**Advances and Applications in Mathematical Sciences**
Volume 21, Issue 6, April 2022, Pages 3143-3159


# REAL TIME FACE AUTHENTICATION USING DENOISED AUTOENCODER (DAE) FOR MOBILE DEVICES

**SHOWKAT A. DAR[1] and S. PALANIVEL[2]**

[1,2]Department of Computer
Science and Engineering
Annamalai University, Chennai, India

## Abstract

FBAs (Facial Based Authentications), a non-contact biometric technology has been evolving since its inception. FBAs when implemented as a part of technology have enabled the use of online service accesses for customers. Law enforcements, security and industrial efficient monitoring solutions. FBAs can be used to unlock devices by showing their faces in front of devices. Though at the outset, it seems an easy solution, it has remained a challenging issue in computer vision where conventional methods fail to fulfill application's demands mainly due to improper authentications or spoof attacks. DLTs (Deep Learning Techniques) have been receiving increased interests in FBA applications. Many proposals have used DLTs in this area. This chapter proposes DAEs (Denoised Auto Encoders) for real time classification of human faces. The proposed scheme balances accuracy with constraints of resource and time. The proposed DAE technique uses MDCs (Mobile Device Cameras) for FBAs as it can address spoof or windows based attacks. The proposed DAE technique eliminates possible attacks on windows by immediately recognizing impostors. Moreover, feature extraction in DAE is dynamic and thus authenticates humans based on their facial images. Facial videos collected from MDCs results in realistic assessments. Spoof attacks using MDCs for bypassing security mechanisms are identified by DLTs in authentications.

## 1. Introduction

The current evolutional growth in technology has made it possible to embed heavy computational power in HHDs (Hand Held Devices) like PDAs (Personal Digital Assistants), SPs (Smart Phones), tablets and mobiles where

2020 Mathematics Subject Classification: 68-XX.
Keywords: Facial authentication, Feature extraction, Biometrics, Deep learning, Denoised autoencoder (DAE), Classifier, Mobile banking, And mobile devices.
*Corresponding author; E-mail: showkatme2009@gmail.com
Received September 14, 2021; Accepted January 14, 2022

HHDs are a part of daily life activities. HHDs have multi-touch displays with user friendly interfaces and easy operational procedures. Current mobiles are used for voice calls, sending and receiving messages, taking photographs and playing games. Additionally many financial and personal transactions can be done with these gadgets. HHDs store user's personal information and use them during financial transactions like money transfers, handling multiple bank accounts, online payments, indulge in stock trading and many other useful applications which can be executed at anytime and from anywhere. This has resulted in complications of authenticating HHDs (Ortiz-Yepes et al., [16]).

Authentication of users is confirming their usage using their personal identities where their known identities are verified. Users can be authenticated using different mechanisms namely password based identifications or using User IDs, security tokens, device IDs or using their biometric identifiers like fingerprints. These user identifications authenticate them and grant access to transactions or digitally signed documents. Thus, many systems incorporate multitude of afore said security mechanisms including PINs (Personal Identification Numbers). But these mechanisms are prone to various forms of attacks like smudge attacks (Aviv et al., [3]). Moreover, such authentications are limited intrinsically as they provide onetime authentications for entire device's access. This one time authentications leave devices open to attacks when users fail lock their resources.

Current studies on mobile security have proposed usage of biometric authentications for overcoming issues in traditional security mechanisms (Frank et al., [9]). Human biometrics is individualistic and distinguishable making its exploitation in authentications a justifiable area of approach. The approaches can be based on behavioral or physiological biometrics characteristics where physiological approaches use measurements of human body parts like face or retina or fingerprints or hands.

Physiological biometrics usage yield better results as they are less susceptible to changes. Further, biometric authentications based on physiological factors using mobile devices are stronger as it can combine a human being's past and present. Many applications in the areas of telecom, banking, and security use biometric authentications making FBAs an active

area of research. Google has incorporated FBA in mobile Android (Smart Lock) while Apple has done the same in iPhone (Face ID). However, these applications have one-time authentication FBAs. Hence, this work focuses on authentications using classifiers for mobiles.

