2012 International Conference on Information and Knowledge Management (ICIKM 2012)
IPCSIT vol.45 (2012) © (2012) IACSIT Press, Singapore

Face Recognition Application for Automatic Teller Machines (ATM)

Hossein Reza Babaei[+], Ofentse Molalapata and Abdul-Hay Akbar Pandor

Faculty of Information and Communication Technology, Limkokwing University of Creative Technology, Cyberjaya, Malaysia

Abstract: In this article about biometric systems the general idea is to use facial recognition to reinforce security on one of the oldest and most secure piece of technology that is still in use to date thus an Automatic Teller Machine. The main use for any biometric system is to authenticate an input by Identifying and verifying it in an existing database. Security in ATM's has changed little since their introduction in the late 70's. This puts them in a very vulnerable state as technology has brought in a new breed of thieves who use the advancement of technology to their advantage. With this in mind it is high time something should be done about the security of this technology beside there cannot be too much security when it comes to people's money.

Keywords: Biometrics, Facial Recognition, Biometric Standards, Automatic Teller Machine Technology, Biometric Predecessors.

1. Introduction

In the field of Biometrics, with the general term used alternatively to point out a characteristic or process. As a characteristic it's a measurable biological otherwise known as anatomical and physiological and behavioural characteristic that can be used for automated recognition. As a process it encompasses automated methods of recognizing an individual based on measurable biological anatomical and physiological and behavioural characteristics. Biometrics is an automated methodology to uniquely identify humans using their behavioural or physiological characteristics [1-4, 23, 24].

Recognition in this technology plays a major role, recognition used in the description of biometric systems like facial recognition, finger print or iris recognition relating to their fundamental function, the generic term how ever does not necessarily imply verification closed-set identification or open-set identification [7-9, 22, 24].

Verification is the task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates [14-18]. Figure 1 show the concept of recognition and verification which is feather illustrated by the picture below where the first image resembles the second image [10-14, 18].

Figure 1: Image resembling

Identification is the task where the biometric system searches a database for a reference finding a match for the submitted biometric sample; a biometric sample is collected and compared to all the templates in the database. If it is close-set identification, the submitted biometric is known to exist in the database. If it is open-set identification, the submitted biometric sample is not guaranteed to exist in the database, the system determines if the sample exists or not [18]. Figure 2 shows the process of identification.

In ATM's such a concept could be used to reinforce the one used by ATM's being Card + Password will allow you to access your banking details, as robust as this might seem, if someone has access to the two it

[+] Corresponding author. Tel.: + 60 12 2733532.
E-mail address: *Babaei@limkokwing.edu.my*.

will be easy to obtain your life savings[4,6]. However if there is one thing one can't get hold of is your face making this an impenetrable system which will not need much processing time [4].

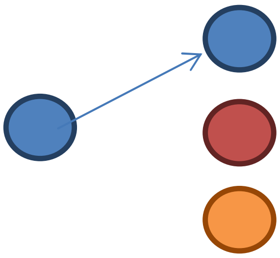

Figure 2: Process of identification

2. Biometric Predecessors

The first form of biometrics ever used date way back to the cave men who used hand prints as an unforgeable signature these prints can still be seen in caves such as the caves in Tsodilo hills in Botswana (Africa) which has paintings thought to be more than 20,000 years old, however some evidence suggests fingerprints were used as people mark as early as 500 B.C

The early Chinese merchants used fingerprints to settle business transactions they also used finger and footprints to distinguish between children from each other.

The early Egyptian traders were identified by physical descriptors to distinguish between trusted traders of known reputation and previous successful transactions, and those new to the market.

3. Standards of Biometrics

Biometric technology is used to help users deploy and maintain systems in an easier manner, with no need to remember codes or eliminate the use of keyboards or even keys for that meter. Can be used to promote longevity and enable interoperability. For national and international efforts developing standards for; Technical interfaces, Data interchange formats, testing and reporting, societal issues.

3.1. Uses of Biometric Systems

- National security- automated methods capable of rapidly determining an individual's identity, previously used identities and past activities.
- Homeland security and law enforcement- technologies to secure countries while facilitating legitimate trade and movement of people and to identify criminals in the civilian law enforcement environment.
- Enterprise and E-government Services- administration of people, processes and technologies.
- Personal information and business transactions- business plans that meet customer demands for service at any time, from any location and through multiple communication device.

