International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Sequential Face and Voice Biometric System for Access Control into a Security Safe

Bisiriyu, Akeem Olawale[1], Olawale, Babatunde Olumide[2]

[1]Department of Electrical and Electronic Engineering, Osun State Polytechnic, Iree. Nigeria

[2]Department of Computer Engineering, Osun State Polytechnic, Iree. Nigeria

Abstract: ***The security safe is a place or building where classified document and precious items are kept. To prevent unauthorised persons from gaining access to this safe a lot of technologies had been used. But frequent reports of an unauthorised person gaining access into security safes with the aim of removing document and items from the safes are pointers to the fact that there is still that security gap in the recent technologies used as access control for the security safe. This work is a Sequential Multimodal Biometric System based on deep learning technique that used a pre-trained Alexnet convolutional neural network CNN. The developed system was trained on both face images and voice signals of 50 candidates. The face biometrics of those candidates was first captured by a camera while the user's speech data were also captured by a microphone unit. The captured data were registered and stored in two different databases. The pre-trained deep-learning model CNN was trained in a MATLAB 2020 platform with face and voice data in the database for feature Extraction and recognition. The safe was accessed in a sequential order by the combination of face and voice pattern recognition. A failure-rate of 0.02% was obtained to give access to authorised users while declining unauthorised person access to the security safe.***

Keywords: Access Control, Multimodal Biometrics, Verification, Security Safe.

1. Introduction

Biometrics is the science which establishes the identity of a person through semi-or fully-automated techniques based on person's behavioral and or physical traits. Examples of behavioral traits are voice or signature while physical traits are the iris and the finger print (Alay and Al-Baity, 2020). These traits can be used to access secured safe, places and other highly classified and security-protected areas. Figure1 shows the stages involved in a typical biometric system.

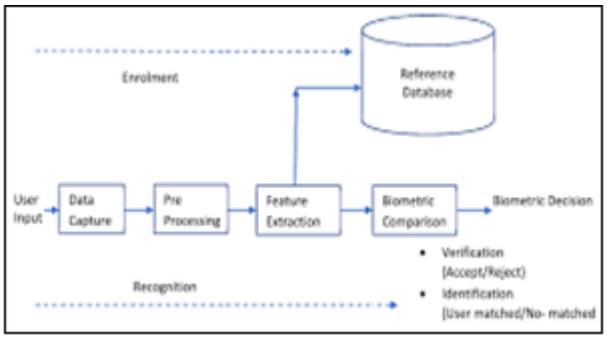


Figure 1: Stages in a Typical Biometric System
Source: (Gayathri *et al., 2020*)

It acquires biometric traits and stores them for the purpose of identifying the user by comparing with a collection of the same traits from multiple users (Obed-Emeribe, 2013). The input given to a system is pre-processed, its feature is extracted and it is stored in the database for identification and verification (Gayathri *et al., 2020*).

The traditional security system uses password or security key for authentication purpose to get access into systems; those password and security key can be easily stolen (Verma and Jain, 2015). While a unimodal biometric system uses a single biometric trait for authentication (Sengar *et al.*, 2020), a Multimodal biometric system combines many biometric traits as sources of authentication and identification (Mahalakshmi *et al.*, 2014). It involves the use of more than one biometrics for securing the system. The biometric data which is obtained from different sensors are combined together by different fusion techniques (Jagadiswarya and Saraswady, 2016).

This work utilized deep learning techniques for face and voice recognition using the inherent feature extraction property of convolution neural network.

2. Review of Relevant Literatures

2.1 Unimodal Biometric System

The study of Sakthi (2019) developed an automatic identification system based on hand vein biometric trait. Hand image of a live body, which includes vein pattern, shade of finger muscles, bones, and tissues, is captured by a web camera through infra-red light transmission. In the result of the experimental tests, the proposed system which was simulated in MATLAB and implemented in embedded hardware-based platform was able to give reduced false acceptance rate and false rejection rate.

Al-Waisy *et al.* (2018) developed a framework that included the local handcrafted feature descriptors and deep-belief network, DBN to address the face recognition problem in unconstrained conditions. When the proposed approaches were evaluated on four large-scale face datasets: the SDUMLA-HMT, FERET, CAS-PEAL-R1, and LFW databases, the results obtained outperform other state-of-the-art of approaches (e. g., LBP, DBN, WPCA).

Lin *et al. (*2020) developed a feature fusion of a dual-input CNN for the application of face biometric for a gender classification system for improved traditional feature fusion method. The experimental results achieved average accuracy

Licensed Under Creative Commons Attribution CC BY

rates of 99.98% and 99.11% on the CIA and MORPH data sets respectively, which is superior to the traditional feature fusion method.