DLTs have established their significance in FBAs (Chaudhuri, [4]); (Singh et al., [18]). Facial recognitions need to leverage on a hierarchical architecture for discriminating instances (Mehdipour Ghazi and Kemal Ekenel, [14]); (Prasad et al., [17]). DLTs, with the use of multiple layers, learning data representations for efficient feature extractions and thus improve any system's performance appreciably when applied on discriminative tasks or in learning data. This chapter introduces TSFAS (Two-Step Face Authentication Scheme) by combining physiological and patterns with PINs, a system that can be applied on modern mobile device based banking Systems. The proposed scheme uses dual authentication based on different studies (Ortiz-Yepes et al., [16]).

## 2. Background

The study by Eldefrawy et al., [7] proposed a 2FA (2-Factor Authentication) scheme using many OTPs (One Time Passwords). Their scheme two different nested hash chains and used an initial seed. The first chain updated seeds while the second produced OTPs. Other techniques were used to constrain applications. Their analysis showed better results in terms of security and performances when compared with other techniques.

Physiological and behavioral factors were used by Koong et al., [12] in their study. Their proposed scheme used multiple biometrics in user authentications. The scheme called pbLogon (physiological and behavioral user authentications) combined biometric factors from two sources namely physiological and behavioral received as input from multi-touch panel of mobiles. pbLogon used user's finger rotations on mobiles for enhanced security. The scheme also allowed user credentials to be replaced for tight security of privacy.

Biometric framework was formulated by Verma et al., [22] in their study. The study's optical transformations were used in security authentications. The FBAs transformed faces using a phase retrieval algorithm. The

framework used sparse mask subsequently for retrieving optimal features and making the process non-invertible. The extracted features were pooled into a chaotic strategy for storage. The study's chaotic parameters were linked to passwords and used in enrolments. The study's authentication scheme used two factors where user's face provided the initial knowledge on biometrics while chaotic parameters substantiated verifications. The proposed framework's security was evaluated in terms of collision resistance, non-invertible capability and sensitivity. Their simulation results showed high recognition rates by discriminating original and imposter faces in samples.

FBAs were clubbed by with voices by Kasban [11] in their study's multi-modal biometric scheme. The scheme recognized voices of users using voice timbre and statistical/cepstral coefficients for comparisons. Voice recognitions were executed by GMM (Gaussian Mixture Model) while three techniques were used for facial recognitions namely LDAs (Linear Discriminate Analysis), Eigen faces and GFs (Gabor Filters). Their FBA scheme combined voice and biometric factors as a single multi-modal biometrics system which fused and assigned scores for features. Their experimental results showed good performances in terms of facial recognitions using obtained features.

OTPs were also used by Song et al., [20] in their study. The proposed scheme used 3 factors for authenticating mobile banking procedures. The user's facial image was captured using MCDs and the face's brightness and background were stored as points $(X, Y)$. The scheme computed distances between eyes, nose and mouth in the acquired image along with contours of the face which were then compared with previously stored facial features. Only when matches were found in the facial recognition database, the user was authenticated.

Behavioral features were exploited by Sitová et al., [19] in their study. The scheme used HMOG (Hand Movement, Orientation, and Grasp) sets for continuous authentications of smart phone users. The study used HMOG for capturing minute movements and orientations of the user's face while grasping or holding or tapping the smart phone. The study's proposed authentication scheme was evaluated for in terms of BKGs (Biometric Key Generations) based on HMOG features of a dataset collected from virtual

keyboard typing of 100 subjects. The study collected this data with subject's sitting and walking positions. Their experimental results showed that HMOG features had the capability to capture distinct bodily movements and specifically with subjects walking and taps on smart phones. The study's HMOG features, extracted at a sensor sampling rate 16 Hz with minimal overheads of 7.9% enhanced facial recognition accuracy.

