Research Article

Advances in Machine Learning & Artificial Intelligence

Proposed Enhanced Security on Face Recognition Technology for Mobile Devices

Uwizeyimana Abdulkarim[1], Kareangabo Gabriel[1*], Umurerwa Marie Adeline[1], Semuranzi Damascene[1], Kavamahanga Lambert[1] and Dr. Dagmawi Lemma[2]

[1]*Msc. IoT-Wireless Intelligent Sensor Networking, African Centre of Excellence in Internet of Things*

[2]*Department of Computer Science University of Addis Ababa*

[*]Corresponding author
Kareangabo Gabriel, Msc. IoT-Wireless Intelligent Sensor Networking, African Centre of Excellence in Internet of Things

Submitted: 03 Jan 2022; **Accepted**: 12 Jan 2022; **Published**: 27 Jan 2022

Citation: *Uwizeyimana Abdulkarim, Kareangabo Gabriel, Umurerwa Marie Adeline, Semuranzi Damascene, Kavamahanga Lambert and Dr. Dagmawi Lemma (2022) Proposed Enhanced Security on Face Recognition Technology for Mobile Devices. Adv Mach Lear Art Inte, 3(1): 12-16.*

Abstract

Although Face Recognition has many advantages over traditional technology (fingerprint, keystroke, Passwords, Pins, Patterns and voice) like feature used for protection and reduction risks of accessing other's information without permission and provide fast and easy accessibility of the information stored in the device for authorized user. However, some of the systems can be fooled with a picture or video of a user's face that can be unlocked by someone that looks similar to you (such as a twin), other point if the mobile phone user was kidnapped and be forced to unlock his /her device for Froude use. As mentioned above issues, they are still having a leakage about the security of information stored in the device according to their working algorithm. In this paper, we are proposing a way to enhance the security on face recognition for mobile devices by connecting the mobile device to the other wearable device in order to increase security on face recognition to the mentioned issues and ensure that the information is more secured.

Keywords: Face recognition, Enhanced security, Mobile Devices.

Introduction

In today's networked world, A portable device is the latest Mobile technology which is available in all over the world and mostly used than computers. People have saved their private personal information on their mobiles as they believe, they are secured. As most of us are working from home or teleworking due to coronavirus pandemic break out. Mobile devices are being used to check bank account, or reply some emails than using our very secure offices. Most of the current phones have security for Authentication to verify that users or systems are who they claim to be, based on identity (e.g., username) and credentials (e.g., password). Mobile devices are easily lost or stolen; moreover, Password could be easily hacked or detected [1].

For that purpose, high level of authentication for mobile devices is needed. Passwords and PINs have been used for strong protection in mobile devices; after deep analysis and discovery of the weaknesses the protection developed algorithm presented, face recognition has been introduced where users/customers would not have to use passwords and PINs only but would also use the image of their face and Iris for Strong protection. The face recognition development algorithm presents four aspects such are: face detection, normalization, feature extraction and face recognition [1]. However, this strong protection remains with some issues. Using face recognition in mobile devices such as smartphones, tablets, laptop computers, smart watches and e-readers in businesses present security threats. Either the device owner can be harmed when intelligence force him/her to unlock some his/her device information extraction. These risks posed by this security can frighten some people and fear to use it in business Therefore, the enhanced security on face recognition for mobile devices is needed.

Problem Statement

Although a number of security experts say that facial recognition can make consumers safer, some of the systems can be fooled with a picture or video of a user's face.

Someone that looks similar to you (such as a twin) can unlock your phone. This makes Face recognition less secure than Pattern, PIN, Iris, or Fingerprint [2]. And the technology can't be used to authorize payment through mobile phone Pay; In addition to that the use of biometrics relinquishing control of a piece of information that could be used to identify you forever as they have little recourse, this needs more attention before using it. The proposed enhanced security for face recognition in mobile devices will be the use of

complex technology where by a wearable device like smart watch that will monitor the heart beat and blood pressure of the smart phone user authenticated with face recognition technology. This means that without the smartwatch the face recognition will no longer work.

Objectives

- To enhance security of mobile devices on face recognition by combining biometric with face recognition system in order to prevent data theft stored in the device by preventing an authorized access to the device.
- Protection of user's data
- Provide user mood status for fast rescue
- Increase the number of the users of smart phones because of the protection of the data
- The proposed solution is likely to be implemented to the edge not via the cloud. Change the way user will be accessed.

