Conference Paper

Facial Recognition System for Secured Mobile Banking

Fatema A. Albalooshi[1], Max Smith-Creasey[2], Yousif Albastaki[2], and Muttukrishnan Rajarajan[2]

[1]College of IT, University of Bahrain, Sakheer, Kingdom of Bahrain, P.O. Box 32038
[2]School of Mathematics, Computer Science and Engineering, University of London, London, UK

Abstract

As biometrics offer greater security than traditional methods of personal recognition, a great deal of effort has been made on making mobile banking more efficient with less imposter attacks by utilizing biometric authentication systems. In this article, the authors propose a machine-learning-based automated facial recognition system that employs face recognition to initially perceive the presence of an authorized person, in order to grant the individual access to secure banking environments. In detail, a neural network-based face recognition is introduced, where a pre-trained neural network is utilized to guide the system. This procedure improves the performance of traditional mobile banking systems. Utilizing the proposed algorithm allows predicting imposter attacks in highly secured and restricted places.

Keywords: Face Recognition, Secured Mobile Banking, Neural Network, Deep Believe Networks, Restricted Boltzmann Machine, Machine Learning

Corresponding Author:
Fatema A. Albalooshi
falbalooshi@uob.edu.bh

Received: 18 September 2018
Accepted: 10 October 2018
Published: 15 October 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the Sustainability and Resilience Conference Committee.

1. Introduction

The high-tech developments of mobile devices like improved computational ability has recently allowed for new paths to more secured online banking. Financial institutions have started to provide mobile banking opportunities for their clients after realizing the benefits to be gained from mobile banking, to allow clients to perform banking operations like paying bills, checking on account balance, and transferring money at anytime from anywhere. Since security has been always the major concern in online banking, authentication on mobile devices can be the glue that binds together online banking and mobile banking in a way that combines security with convenience. For online financial transactions, the security level at both the client and the banking server end must be maintained carefully. Traditional methods for authorization in online mobile banking include information the client knows. Such practices mostly take the form of a

PIN, password, tokens, keys, or security questions, which can be stolen or guessed by impostors who may use the data for malicious purposes. As a result, the trust over the trust over the technology may get affected and reduced number of people will switch to online banking (Jafri & Arabnia, 2009).

Driven by current developments in human-centered computing, an automatic system for facial recognition has emerging applications in secured access and mobile banking areas.

Moreover, mobile devices present a vital role in our lives as they are used widely in personal and professional atmospheres. This brings up the idea of facial recognition systems using mobile devices which can be more reliable and can help to build the trust with clients and online banking systems.

This paper presents a proposed design that implements face authentication based on Deep Belief Network (DBN) (Hinton, Osindero, & Teh, 2006) to reduce the risks of fraud in mobile banking. Thus, when a customer initiates a mobile banking transaction, the facial recognition system would request that the user takes a picture form the front facing camera of the mobile device, and the system would compare the captured picture to the one already stored on the bank mobile transaction server. The comparison is based on deep believe neural networks which provide higher accuracy compared to other state-of-the-art methods (Hinton et al., 2006). A decision is made whether the user should be granted access, then the system would then send the transaction request and the result of the face recognition to the bank server for approval and execution of the transaction. The primary contributions of this paper are:

- We propose a facial authentication scheme based on deep believe networks for online banking. We show the lack of ordinary authentication approaches to provide reliable mobile banking.
- We show that our facial authentication system can provide greater usability whilst maintaining device security. Our uses trust to adjust the authentication tier.

The rest of this paper is organized as follows. In Section II, we briefly summarize the previous work in the areas of facial authentication on mobile devices. Section III presents the general concept for our system Section IV concludes our research and discusses the future work that can be derived from our system.