Active user authentications were investigated by Fathy et al., [8] in their study. The proposed scheme of FBAs was aimed at smart phones and examined videos recording of the user's face for authentications. The user videos were acquired under varying ambient conditions i.e. while performing different tasks for assessment of device mobility.

Their investigations of the acquired videos revealed unique favourable/challenging facial properties of smart phone videos. Additional challenges included partial faces, facial poses, facial blurs and facial fiducial point's localization errors from facial datasets. The study evaluated still images and image sets with facial intensity features around fiducial points using FBA algorithms. The study found that recognition rates dropped drastically when the test videos and enrolment videos belonged to different sessions.

Active authentications were reviewed by Mahfouz et al., [13]. The study highlighted components used by operational procedures of active authentications while giving an overview of behavioral biometric traits useful for development of such systems. The review's evaluations on smart phones projected each behavioral biometric trait's issues and limitations along with their strengths. The study concluded by discussing open research problems in the reviewed area.

A framework for reliability of authentications was proposed by Meng et al., [15] in their study. The study's multimodal biometric proposal for user authentications was found to be appropriate. Their experimental validations of the proposed framework on touch enabled phones showed that by deploying the scheme false rates of single biometric systems reduced drastically. The study also identified challenges and issues in making user touchs the main aspect of future mobile based user authentications.

The study by Abuhamad et al., [1] used DLTs for FBAs. The proposal

called AUToSen used embedded sensors for identifying distinct behaviours of users with and without their smart phone interactions. The study also explored sensed data sufficiency for authenticating users accurately. AUToSen's experimental results showed expected accuracy levels in the readings of gyroscope, accelerometer, and magnetometer sensors.

FBAs using ROIs (Regions of Interests) were used by Hu et al., [10] in their study. Their proposal included eye based detections. The study pre-processed images with ROIs followed by LBPs (Local Binary Patterns) for feature extractions. The extracted features were reduced in terms of dimensionality using PCAs (Principal Component Analysis) and LDAs (Linear Discriminant Analysis) which were classified using minimum distances. The study implemented using Open CV (Open Source Computer Vision) SDKs. The study's experimental results on Android mobile facial samples demonstrated the scheme's effectiveness. The study proposed use of DLTs with XFace system as their future scope.

Tsai et al., [21] used OTPs for authenticating M-banking transactions. The proposal combined OTP with personal biometrics. The procedure followed in the study starts from a client side request to a bank's server for M-banking service. The server then generates and transmits an OTP valid for a specific time period in M-banking systems. The transmitted OTP is verified at the client side before getting registered on the server for M-banking system services. ON registration, the server captures user's personal biometrics like fingerprints or iris image or facial image on the first service request from the registered client. This procedure not only adds strength to the authentication procedure but also prevents fraudulent requests. These biometrics are compared with older copies and if found the process is terminated by the M-banking server. Once the credentials are verified the client and server co-operate for M-banking transactions. The study proved that their proposal was a secure scheme with defined process stages allowing M-banking customers to secure their transactions from hackers and disallowing execution of transactions from stolen mobiles thus preventing client rights and personal information.

Risks in using smart phones were detailed by Alzubaidi and Kalita, [2] in their study. The study projected potential risks for users when their smart phones were stolen or seized while detailing on continuous authentications.

The study also analyzed existing approaches using behavioral biometrics in terms of methodology, datasets and evaluation metrics.

Hierarchical Correlations were used by Xi et al., [24] in their study. The proposed scheme called HCFA (Hierarchical Correlation Based Face Authentication) aimed resource-constrained HHDs including mobiles and PDAs. The HCFA scheme generated partial correlation output peaks from selected facial regions which were then analyzed for relationships between cross correlation output peaks in conjunction with direct cross-correlation approaches. The study experimented their proposed scheme on public databases where their scheme achieved better performances when compared to direct correlation based approaches. Further, HCFA implementations on Nokia S60 CLDC emulator using Java ME to test the scheme's applicability showed it was implementable on most mobiles.