Related Work

With a rapid rise of Internet of Things, the personal and institutional data security and privacy challenges increasingly appealed for more researches, which lead to biometric methods and technologies among other methods. That is how facial recognition approach; one of the biometric technologies; started being developed to tackle the very challenging problem of systems' security and individuals' privacy.

Hung Lin (2000), examine Biometric access control which are automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristics, such as fingerprints or facial features, or some aspects of the person's behavior, like his/her handwriting style or keystroke patterns. Hung Lin believes that, it was difficult to forge, since biometric systems identify a person by biological characteristics, though some other researchers found that there was more leakage [3].

In 2010, Bayan Ali Saad Al-Ghamdi et al., proposed a system to recognize a human face by Face Recognition System using 3D [4]. The use of 3D technology will provide to the system with high accuracy by making a proper alignment to determine the head exact position.

Cammozzo Alberto (2011), in his research explained that biometric signatures extracted from the unknown face exemplar(s) and the biometric signature(s) stored during the enrollment stage as reference template(s) are similar [5].

In 2012, Cahit Gurel and Abdulkadir Erden, presented a "Design of Face Recognition System" which used a combination knowledge-based method for face detection, on one side, and the other side, the neural network approach for face recognition [6]. This combination allows the smooth applicability and reliability.

As far back as 2015, M.H Maras state that these new devices linking property, people, plants, and animals to the Internet are vulnerable to hackers. Research continues by explaining, a hacker can gain unauthorized access to IoT devices due to their set-up; that is, because these devices are connected, Internet-enabled, and lack the necessary protective measures.

Maras continue by saying, because of these vulnerabilities, personal information collected by IoT devices could be misused. Particularly, if a device collects and stores, personal, medical and/or financial data, a hacker could steal this information to facilitate identity theft (IoT_Security- privacy) [7].

In 2017, Narayan T. Deshpande et al., proposed a facial recognition system combining Viola-Jones algorithm (for face detection), fusion of principal component analysis (PCA) approach (for face recognition) and artificial neural network (ANN) method (for system accuracy) whereby an efficient and accurate image detection and person identification using standard image database [8]. In 2017, Apple released a new handset iPhone X equipped with an innovative and secure new way for customer to unlock, authenticate and pay using Face ID taking advantage of TrueDepth camera characteristics [9].

In 2020, Bendjillali Ridha Ilyas et al., in "Enhanced Facial Recognition System Based on Deep CNN"; have proposed a system to obtain a powerful recognition algorithm with high recognition rate using Viola-Jones algorithm [10].

With the Viola-Jones algorithm, the system allows efficient detection of various parts of the human face such as nose, eyes, mouth, lips, nostrils, ears, etc. Liu (2020), examines other special way to increases facial recognition, The authors present the compact and low-cost fluorescence detector which is capable of quantifying the amplicons of the loop-mediated isothermal amplification (LAMP) reaction in real-time.

Moreover, the results show that the paper-based sensor can detect multiple genes of the genomic DNA extracted from Escherichia coli and Campylobacter jejuni, with the concentration as low as 2 × 103 copies/μL.

As a diagnosis tool, the sensor has the potential to measure multiple target genes simultaneously. This approach may not be suitable for all organizations but can be used to develop alternative strategies [11].

Face Recognition Working Principle

The facial recognition process normally has four interrelated phases or steps, which are

I. Face detection,
II. Normalization,
III. Feature extraction, and
IV. Face recognition [1].

These steps depend on each other and often use similar techniques

as shown in Figure 1. They may also be described as separate components of a typical FRS. Detecting a face in a probe image may be a relatively simple task for humans, but it is not so for a computer. The computer has to decide which pixels in the image is part of the face and which are not. Once the face has been detected (separated from its background), the face needs to be normalized. This means that the image must be standardized in terms of size, pose, illumination, etc., relative to the images in the gallery or reference database.

After the face image has been normalized, the feature extraction and recognition of the face can take place. In feature extraction, a mathematical representation called a biometric template or biometric reference is generated, which is stored in the database and will form the basis of any recognition task.

Facial recognition algorithms differ in the way they translate or transform a face image (represented at this point as grayscale pixels) into a simplified mathematical representation (the features) in order to perform the recognition task.

