Global Educational Journal of Science and Technology

Vol. 2 (3), pp. 129-135, November, 2014. © Global Science Research Journals
http://www.globalscienceresearchjournals.org/

Review

Integrated Improved Security System Techniques in Combating Crime Using the Biometrics at the National Airport of Zimbabwe

[1]Godfrey Sithole and *[2]Noreen Sarai

[1,2]School of Information Sciences and Technology, Harare Institute of Technology, PO Box BE277, Belvedere Harare, Zimbabwe.

Accepted 4 November, 2014

Abstract

Biometrics has become very popular as a tool in combating crime in the world. Despite all the research that has been carried out the improvement of the algorithms still has not been exhausted. In the past research community has focused primarily on the password, and national identity cards and biometrics with less effective algorithms. However current and future complex crimes require better algorithms with improved time and space complexities. The proposed algorithm was subjected to the fingerprint authentication. The results were recorded. Then the algorithm was improved and better results were achieved. Surprisingly, extremely little research to date has considered continuous systematic and logical improving the algorithms to achieve authenticated results.

Keywords: Biometrics, algorithm, minutia matching**,** fingerprint

INTRODUCTION

There have been many world events that have directed our attention towards safety and security. Most of the attention to security has been obvious such as improved screening of people access to the particular place. Does visible security actually aid computer attackers or terrorists who play close attention to the development of such security techniques? Would we feel safer if security were transparent to us or would it be an invasion of privacy? What about combating crime using the non-biometrics and biometric techniques? This study will look at integrated improved techniques to combat crime using the biometrics. Biometrics refers to the identification of a person based on his or her physiological on behavioral characteristics. The idea follows in the matching process with the previously stored information to prove somebody's identity. This study will concentrate on the integrated improved security system techniques and the algorithms used in the matching process.

Corresponding Author's Email: noreyn@gmail.com, **Tel**: 263-773-884-666

Aims and Objectives

The aim of this research is to investigate the appropriateness of integrated improved security system techniques in combating crime using the biometrics. It is also the aim of this study to improve the algorithms used in the matching process. To evaluate the appropriation and to test and analyze the effectiveness of the integrated improved security system approach to combat crime using the biometric.

Scope of the Study

To improve the algorithm in the matching process. The improved algorithm is meant to give future security system techniques.

LITERATURE REVIEW

The domain of biometrics include fingerprints, hand geometry, retina and iris patterns, facial geometry, signatures and voice recognition. Therefore individual to be identified is required to physical be present at the point of identification.

Two distinct function for biometric derive include that to prove you are who you say you are and to prove you are not who you say you are not. The main purpose of the first function is to prevent the use of a single identity by multiple people. It assist for a possible criminals to use the National Airport to go to other countries for fear of arrest. Now it is important for the biometric device be able to differentiate between a live biometric presented to the scanner i.e. a real finger or a spoofed biometric trying to fool the scanner.

The Properties of Biometrics

The automatic capturing of biometrics sample data and comparison or matching with previously stored characteristics.

- **Invariance**: Biometric properties should be constant over a long period of time to eliminate the need for constant updating of the template that is stored in the system.
- **Measurability and Timeliness:** The individual properties must be able to be automatically matched to an expected norm instantly.
- **Singularity**: organ being used for identification must have sufficient unique properties in order to differentiate one individual from another.
- **Reducibility**: The stored data should be able to being reduced to a size that is easy to handle but impossible to duplicate.
- **Reliability**. The airport matching system need to be reliable since would be costly to have a system that does not provide constant result.
- **Privacy**: The fingerprint technique should ensure the privacy of the person using the system so that their privacy is not being violated in any way.