Sensor assisted FBAs were used by Chen et al., [5] in their study with the aim of overcoming FBA shortcomings. Their proposal used motion/light sensors as defence against 2D media and virtual camera attacks without compromising authentication speeds. Their experimental results indicated enhanced levels of security obtained by their scheme while being 10 times quicker in operations (3, 30) when compared to existing 3D FBAs.

## 3. Main focus of the Paper

Mobile based e-commerce, specifically; banking from home (M-banking) has gained popularity. M-banking, a result of growths in technology and communications, have versatile and convenient functions built for HHDs. Trusted M-banking services are also an indispensable part of these applications.

Recent studies have projected the possibilities of using biometric authentications with physiological attributes in HHDs. FBAs can be used in locking HHDs or websites or any equipment with front cameras. Applications The major constraints in using FBAs in HHDs are ease of use and trusted security. Hence, these shortcomings have propelled researchers into the area of enhanced security for HHDs using FBAs.

Hence, this paper focuses on FBAs for HHDs in the case of M-banking applications. A major objective of this work is systematically detail about the

vulnerability of generic biometric authentications in HHDs. This work proposes two step face authentication system (TSFAS) scheme for reliable user authentications on HHDs which are better than single biometric based authentications. The proposed work's framework characterizes and details face based authentication (FBA) elements for reliable authentication mechanisms in HHDs.

## 4. Solutions and Recommendations

This study introduces (TSFAS) scheme for authenticating users on HHDs based on their facial characteristics. This work attempts to solve security concerns identified and reported by previous studies. The proposed TSFAS scheme monitors user videos captured using mobile device camera (MDC). The proposed scheme's observations begin the moment a user unlocks a device and continues to use the device until end of user's session and relocks the device. This proposal is an active authentication system and similar to biometric recognitions which encompass two main stages namely enrolment and recognition stages as depicted in figure 1.

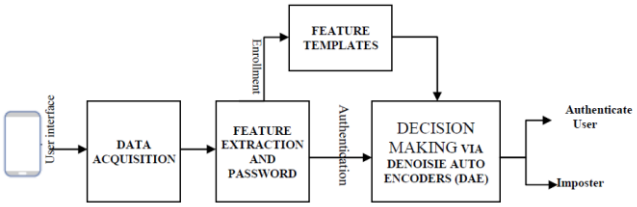


**Figure 1.** Architecture of the Proposed TSFAS Scheme.

During enrolments, the proposed system gathers biometric data for extraction of distinctive features after analyzing them. These features are used to build a feature template similar to classifier training process. Enrolments are followed by recognitions where biometric details of the user are acquired freshly.

These details are compared with previously stored information for verification of the user's identity. The basic procedures followed in this study can be included in active authentications are detailed below:

1. Data acquisition Procedure: This is the preliminary step where user's

raw biometric data is collected using smart phones where the quality of acquisition is significant recognitions and subsequent authentication procedures. MSU-MFSD (Mobile Face Spoofing Database) is a popular dataset which includes genuine and spoofed faces using MCD (Wen et al., 2015). MSU-MFSD dataset includes 280 video clips from 35 users along with photo/video attack attempts. The collection includes captured genuine facial information using two types of cameras: Mac Book Air's built-in camera and Google Nexus 5 Android phone's front camera. Spoofing attack videos were generated during acquisition of genuine facial video captures. Spoofing attacks encompass three types: iPad Air screen sourced high resolution replay video attacks while capturing videos from Mac Book and Nexus devices; iPhone 5S screen based mobile replay video attacks while capturing videos from Mac Book and Nexus devices and printed photo attacks on user facial images while capturing facial images from Mac Book and Nexus devices

2. Feature extraction Procedure: The acquired raw biometric data is pre-processed for extracting distinctive features. The pre-processing part detects and eliminates outliers resulting in an improved quality of data. This is mainly done as data collected includes un-cooperative users in uncontrolled environments. This cleaning of data is followed by identification of discriminative features for extractions. This work extracts relevant features automatically using DAEs.

