International Journal of Management, IT & Engineering
Vol. 8 Issue 7, July 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

PHYSIOLOGICAL TRAIT-BASED FRAUD PREVENTION SYSTEM IN ATM TRANSACTIONS

Ismaila W. Oladimeji*

IsmailaFolasade. M**

Bello Oniyide A***

Abstract

Knowledge-based and token-based automatic personal identificationapproaches have been the two traditionaltechniques widely used. Because knowledge-based and token-based approaches are unable to differentiate between an authorized person and an impostor who fraudulently acquires the token or knowledge of the authorized person. This paper investigate the use of Physiological traits in online transactions using particle warm optimization. In this experiment 120 tongue images and fingerprints of different individuals were acquired using digital camera and webcam. The traits were preprocessed using segmentation scheme and particle swarm optimizationwas used to select salient features**.**Three testing scenarios were created; (i) testing with all images in database and (ii) testing with another selected pose of images in database and (iii) poses of images not in databasebut captured in a bad illumination. The decision to recognize or classify the images was determined by threshold at

Keywords:

Physiological traits;

Tongue;

Particle swarm optimization;

Fingerprints;

ATM system.

* **Doctorate Program, Linguistics Program Studies, Udayana University Denpasar, Bali-Indonesia**

** **STIMIK STIKOM-Bali, Renon, Depasar, Bali-Indonesia**

*** **English Language Specialist, Oller Center, Carriage House, 2nd Floor, California, USA**

0.50. Scenario 1 results showed that the experiment produced sensitivity of 94.6%, specificity of 95.7% and accuracy rate of 94.6% for tongues and sensitivity of 87.2%, specificity of 81.4%, and accuracy of 90.1% for fingerprints. Scenario 2 results showed that the experiment produced sensitivity of 78.6%, specificity of 74.7% and accuracy of 93.3% for tongues while fingerprints has sensitivity of 65.2%, specificity of 69.4%, and accuracy of 75.5%. while scenario 3 results produced sensitivity of 0.6%, specificity of 0.77% and accuracy of 0.0% for fingerprints and sensitivity of 22.6%, specificity of 18.4%, and accuracy of 20.7% for fingerprints. However, using tongue along with PSO will enhance better performance accuracy for this automatic identification and authentication in ATM system.

.

1. Introduction

Questions related to the identity of individuals such as “Is this theperson who he or she claims to be?,” “Has this applicant been here before?,”“Should this individual be given access to our system?” are asked millions oftimes every day by organizations in financial services, health care, e-commerce,telecommunication, and government. In fact, identity fraud in welfare disbursements, creditcard transactions, cellular phone calls, and ATM withdrawals totals over $6 billion each year. For this reason, more and more organizations arelooking to automated identity authentication systemsto improve customer satisfaction and operatingefficiency as well as to save critical resources (see Figure1). Furthermore, as people become moreconnected electronically, the ability toachieve a highly accurate automatic personalidentification system is substantially more critical. Personal identification is the process ofassociating a particular individual with anidentity. [1].

Knowledge-based and token-based automatic personal identificationapproaches have been the two traditionaltechniques widely used [2]. Token-based approaches use something you have to make a personal identification, such as a passport, driver’s license, ID card, credit card, or keys. Knowledge-based approaches use something you know to make a personal identification, such as a password or a personal identification number (PIN). Since these traditional approaches are not based on any inherent attributes of an individual to make a personal identification, they suffer from the obvious disadvantages: tokens may be lost, stolen, forgotten, or misplaced, and a PIN may be forgotten by a valid user or guessed by an impostor. (Surprisingly, approximately 25% of the people appear to write their PIN on their ATM card, thus defeating the protection offered by PIN when ATM cards are stolen!) Because knowledge-based and token-based approaches are unable to differentiate between an authorized person and an impostor who fraudulently acquires the token or knowledge of the authorized person [2], they are unsatisfactory means of achieving the security requirements of our electronically interconnected information society. Thus this called for biometric technologies to strengthen the security online transactions. In recent time, several biometrics based ATM machines have deployed to some countries, samples are shown in figure 1. For instance, companies that make automated teller machines have found budding markets for the fingerprint technology in South America, where citizens already are accustomed to the use of fingerprints for general identification, such as ID cards; also Diebold Incorporation of North Canton, Ohio, has supplied fingerprint-capable ATMs to a bank in Chile that is using them in a pilot project. [5].