Table 1: shows the evolution of biometric systems

1858	First systematic capture of hand images for identification purposes is recorded
1870	Bertillon develops anthropometrics to identify individuals
1892	Galton develops a classification system for fingerprints
1896	Henry develops a fingerprint classification system
1936	Concept of using the iris pattern for identification is created
1960s	Face recognition becomes semi-automated
1960	First model of acoustic speech production is created
1965	Automated signature recognition research begins
1969	FBI pushes to make fingerprint recognition an automated process
1974	First commercial hand geometry systems become available
1986	Exchange of fingerprint minutiae data standard is published
1988	First semi-automated facial recognition system is deployed
1992	Biometric Consortium is established within US Government
1997	First commercial, generic biometric interoperability standard is published
1999	FBI's IAFIS major components become operational
2002	M1 Technical Committee on Biometrics is formed
2003	Formal US Government coordination of biometric activities begins
2004	US-VIST program becomes operational
2004	DOD implements ABIS
2005	US patent on iris recognition concept expires

3.2. How biometrics works

In biometrics a series of steps are followed to get the aimed goal, the steps are as shown in the figure 3 below:

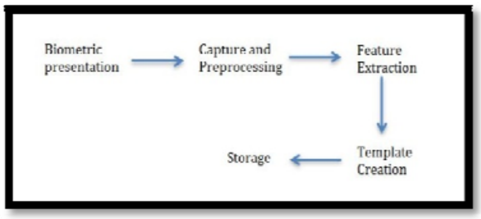

Figure 3: Biometrics steps to get the aimed goal

- **Sensor:** A sensor collects data and converts the information to a digital format
- **Signal processing algorithms:** This is where quality control activities and development of the template takes place
- **Data Storage:** Keeps information that new biometric templates will be compared to
- **Matching algorithm:** Compares the new template to other templates in the data storage
- **Decision process:** Uses the results from the matching component to make a system level decision.

3.3. Biometric Implementation Factors

In order to implement a biometric system these are the factors to first consider.

- Location
- Security Risks
- Task (Identification or verification)
- Expected number of users
- User circumstances
- Existing Data

4. Analysis (Biometric Modalities)

i. **Fingerprint:** Fingerprints have uneven surfaces of ridges and valleys that form a person's unique pattern, fingerprints are still widely used to date. Figure 4 shows a finger print.

Figure 4: Finger print sample

ii. **Face Recognition:** The use of infrared detectors to capture a 3D pattern of person's cranial physiognomy. Figure 5 shows how infrared technology is used to get the image [3].

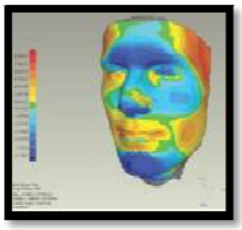

Figure 5: Usage of Infrared technology to get the image

iii. **Iris Recognition:** Iris image processing is illuminating the iris with near infrared light, which takes the illuminated picture of the iris without hurting or causing any discomfort to the person. Figure 6 shows the area of focus in the eye when using Iris recognition.

Figure 6: Area of focus in the eye

iv. **Hand/ Finger Geometry:** This is one of the first successful commercial biometric products. A person places their hand on a device and the system takes a picture of the hand using mirrors, the picture shows top and side hand views, then measures digits of the hand and compares to those collected at enrollment. Figure 7 show how hand/finger geometry is used in biometrics.

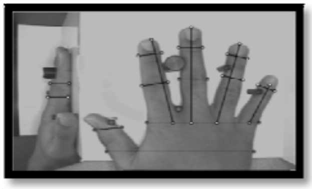

Figure 7: Hand/ Finger Geometry

Initial Analysis

Out of all the biometrics modalities I have chosen Facial recognition as the best technique for my project. This is because of the many algorithms that can make it more secure and more easy to use. In the current state facial recognition is used in high-level national security by the FBI, CIA and the Secret Service in the United States of America.