Fingerprint Matching Techniques

Sophisticated fingerprint matching methods have emerged since the beginning of this technique of verification. Some complicated techniques available are:

- Optical sensors with CCD or cmos camera. The fingerprint is placed on a plate. Then through a prism and a system of lenses, the image is projected on a camera. The frame grabber technique are used and the image in stored and ready for analysis
- Ultrasonic sensors: Using ultrasonic sensor, a scan of the fingerprint with a resolution of about 500 dots per inch is done. The technique is able to offer templates which are full of useful detail of finger print information.
- Electronic field sensor: The method creates an electric field with which an array of pixels can measure variations in the election field that are caused by the ridges and valleys in the fingerprint
- Capacitive sensors: The method is similar to electronic field sensor except that when the finger is placed on the sensor an array pixels measures the variations in capacity between the valleys and the ridges of the fingerprint
- Temperature Sensors: The method makes distinction between the temperature of the ridges and the temperature on the valley on the fingerprint. A temperature match can be taken by simply swiping the finger over the sensor.

Minutia Matching Algorithm

This method uses for each detected minutia uses for each detected minutia, and then realizes the following parameters.

i. x and y coordinates of the fingerprint point.
ii. The orientation which is defined as the local ridge orientation of the associated ridge.
iii. The type of the fingerprint point that is whether the minutia is ridge ending or ridge bifurcation.
iv. The associated ridge is represented by points sampled at the average inter- ridge distance along the ridge linked with the corresponding fingerprint point.

Conceptual Design

Current operations

The International Airport of Zimbabwe is the place that controls the movement of people from and to Zimbabwe. It also detects criminals who will be leaving or coming to Zimbabwe. The people who are involved in this class travel by air. This mostly includes the first class of people of most countries. The busiest airport is the National Airport of Zimbabwe situated in Harare. This is where the central decision making process is carried by respective decision makers. The authentication has been working since the inception. The fingerprint authentication/verification, decision makers used to produce quarterly and yearly by directly doing the pattern matching algorithms. The Police at the National Airport get the fingerprints of the suspects from Criminal Investigation Department (CID). The CID gets the names of the suspects from the police stations in the country. Then the pattern matching algorithm takes some time to do the fingerprint authentication since the fingerprint(s) has several minutiae patterns. The top management work under a lot of pressure when it comes to the end of quarter or end of year.

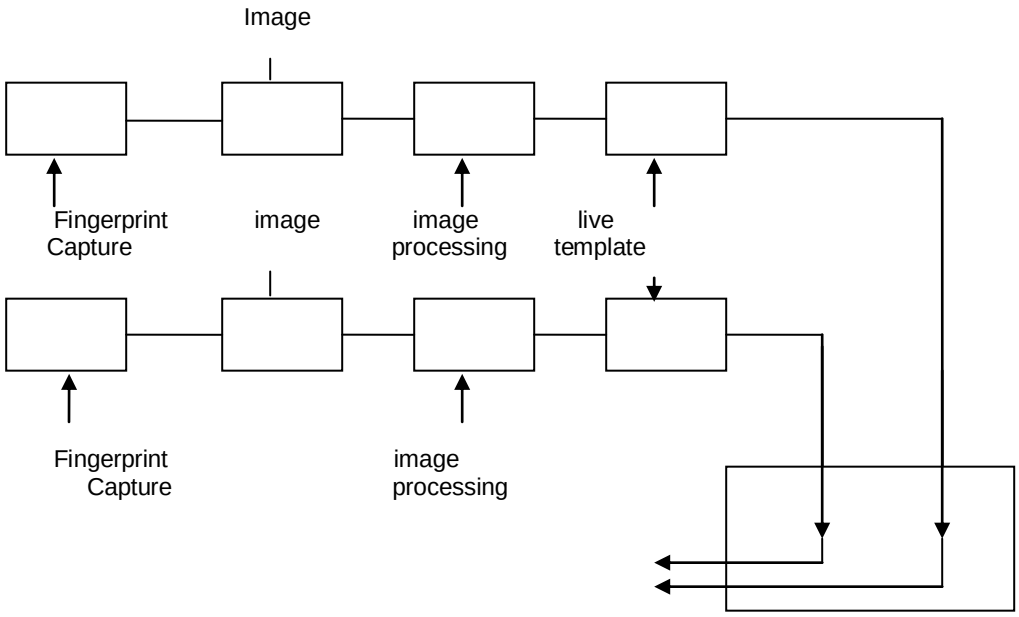

Figure 1: Architecture of Existing System

Architecture of Existing System

Figure 1 shows the existing system at the Zimbabwe airport from finger print capturing to matching results. The existing pattern matching algorithm is based roughly on the following steps:

- The authorized user introduces his/her fingerprint information to the template.
- The fingerprint is captured as the live template.
- The image of the fingerprint information characteristics are extracted which is represented in Cartesian coordinates.
- The fingerprint then moves through processing using the pattern matching algorithm tailored to match the fingerprint with that in the database.
- The matching is done and the result displayed.

When the reports of the authentication are needed then, they are printed. The system does the authentication from the sources each time. When the authentication is posed this will result in inefficiency and delay in the verification especially when the fingerprints are almost identical.

Proposed Integration Improved Minutia Algorithm

After making some considerations of a minutia authentication algorithm the author found out that the following can be one of the most appropriate system alternatives to combat crime at the National Airport. The minutia algorithm will help in the strategy for the decision makers for the National Airport.

Proposed Solution Architecture

The solution is to create an algorithm with a better time and space complexity. Also the algorithm uses the polar coordinates. Then if the user invokes the system to authenticate the algorithm does that using all the fingerprint features. The solution has vast advantages since all the minutiae of the fingerprint are considered. There is also the advantage of rotation alignment stage and the matching stage. The only major disadvantage is that the spoofed fingerprint made from cyanoacrylate is not detected. Figure 2 shows the proposed biometric system with an algorithm which uses polar coordinates

Components of the Architecture

- The ANSI/NIST – CSL 1 – 1993 and ANSI/NIST ITL 1a – 1997 process the fingerprint image data.
- The ANSI/NIST ITL 1a – 1997 specifies common format to exchange the image data information between dissimilar assisted system or systems made by different manufacturers.
- ANSI/NIST ITL 1-200 Consolidation of ANSI/NIST-CSL 1-1993 and ANSI/NIST – ITL 1a-1197.
- ANS X9 84-2001 manages and securing biometric information for use in the fingerprint capturing.
- X9 84: specifies cryptographic massage formats and key management techniques that is used for the fingerprint authentication, data integrity and privacy for biometric matching.

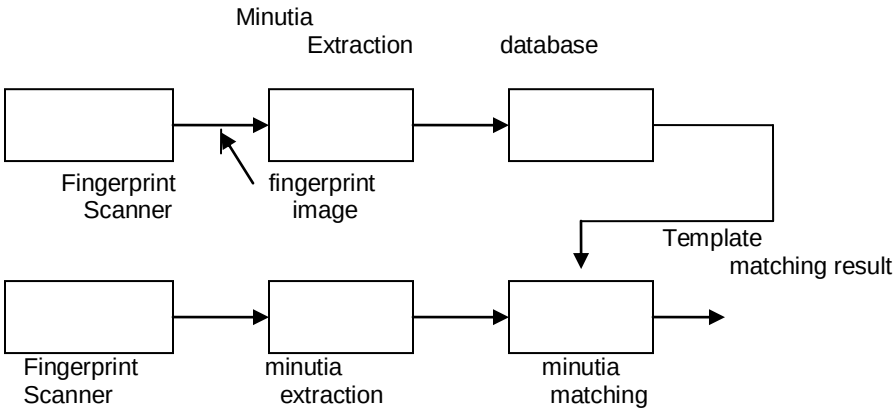

Figure 2: Proposed Architecture

- The X9 84 standard: defines a set mandatory fingerprints characteristics requirements to manage biometric information securely.
- API – application programming interface in the Bio API specification version 1.1 2001.
- This is for the fingerprint input and output to the Biometric Service Provider.
- The wave/scalar quantization (WSQ 93) algorithm I is the FBI standard for digital fingerprint compression.
- CJIS – RS – 0010 FBI: is the fingerprint transmission.