The unimodal biometric system has the shortcomings due to noise, intra class variations, spoof attacks, non-universality etc. It also produces high False Acceptance Rate (FAR) and False Rejection Rate (FRR) and it has limited discrimination capability (Sengar *et al*,.2020).

The multiple biometrics is more exclusive to an individual than a single biometric trait; also the fusion of multiple biometric characteristics effectively reduces the overlap between the feature distributions of dissimilar individuals (Jagadiswarya and Saraswady, 2016).

2.2 Multimodal Biometric System

The work of Chandran (2009) proposed a multimodal system through fusion of face, fingerprint and iris for a multimodal biometric system for identity verification. The system was tested and the overall accuracy of the system was found to be more than 98.5% with FAR and FRR of 1.25% and 0.98% respectively.

The work of Jagadiswarya and Saraswady (2016) proposed an enhanced multimodal authentication system based on feature extraction (using fingerprint, retina and finger vein) and key generation (using RSA). The experimental evaluation showed a significance improvement in the performance of the multimodal biometrics with GAR of 95.3% and FAR of 0.01%.

2.3Deep Learning Approach

In contrast to handcrafted-descriptor techniques, the applications making use of deep learning approaches can generalize well to other new fields (Al-Waisy *et al.*, 2018).

Fingerprint, palm print and finger knuckle-print biometric traits were used in the work of Mahalakshmi *et al.* (2014) as input into neural network algorithm for feature extraction and minutiae point detection. The proposed method achieved excellent recognition rate.

The effect of fusion approaches on recognition performance was tested in the work of Alay and Al-Baity (2020) for human identification system which used the biometrics of iris, face, and finger vein**.** Feature extraction and image classification for each of the three biometrics were carried out by three independent convolutional neural networks (CNNs) models. The performance of the developed system was empirically evaluated with several experiments on the SDUMLA-HMT dataset, which is a multimodal biometrics dataset. The three-biometric trait identification system outperformed other state-of-the-art methods by achieving an accuracy of 99.39%, with a feature level fusion approach and an accuracy of 100% with different methods of score level fusion.

2.3.1 Convolutional CNN Models

The Convolutional Neural Network, CNN algorithm receives an input image, which passes through CNN layers in order to identify its features and extract features from images using kernels or filters, which move over the input image to detect information from the image. Filters locate features through a convolution process that finally produces a feature map as its output. As the image passes through the pooling layer, the complexity of CNN's is reduced. The fully connected layers combine features in a one-dimensional vector and give the classification result using the softmax classifier (Alay and Al-Baity, 2020).

3. Methodology

Figure 2 shows the algorithm of the developed method which is a CNN-based multimodal biometric algorithm with the face and voice signals as the input traits. Firstly, the face images and voice signals of the candidates were enrolled and registered. Then, the user's biometrics, the face images and voice signals were recaptured in sequential order for verification in the database which had been created during the enrolment process in the MATLAB 2020 version platform. The user's face was captured by the camera / sensor while speech was captured by the microphone unit.

