Sixth LACCEI International Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2008)
"Partnering to Success: Engineering, Education, Research and Development"
June 4 – June 6 2008, Tegucigalpa, Honduras.

Biometric Authentication in Cluster Computing

Carlos Cabrera
Florida International University, Miami, Florida, USA, ccabr016@fiu.edu

Abstract

Various research studies have been conducted to prove that the study of biometrics in network and computer security is a rising field of study. Biometric authentication is based on distinctive and quantifiable elements such as: physical, biological or behavioral characteristics that are unique and distinctive of each individual. Biometrics is a multidisciplinary science that evolves complex problem solving in areas such as: engineering, digital image processing, mathematics, statistics, psychology, computing and policy. Biometric technology offers a capable progress toward any secure application or network. Compared to the current or classical method of authentication and identification methods based on photo ID or magnetic swipe identification cards were two images are aligned, for authentication or verification purposes, using a process called image registration. The use of biometrics is recurrently more suitable for end users and helps reduce the possibility of fraud since it provides an additional and unique level of security.

Keywords: Biometrics, authentications, cluster computing, palm.

1. Introduction

We propose a special and unique method of authentication using palm recognition, digital image processing, encryption and cluster computing. We obtain this by redefining the basic principals (model) of biometric authentication, basically instead of superimposing two images (image registration[1]) we instead digital process each image and later compare their unique and distinctive digital signature, i.e. we compare the matrix of bits (zero's and one's) generate by each image.

Day after day, the need for security is gaining additional significance, especially after the event of September 11, 2001. A number of diverse techniques have been develop, each with their own rewards and shortcomings, according to user requirements and factors such as: cost, user friendliness, performance, etc. From these factors irrelevant of the purpose, implementing the use of biometric traits falls into two basic reasons:

A. Identification:
    a. Matches one biometric trait against many on file. (one to many)
B. Authentication:
    a. Matches one biometric trait against previous stored data. (one to one)

Each one with its own level of involvement:

A. Passive:
    a. Does not require the user too actively (willing) submit to measurement. Slang – Covert.
    b. Non invasive

[1] The process of super imposing two images to compare them.

Examples: Voice, Face and Gait

B. Active:
   a. Does require user to actively submit to measurement
   b. Invasive, Slang – Overt

Examples: Fingerprint, Palm Geometry, Iris, Retina, DNA.

Throughout this paper we will be introducing a new method of authenticating a user with the use of a hand geometry biometric authentication system.

2. FEATURE EXTRACTION

The propose of the system's first step is to confine a sample of the user's biometric trait. During this extraction process, a large number of distinctive features that characterize that specific user among the database registered population. One unique characteristic of the human palm is its heterogeneous layout in regards to distinctive features is related. Certain areas of the palm "contain" or "embrace" more information that other areas. This however, creates numerous problems when we "extract" the information form the trait. However, we have solved this problem using Wavelet Coefficients. I further expand this concept in section 5.

3. Image Capture

The biometric trait is obtained with the use of a scanner, equipped with "tabs" to align the hand in a precise manner. The image captured is a 1280 x 720 pixel black and white image in a JPEG format.

4. Image Processing

Once the trait is obtained, it must be processed in a manner such that the relevant and unique information can be extracted and processed. Such process is defined has: hand segmentation, and basically is divided into two steps:

A. Determine Surface Area

B. Divide Surface Area in a Matrix M x M

Note figure No. 1

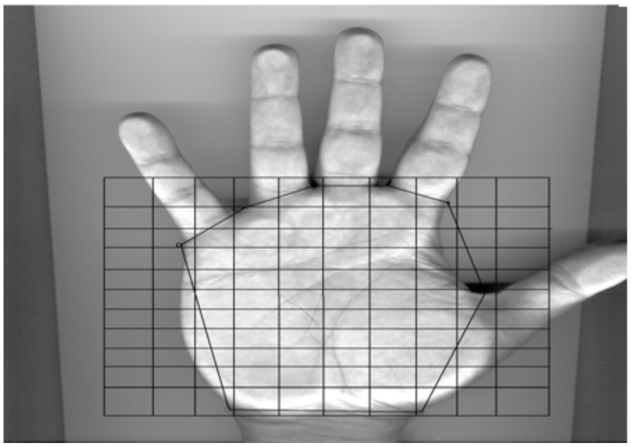

Figure No. 1 Hand Segmentation

5. Wavelet Coefficient Conversion

Once the system has completed steps one and two, we can state that we no longer have “one” image however we have M² number of “Cells”, where we define the matrix L has L=M x M. In essence we have divided the palm surface “trait” into a matrix. Now the main characteristic of each new “Cell” is that each one holds independent, unique and relevant information regarding the trait has a whole. Contrary to the technique of Image Superposition used widely today in fingerprint identification, we propose converting each cell into a series of wavelet coefficient. The purpose of using and converting each cell into these coefficients is to ensure the integrity of the information contained in each cell, since this process is lossless, compared to other formats like JPEG which are lossly. Also, we have chosen this technique, although complex, since it has to be capable of handling multi-resolution images. This goes back to the specific characteristic of the palm; it is heterogeneous. This principal applies not only to the palm as a whole but once we have generated the matrix it is easy to observe that each cell is heterogeneous on its own, having different resolutions within.