The Algorithm

1. Match the ridge associated with each input fingerprint characteristic against the ridge associated with each template characteristic and then align the patterns according to the stages.
2. Change the specification of the template and input characteristics into the polar coordinate system from the Cartesian coordinate system in respect of the fingerprint characteristics. After this the alignment is done and the two diagrams of strings are forward by concatenating each characteristic in an increasing order of radial angles. The following inputs are considered:

$Pp = ((r_1^p, e_1^p, \theta_1^p)^T \ldots (r_m^p, e_m^p, \theta_m^p))^T$

$Qp = ((r_1^Q, e_1^Q, \theta_1^Q)^T \ldots (r_N, e_N^Q, \theta_N^Q))^T$

r: radius

e: radial angle

θ: the normalized fingerprint orientation

3. Match the resulting strings Pp and Qp with a modified dynamic – programming described below to find the edit distance between Pp and Qp.
4. Compute the matching score of the template and input fingerprint characteristics as the minimum edit distance.

$$M_{pq} = \frac{100 \text{ pair}}{\text{Max } \{M, N\}}$$

N pair is the number of fingerprint pairs which fall within a given boundary.

Alignment of Point Patterns

All the fingerprint characteristics is associated with a ridge. The alignment is then achieved by matching and aligning the corresponding fingerprint features: then matching the corresponding normalized ridges, the relative pose transformation between the input characteristics and the template can be estimated. The estimated pose transformation, the input minutia can be then translated and rotated to align the template minutiae.

Align Point Pattern Matching

When two identical point patterns are exactly aligned, each pair of corresponding points are completely overlapping. The situation a point pattern matching can be simply made by counting the numbers of overlapping pairs.

The Experimental Results

The system was tested on a number of fingerprints. The set of fingerprints were downloaded from the internet. The fingerprints were stored in the folder. The spoofed fingerprints were also downloaded. As already mentioned that the weakness of the system was that did not identify the spoofed fingerprint. The other problem was that when the results were posted to an excel document they were eventually corrupted by the virus as will be shown on the diagrams in the next chapters

The set contains at least 10 images (380 x 380) per fingerprint from the internet. In the actual context the scanner was supposed to be used and the manufacturer identified. At this stage it was also important why the preferred hardware incorporated into the project. The advantage over the other hardware was of great significance.

The downloaded fingerprint varied in quality. Approximately 80% were of good and satisfactory quality.