3. Generation of Feature templates: Feature templates of this work are repository databases generated by concatenating user's (device owner) extracted feature vectors. The templates are built in the enrolment stage and subsequently used in the recognition stage for verifying matches between feature samples and claimed identities.

4. Authentication Procedure: This final procedure is a recognition process where user's extracted features are compared against feature templates. This work generates a matching score to take decisions on user identities. Thus, the proposed procedure identifies original and pseudo users using DAEs.

**Biometric Modes**

Biometric based systems can be operated based on recognition contexts or verifications and identifications.

**Verifications**

Verifications involve 1-1 matches where claimed identities are comparing with stored identities. These matches generate a matching score based on a predefined threshold $t_h \in (0, 1)$. When the score is greater than $th$, the claimed identity is legitimate. When it is lower than $th$, the claimed identity is not accepted as it may belong to an imposter. These authentications based on verifications when treated as binary classifications, the decision rules can be computed using Equation (1):

$$p(us_i) = \begin{cases} \text{authenticata if } p(us_i) > th \\ \text{imposter if } p(us_i) < th \end{cases} \tag{1}$$

Where, $p(us_i)$-user's $(us_i)$ authentication score as computed using DAEs and pre-defined threshold $th$ whose value lies in the interval $[0, 1]$.

**Identifications**

Identifications involve a 1-n relationship in matches where the system recognizes presented face with stored face templates of users. The algorithms used for identifications identity samples based on their matching scores and pre-defined thresholds. The matching scores generated for users is examined for the highest score for selections as shown in Figure 2.

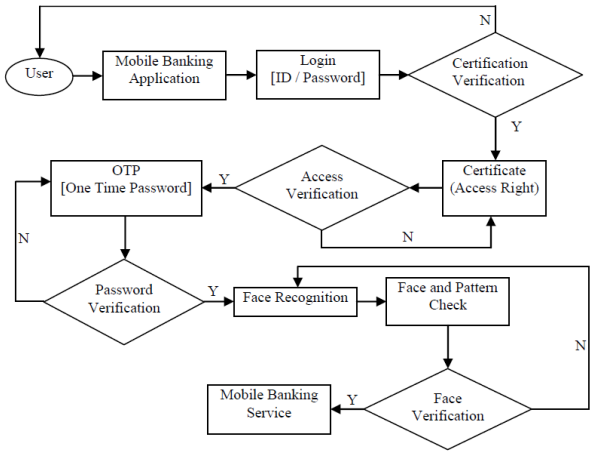


**Figure 2.** Proposed TSFAS Framework in M-Banking Application.

The overall process of authentication through face verification is

implemented as follows: an image of the user is acquired using MDC and when the extracted results correspond to the data saved in a facial recognition DB (database), the user is authenticated. The authentication system operates by image acquisition, feature extraction, face standardization and face verification. Figure 2 depicts the flow of face authentication technology; in the preprocessing, a user registers one's face to the DB; the first step is the extraction of face features via the deep learning model. The recognition part matches the face with the registered data on the DB and the service is executed after the user authenticates by matching (face and PIN/pattern of the user).

Facial matches using DAEs are executed by training the network with AEs (Auto Encoders) where outputs are constrained by equating them to inputs and thus making input and output nodes equivalent (Chen et al., 2014). The weights in layers are adjusted based on the reconstruction errors that get generated between network's inputs and outputs. This results in better learning if features by AEs from inputs. Also, AEs being an unsupervised technique do not need labelling. Though DAEs are based on AEs, they are more robust as they assume inputs have noises making them an ideal technique for learning of noisy images. Moreover, DAEs generalisation capabilities are far superior to AEs generalisation capabilities.

