

Eye Blink Based Biometric Authentication System

G Umashankar
Department of Biomedical Engineering
GRT Institute of Engineering and
Technology
Tiruttani, India
umashankar.bme@gmail.com

G Hari Krishnan
Department of Electrical and
Electronics Engineering
Sree Vidyanikethan Engineering
College, Mohan Babu University
Tirupati, India
haris_eee@yahoo.com

T. Sudhakar
Department of Biomedical Engineering
Sathyabama Institute of Science &
Technology
Chennai, India
0000-0002-2569-4112

G Mohandass
Department of Biomedical Engineering.
Agni Institute of Technology
Chennai, India
g.mohandass@gmail.com

T Devaraju
Department of Electrical and
Electronics Engineering
Sree Vidyanikethan Engineering
College, Mohan Babu University
Tirupati, India
0000-0002-1502-4334

V Devika
Department of Biomedical Engineering
GRT Institute of Engineering and
Technology
Tiruttani, India
devikavgrt@gmail.com

Shaina Banu S
Department of Biomedical Engineering
GRT Institute of Engineering and
Technology Chennai, India
banushainas@gmail.com

Abstract—Devices are locked and unlocked using biometric security based on eye blinks rather than PINs. On the other hand, using devices in uncontrolled situations makes you extremely vulnerable to spoofing by replay assaults. Stationary facial expression authentication is an instance of a biometric; hackers use the facial images of fictitious individuals to activate devices, leading to unprotected activities and the unintentional disclosure of personal data. In place of static face authentication, we addressed a biometric security system that tracks a person's eye blinking motions as well as their face. The suggested system gets a stream of images as information by instructing the user to follow an eye-blink pattern. The developed scheme then confirms the individual's identity using the proper eye-blink pattern.

Keywords—Biometric authentication, spoofing, eye blink and person's identity

I. INTRODUCTION

Every organization must prioritize security; automatic service access is essential to enhancing security and privacy [1]. Security is the most important aspect of any organization. Biometric recognition's primary objective is to reliably distinguish between individuals and applications using one or more signals produced by physical or behavioral characteristics like fingerprints, faces, iris, voices, hands, or a written signature. Biometric technology has several benefits over conventional security measures [2]. A password or PIN that could be lost or stolen is not required to be remembered, nor is it necessary to carry a key or card with you at all times [3]. However, biometric systems have several disadvantages, including a lack of privacy because it is possible to access facial photographs from social media or be accidentally clicked, and anyone might obtain fingerprints [4].

The proposed research work aims to create a prototype based on a biometric authentication system based on a person's eye blink. As a first stage, it analyzes the possibilities for constructing the authentication system before

it can be designed for an authentication system. There is a lot of spoofing or assault in the field of biometric systems nowadays. To create a prototype biometric authentication system based on a person's eye blink, detect the eye blink with the help of a button change, and then confirm the authentication [5], [6].

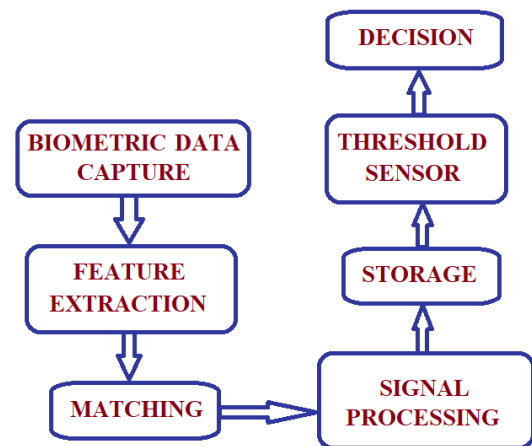


Fig. 1. Architecture of the Generic Biometric System

These days, security is being discussed more and more in a wide range of industries, as well as the technological tools that can be used to combat it: computer access control, e-commerce, banking, and so forth [7] [8]. There are two conventional ways to establish someone's identity. The first approach is based on knowledge. A person's ability to activate a mobile phone is based on their knowledge of personal information, such as a PIN number. The second option is to base ownership on tokens. It might be as straightforward as a badge, a key, or another piece of identification. These two types of identification can be used together to boost security in situations like those involving bank cards [9, 10]. They do, however, each have shortcomings of their own. In the first example, the password

is utilised; however, a third party could guess the password or forget it. In the second situation, the badge (or ID, or key) may be lost or stolen [11] [12].