Figure 1: Biometrics ATM Systems.

Biometrics is related to human characteristics and traits, which are characterized as physiological versus behavioural characteristics. Physiological refers to the shaper of the body and include but at the same time not limited to finger prints, face recognition, DNA, Palm Print ,hand geometry, iris recognition and odor/scent. Behavioural Characteristics are related to personal behaviour of the person includes typing speed, gait, digital signature and voice. In this paper, fingerprints and tongue will be considered.

Tongue, as shown in figure 2, was discovered to be a unique organ which reside inside the mouth, proven to be difficult to forge or affected by external environment and does not react to factors such as mood, health, and/or clothing. The explicit features of the tongue cannot be reverse engineered, meaning that tongue verification protects the privacy of users better than other biometrics.[3] [13]

Fig. 2.A typical tongue Image

Fingerprints- Fingerprints, as shown in figure 3, are the patterns formed on theepidermis of the fingertip. Fingerprints are made up ofseries of ridges and valleys (also called as furrows) on the surface of the fingertip and have core around which pattern like swirls, whorls, loops or arches are curved to ensure that each print is unique. The interleaved pattern of ridges and valleys are the most evident structural characteristic of a fingerprint. The most commonly used finger-print features are minutiae.

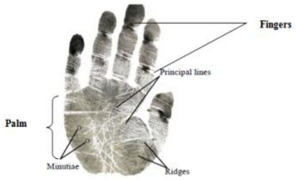

Figure 3. Human hand showing Fingers

Feature selection (FS) is a global optimization problem in machine learning, which reduces the number of features, removes irrelevant, noisy and redundant data, and results in acceptable recognition accuracy. It is the most important step that affects the performance of a pattern recognition system [4].PSO is a computational paradigm based on the idea of collaborative behavior inspired by the social behavior of bird flocking or fish schooling. Particle Swarm Optimization-based feature selection algorithm is utilized to search the feature space for the optimal feature subset where features are carefully selected according to a well-defined discrimination criterion. In study, experimental results have shown that the PSO-based feature selection algorithm was found to generate excellent recognition results with the minimal set of selected features [3].

Rabab and Rehab [6] presented a novel feature selection algorithm based on particle swarm optimization (PSO). The algorithm is applied to coefficients extracted by two feature extraction techniques: the discrete cosine transforms (DCT) and the discrete wavelet transform (DWT). Experimental results show that the PSO-based feature selection algorithm was found to generate excellent recognition results with the minimal set of selected features. AsmitaS.Deshpande et al. [7] have proposed a Multimodal Biometric Recognition System based on Fusion of Palmprint, Fingerprint and Face. To overcome limitations such as non-universality, noisy sensor data and susceptibility, multibiometric recognition systems, which aggregate information from multiple biometric sources, are gaining popularity. To spoofing over the single biometric systems, multibiometric systems promise significant improvements as higher accuracy and increased resistance. They presented a method which integrates fingerprint, palmprint and face and performs the fusion at score level. Kumar et al [8] proposed the palm print and hand geometry features of an individual are obtained from the same hand image. Two schemes for the fusion of features, fusion at the decision level and at the representation level, were considered. The decision level fusion with max rule gave better results. [9] Discussed Hand geometry, palm print and finger surface biometric features are used for fusion. Two different levels of fusion are applied for authentication such as score level fusion for the five finger surface features and decision level fusion for various modalities, based on the majority vote rule. The authors in Raghavendra et al. [10] have presented an efficient feature level fusion scheme applied on face and palmprint images. Particle Swarm Optimization (PSO) approach was used to reduce the dimension of the vector. Results of the proposed feature fusion-PSO approach reduced the fused feature space dimension by a factor of 45% roughly.