2. Related Work

vast amount of research is dictated to biometric authentication on mobile devices due to the advancements and added sensors on such devices (Smith-Creasey & Rajarajan, 2017; Primo, Phoha, Kumar, & Serwadda, 2014; Fridman, Weber, Greenstadt, & Kam, 2017). Oka Sudana et al. (Sudana, Putra, & ARISMANDIKA, 2014) Introduced a face recognition technology using eigenface technique in android device. They used color segmentation combined with template matching to perform the recognition process. Their results show accuracy reaching 94

Moreover, Smith-Creasy et al. (Smith-Creasey, Albalooshi, & Rajarajan, 2018) implemented a novel structure for continuous face authentication using mobile device cameras that addresses the issue of spoof attacks and attack windows in state-of-the-art approaches. They utilized live faces were warped to a standardized pose and textual features extracted into a vector and scored using distance algorithms, improving on previous works. They incorporated LBP-based liveness detection to avoid spoofing threats.

The researchers in (Clarke, Karatzouni, & Furnell, n.d.) suggested a transparent facial recognition scheme for mobile devices. Their findings show that improved accu- racy can be achieved when taking into consideration facial orientation. Their study lacks in that the dataset used does not illustrate real-world scenarios.

3. Mobile Banking Face Authentication Scheme

3.1. General idea

In our proposed system, the users will be using their faces to log into their bank accounts to gain faster access and enhance security. In our face recognition system, there are two main modes including training mode and identification mode. In the training mode the system enlightens the registration process to obtain the training image as a reference which will be saved in the database.

The identification mode includes the process of test image recognition which is compared with the trained image in the database.

Thus, our scheme starts with acquiring the input image from the front facing camera of the mobile device. After that, face detection process is performed using Viola-Jones method (Viola & Jones, 2001). Then features from detected face are constructed by deep believe networks (Hinton et al., 2006). The facial recognition process contains

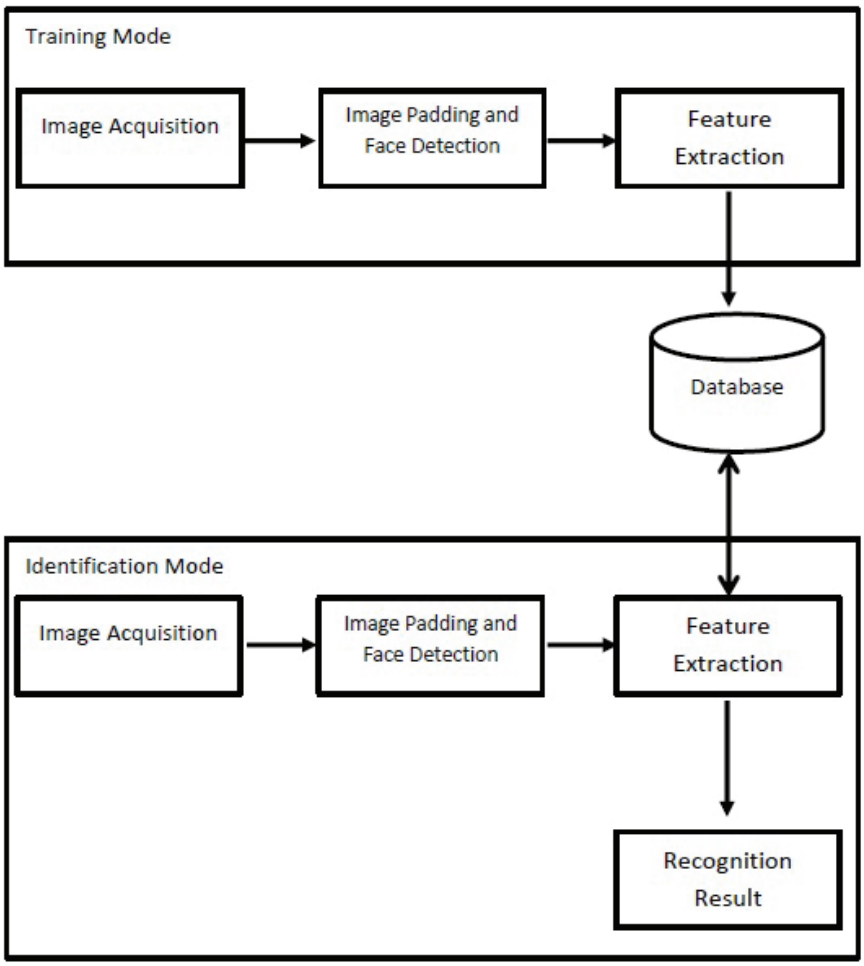

Figure 1: System flowchart.

feature training and feature classification processes. Moreover, system flowchart is shown in Figure 1.