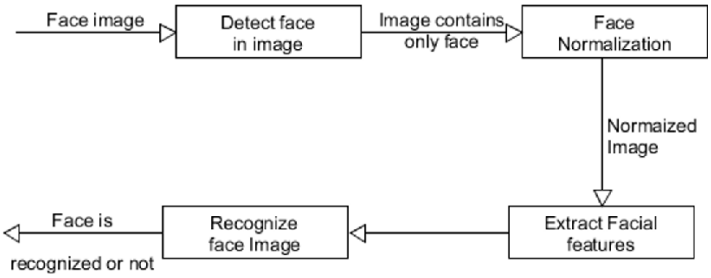

Figure 1: Face recognition basic steps

Proposed System

A blockchain is a distributed ledger technology that protects a digital transaction through complex mathematical algorithms [12].

Block chain applications go far beyond cryptocurrency and bitcoin. With its ability to create more transparency and fairness while also saving businesses time and money, the technology is impacting a variety of sectors in ways that range from how contracts are enforced to making government work more efficiently it has even gone far to be used as personal identity security protection [13].

Identity is integral to a functioning society and economy [12]. Having a proper way to identify ourselves and our possessions enables us to create thriving societies and global markets. At its most basic level, identity is a collection of claims about a person, place or thing.

For people, this usually consists of first and last name, date of birth, nationality, and some form of a national identifier such as passport number, social security number (SSN), driving license, etc. These data points are issued by centralized entities (governments) and are stored in centralized databases (central government servers).

However decentralized storage is one of the core components of secure identity data management. In a decentralized framework, credentials are usually stored directly on the user's device (e.g., smartphone, laptop) or securely held by private identity stores.

Decentralized storage solutions, which are tamper-proof by design, reduce an entity's ability to gain unauthorized data access in order to exploit or monetize an individual's confidential information.

When solely under the control of the user, identities are considered self-sovereign. This, in turn, means the user can both fully control access to the data without having to worry about access being revoked. Data under the user's control makes the information more interoperable, allowing the user to employ data on multiple platforms, use the information for different purposes, and protect the user from being locked into one platform.

A key element of securing decentralized identities is cryptography. In cryptography, private keys are known only to the owner, while public keys are disseminated widely. This pairing accomplishes two functions. The first is authentication, where the public key verifies that a holder of the paired private key sent the message. The second is encryption, where only the paired private key holder can decrypt the message encrypted with the public key.

In order to get to the cryptography stage, in our system we have thought about adding the correction of real time data from the user smartphone and smart watch which will be facial recognition and current heart beat rate ratio in order to user information.

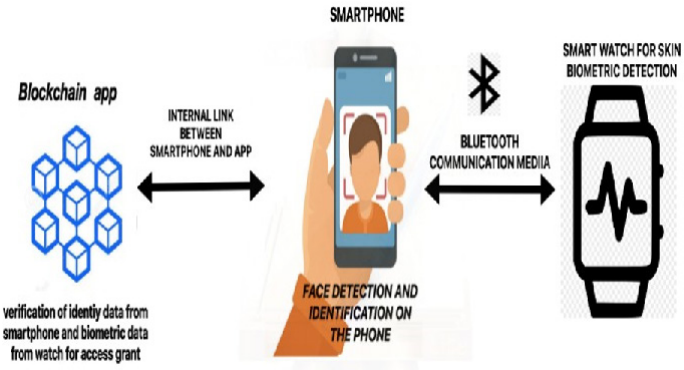

Figure 2: Proposed system block diagram

Devices To Be Used

Smart Watch

A smartwatch is a wearable computer in the form of a watch; modern smartwatches provide a local touchscreen interface for daily use, while an associated smartphone app provides for management and telemetry. In our project, we suggest to incorporate ECG and GSR sensors in smartwatch for heat beat rate and sweat gland detection [14].

GSR Sensor

GSR represents galvanic skin reaction, is a technique for estimating

the electrical conductance of the skin. It estimates changes in sweat organ action on the skin as a sign of physiological or mental excitement, utilizing changes in skin conductivity. During stress, opposition of skin drops because of expanded emission in perspiring organs [15].

Figure 3: GSR Sensor

ECG

Electrocardiogram (ECG) signal can be utilized so as to identify whether the individual is Stressed Electrocardiography is a technique utilized in estimating the electrical movement of the heart. The ECG records the electrical movement that outcomes when the heart muscle cells in the atria and ventricles contract. Figure 4 is the ECG hardware that is commonly utilized for pulse observing [16].