As shown in Figure 1, the major modules in the generic biometric authentication system are the capture module, which is the biometric system's entrance point and consists of capturing biometric data to extract a digital representation [13] [14]. In order to expedite the verification and recognition stages [15], signal processing modules enable the optimization of processing time and the digital representation collected during the enrollment phase [16] [17]. To determine how comparable the two sets of biometric information are, the matching module compares the information retrieved by the extraction module with the information of the registered models [18], [19]. The judgment module evaluates whether the similarity index returned by the matching module is adequate to identify a specific person [20] [21]. Biometric systems can be used for a wide range of applications. Biometrics can help with security problems in transactions, making everyday life safer and more practical.

Biometric solutions are utilised to satisfy the following domain requirements: Biometric technology and law enforcement have a long history of collaboration, and as a result of this mutually beneficial relationship, some significant achievements in identity management have occurred. The police force's use of biometrics is now truly multimodal. Fingerprint, face, and voice recognition are all important tools for improving public safety and locating the people we're looking for. Biometric technology can be used in a variety of settings, including at the border. Border crossing procedures can be automated with the help of biometric technologies. Passenger screening programmes that are reliable and automated, as well as automated SAS, help government agencies be more efficient while still keeping borders safer than ever. In the sphere of healthcare, biometrics provides an improved model. Medical records are among the most sensitive personal documents, and professionals need to be able to access them quickly and properly. A lack of security and proper accounting can distinguish between a quick and correct diagnosis and health fraud.

II. EXISTING BIOMETRIC AUTHENTICATION SYSTEMS

The main objective behind the facial recognition system is the certainty that every person has a unique face [10]. As we know that every person has a unique fingerprint, similarly, every individual face has unique features. Here we use features of the face of an individual. We can store the features of the faces of many individuals, and they can be identified according to their facial features. Facial testimony and facial recognition are difficult and challenging pieces of work. For facial recognition systems to be authentic, they must work accurately and precisely. The facial recognition technique captured the image using the camera and mapped it for comparison with the images stored in the database. If the captured image matches any of the stored images, it displays face matched; otherwise, it displays face not matched. This paper elaborates in detail on the entire process of a facial recognition system using the OpenCV library. We use the OpenCV library and the Haar cascading algorithm for face detection.

This work provides a feasibility study of faraway interest degree estimation primarily based on eye blink frequency [11]. The proposed blink detection device was entirely based on convolutional neural networks (CNNs). Systems and strategies for spoofing detection in photos are defined herein. A camera can produce a collection of photographs, a primary plurality of photographs within the collection of photographs, including an illustration of a person's frame, and a 2D plurality of photographs within the collection of photographs, including an illustration of the human's surroundings [12].

III. MATERIALS AND METHODOLOGY

The "Internet of Things" (IoT) is the term used to describe the countless numbers of physical devices that are attached to the internet and are actively gathering and modifying data. Thanks to the introduction of reasonably priced laptop chips and the widespread accessibility of wi-fi networks, it is now possible to demonstrate the entirety of the Internet of Things, from a tablet to a jet. Gadgets that would normally be dumb are given a level of virtual intelligence by linking all of those different items and attaching sensors to them, enabling them to bring real-time data 33 without involving a user.

The digital and physical worlds are coming together through the Internet of Things to establish a smarter, more customer satisfaction for us. A sizable open-source library for computer vision, machine learning, and image processing, OpenCV currently plays a crucial role in real-time operations, which may be crucial in cutting-edge systems. In pictures and films, it has the ability to find objects, faces, or even human handwriting. The suggested eye blink biometric system block diagram and software execution steps are shown in Figure 2.

