Biometric Automated Teller Machines based Anti-Spoofing Fingerprint System

Ismaila W. Oladimeji, Ogunjinmi Temitope O., Babalola O. Richard, Ismaila Folasade.
Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria and Osun State Polytechnic, Iree, Nigeria

Abstract:
Transaction security is critical to e-trading's future growth and there is serious concern over the sufficiency of current solutions. The concerns with personal identification numbers and identity tokens are that they do not guarantee the identity of the person who uses them. With increasing growth for fingerprint recognition system, there are also increasing concerns about spoofing, duplications, masking etc, that can bypass the authentication process. Fingerprint liveness detection methods have been developed as an attempt to overcome the vulnerability of fingerprint biometric systems to adulterations. Thus, this work aimed at experimenting a biometric Automated Teller Machines (ATM) based liveness fingerprint system (BALFS). The BALFS system employed an principal component analysis (PCA) for feature extraction and back-propagation neural network (BPNN) for subjects matching. The dataset as enhanced by Contrast Limited Adaptive Histogram Equalization (CLAHE). PCA extracted features from ridges-cum-pores of fingerprints and BPNN was used for classification. The results showed that when the BALFS system matched sample A on itself; matched sample B on sample A; and matching of sample B on itself produced recognition accuracies of 100.0%; 94.5%; and 98.5% at 0.85 thresholds respectively. However, the matching of sample C (spoofing samples) on sample A and sample B produced accuracies of 100% and 86.5% for non-matching subjects at 0.85 threshold respectively.

Keywords: ATM, Liveness fingerprint, PCA, BPNN, Spoofing.

1. INTRODUCTION

ATMs innovation paralleled the increase in personal computers and communications industries. Each machine operated in a local mode without any connection to the banking systems, and transaction authorization took place based on the information stored in the cards magnetic cores. Reports showed that credit card fraud cost over three hundred million pounds per year and ATM fraud was on the high side of over three billion pounds. Nowadays, various technologies have evolved for authentication of persons and these include biometrics. However, some biometric traits are sensitive to duplications like spoofing, masking etc. A spoof attack is to apply an artificial replica of a biometric used in an attempt to circumvent a secured system. [3,19]. The feasibility of a spoof attack is much higher than other types of attacks against biometric systems, as it does not require any internal knowledge of the system, such as the feature extraction and/matching algorithm used [16, 17, 18, 19]. Thus, this paper aimed at experimenting a biometric ATM based liveness fingerprint system (BALFS) using principal component analysis for feature extraction and back-propagation neural network for classification using online database. The general task of liveness detection is to detect whether a biometric probe (e.g. a fingerprint) belongs to a living subject that is present at the point of biometric capture [2]. The remainder of this paper is organized as follows. Section II discusses the technology of liveness fingerprint. Section III presents the methodology required to prepare the BLFDS system for implementation. While section IV describes implementation and discussion of results. Section V entails the conclusion.

II. LIVENESS FINGERPRINT TECHNOLOGY

A liveness fingerprint (as shown in figure 1a) is the representation of the epidermis of a finger: it consists of a pattern of interleaved ridges and valleys collectively regards to as minutiae, used as evident structural characteristics of a fingerprint which are presents and different in individual fingerprints. Spoof images (as shown in figure 1b) are made up of Crossmatch, Clay, Play-Doh, Gelatin, Silicone and Identix. Liveness detection methods are generally classified into two types: (i) Hardware-based techniques, which add some particular device to the sensor in order to detect Exacting properties of a living trait (e.g., blood pressure, fingertip sweat, etc) (ii) Software-based techniques, in this type the fake trait is detected once the sample has been acquired with a normal [1].

![Figure 1. (a) Liveness Fingerprint Minutiae (b) Gelatin Spoofing Image](http://ijesc.org/)
III. RELATED WORKS

Fingerprint liveness detection methods have been developed as an endeavour to overcome the sensitivity of fingerprint biometric systems to spoofing attacks. The researchers in [4] several conventional methods have been developed to evaluate the performance of supervised models using both live and spoof samples. [5] authors in 2008 presented a new method based on the wavelet transform on the ridge signal extracted along the ridge mask which could detect the perspiration phenomenon using only a single image. Statistical features are extracted for multi-resolution scales to discriminate between live and non-live fingers. A classification tree was used to generate the decision rules for the liveness matching. The method was tested on two different online datasets which contained live and spoof (made from gelatin) subjects. [6] researchers introduced a new convolutional neural networks architecture for fingerprint liveness detection problem. The proposed method employed squared regression error for each receptive field without the usage of the fully connected layer but the squared error layer allowed them to set up a threshold value. And the absence of a fully connected layer allows them to crop the input fingerprints such that a trade-off between accuracy and computation time could be made without the negative effects of re-scaling. The author in [7], in 2005, proposed a novel fingerprint liveness detection method based on Deep Convolution Neural Network and voting strategy, which performed better than handcraft feature. Also the work optimized the process of feature extraction and classifier training simultaneously. The experimental results on the datasets of LivDet2011 and LivDet2013 showed that the proposed algorithm has great improvement compare to the former state-of-the art algorithm, and keep highly real-time performance at the same time. In 2016, the authors in [8] proposed a software-based fingerprint liveness detection method based on multi-scale difference co-occurrence matrix (DCM). After the preprocessing of the decomposition of the original image, DCMs were computed by using the Laplacian operator. Then, recognition accuracy of the system was determined. In addition to the pore spacing features, the total number of pores detected relative to the total length of all ridge segments is determined. In 2016, the authors in [8] proposed a software-based fingerprint liveness detection method based on multi-scale difference co-occurrence matrix (DCM). After the preprocessing of the decomposition of the original image, DCMs were computed by using the Laplacian operator. Then, recognition accuracy of the system was determined. In addition to the pore spacing features, the total number of pores detected relative to the total length of all ridge segments is determined.