Kaushik and Mohamed [11] have introduced a multimodal system for the integration of iris, face, and gait features based on the fusion at feature level. PSO is used to select the subset of informative features. This PSO-based dimensionality reduction method trimmed down the fused feature space dimension by a factor of 77% roughly. Punam et al [12] presents a robust multimodal biometric image watermarking scheme using Particle Swarm Optimization (PSO). The key idea is to watermark an individual’s face image with his fingerprint image and demographic data. PSO is used to select best DCT coefficients in the face image for embedding the watermark. Experimental results show that the proposed technique embeds private biometric data securely in another biometric content without affecting the latter’s visual quality. The authors in [13] presents an efficient tongue recognition biometric system for authentication based on Dual Tree Complex Wavelet Transform. A method for identifying a person based on their tongue is provided in which an image of a tongue of individual person is compared to recorded details of tongues in database. Here feature extraction of tongue image has been done using 2D Dual Tree Complex Wavelet Transform (2D-DT-CWT).

2. Research Method

The system architecture is designed in figure 4, for recognition of tongue images in online transactions. The architecture shows bank headquarter that has a central database, bank branches and their ATM outlets being connected by internet facilities. The ATM machines are equipped with biometric system to capture the cardholder traits for authentication. The biometric system consists of five modules: (a) Images Acquisition (b) Images preprocessing (c) Images feature selection using PSO(d) Pattern Matching (e) Evaluaton

Images Acquisition The images of tongues and fingerprints used for this experiment were acquired using a digital camera. A total of 120 images for tongues and 120 images of fingerprints (three fingers from both hands including their thumbs) of 20 individuals were used in the course of the experiment. Images were acquired in Joint Photographic Expert Group(JPEG) formats.