Licensed Under Creative Commons Attribution CC BY

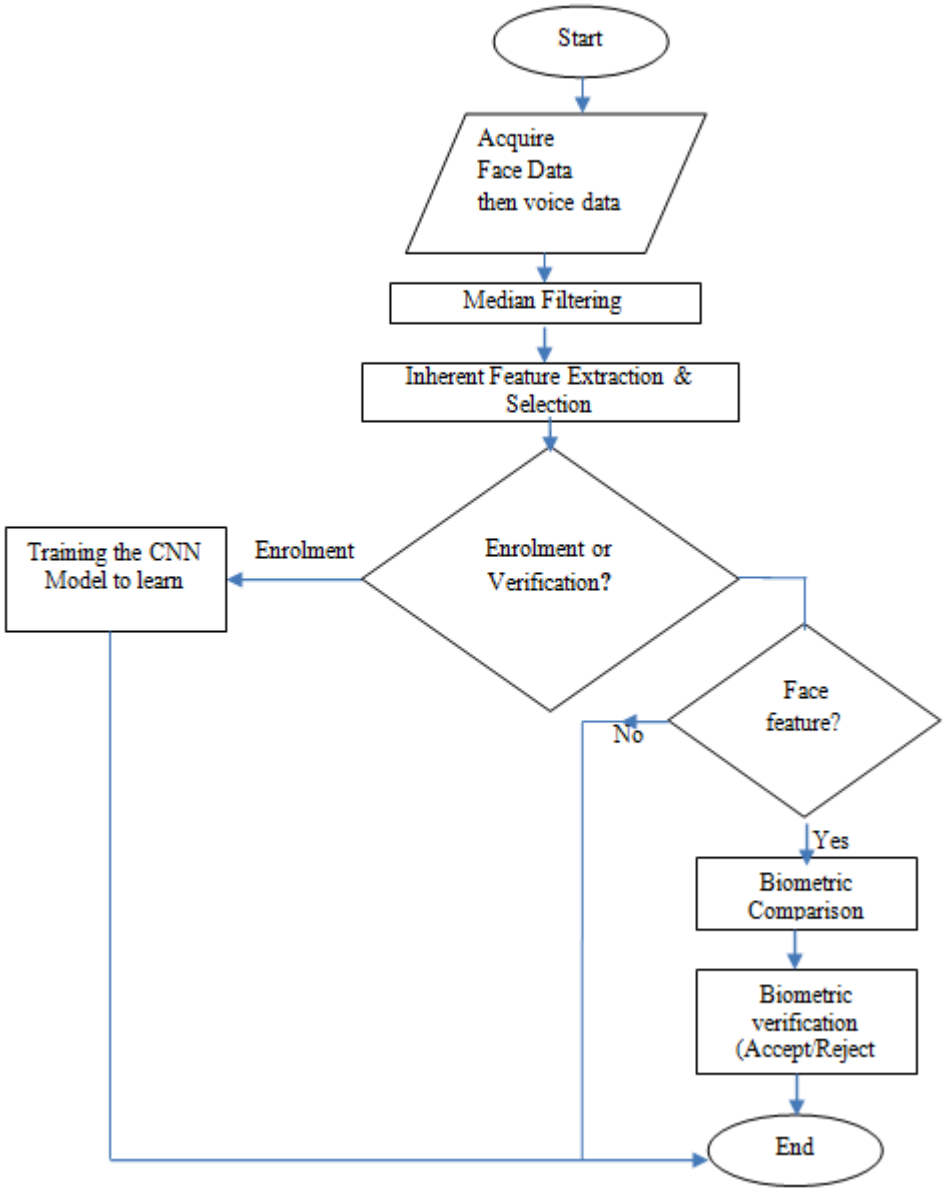
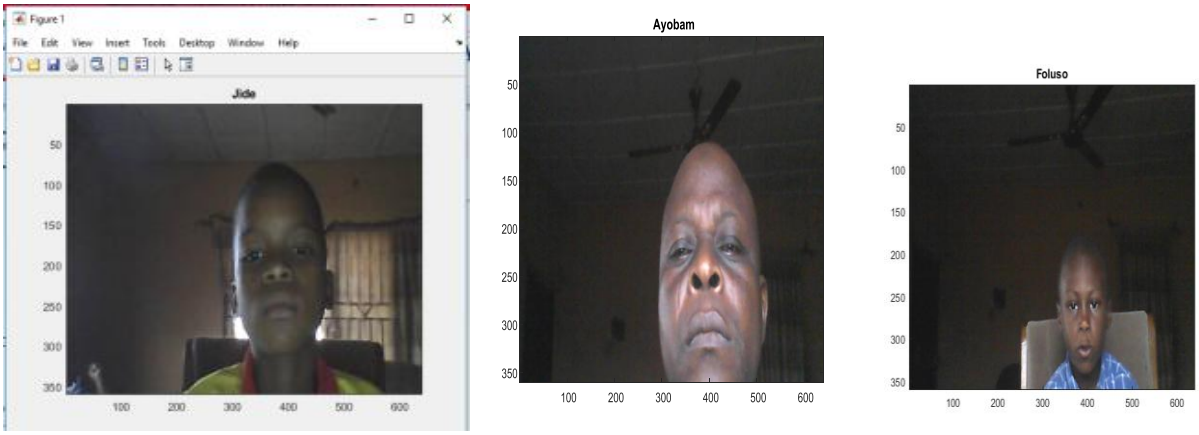


Figure 2: Algorithmic Implementation of the Method

4. Results and Discussion

Figure 3 and figure 4 respectively show the results obtained in the verification process of the face and voice data of the candidates initially enrolled in the developed CNN-based multimodal biometric recognition system. The system was able to verify correctly the users. Only those candidates initially enrolled in the system were authenticated and then given access in to the secured safe but in the sequential order of face biometric input first followed by the user's voice.