IV. METHODOLOGY

This section entailed the steps involved in executing this proposed liveness fingerprint system viz: Sample dataset, Image pre-processing, feature extraction, and image matching as shown in figure 3.

Sample dataset: The sample dataset used for the experimentation was the development set provided in the Fingerprint Liveness Detection Competition. LivDET 2011 consists of live and spoofed images of which 200 live and 200 spoofed images were selected from Biometrika FX2000 samples.

Image pre-processing: The Preprocessing stage involved enhancement of image by using (i) histogram equalization variant, CLAHE, [15] (is a technique for adjusting the pixel intensities of image to enhance the contrast), (ii) binarization (the operation that converts the gray scale image into binary image. It is used to transform 8-bit gray fingerprint image into one-bit image with zero value for ridges and one value for furrows) and (iii) morphological thinning (was used to remove selected foreground pixels from binary images, that is, binary ridge segments are thinned to a single pixel wide skeleton, which identifies a center line for each ridge segment).

Feature Extraction: After the enhancement of the fingerprint image the next step was feature extraction by PCA algorithm. This method extracted the ridge endings and bifurcations from the skeleton image by examining the local neighborhood of each ridge pixel. Also, the frequency /number of pores along the ridge segments is extracted. In addition to the pore spacing features, the total number of pores detected relative to the total length of all ridge segments is determined.

Matching: can be the first step in identification tasks as it reduces database entries requiring searching. A biometric identification system’s task is finding a biometric object in a database matching a query biometric object. A matcher operating at a high threshold, has a low FMR and high FnMR; a low threshold means high FMR (security breaches) and low FnMR (inconvenience). In this work SVM was used for the classification of fingerprints into either “Live” or “Spoof”.

Evaluation Metrics: The performance of developed PCA-BPNN liveness fingerprint system was measured using false match rate, false non-match rate and recognition accuracy.

(i) Recognition Accuracy is the proportion of genuine/impostor attempts that are correctly declared to match a template.
(ii) False Match Rate (FMR): Proportion of impostor attempts that are falsely declared to match a template of another subject.

(iii) False Non Match Rate (FnMR): Proportion of genuine attempts that are falsely declared not to match a template of the same subject.

V. IMPLEMENTATION AND RESULTS

The system was developed in MATLAB environment, the interface of the system is shown in figure 4. The extracted data used consists of three samples viz (i) sample A (liveness fingerprints) and sample B (non-live fingerprints) are and sample C (spoofed fingerprints that were gotten from sample A and B). The developed BALFS system was trained and tested.

The parameters listed below were chosen using cross-validation of dimension 5x2 fold.

i. PCA: number of components chosen was 1000

ii. BPNN: number of layers (4); number of filters (1024 for each layer).

The results of performance metrics of the system at different threshold values of 0.35, 0.55 and 0.85 are discussed as follows. When the system operated on sample A only on the sample B database (that is liveness samples matched with non-liveness samples), it produced recognition accuracy of 100.0%, FMR and FnMR are of the same value of 0.0% respectively at all thresholds. When the system operated sample B only on the sample A database (that is matching of non-liveness samples with liveness samples), it produced recognition accuracy of 100.0%, 92.5%, 91.3%, FMR of 7.4%, 0.0%, 0.0% while FnMR of 4.7%, 0.0%, 0.0%, at 0.35, 0.55 and 0.85 thresholds respectively. While the operation of the system on sample B onto its database (that is matching of non-liveness samples on itself), produced recognition accuracy of 93.5%, 93.5%, 90.3%, FMR of 14.6%, 7.5%, 7.5% and FnMR of 9.6%, 5.2%, 5.1%, at 0.35, 0.55 and 0.85 thresholds respectively. The matching of sample C (spoofing samples) on sample A produced accuracy of 100.0%, FMR and FnMR of 0.0% each at all thresholds respectively for not matching any spoof samples. While the matching of sample C on sample B database gave accuracy of 86.7%, FMR 8.3% and FnMR of 0.0% each at all thresholds respectively for not matching any spoof samples.

VI. CONCLUSION

The contribution of fingerprint pore analysis to liveness detection is somewhat dependent on the particular data on which it is used. These data factors can be related to the sensing technology as well as the types of spoofing attacks that may be used against the particular system. This paper evaluated the efficiency of principal component analysis for feature extraction and back-propagation neural network as classifier on liveness fingerprint system in ATM at different thresholds. The experimental results obtained revealed that when the BALFS system matched sample A on itself; matched sample B on sample A; and matching of sample B on itself produced recognition accuracies of 100.0%; 94.5%; and 98.5% at 0.85 thresholds respectively. However, the matching of sample C (spoofing samples) on sample A and sample B produced accuracies of 100% and 86.5% for non-matching subjects at 0.85 threshold respectively.

VII. ACKNOWLEDGEMENT

I acknowledge the Tertiary Trust Fund (TETFUND) Nigeria for sponsoring this research work and publication

VIII. REFERENCES