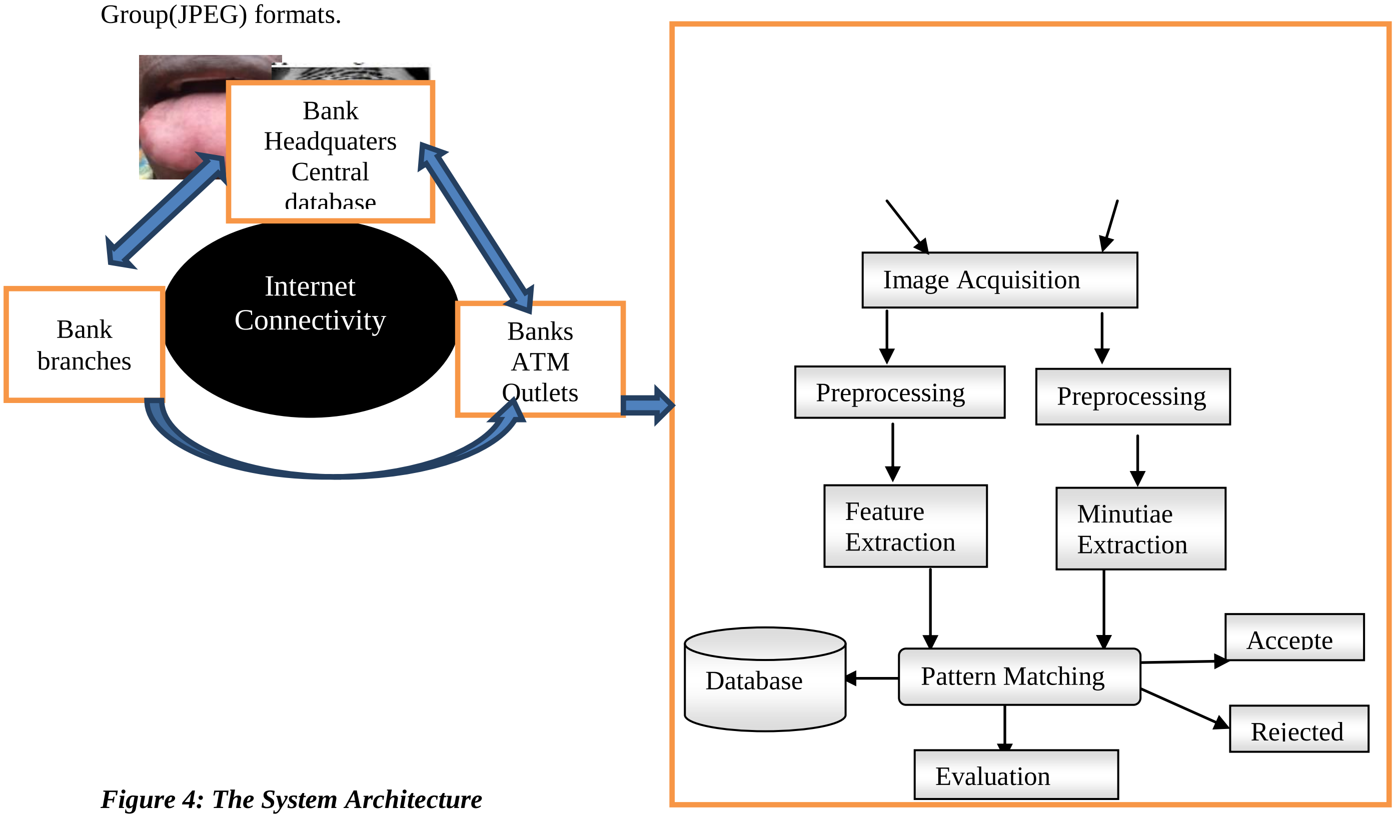

Figure 4: The System Architecture

Images pre-processingThe image pre-processing involved extraction of region of interest(minutiae points in fingerprints) and then normalizing the tongue and fingerprints images. The extraction of region of interest involves detecting the portion of the image containing the tongue and fingerprints. This will help to remove every background image from the captured image. The extraction of region of interest was done by binary mask. After the extraction of region of interest, the tongue and fingerprints images were then normalized by the histogram equalization technique to remove any common features that all the tongue and fingerprints mages shared together.

Feature Selection Particle Swarm Optimization was used to select salient features tongue and fingerprints images. PSO is an algorithm based on the social behavior associated with bird flocking to solve an optimization problem. When PSO is used to solve an optimization problem, a swarm of computational elements, called particle, is used to explore the solution space for an optimum solution. Each particle represents a candidate solution. The system is initialized with a population of random solutions and searches for optima by updating generations. The search process utilizes a combination of deterministic and probabilistic rules that depend on information sharing among their population members to enhance their search processes.

By simulating individual learning and social cultural transmission, PSO attains both simplicity and efficiency (speed of convergence). Some of the advantages of PSO are; it has performed well on variety of benchmark problems, such as, Schaffer function [12] and global minimum. The pseudo code of the initial version of PSO for real valued variables is given in figure 4 as follows,

```
For each particle
{
   Initialize particle
}

Do until maximum iterations or minimum error criteria
{
   For each particle
   {
      Calculate Data fitness value
      If the fitness value is better than pBest
      {
         Set pBest = current fitness value
      }
      If pBest is better than gBest
      {
         Set gBest = pBest
      }
   }

   For each particle
   {
      Calculate particle Velocity
      Use gBest and Velocity to update particle Data
   }
```

Figure 5: Pseudo Code for PSO

Images MatchingIt is used to compare the extracted biometric raw data to one or more previously stored biometric templates. The module therefore determines the degree of similarity (or of divergence) between two biometric vectors.The extracted features of the tongue are compared with the tongue images in the database by Euclidean distance formula. Euclidean Distance: The Euclidean distance is one way of defining the closeness of match between two iris feature templates. It is calculated by measuring the normal between two moment vectors. X_2 and X_1 are x-axis moment values and Y_2 and Y_1 are y-axis moment values.

$$D = \mathrm{Sqrt}\{ (X_2-X_1)^2 + (Y_2-Y_1)^2\} \qquad (1)$$

3. Results and Analysis

The dataset used contain 120 tongue images, that is, 6 images of 20 subjects, 64 images were trained meaning 4 images per 16 subjects while 56 images were used to test the technique meaning 2 images per sixteen subjects plus the 6 images of the remaining untrained 4 subjects.Acquired tongue and fingerprints images are fed into the tongue system as shown in figure 5. The image is subjected to pre-processing which comprises of normalization, extraction of region of interest and binarization. PSO is then applied to extract necessary features which are then stored in database.