Figure 4: ECG

Smart Phone

A mobile phone is a wireless handheld device that allows users to make and receive calls. While the earliest generation of mobile phones could only make and receive calls, today's mobile phones do a lot more, accommodating web browsers, games, cameras, video players and navigational systems.

Future Work

In this paper, the access control to mobile devices for enhanced security facial recognition has been reviewed, whereby data and/or information security; hence user's privacy; can be improved. The combination of face recognition algorithm and data collected by wearable sensors (like watches) from user's body with instant behavior in accordance with his/her current situation to better control access in mobile device. However, considering the role of electronic mobile devices in nowadays critical activities like bank transactions and online payments.

We recommend further research in the future on blockchain system where by the system's blockchain would help to protect privacy of mobile devices users.

Conclusion

Face recognition is a both challenging and important technique that significantly improves security and privacy. However, the method itself needs additional techniques to enhance security for systems using it more especially mobile devices.

The present paper, security and privacy challenges have been discussed and solution to tackle them is proposed to prevent unauthorized access to the device when the owner is not in his/her full intellectual capacity like in kidnapping situation in which case kidnaped users are stressed which generally causes blood pressure to go high and increases heart beat rate.

References

1. H Soliman, A Saleh, E Fathi (2013) "Face Recognition in Mobile Devices," Int. J. Comput. Appl., vol. 73: 13-20.
2. Thomas Germain (2017) "Why Facial Recognition Could Be the Best Way to Unlock Your Next Phone," consumerreports, 2017. https://www.consumerreports.org/smartpho nes/why-facial-recognition-could-be-the- best-way-to-unlock-your-next-phone/.
3. S. Lin (1997) "An Introduction to Face Recognition Technology," 1995: 1-7, 1997.
4. B A S. Al-ghamdi, S R Allaam, S Soomro (2010) "Recognition of Human Face by Face Recognition System using 3D," Inf. Commun. Technol. 4: 27-34.
5. A Cammozzo (2011) "Face Recognition and Privacy enhancing techniques 1 Alberto Cammozzo," no. September 2011: 14-16.
6. A Gurel, C Erden (2012) "Design of a Face Recognition System," 15th Int. Conf. Mach. Des. Prod. 1: 1-12. https://www.researchgate.net/publication/2 62875649_Design_of_a_Face_Recognition_System.
7. M H Maras (2015) "Internet of things: Security and privacy implications," Int. Data Priv. Law 5: 99-104,
8. N T Deshpande, S Ravishankar (2016) "Face Detection and Recognition using Viola- Jones algorithm and

fusion of LDA and ANN," IOSR J. Comput. Eng 18: 1-6.ˆ https://pdfs.semanticscholar.org/c5cf/c1f5a430ad9c103b381d016adb4cba20ce4e.pdf.
9. Apple (2017) "Face ID Security. https://www.apple.com/ca/business- docs/FaceID_Security_Guide.pdf.
10. R I Bendjillali, M Beladgham, K Merit, A Taleb-Ahmed (2019) "Improved facial expression recognition based on DWT feature for deep CNN," Electron 8: 2019.
11. Mingdian Liu, Yuxin Zhao, Hosein Monshat, Zheyuan Tang Zuowei Wu, et al (2020) "An IoT-enabled paper sensor platform for real-time analysis of isothermal nucleic acid amplification tests," Biosens. Bioelectron 169: 112651.
12. G Coppi, L Fast (2019) Blockchain and distributed ledger technologies in the humanitarian sector," Humanit. Policy Gr 46: 2019. https://www.odi.org/sites/odi.org.uk/files/re source-documents/12605.pdf.
13. Xin Guo, Muhammad Arslan Khalid, Ivo Domingos, Anna Lito Michala, Moses Adriko (2021) "Smartphone-based DNA diagnostics for malaria detection using deep learning for local decision support and blockchain technology for security," Nat. Electron. 4: 615–624.
14. G Spandan, T Ahmed, S M Rajesh (2020) "IoT Application: Human Emotions Management System," Int. J. Recent Technol. Eng. 9: 1261-1265.
15. G Giannakakis, D Grigoriadis, M Tsiknakis (2015) "Giannakakis- et.al.2015_StressAnxietyEEG."
16. T Stamkopoulos, K Diamantaras, N Maglaveras, M Strintzis (1998) "ECG analysis using nonlinear PCA neural networks for ischemia detection," IEEE Trans. Signal Process 46: 3030-3044.

Copyright: *©2022 Kareangabo Gabriel, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.*