DAEs encompass three layers (Input, Hidden, Output) where the hidden and output layers are encoding and decoding layers. Assuming $I \in R^d$ is a facial image where the data dimension is represented by $d$, and then DAE initially outputs a feature vector $\widetilde{I}$ by assigning certain elements a value of 0 or by introducing Gaussian noises. DAEs use this generated image $\widetilde{I}$ as an input image with where input layer units are $d$ and equal in dimension to the input image. DAE encoding are non-linear transformations using Equation (2),

$$y = f_e(W\widetilde{I} + b) \tag{2}$$

Where, $y \in R^h$ -hidden layer outputs (Feature representations), $h$-hidden layer count, $W$-input-to-hidden weights, $b$-bias, $f$-hidden layer inputs (activation function). This work uses ReLU function (Meng et al., 2014) as the activation function and depicted in Equation (3),

$$f_e(W\widetilde{I} + b) + \max(0, W\widetilde{I} + b) \tag{3}$$

When the value of $(W\widetilde{I} + b) < 0$, then the hidden layer's outputs will also be 0. Hence, ReLU activation produces sparse feature representations of input facial images. Further, ReLUs can train NNs (Neural Networks) faster on voluminous data effectively when compared to other activation functions. Decoding or reconstruction of DAE can be obtained by a mapping function given as Equation (4),

$$z = f_d(W'y + b') \tag{4}$$

Where, $z \in R^d$-DAE output and also reconstructed facial image of original input image. Since, the output layer nodes equal in number to input nodes, $W' = W^T$ is called tied weights. When in the interval between 0 and 1, softplus function is chosen as the decoding function else the image is pre-processed by ZCA (Zero-Phase Component Analysis) whiteners and a linear function decodes values using Equation (5),

$$f_d(a) = \begin{cases} \log(1 + e^a), & I \in [0, 1] \\ \text{a, else} \end{cases} \tag{5}$$

Where $= W'y + b'$. DAEs use reconstruction oriented training to train the network by output authentication of images to reconstruct input face images. Hence, reconstruction errors defined by Equation (6) is used as the objective or cost function. (6),

$$Cost = \begin{cases} -\frac{1}{m}\sum_{i=1}^{m}\sum_{j=1}^{d}[I_j^{(i)}\log(z_j^{(i)}) + (1 - z_j^{(i)})\log(1 - z_j^{(i)})] + \frac{\lambda}{2}\|w\|^2, I \in [0, 1] \\ \frac{1}{m}\sum_{i=1}^{m}\| I^{(i)} - z^{(i)} \|^2 + \frac{\lambda}{2}\|w\|^2, \text{else} \end{cases}$$

Where cross-entropy function is used when the value of input face image is ranged from 0 to 1; the square error function is used otherwise. $I_j^{(i)}$ denotes $j^{\text{th}}$ element of the $i^{\text{th}}$ sample and $\|w\|^2$ is L2-regularization term, which is also called weight decay term. Parameter $\lambda$ controls the regularization term. The MSGD (Minibatch Stochastic Gradient Descent) algorithm (Abuhamad et al., [1]) solves the optimization problem, and $m$ in equation (6) denoting the size of the mini-batch.

## 5. Experimental Results

Experiments with the proposed work's facial authentication system are detailed in this section. The method is assessed for its robustness as well as facial recognition accuracy. Figure 3 depicts real-world accesses and attacks from the MFSD database.

**Figure 3.** MSU-MFSD Database Samples. Images in the Top Row are Attack Images While the Bottom Row Displays True Access Images.