During testing, the inputted tongues and fingerprints (impostors) undergo the same processes and then matched with the images in the database using Euclidean distance. In order to evaluate the effectiveness of the proposed method, experiments were carried out for real images at different postures. Three testing scenarios were created; (i) testing with all images in database and (ii) testing with another selected pose of images in database and (iii) poses of images not in database but captured in a bad illumination. The decision to recognize or classify the images was determined by threshold at 0.50.Scenario 1 results showed that the experiment produced sensitivity of 94.6%, specificity of 95.7% and accuracy rate of 94.6% for tongues and sensitivity of 87.2%, specificity of 81.4%, and accuracy of 90.1% for fingerprints. Scenario 2 results showed that the experiment produced sensitivity of 78.6%, specificity of 74.7% and accuracy of 93.3% for tongues while fingerprints has sensitivity of 65.2%, specificity of 69.4%, and accuracy of 75.5%. while scenario 3 results produced sensitivity of 0.6%, specificity of 0.77% and accuracy of 0.0% for fingerprints and sensitivity of 22.6%, specificity of 18.4%, and accuracy of 20.7% for fingerprints.

4. Conclusion

Biometrics is very useful, safe and effective in authentication systems because it is difficult to falsify. This paper presented the use of physiological traits (fingerprint and tongue) for security in ATM online transactions. Although fingerprints have been used and even deployed with ATM machines in some countries but the fear of its prone to falsification gave room for other human traits like tongue, which is not prone to falsification at present to be used. The two traits were subjected to pre-processing and feature selection algorithm (Particle Swarm Optimization). The features matching was done by Euclidean Distance on three formulated scenarios and the results were analysed and compared. Thus it was deduced that that tongue provided a better results than fingerprints in terms of sensitivity, specificity and accuracy.

References

[1]. Jain, A.K. Bolle, R. and Pankanti S. (eds.). Biometrics: PersonalIdentification in Networked Society. Kluwer, New York, 1999.

[2]. Miller, B. Vital signs of identity. IEEE Spectrum 31, 2 (1994),22–30.

[3]. BhosaleS.T., and SawantB.S (2012). Security in E-Banking Via Card Less Biometric ATMS, International Journal of Advanced Technology & Engineering Research (IJATER).Vol. 2, Issue 4, page 9-12.

[4]. Lin H. “Automated Biometrics of Audio- Visual Multiple Modals ” PhD Thesis, University of Florida Atlantic, USA. 2010

[5] Kennedy J., and Eberhart. R. C. and Shi, Y. “Swarm intelligence.” *Morgan Kauffmann Publishers, San Francisco*, CA. pp. 234-345. 2001.

[6] Rabab M. R. and Rehab F. A.. “Particle Swarm Optimization for human face recognition” *Signal Processing and Information Technology (ISSPIT).*2009.

[7] AsmitaS.Deshpande, S.M.Patil and RekhaLathi, "A Multimodal Biometric Recognition System based on Fusion of Palmprint, Fingerprint and Face", International Journal of Electronics and Computer Science Engineering.(16)

[8] Kumar, A., Wong, D., Shen, H. and Jain, A.“Personal Verification Using Palm print and Hand Geometry Biometric”, in Proc. 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, U. K., pp. 668-678. 2003

[9] T Sanches, J Antunes, and P L Correia, "A Single Sensor Hand Biometric Multimodal System," in 15th European Signal Processing Conference (EUSIPCO), Poznan, Poland, 2007, pp. 30-34.

[10] R. Raghavendra, Bernadette Dorizzi, Ashok Rao and G. Hemantha Kumar, "Designing efficient fusion schemes for multimodal biometric systems using face and palmprint", Pattern Recognition, vol.44, no.5, 2011.(18)

[11] R. Kaushik and S. Mohamed “Multibiometric System using level Set method and Particle Swarm Optimization”, A. Campilho and M. Kamel (Eds.): ICIAR 2012, Part II, pp. 20–29, 2012. © SpringerVerlag Berlin Heidelberg 2012.

[12] Punam B., Roli B., Priti S. Multimodal Biometric Authentication using PSO based Watermarking. Procedia Technology, 4 (2012) pp. 612 – 618

[13] Amit, B., Komal, C., Pradip, A., Rupali, K. Tongue Recognition System for Authentication. International Journal for Research in Applied Science & Engineering Technology (IJRASET). 3(3), pp. 76-80.2015.