Methods of Face Recognition

i. **Appearance-based (View-based) face recognition:** Appearance-based approaches represent an object in terms of several object views (raw intensity images).

ii. **Adaptive Contrast Enhancement:** The idea is to enhance contrast locally analyzing local grey differences taking into account mean grey level. Figure 8 shows Adaptive Contrast Enhancement.

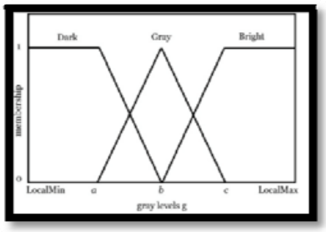

Figure 8: Adaptive contrast Enhancement

iii. **Gamma Correction:** Gamma correction operation performs nonlinear brightness adjustment. Brightness for darker pixels is increased, but it is almost the same for bright pixels. Figure 9 shows Gamma Correction.

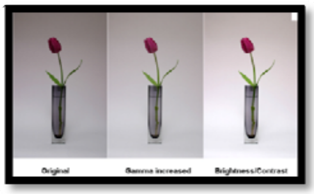

Figure 9: Gamma Correction

5. Research Methodology

The aim of this research is to design and develop a facial recognition application for Automatic Teller Machine (ATM) to reinforce security.

Development Methodology:

In this research about Facial recognition it was best to use Rapid application Development (RAD which is a development lifecycle designed to give much faster development and higher-quality results than those achieved with the traditional lifecycle. It is designed to take the maximum advantage of powerful development software that has evolved recently. Rapid Application Development is a method used to help developers to get first-hand information from customers about an on-going project and even make changes where necessary [8].

Rapid Application Development (RAD):

Rapid Application Development (RAD) refers to a development life cycle designed to give much faster development and higher quality systems than the traditional life cycle. It is designed to take advantage of powerful development software like CASE tools, prototyping tools and code generators [6]. RAD is a people-centred and incremental development approach. Active user involvement, as well as collaboration and co-operation between all stakeholders are imperative. Testing is integrated throughout the development life cycle so that the system is tested and reviewed by both developers and users incrementally. The key objectives of RAD are:

- High Speed
- High Quality
- Low Cost

The RAD life cycle composes of four stages:

- Requirements Planning
- User Design
- Rapid Construction
- Transition[9]

Figure 10 shows the necessary steps in Rapid Application Development.

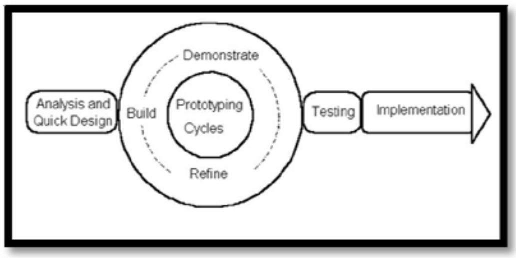

Figure 10: Necessary steps in RAD

6. System Design

In the case of this system Infrared Facial Recognition seems to be the best technique. This means an infrared light camera is placed strategically to see the human face without moving the lens and getting a 3D geometry of the face and verifying it while the person is entering their password. Infrared Light cameras are used because they are less prone to defection due to light and can be used in complete darkness, this gives the system an edge over other biometric systems as they require intense quality control. This means there is more processing time required to run the system hence efficiency of the ATM is lost with the expense of a reinforcement application which makes the system as a whole less feasible.

7. Conclusion

As facial recognition has proven to be the most secure method of all biometric systems to a point it is widely used in the United States for high level security, entrusting the system even to help in the fight against terrorism. If this system is used at this level it should show how much technology has changed in order to make this method effective in the processes of identification and verification. With new improved technics like Artificial Intelligence that help eliminate more disturbances and distortions that could affect the rate of effectiveness of the system, will help in increasing the margin of security from a simple 60-75% accuracy to 80-100% accuracy rate. These technics will make this system impenetrable.

8. Acknowledgement

The special thank goes to our helpful advisor Dr. Arash Habibi Lashkari for his supervising and advising in the progression of our dissertation and project.

9. References

[1] PENG Zhao-yi, ZHU Yan-hui, ZHOU Yu "Real-time Facial Expression Recognition Based on Adaptive Canny Operator Edge Detection", 2010 Second International Conference on MultiMedia and Information Technology, pp 154-157, 2010.