### Evaluation Metrics

This work's proposed TSFAS scheme was tested for its effectiveness using performance metrics detailed below:

(1) FAR (False Acceptance Rates): This metric shows the rate of impostors wrongly classified as genuine users and computed using Equation (7).

$$FAR = \frac{\text{Imposter Samples Accepted}}{\text{Number of imposter samples}} \tag{7}$$

(2) FRR (False Rejection Rates): This is the metric which specifies the ratio between genuine samples that were rejected assuming them as imposters to the total genuine samples and depicted in Equation (8).

$$FRR = \frac{\text{Genuine Samples Rejected}}{\text{Number of Genuine Samples}} \tag{8}$$

(3) TRR (True Rejection Rates): This rate specifies impostors identified and rejected against total imposter samples and computed using Equation (9).

$$TRR = \frac{\text{Imposter Samples Rejected}}{\text{Number of Imposter Samples}} \tag{9}$$

(4) TAR (True Acceptance Rates): This metric is defined as genuine samples exactly identified against the total genuine samples and computed using Equation (10).

$$TAR = \frac{\text{Genuine Samples Accepted}}{\text{Number of Genuine samples}} \tag{10}$$

(5) EER (Equal Error Rates): This is a joined metric with equal FARs and FRRs obtained based on adjusted acceptance threshold value. FARs and FRRs are correlated and one vale increases the other decreases correspondingly. EERs is the error rate at which $FAR = FRR$.

$$EER = \frac{FAR + FRR}{2} \tag{11}$$

**Table 1.** Performance of face authentication using MSU-MFSD Dataset.

| METHODS | TRR (%) | FAR (%) | TAR (%) | FRR (%) | ERR (%) |
|---|---|---|---|---|---|
| 2FA | 75.18 | 30.15 | 77.56 | 27.18 | 28.665 |
| HCFA | 84.25 | 25.41 | 87.71 | 23.67 | 24.541 |
| TSFAS | 92.58 | 18.43 | 93.47 | 15.46 | 16.945 |

Table 1 shows the performance of face authentication using MSU-MFSD dataset. Results show the TRR, FAR, TAR and FRR for each authentication method. Notice that the proposed TSFAS system appears to be superior at identifying spoofed facial images than the 2-factor authentication (2FA) and hierarchical correlation based face authentication (HCFA). Best performing TRRs exceed 92.58%, whereas other methods such as 2FA and HCFA give only 75.18% and 84.25 % respectively.

## 6. Conclusion

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 chapter, a deep learning based automated facial authentication system (Two-Step Face Authentication Scheme (TSFAS)

framework) that employs face authentication to initially perceive the presence of an authorized person, in order to grant the individual access to secure banking environments.

The key benefit of physiologically based biometric authentication is its ability to provide continuity in authentications using FBAs and PINs in M-banking applications where users communicate from their mobiles. The proposed scheme has also been evaluated for its accuracy, robustness for deducing genuine faces on the MSU-MFSD dataset.

## 7. Future research directions

Future analysis will concentrate on improving the system by fixing its existing flaws. First, look into the possibility of using CNNs (Convolutional Neural Networks) and other deep learning classifiers to improve the facial recognition of the proposed scheme.

Examining procedures for addressing facial authentications for partially visible faces. Current methods are implemented for accessing the banking services such as ATM access, internet banking, passport verification, and online exam for reducing the fraudulent and crime activities with a multi-biometrics such as face, finger, and eye.

Conflicts of Interest

There is no conflict of interest among authors

## References

[1] M. Abuhamad, T. Abuhmed, D. Mohaisen and D. Nyang, AUToSen: Deep-learning-based implicit continuous authentication using smart phone sensors, IEEE Internet of Things Journal 7(6) (2020), 5008-5020.

[2] A. Alzubaidi and J. Kalita, Authentication of smart phone users using behavioral biometrics, IEEE Communications Surveys and Tutorials 18(3) (2016), 1998-2026.

[3] A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze and J. M. Smith, Smudge attacks on smart phone touch screens, Woot 10 (2010), 1-7.

[4] A. Chaudhuri, Deep learning models for face recognition: a comparative analysis, In Deep Biometrics (2020), 99-140.

[5] S. Chen, A. Pande and P. Mohapatra, Sensor-assisted facial recognition: an enhanced biometric authentication system for smart phones, Proceedings of the 12th Annual International Conference on Mobile Systems, Applications and Services (2014), 109-122.

