International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.2, Issue No.9, pp : 892-894 1 Sept. 2013

Biometric Security System based on Fingerprint Recognition

Amber Habib, Ijlal Shahrukh Ateeq, Kamran Hameed
Sir Syed University of Engineering and Technology, Department of Biomedical Engineering, Karachi, Pakistan. ishahrukh@yahoo.com

ABSTRACT:

Biometrics refers to methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In information technology, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.Biometric characteristics can be divided in two main classes:

Physiological are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, hand and palm geometry, iris recognition, which has largely replaced retina, and odor/scent.

Behavioral are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics for this class of biometrics.

This paper presents a new idea for biometric security system based on fingerprint recognition. The paper refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. The old way of providing personal information is taken over by biometric which extract information from a person's body itself. [1]

This paper deals with all information regarding the said biometric security system, and also discusses its characteristics, features, and applications. The biometric systems are really helpful in many places which require high security and protection.

Keywords: biometrics, template, image enhancement, minutiae.

I. THEORETICAL INVESTIGATION:

The process model behind a biometric system is generally the same regardless of the biometric being used. While there will be obvious differences in how measurements are collected, stored, etc., depending on the biometric chosen or the specific product, the theoretical model remains the same across all types.

Following is a brief summary of the processes utilized in most biometrics systems.

- The biometric system/device.
- Live sample is presented for collection and enrollment.
- Template is built and stored on the Network.
- Live sample is presented for comparison and matching.
- Transaction data or audit trail is stored after verification.

Generally, a biometric system for positive verification purposes proves that the individual is the same person that was enrolled in the security system. Humans have used body characteristics such as face, voice, and gait for thousands of years to recognize each other.

Fingerprint recognition systems functionality relay on the processing power of the underlying system that implements efficient algorithm for the fingerprint image analysis rather than on the image data acquisition principle efficiency.

PRINCIPLE OF OPERATION:

The main technologies used to capture the fingerprint image with sufficient detail are optical, silicon, and ultrasound. There are two main algorithm families to recognize fingerprints:

1. Minutia matching compares specific details within the fingerprint ridges. At registration (also called enrollment), the minutia points are located, together with their relative positions to each other and their directions. At the matching stage, the fingerprint image is processed to extract its minutia points, which are then compared with the registered template.

2. Pattern matching compares the overall characteristics of the fingerprints, not only individual points. Fingerprint characteristics can include sub-areas of certain interest including ridge thickness, curvature, or density. During enrollment, small sections of the fingerprint and their relative distances are extracted from the fingerprint. Areas of interest are the area around a minutia point, areas with low curvature radius, and areas with unusual combinations of ridges.

The two main functions of a biometrics system are storing and comparing. The storing process differs between different systems, as some systems store a great deal more information and will digitize and compress the information.
Once the print information is stored in an accessible database, a user's prints can be compared whenever the system is accessed. You are authenticated when both the stored and user's print match. Finger print readers use this uniqueness to generate a code - rarely do they actually use the full print for identification - based on areas where print lines merge, form, or loop like the round "whirl" that you can find in the middle of all finger prints.

II. THE DESIGN OF OUR EQUIPMENT

Components are divided into hardware and software.

2.1 Hard ware

Finger print scanner
Interfacing components
Acquisition device

2.2 Software (MATLAB)

III. FEATURES OF THE SYSTEM

The basic block diagram of a biometric system works in the following two modes. In verification mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. In Identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. [1]

1. MATLAB software

An improved algorithm used in fingerprint matching, highly recommended for high-performance applications, biometric system improved database.

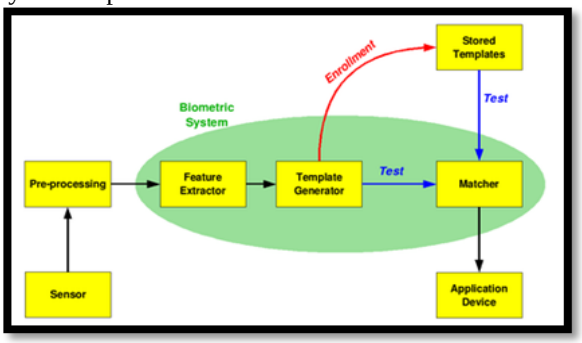


Fig. Biometric system diagram

2. Sensors

Block (sensor) is the interface between the real world and our system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics we want to consider.

3. Pre-processor

Performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. Removing some noise), to use some kind of normalization, etc.

4. Feature extractor

We have to extract the features we need. This step is really important we have to choose which features to extract and how. Moreover we have to do it with certain efficiency.

5. Template generator

We can have a vector of numbers or an image with particular properties: all those data are used to create a template. A template is a synthesis of all the characteristics we could extract from the source, it has to be as short as possible (to improve efficiency) but we can't discard too many details, thus losing discrimination ability. Then the behavior of the system changes according to what was requested.

6. Matcher

It matches the image with the previously stored memory.

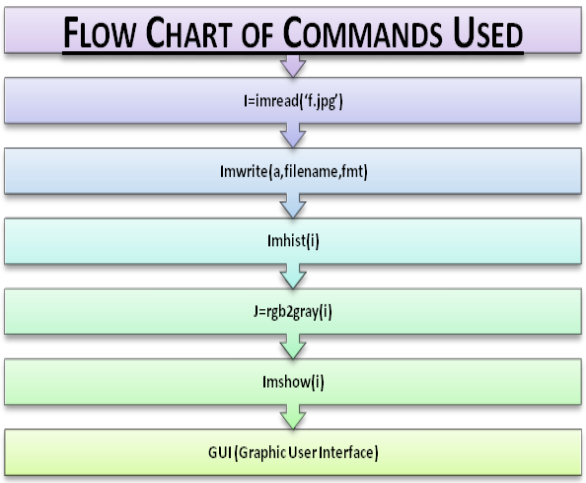
7. Stored templates

The obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hammering distance).