When used in conjunction with certain other modules, like NumPy, Python can systematize the OpenCV array shape for evaluation. In order to find visible styles and their various abilities, we rent vector areas and perform mathematical operations on those capabilities. The original OpenCV model was updated to version 1.0. OpenCV is free for both academic and commercial use because it is released under the BSD license. It provides C++, C, Python, and Java interfaces and supports Windows, Linux, Mac OS, iOS, and Android. The main objective of OpenCV's development was to create real-time programs that were as environmentally friendly as possible.

OpenCV is a terrific device for photograph processing and PC vision. It's an open-supply package deal for duties such as face detection, objection tracking, landmark detection, and more. Python, Java, and C++ are a few of the languages supported. Hundreds of helpful functions and algorithms are included in the library, all of which are freely available to us. Some of these functions are quite broad and can be found in nearly every computer vision application. On the other hand, numerous of the functions are still unknown and have not gotten important attention. OpenCV's most outstanding features, which may be applied in a variety of operations, include the following:

To improve the application of screen unlocking by a human face, an eye-blink approach (see Figure 2) in conjunction with facial recognition is proposed. When a user controls a mobile device, facial recognition authentication is required to complete the user's identity

identification before the user may access the device's system. As shown in Figure 2, face acquisition, face detection, eye detection, eye blink detection, and password authentication are the five blocks that make up the system architecture.

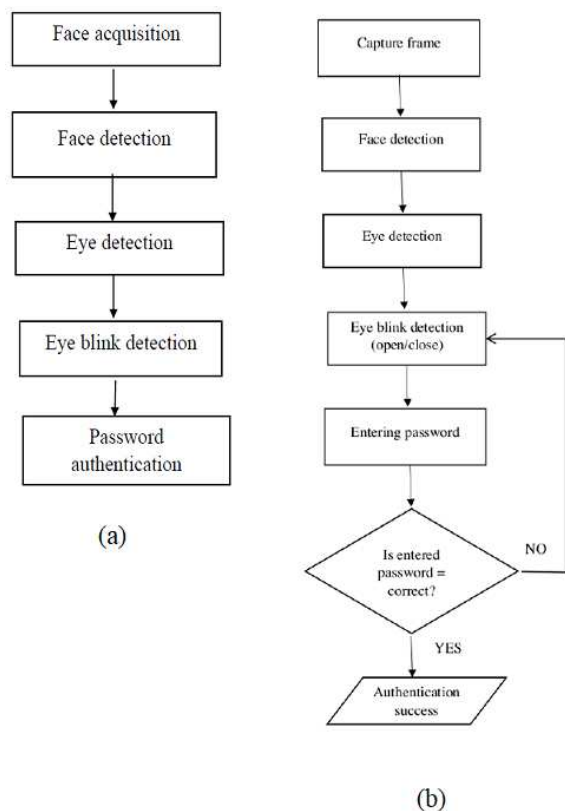


Fig. 2. Proposed eye blink based biometric system (a) block diagram and (b) software flow

Face acquisition: A face image is captured using the graphical user interface of an Open CV, the front-facing camera of a mobile device, or the webcam in a laptop.

Face detection: It detects our faces while we are facing the camera on our laptop, mobile device, or webcam.

Eye detection: The open CV detects the presence of eyes and indicates whether they are closed or open.

Keyboard frame work with the help of an eye blink is done based on the password with the assistance of the GUI. The keyboard has keys from 0 to 9, and the keyboard frame works with the aid of eye blinks based on the password with the help of the GUI.

Password authentication: When a button on the keyboard is changed with the aid of the eye.

IV. RESULTS AND DISCUSSION

The authentication process was experimented with the help of 10 student volunteers, ages 20 to 24. Our proposed study is non-invasive, requiring only a non-contact webcam for authentication. Figure 3 shows Opening the program in an IDLE shell (Python 3.10, 64-bit) and running the program code with the help of the Run module After execution, a GUI tab and button change frame will open in the GUI; users' aliveness is detected, and it also shows the eye detected and eyes open; the next eye blink is detected; and the button

change frame has a sequence of numbers from 0 to 9, which is helpful for entering the password. If the user enters the correct password, it will show authentication success, and finally, the output is authentication success. The password that was entered by the user is (1, 2, 3).