[6] Y. Chen, Z. Lin, X. Zhao, G. Wang and Y. Gu, Deep learning-based classification of hyper spectral data, IEEE Journal of Selected topics in applied earth observations and remote sensing 7(6) (2014), 2094-2107.

[7] M. H. Eldefrawy, M. K. Khan, K. Alghathbar, T. H. Kim and H. Elkamchouchi, Mobile one-time passwords: two-factor authentication using mobile phones, Security and Communication Networks 5(5) (2012), 508-516.

[8] M. E. Fathy, V. M. Patel and R. Chellappa, Face-based active authentication on mobile devices, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2015), 1687-1691.

[9] M. Frank, R. Biedert, E. Ma, I. Martinovic and D. Song, Touchalytics: On the applicability of touch screen input as a behavioral biometric for continuous authentication, IEEE Transactions on Information Forensics and Security 8(1) (2012), 136-148.

[10] J. Hu, L. Peng and L. Zheng, XFace, A face recognition system for android mobile phones, IEEE 3rd International Conference on Cyber-Physical Systems, Networks and Applications (2015), 13-18.

[11] H. Kasban, A robust multimodal biometric authentication scheme with voice and face recognition, Arab Journal of Nuclear Sciences and Applications 50(3) (2017), 120-130.

[12] C. S. Koong, T. I. Yang and C. C. Tseng, A user authentication scheme using physiological and behavioral biometrics for multitouch devices, The Scientific World Journal 2014 (781234) (2014), 1-12.

[13] A. Mahfouz, T. M. Mahmoud and A. S. Eldin, A survey on behavioral biometric authentication on smart phones, Journal of Information Security and Applications 37 (2017), 28-37.

[14] M. Mehdipour Ghazi and H. Kemal Ekenel, A comprehensive analysis of deep learning based representation for face recognition, In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (2016), 34-41.

[15] W. Meng, D. S. Wong, S. Furnell and J. Zhou, Surveying the Development of Biometric user Authentication on Mobile Phones, IEEE Communications Surveys and Tutorials 17(3) (2014), 1268-1293.

[16] D. A. Ortiz-Yepes, R. J. Hermann, H. Steinauer and P. Buhler, Bringing strong authentication and transaction security to the realm of mobile devices, IBM Journal of Research and Development 58(1) (2014), 4-1.

[17] P. S. Prasad, R. Pathak, V. K. Gunjan and H. R. Rao, Deep learning based representation for face recognition, In ICCCE 2019 (2020), 419-424.

[18] N. S. Singh, S. Hariharan and M. Gupta, Facial recognition using deep learning, In Advances in Data Sciences, Security and Applications (2020), 375-382.

[19] Z. Sitová, J. Sedenka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, HMOG: New behavioral biometric features for continuous authentication of smart phone users, IEEE Transactions on Information Forensics and Security 11(5) (2015), 877-892.

[20] J. Song, Y. S. Lee, W. Jang, H. Lee and T. Kim, Face recognition authentication scheme for mobile banking system, International Journal of Internet, Broadcasting and Communication 8(2) (2016), 38-42.

[21] C. L. Tsai, C. J. Chen and D. J. Zhuang, Trusted M-banking verification scheme based on a combination of OTP and Biometrics, Jo C., 3(3) (2012), 23-30.

[22] G. Verma, M. Liao, D. Lu, W. He and X. Peng, A novel optical two-factor face authentication scheme, Optics and Lasers in Engineering 123 (2019), 28-36.

[23] D. Wen, H. Han and A. K. Jain, Face spoof detection with image distortion analysis, IEEE Transactions on Information Forensics and Security 10(4) (2015), 746-761.

[24] K. Xi, J. Hu and F. Han, Mobile device access control: an improved correlation based face authentication scheme and its java me application, Concurrency and Computation: Practice and Experience 24(10) (2012), 1066-1085.