8. Application device:

The decision that the matcher has taken is sent as output, so that it can be used for any purpose .it can allow a purchase or the entrance in a restricted area.

FLOW CHART OF COMMANDS USED:



Following were the commands being used:

I=imread('f.jpg')

Description: it reads a grayscale or color image from the file specified by the string filename. If the file is not in the current folder, or in a folder on the MATLAB path, specify the full pathname.

Imwrite(a,filename,fmt)

Description: it writes the image A to the file specified by filename in the format specified by format. Filename is a string that specifies the name of the output file.

Imhist(i)

Description: it displays a histogram for the image I above a grayscale color bar. The number of bins in the histogram is specified by the image type. If I is a grayscale image, imhist uses a default value of 256 bins. If I is a binary image, imhist uses two bins.imhist (I, n) displays a histogram where n specifies the number of bins used in the histogram. N also specifies the length of the color bar. If I is a binary image, n can only have the value 2.

J=rgb2gray(i)

Description: converts the true color image RGB to the grayscale intensity image I. Rgb2gray converts RGB images to grayscale by eliminating the hue and saturation information while retaining the luminance.

Imshow(i)

Description: It displays the grayscale image I, specifying the display range for I in [low high]. The value low (and any value less than low) displays as black; the value high (and any value greater than high) displays as white. Values in between are displayed as intermediate shades of gray, using the default number of gray levels. If you use an empty matrix ([]) for [low high], imshow uses [min(I(:)) max(I(:))]; that is, the minimum value in I is displayed as black, and the maximum value is displayed as white.

GUI (Graphic User Interface)
Description: A graphical user interface (GUI) is a graphical display in one or more windows containing controls, called components that enable a user to perform interactive tasks. The user of the GUI does not have to create a script or type commands at the command line to accomplish the tasks. Unlike coding programs to accomplish tasks, the user of a GUI need not understand the details of how the tasks are performed.

V. MAIN FINDINGS OF THE PROJECT

- Following are the main finds of our project:
- Take finger print impression from general purpose scanner.
- Load the image impressions on MATLAB by using MATLAB command.
- Taking histogram of these images.

Fig: Scanned fingerprints

- Comparing the results of this impression by using MATLAB command.
- Compile all these to get the objective of this project.

VI. APPLICATIONS OF BIO-METRIC SECURITY SYSTEM

Following are the applications of bio-metric security system
(1) Electronic ID card.
(2) Computer network login.
(3) Electronic data security.
(4) Bio metric attendance.
(5) Corpse identification.
(6) Correctional facility.
(7) Cryptographic techniques.
(8) Biometric-based patient information system.

VII. CONCLUSION

7.1 PROBLEMS ENCOUNTERED

The major difficulties that we went through were with respect to programming. To start off with, we first had trouble in matching the matrix. Then the next problem that we came across was with the storage of the fingerprint data in MATLAB. Then, the third problem that we had to come across was the verification of fingerprint. We tried a couple of commands in MATLAB to resolve the problem. Then due to the difference of version, some of the commands that we tried did not work. To overcome that problem, we installed the new version of MATLAB.

We would like to conclude the topic in a few lines by sharing that reliable personal recognition is critical to many business processes. . As biometric technologies advance, uses and applications become more prevalent and relevant to many different industries.

VIII. REFERENCES

i. en.wikipedia.org/wiki/biometrics#performance

ii. *d. A. Black, "forgery above a genuine signature," j. Criminal law,Criminal. Police Sci., vol. 50, pp. 585–590, 1962.*

iii. *T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of Artificial gummy fingers on fingerprint systems," Proc. SPIE, vol. 4677, pp. 275–289, Feb. 2002.*

iv. *A. K. Jain, R. Bolle, and S. Pankanti, Eds., Biometrics: Personal Identi- Fication in Networked Society.*

v. *(2002) Schiphol Backs Eye Scan Security. CNN World News. [On-Line].*

vi. *2002/WORLD/europe/03/27/schiphol.security*

vii. *J. Daugman, "Recognizing persons by their Iris patterns," in Biometrics: Personal Identification in a Networked Society, A. K. Jain, R. Bolle, and S. Pankanti, Eds.*

viii. *L. O'Gorman, "Seven issues with human authentication technologies,"In Proc. Workshop Automatic Identification Advanced Technologies (Au-toid), Tarrytown, NY, Mar. 2002, pp. 185–186.*

ix. *A. Eriksson and P. Wretling, "How flexible is the human voice? A case Study of mimicry," in Proc. Eur. Conf. Speech Technology, Rhodes, 1997, pp. 1043–1046*

x. *D. A. Black, "Forgery above a genuine signature," J. Criminal Law, Criminol. Police Sci., vol. 50, pp. 585–590, 1962.*

xi. *L. Hong and A. K. Jain, "Integrating faces and fingerprints for personal Identification," IEEE Trans. Pattern Anal. Machine Intell., vol. 20, pp. 1295–1307, Dec. 1998.*

xii. *Paul Rosenzweig, Alane Kochems,and Ari Schwartz. (June 21, 2004). Biometric Technologies: Security, Legal, and Policy Implications. Retrieved August 4, 2008 from*

xiii. *Biovericom Incorporated. (2004). Biometric Technology. Retrieved August 4, 2008 from http://www.biovericom.com/biotech*