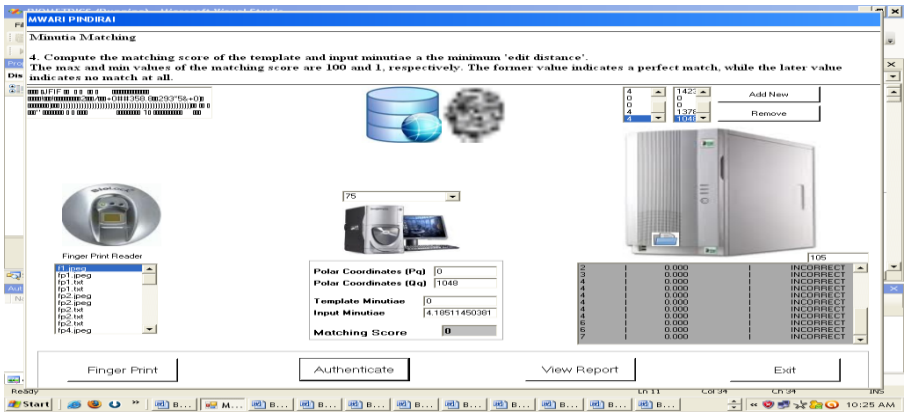

Figure 3: Main Interface

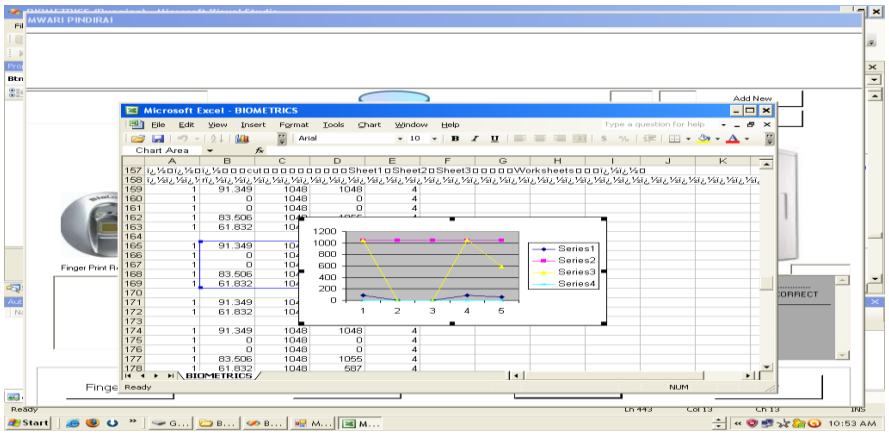

Figure 4: Result Screen shot 1

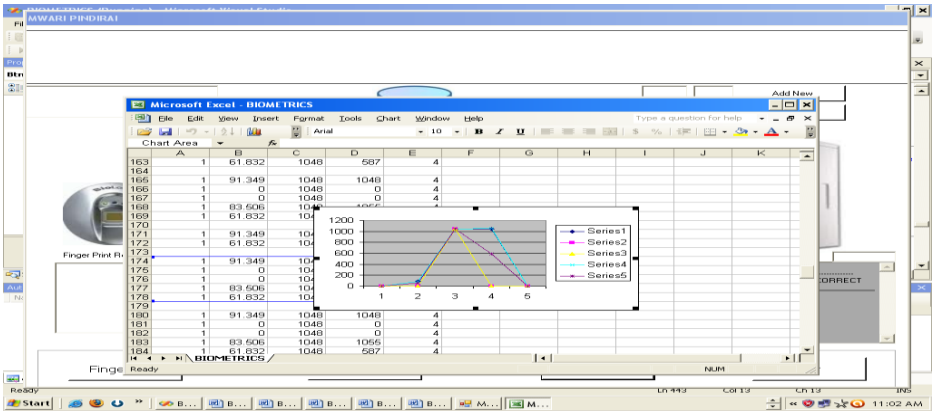

Figure 5: Result screen shot 2

The remaining 20% was of poor quality including the spoofed fingerprint.

Nearly all the fingerprint in the test set was matched with other fingerprint in the set. The matching was labeled correct when the matched fingerprint was among the 80% correct and the option incorrect if they were from the 20%.

The observation was that the incorrect matching occurs mainly to the fact that the fingerprint images was of poor quality or spoofed.

The User Interface

The proposed system makes use the graphical user interface which is user friendly. The users with little or no computing experience can learn to use the interface after a short period of training. The screen that appears when the system is executed is where the user can select the fingerprint to authenticate. Then add as many as the user wants using the option open in the same data base. Then add one or more fingerprints to the database. There is also an option of removing if the user had made a mistake. The other option is authenticate to match the fingerprint in the database with the input. Figure 3, 4 and 5 shows sample screen shots are shown on the following page.

CONCLUSION

The research work satisfied its predefined objectives. The justification of the appropriateness of the integrated improved security system techniques to combat crime was ascertained after the simulation. Depending on the data required by different users the system seems to work well giving accurate data necessary for decision making purposes concerning the rate of crime.

Limitations

The system does not detect the spoofed fingerprints. The high cost to set the real world is not feasible at the National Airport of Zimbabwe due to hardware, software and application systems needed.