[2] PatilK, GiripunjeSD, BajajPR "Facial Expression Recognition and Head Tracking in Video Using Gabor Filter", Third International Conference on Emerging Trends in Engineering and Technology, pp 152-157, 2010.

[3] Zhao, Huang, Dellandre ́a, Che, " Automatic 3D facial expression recognition based on a Bayesian Belief Net and a Statistical Facial Feature Model", 2010 International Conference on Pattern Recognition, France, pp3724-3727, 2010.

[4] Cornelis Robat., *Automatic teller machine ATM*, 2006

[5] Zharkova & Ipson, Valentina & Stan, Survey of Image Processing Techniques. *Survey of Image Processing Techniques*, EGSO-5-D1_F03- 20021029, 3, 2003

[6] RAD - Rapid Application Development Process. *RAD - Rapid Application Development Process*, 2011

[7] SEC Ventures | Consulting Services | Methodology. 2011. *SEC Ventures | Consulting Services | Methodology.*

[8] RAPID APPLICATION DEVELOPMENT. 2011. *RAPID APPLICATION DEVELOPMENT.*

[9] Rapid application development (RAD). 2011. Rapid application development (RAD).

[10] Matai, Irturk, Kastner, "Design and Implementation of an FPGA-based Real-Time Face Recognition System", IEEE International Symposium on Field-Programmable Custom Computing Machines, United States, pp97-100, 2011.

[11] Professional Development - Rapid Application Development. *Professional Development - Rapid Application Development*, 2011

[12] Li, Phung, Bouzerdom, Tivive, "Automatic Recognition of Smiling and Neutral Facial Expressions", 2010 Digital Image Computing: Techniques and Applications, Australia, pp581-586, 2010.

[13] Juebo, Hehua, Lianhua, "A Cloud Model-based Approach for Facial Expression Synthesis", Journal Of Multimedia, Vol. 6, No. 2, China, pp217-224, 2011.

[14] Pazoki Z, Faroki F, "Effective feature selection for face recognition based on correspondence analysis and trained artificial neural network", Sixth International Conference on Signal-Image Technology and Internet Based Systems, Iran, pp80-84, 2010.

[15] Lao, Han, Murase, "Efficient Facial Attribute Recognition with A Spatial Codebook", International Conference on Pattern Recognition, Japan, pp1461-1464, 2010.

[16] Wang, Zhang, "Facial Recognition Based on Kernel PCA", Third International Conference on Intelligent Networks and Intelligent Systems, China, pp88-91, 2010.

[17] Rao I, Murphy P, Nandy S, Rao V, "A Real World System For Detection And Tracking", International Conference on Advances in Recent Technologies in Communication and Computing, India, pp939-943, 2009.

[18] Deng J, Li J, Zou X, "Extraction Of Litchi Stem Based On Computer Vision Under Natural Scene",

[19] International Conference on Computer Distributed Control and Intelligenct Environmental Monitoring, China, pp832-835, 2011.

[20] Miller G, Fels S, Oldridge S, "A Conceptual Structure for Computer Vision", Canadian Conference on Computer and Robot Vision, Canada, pp168-174, 2011

[21] Bhaumik G, Mallick T, Chowdhury K S, Dr. Sanyal G, "Analysis and Detection of Human Faces by using Minimum Distance Classifier for Surveillance", International Conference on Recent Trends in Information, Telecommunication and Computing, pp265-267, 2010.

[22] Lei Z, Wang C, Wang Q, Huang Y, "Real-Time Face Detection And Recognition For Video Surveillance Applications", 2009 World Congress on Computer Science and Information Engineering, pp168-172, 2009.

[23] W. ZHAO, R. CHELLAPPA, P. J. PHILLIPS and A. ROSENFELD., Face Recognition: A Literature Survey. ACM Computing Surveys. 4, 2003

[24] Fanglin Chen, Jie Zhou, Senior Member, IEEE, and Chunyu Yang, Reconstructing Orientation Field From Fingerprint Minutiae to Improve Minutiae-Matching Accuracy. IEEE TRANSACTIONS ON IMAGE PROCESSING. 18 (7), 1057-7149, 2009