6. TRANSMISSION

At this moment the trait is ready to start the transmission and authentication process. We have taken an image and converted into a matrix: See Figure No. 2

$$L(I,J) = M(I)+M(J)$$

Since our matrix has M² cells and we have established that each one is unique in its information we can authenticate with random individual cells or group of cells chosen at random or in a unique sequence, as a replacement for authenticating the image has a whole. There are several advantages of our proposed method:

A. Security – Contrary to sending an whole image, we are sending cells, also these cells are not images, they are a series of coefficients, i.e. a group of zero’s and one’s.
B. Bandwidth – Each cell is only L(I,J)/M² of the entire trait.
C. Integrity – By converting these into wavelet coefficients the integrity of the trait remains, essential in biometric authentication.

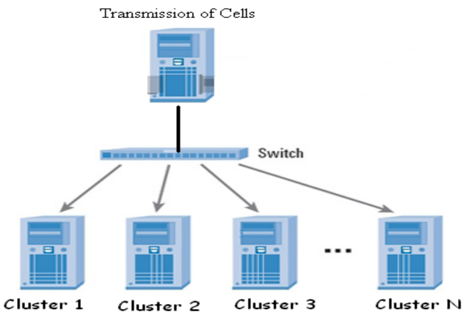

Figure No. 2 Transmission of Cell through a Network

7. CLUSTER DATABASE

During the authentication process, the Cells are sent to more than one clustered database, each of these database's independent from the other with no means of communication among themselves and without knowledge of the stored information of each one, i.e., no cluster system has the entire Matrix hence, increasing the level of security safe guarding the biometric treat. Once the biometric trait has been obtained, random cells are chosen for example: In a matrix L(I,J) that is composed of M x M elements if M=10, then L(I,J) would be: L(10,10). The random cell used for authentication can be for example: L(5,6), L(2,6) and L(10,6). Each cell is sent directly to a database for authentication. Each cell, unique and independent, takes a different path, is independent and contains no "real" relevant information to an outside "user" hence, increasing security and minimizing the use of bandwidth. In each step of the process band width reduction is obtained. Each database authenticates each cell independently and replies back to with a: "No = 0" or a "Yes = 1", a one bit response. See Fig. No. 3.

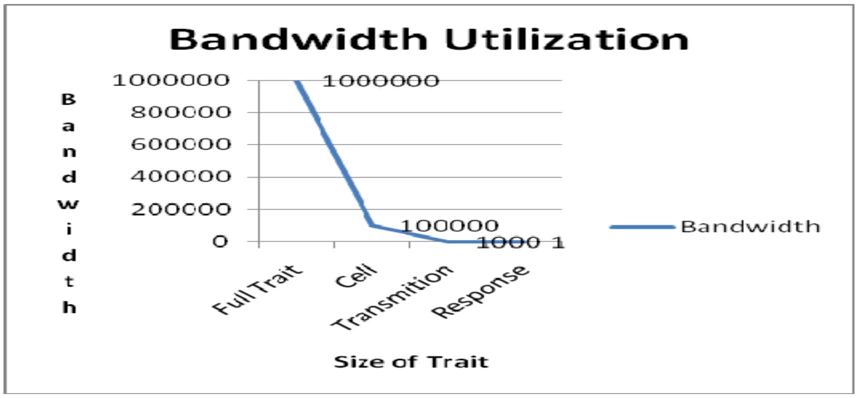

Figure No. 3 Bandwidth Utilization

8. CONCLUSION

A biometric palm authentication system has been stated. We have detailed each governing step and given the benefits of each one. Experimental data is been conducted as this paper is written, with a positive success ratio. However, further work should be conducted to prove that the above approach can be generalized.

9. FUTURE WORK

This paper bring just the beginning of our research, currently we are running simulations on the number of cells need to generate a positive authentication. Also, we took this paper has the initial point in another research that we hope to present in next year's conference, titled "Multimodal Authentication in a Clustered Database." Also, simultaneously we are working in areas related to this topic such has, encryption, storage and biometric fusion.

10. ACKNOWLEDGEMENT

To Dr. Kia Makki at the Telecommunications and Information Technology Institute - IT2 at Florida International University, Miami, Fl USA.

11. REFERENCES

Hao, Feng and Anderson, Ross. 2006. Combining Crypto with Biometrics Effectively. Vol. 9, 2006, IEEE TRANSACTION ON COMPUTERS, Vol. 55, p. 1081.

KoeningGregory, YurcikWiliam
Security Issues in On-Demand Grid and Cluster Computing. Urbana-Champaign, IEEE 2005.

KungS.Y., MakM.W., LinS.H. Biometric Authentication. s.l. Prentice Hall 2004