3.2. Face detection

it is found that faces taken from the front facing camera of mobile devices usually take up a significant portion of the frame which can affect the performance of detection process. Therefore, we suggest to add padding to the picture frame by extending the width and height through repeating the edge pixels as in (Smith-Creasey & Rajarajan, 2017; Fathy, Patel, & Chellappa, 2015).

Moreover, Viola-Jones method is used here for face detection. This method is generally used for object detection (Viola & Jones, 2001). Although training process is time consuming, detection is fast due to the fact that this method utilizes Haar basis

feature filter that does not use multiplications, which makes it suitable to real-time applications.

Viola-Jones face detection occurs within a detection kernel that is moved across the input image as follows:

1. Setting the minimum kernel size, and sliding step corresponding to that size.
2. Sliding the kernel vertically and horizontally within each step.
3. At each step, a set of N face recognition filters are applied. If one filter gives a positive answer, the face is detected in that current kernel.
4. The procedure stops when the size of the kernel reaches the maximum size.

3.3. Boltzmann machine

A Boltzmann Machine (BM) is a neural network that contains a set of visible units $v \in \{0,1\}^D$ that are symmetrically combined with a set of hidden units $h \in \{0,1\}^P$, where *D* and *P* represent the number of the visible and hidden units respectively. The energy of the state $\{v, h\}$ can be defined as

$$E(v, h; \theta) = -\frac{1}{2} v^T L v - \frac{1}{2} h^T J h - v^T W h. \quad (1)$$

where θ = $\{W, L, J\}$ are the model parameters: *W, L, J* represent visible-to-hidden, visible-to-visible, and hidden-to-hidden symmetric interaction terms respectively (Salakhutdinov & Hinton, 2009). If we set both *J* and *L* to 0, it forms the well- known Restricted Boltzmann Machine (RBM) (Smolensky, 1986), where its learning algorithm was discussed by Hinton and Sejnowski (Hinton & Sejnowski, 1986).

3.4. Restricted Boltzmann machines and deep belief network

Unlike BMs, an RBM has no connections between visible or hidden layers which helps in making the learning process simpler. An RBM can learn a layer of features unsupervisly by converting its data patterns into an aggregated posterior patterns over the invisible blocks. Furthermore, RBMs are energy-based undirected generative models where the likelihood patterns over the visible and hidden variables are defined through an energy function, given by (Mohamed, Dahl, & Hinton, 2012)

$$E(v, h|\varphi) = -\sum_i \sum_j w_{ij} v_i h_j - \sum_i b_i v_i - \sum_j a_j h_j \quad (2)$$