Recommendation

The issue of biometrics to fight crime is an issue these days. All the stakeholders, creditors and other people are worried by the high and magnitude of crimes which are prevalent these days. Furthermore the citizens are patiently asking for the use of technology to improve the detection rate of the criminals. Combating crime using biometrics have become an important research topic in recent years, mostly because it produces interoperability, high performance and efficiency. I suggest the former to be done using the three dimensional coordinates. The fundamentals of the system remain the same but with improved complexity and space. Since the criminals are committing high profile cases the system would be used to curb the phenomenon.

REFERENCE

[1] Zhang D (2002) Biometrics Solutions for Authentication in an E-world.

[2] Anderson E (2002) " A Demonstration of the Subversion Threat Facing a Critical responsibility in the Defense of Cyberspace", Naval Postgraduate school, Monterey, C.A. Master's Thesis, department of Computer science

[3] A Ranade and A Rosenfeld (1993). Point Pattern Matching by relaxation, *Pattern Recognition,* Vol 12, 2, pp 269-275.

[4]. Bruderlin R. "what is biometrics?" Paper, 1999-2001

[5] Chua J Biometrics (2001). "The future of security" CBC News Online , September 2001.

[6] Daugman J (2000) "Combining Multiple Biometrics" the Computer Laboratory at Cambridge University,

[7] Daugman J (2000). How iris recognition works.

[8] Degami A and Winer EL (1997). Procedure in Complex Systems, The Airline Cockpit NASA contractor report 177642, Moffett Field, CA NASA Ames Research Centre.

[9] Degami A (1994) On the Design of Flighter deck Procedures NASA contractor report 177642, Moffett Field, CA NASA Ames research Centre.

[10] Degami S and Winer EL Procedures in Complex system. The Airline Cockpit NASA contractor report 177642, Moffett Field, CA NASA Ames Research Centre

[11] Esser M (2000) "Biometric authentication'. Essay October 2000.

[12] General Aviation Manufactures Association. Recommended Practices and Guideline for Part 23 Cockpit/Flight deck Design GAMA Publication No 10 September 2000.

[13] Go Team 9- Biometrics, US Department of Transpiration , Transportation security Administration technical Report.

[14] Govindarajan S (2002). Are these Prying Eyes, article, available http//wwwkrify.com/articles/pryyingers.htm

[15] Hong L and Jain A.K Integrating Faces and Fingerprints IEE Trans Pattern Anal Machine Intell. Vol 20 No 12 pp.12 1295-1307, December 1998.

[16] Info security Magazine, "Biometrics technology" making Moves in the security Game. Pp 28-34 Volume 12#3 March 2002.

[17] International Biometrics group Tech Reports "Facial Scan technology, January 2002.

[18] Jain A.K and Arun R. Learning user-specific parameters in a multibiometer system. Department of Computer Science and engineering – Michigan State University, no date given.

[19] Kolettis H, Stepping up Security, 2002.

[20] Liu S and Silverman M, A Practical guide to biometric technology, January 2000.

[21] Manfield T, Kelly G, Chandler D, Kane J. Biometric product testing final report CFSG contract X92A/4009309 Issue 10, March 2001.

[22] Mansfied A.J and Wayman J.L Best Practices in testing and reporting performance of Biometric devices. August 2002.

[23] National Center for State Court, " Hand Geometry no date given

[24] Prabhakar J and Pankanti (2001) "On the Individuality of Fingerprints"

[25] Putte T and Keuing J (2001) "Biometrical Fingerprint Reconition Don't get Your Finger Burned" Paper, September 2001.

[26] Ravishanker Rao (1990). Taxonomy for Taxture Description and Idenfitication, spriger- Verlag, New York.

[27] Schneiner B (2002). "Fun with Fingerprint readers", Crypto- Gram Newsletter. May 15 2002.

[28] Sperry P (2001). “Captains to FAA: Focus on Cockpits,” 2001 article available http://www.rightswatch.org/safer skies/focus cockpits.htm(last accesses: January 2003)
[29] UK Biometrics working Group., Use of biometrics for identification and authentication Advice on product selction , November 2001.
[30] Woodward JD, Orlands NM, Higgins PT (2003). Biometrics Identity Assurance in the Information Age.