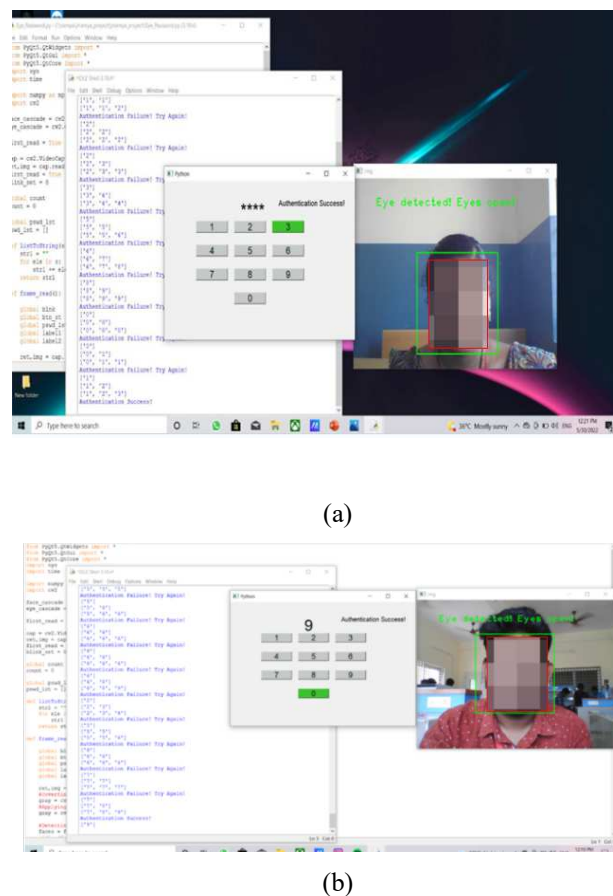


Fig. 3. Real time biometric authentication and password entry for (a) Female volunteer and (b) Male volunteer.

Biometric authentication plays a major role in securing the data. The proposed prototype improves the biometric authentication and verification of humans using eye blinking movements. It runs on a laptop with a webcam. The proposed biometric authentication model has been discussed and implemented. This method is very convenient to use, and there is no need to operate manually. This method is very useful for securing personal data. To provide privacy and data security, we proposed biometric authentication with eye blinking detection. It can also be used by people who are wearing spectacles and sunglasses, but lightning conditions affect the performance of the proposed system.

V. CONCLUSION

People tend to save vital information in their mobile phones due to the popularity of smart phones, such as bank information, photographs, customer data, and subscription information, among other things. When the information is stored on a mobile phone, however, it will require a strong security system to prevent the theft of associated data by others. Face recognition on mobile devices can be easily tricked by using color images of the user. As a result, the eye blink was proposed in this research as a way to improve eye blink detection. Our solution did not require any difficult procedures to verify the user's identification; instead, the user

simply had to blink his or her eyes and enter the proper password to complete the authentication process.

VI. FUTURE WORK

Our proposed work includes developing an automated teller machine (ATM) based on eye blinks. The security system will be improved as a result of this. Another option is to build a person who is paralyzed but is still able to convey their thoughts, ideas, and needs. It will undoubtedly assist paralyzed people in communicating their thoughts through the system's provided language. The objective of this technology is to use an eye movement algorithm to lessen the effort required for disabled people to communicate their thoughts.