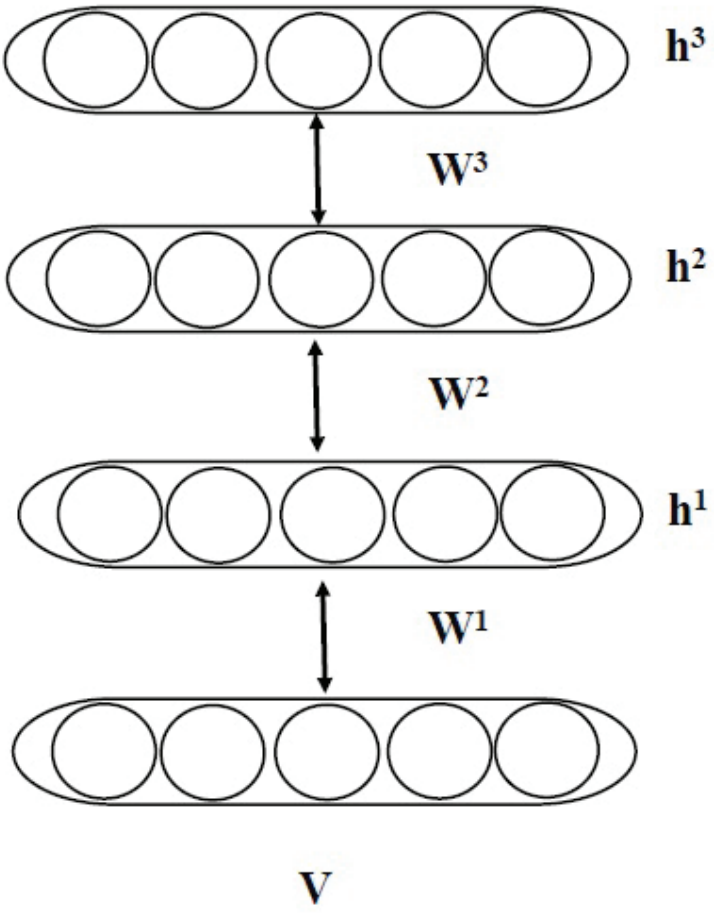

Figure 2: DBN formed by staking several RBMs.

where v_j and h_j are the binary states of visible unit *i* and hidden unit *j*, respectively. φ = $\{w, b, a\}$. w_{ij} is the symmetric weight between visible unit *i* and hidden unit *j* while b_i and a_j are their bias variables. Using this energy function, the probability of a visible and a hidden vector is obtained by (Hinton, 2012):

$$p(v, h) = \frac{1}{Z} e^{-E(v,h)} \tag{3}$$

where the *Z* is the partition function, computed by

$$Z = \sum_{v,h} e^{-E(v,h)} \tag{4}$$

On the other hand, an RBM only considers the connection between visible and hidden layers, the conditional Bernoulli distributions over visible and hidden units are given respectively by

$$p(v_i = 1 | h; \varphi) = \sigma\left(\sum_j w_{i,j} h_j + a_i\right) \tag{5}$$

$$p(h_j = 1|v;\varphi) = \sigma\left(\sum_i w_{i,j} v_i + b_j\right) \quad (6)$$

where $\sigma(x)$ represents a Sigmoid function. RBM training process can be successfully achieved by contractive divergence and that makes RBM suitable as fundamental blocks for building DBN network (Hinton, 2002).

Thus, when multiple RBMs are stacked together and learned in a layer by layer fashion, such that the hidden units of one RBM are treated as the input data for producing a higher-level RBM, the resulting model forms DBN as shown in Figure 2.

3.5. DBN learning

DBN learning is to estimate hidden and visible weights in a given training data. At the beginning, an initial estimate of the parameters can be calculated using an unsupervised bottom-up learning strategy (Hinton et al., 2006). Then, through a bottom-up feed forward process, we can compute the hidden units given the input data. The bottom-up learning procedure is completed for each patch location independently to learn the initial feature representation. The feature vector of the detected face is generated using deep learning as shown in Figure 3.

Figure 3: Generating the feature vector of input image using deep learning. The image is taken from the "Extended Yale Face Database B" (Georghiades et al., 2001).

3.6. Feature classification

A Support Vector Machine (SVM) classifier (Cortes & Vapnik, 1995) is utilized to classify if whether the input face belongs to a genuine user or an imposter. For a set of training data $D = ((\vec{x}_i), y_i)$, where each point is a pair of a vector point $(\vec{x}_i) \in R^d$ and a class label y_i 1, +1 corresponding to it, the classification function f $(\vec{x})$ can be expressed as:

$$f(\vec{x}) = sign(\vec{w}^T \vec{x} + b) \tag{7}$$

Here, w and b are parameters of the classification function.

4. Conclusion and Future Work

In this study, we introduced a deep learning -based facial recognition system to provide a secured and reliable mobile banking. The introduction of the deep believe networks for facial authentication on mobile devices had proven to be effective in maximizing security level when performing banking transactions (Fatahi, Ahmadi, Ahmadi, Shahsavari, & Devienne, 2016). It is expected that the security level of mobile banking to increase with the employment of deep believe networks for face authentication.

