3.2.1 User enrollment Technique using FVC2004 DB

V. LOGIN

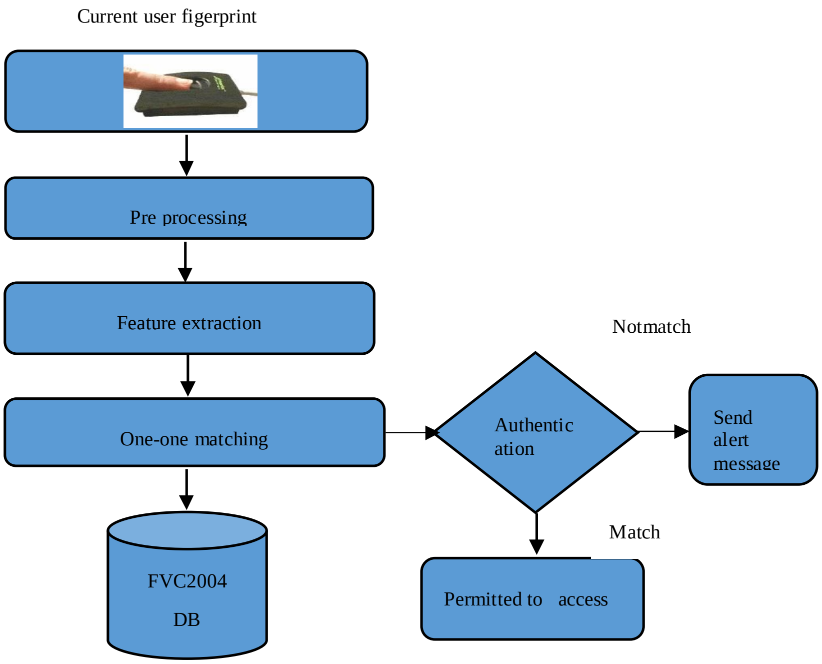
In the proposed project used to implement the security through fingerprint with vb.net coding. Connect the fingerprint sensor and run the vb.net coding and check the fingerprint and then allow accessing PC using FVC2004 DataBase. It is important to recognize that keystroke dynamics, when layered on user ID and password, incorporates the statistical probability of password access control.

VI. READ FINGER PRINT IMAGE

After run the project admin fix the fingerprint image. The image value sends to pc through RS232 cable. If correct value means allow to access the PC otherwise not allowed to access PC and send alert message to the owner. In the user enrollment phase, the quality of a fingerprint image is first checked and then preprocessing, which will be described in fingerprint image processing stage, is performed. Then, features of the fingerprint such as minutiae are extracted and stored on the database.

VII. VERIFICATION OF CURRENT USER FINGERPRINT

In the fingerprint verification phase, preprocessing and feature extraction of input data are first performed similar to the user enrollment phase. Then one-to-one matching between the input data and the template data enrolled in the database is performed. Finally, the user is accepted or rejected based on the result of the matching process. A fingerprint image acquired from a user is generally a gray-scale image. For easy processing, a binarization step is needed that simplifies the image. In the binarization step, a fingerprint image is converted into a binary image that only consists of black and white.



FINGERPRINT VERIFICATION

Figure 7.1 Fingerprint verification phases of the fingerprint-based user identification system.

VIII. PERMITTED TO ACCESS

If current user fingerprint matches with any one of the FVC2004 Database fingerprints then it will allow access to the PC or laptop. Although two fingerprint images are obtained from the same user, they may be identified as different ones due to different environments.

IX. SEND ALERT MESSAGE TO THE OWNER

If current user fingerprint does not matches with any one of the FVC2004 Database fingerprints then send an alert message to the owner using GSM method. This alert message used to find the theft using location finding algorithm like Orientation Extraction Algorithm (OEA).

X. CONCLUSION

The Fingerprint Based System Security System has been developed to satisfy all proposed requirements. The process of interview and Certificate details is maintained more simple and easy. The system is highly scalable and user friendly. Almost all the system objectives have been met. The system has been tested under all criteria. The system minimizes the problem arising in the existing manual system and it eliminates the human errors to zero level.

All phases of development were conceived using methodologies. User with little training can get the required report. The software executes successfully by fulfilling the objectives of the project. Further extensions to the system can be made required with minor modifications there is scope for improvement in the image enhancement step and minutiae matching algorithm.

REFFERENCES

[1] Anil Jain .K, Arun Ross and Salil Prabhakar2(2007) "An Introduction to Biometric Recognition", Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1,pp.896-917.

[2] Bertoncini .C.A, and Hinders .M.K,(2010) "Fuzzy classification of roof fall predictors in microseismic monitoring", Measurement, vol. 43, no. 10, pp. 1690–1701.

[3] Chen .H, Shi .Q, Tan .R, Poor .H, and Sezaki .K,(2010) "Mobile element assisted cooperative localization for wireless sensor networks with obstacles," IEEE Trans. Wireless Commun., vol. 9, no. 3, pp. 956–963.

[4] Jain A .K., Ross .A., and Prabhakar .S.(2011), "Fingerprint Matching Using Minutiae and Texture Features" , Proc. of International Conference on Image Processing,Vol.4,NO.7,pp-1211-1223.