Licensed Under Creative Commons Attribution CC BY

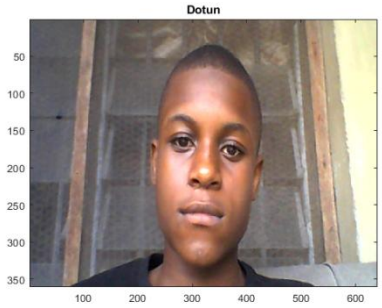
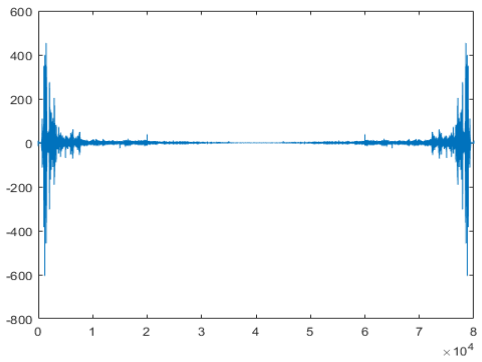
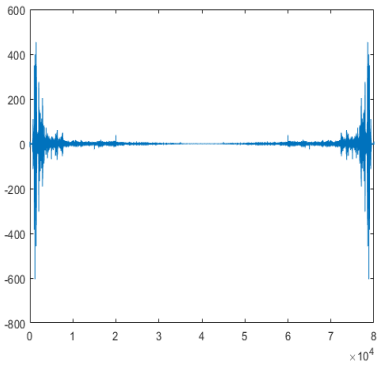


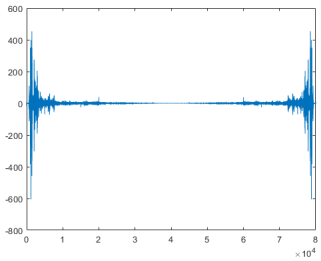
Figure 3: Some of the recognised faces of Candidates



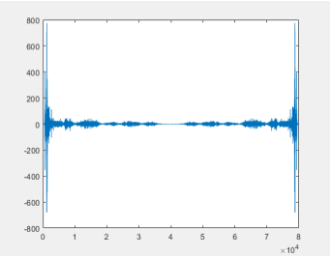
(a) Voice note of Foluso



(b) Voice note of Dotun



(c) Voice note of Jide



(d) Voice note of Ayobami

Figure 4: Some of the recognised voices of Candidates

5. Conclusion

The developed an access control system into a security safe system that based on convolutional neural network which employs multimodal biometric traits of face and voice of intending user to gain access into a safe. The system was implemented using a database created by enrolment and registration of face images and voice data of 50 candidates through the use of a camera and microphone which were respectively attached to the safe. The authentication process involved recapturing of those user's data or sample in order to allow or deny him/her access to the safe. The failure rate of 0.02% was obtained to give access to authorise users while declining unauthorised person access to the security safe.

References

[1] Alay, N. &. Al-Baity, H. H. (2020). Deep Learning Approach for Multimodal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits. Sensors, 20, 5523.

[2] Al-Waisy, A. S., Qahwaji, R., Ipson, S. and Al-Fahdawi, S. (2018). A multimodal deep learning framework using local feature representations for face recognition. *Machine Vision and Applications* 29: 35–54.

[3] Gayathri, M., Malathy, C. &Prabhakaran, M. (2020). A Review on Various Biometric Techniques, Its Features, Methods, Security Issues and Application Areas. Springer Nature Switzerland AG 2020, pp.931–941

[4] Jagadiswarya, D. and Saraswady, D. (2016). Biometric Authentication using Fused Multimodal Biometric. ScienceDirect: International Conference on Computational Modeling and Security (CMS 2016)

[5] Lin, C. J., Lin, C. H. . andJeng, S. y. (2020). Using Feature Fusion and Parameter Optimization of Dual-input Convolutional Neural Network for Face Gender Recognition. Applied Sciences, 10, 3166; doi: 10.3390/app1009316

[6] Mahalakshmi, P., Gunasekaran, K. and Saravanan, D. (2014). Implementation of Multimodal Biometric Authentication using Soft Computing Techniques. NCICCT' 14 Conference Proceedings. *International Journal of Engineering Research & Technology (IJERT)*

[7] Obed-Emeribe, C. (2013). Multimodal Biometric Technology System Framework and E-Commerce in Emerging Markets. International Journal of Advanced

Licensed Under Creative Commons Attribution CC BY

Computer Science and Applications, (IJACSA) 4 (7), Pp: 192-196

[8] Sakthi, P. R. (2019). Automatic Physical Access Control System Based on Biometric Identification by Wavelet Transform Algorithm. International Journal of Recent Technology and Engineering (IJRTE), 7 *(6).*

[9] Sengar, S. S., Hariharan, U. &Rajkumar, K. (2020). Multimodal Biometric Authentication System using Deep Learning Method. International Conference on Emerging Smart Computing and Informatics (ESCI) AISSMS Institute of Information Technology, Pune, India. Mar 12-14.

[10] Verma, I. & Jain S. K. (2015). Biometrics Security System: A Review of Multimodal Biometrics Based Techniques for Generating Crypto-Key. Proceedings of the 9th INDIACom, 2nd International Conference on "Computing for Sustainable Global Development"

Licensed Under Creative Commons Attribution CC BY