The future work of this paper will focus on expanding the current scheme to enhance the usability and security. Firstly, the facial authentication of the scheme will be expanded to factor in noise from external environments. We will employ acoustic scene classification techniques to establish whether the user is in a public or private space such that the trust levels can be adapted accordingly. Secondly, our future work will explore furthering the security via face-authentication-based locking mechanisms. The authentication scheme will incorporate a recognition module that will lock the banking system if it is used by a person other than the genuine user. Our future work will lastly investigate the incorporation of our facial recognition scheme into a larger authentication framework. Such a framework may use the trust levels alongside other trust scores (e.g.: from touch-gestures) to produce a more robust trust score. We posit that, for example, the average of two biometric modalities will reduce the volatility and noise produced by a single modality.

References

[1] Clarke, N., Karatzouni, S., & Furnell, S. (n.d.). Transparent facial recognition for mobile devices.

[2] Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine learning* , *20* (3), 273–297.

[3] Fatahi, M., Ahmadi, M., Ahmadi, A., Shahsavari, M., & Devienne, P. (2016). To- wards an spiking deep belief network for face recognition application. In *6th international conference on computer and knowledge engineering (iccke 2016).*

[4] Fathy, M. E., Patel, V. M., & Chellappa, R. (2015). Face-based active authentication on mobile devices. In *Acoustics, speech and signal processing (icassp), 2015* IEEE International Conference (pp. 1687–1691).

[5] Fridman, L., Weber, S., Greenstadt, R., & Kam, M. (2017). Active authentication on mobile devices via stylometry, application usage, web browsing, and gps location. *IEEE Systems Journal* , *11* (2), 513–521.

[6] Georghiades, A., Belhumeur, P., & Kriegman, D. (2001). From few to many: Illumination cone models for face recognition under variable lighting and pose. *IEEE Trans. Pattern Anal. Mach. Intelligence*, *23* (6), 643-660.

[7] Hinton, G. E. (2002). Training products of experts by minimizing contrastive divergence. *Neural computation*, *14* (8), 1771–1800.

[8] Hinton, G. E. (2012). A practical guide to training restricted Boltzmann machines. In *Neural networks: Tricks of the trade* (pp. 599–619). Springer.

[9] Hinton, G. E., Osindero, S., & Teh, Y.-W. (2006). A fast learning algorithm for deep belief nets. *Neural computation*, *18* (7), 1527–1554.

[10] Hinton, G. E., & Sejnowski, T. J. (1986). Learning and releaming in Boltzmann machines. *Parallel* Distributed *Processing* , *1* .

[11] Jafri, R., & Arabnia, H. R. (2009). A survey of face recognition techniques. *Jips*, *5* (2), 41–68.

[12] Mohamed, A.-r., Dahl, G. E., & Hinton, G. (2012). Acoustic modeling using deep belief networks. *IEEE Transactions on Audio, Speech, and Language Processing* , *20* (1), 14–22.

[13] Primo, A., Phoha, V. V., Kumar, R., & Serwadda, A. (2014). Context-aware active authentication using smartphone accelerometer measurements. In *Proceedings of the IEEE conference on computer vision and pattern recognition workshops* (pp. 98–105).

[14] Salakhutdinov, R., & Hinton, G. (2009). Deep Boltzmann machines. In *Artificial intelligence and statistics* (pp. 448–455).

[15] Smith-Creasey, M., Albalooshi, F. A., & Rajarajan, M. (2018). Continuous face authentication scheme for mobile devices with tracking and liveness detection. *Microprocessors and Microsystems* , *63* , 147 - 157. Retrieved from http://www.sciencedirect.com/science/article/pii/S0141933117305239 doi:

[16] Smith-Creasey, M., & Rajarajan, M. (2017). Adaptive threshold scheme for touchscreen gesture continuous authentication using sensor trust. In *Trustcom/bigdatase/icess, 2017 ieee* (pp. 554–561).

[17] Smolensky, P. (1986). Information processing in dynamical systems: Foundations of harmony theory., Chapter 6, 194-281.

[18] Sudana, A. O., Putra, I. D., & ARISMANDIKA, A. (2014). Face recognition system on android using eigenface method. *Journal of Theoretical & Applied Information Technology* , *61* (1).

[19] Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. In *Computer vision and pattern recognition, 2001. cvpr 2001. proceedings of the 2001 ieee computer society conference on* (Vol. 1, pp. I–I).