REFERENCES

- [1] Albelwi, S., & Mahmood, A. (2017). A framework for designing the architectures of deep convolutional neural networks. *Entropy*, 19(6), 242.
- [2] Jain, A.K., Ross, A., & Pankanti, S. (2006). Biometrics: A toll for information security. *IEEE Transactions on Information Forensics and Security*, 1(2), 125-143.
- [3] Kim, K. W., Hong, H.G., Nam, G.P., & Park, K. R. (2017). A study of deep CNN-based classification of open and closed eyes using a visible light camera sensor. *Sensors*, 17(7), 1-21.
- [4] Komulainen, J., Hadid, A., & Pietikainen, M. (2013). Context based face anti-spoofing. In *IEEE 6th international conference on biometrics: theory, applications and systems* (pp.1-4).
- [5] Maatta, J., Hadid, A., & Pietikainen, M. (2013). Face spoofing detection from single images using micro-texture analysis. In *International joint conference on biometrics (IJCB)* (pp. 1-7).
- [6] Noman, M., Bin, T., Ahad, M., & Rahman, A. (2018). Mobile-based eye-blink detection performance analysis android platform. *Frontiers*, 5,4.
- [7] Vivek Anand, Vimal Singh Parihar, Shubham Kumar Sharma, Vikas Singhal and Pramod Kumar Sethy, (2021) "Facial recognition system using opencv", *International Journal of Creative Research Thoughts*, 2320-2882.
- [8] Roberto Daza, Aythami Morales, Julian Fierrez, Ruben Tolosane (2021) "Feasibility study of attention level estimation via blink detection applied to e-Learning", *AAAI Workshop on Artificial Intelligence for Education (AI4EDU)*, 2021.
- [9] Scott Pfursich, David L. Graumann, Rahul Deva Ghosh, Ansuya Negi, Ranjit S Narjala (2018) "Facial liveness detection in image biometrics" Patent.
- [10] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). An analysis of minutiae matching strength. *Audio and Video-Based Biometric Person Authentication (AVBPA)*, 2091, 223-228.
- [11] Rogmann, N., & Lee, M.K. (2015). Liveness detection in biometrics. In *International conference of the biometrics special interest group (BIOSIG)* (pp. 1-14).
- [12] Singh, S., & Prasad, S. V. A. V. (2018). Techniques and challenges of face recognition: A critical review. *Procedia Computer Science*, 143, 536-543.
- [13] Tang, D., Zhou, Z., Zhang, K. (2018). Face Flashing: A secure liveness detection protocol based on light reflections. In *Network and distributed systems security (NDSS) symposium*.
- [14] V. Anand, G. Krishna, G. Mohandass, R. Hemalatha, and S. Sundaram (2010) Predicting grade of prostate cancer using image analysis software, *Trends in Inform. Sciences and Computing (TISC)*. IEEE, pp 122-124.
- [15] Mohandass, G., Ananda Natarajan, R., Hari Krishnan, G. Comparative analysis of optical coherence tomography retinal image using multidimensional and cluster methods. *Biomedical Research (India)*, 26(2), pp.273-285 (2015).
- [16] Nagarjuna Reddy, A., Hari Krishnan, G., Raghuram, D., "Real time patient health monitoring using raspberry PI, *Research Journal of Pharmaceutical, Biological and Chemical Sciences*, 7(6), pp.570-575 (2016).
- [17] Ganesan, U., Paul, N.E.E., Krishnan, G.H., Aarthi, S., Swamy, I. K., "Detecting Diabetes Mellitus from Tongue Image Hybrid Features and Neural Network Classifier", *Proceedings of 4th International Conference on Cybernetics, Cognition and Machine Learning Applications, ICCCMIA2022*, 2022, pp.425-427.
- [18] Sudhakar, T., Hari Krishnan, G., Prem Kumar, J., ...Devanesan, P.S., Shalini, S., "Inducement of Artificial Sleep using Low Strength Magnetic Waves", *Journal of Physics: Conference Series*, 2022, 2318(1), 012028.
- [19] Sudhakar, T., Hari Krishnan, G., Krishnamoorthy, N.R., ...Pradeepa, M., Raghavi, J.P., "Sleep Disorder Diagnosis using EEG based Deep Learning Techniques", *Proceedings of 2021 IEEE 7th International Conference on Bio Signals, Images and Instrumentation, ICBSII 2021*, 2021, 9445158
- [20] Santhosh S, Juliet V, Krishnan G. H. Impact of Electrodes Separation Distance on Bio-Impedance Diagnosis. *Biomed Pharmacol J* 2021;14(1).
- [21] Santhosh, S., Juliet, A.V., Krishnan, G.H., "Predictive analysis of identification and disease condition monitoring using bioimpedance data", *Journal of Ambient Intelligence and Humanized Computing*, 2021, 12(2), pp. 2955-2963.