Array 8 (2020) 100042

Contents lists available at ScienceDirect

Array

journal homepage: www.elsevier.com/journals/array/2590-0056/open-access-journal

An Investigation of Biometric Authentication in the Healthcare Environment

Janelle Mason [a], Rushit Dave [b,*], Prosenjit Chatterjee [c,*], Ieschecia Graham-Allen [a], Albert Esterline [a], Kaushik Roy [a,*]

[a] Department of Computer Science, North Carolina A&T State University, 1601 East Market Street, Greensboro, NC, 27411, USA
[b] Department of Computer Science, University of Wisconsin-Eau Claire, 101 Roosevelt Avenue, Eau Claire, WI, 54701, USA
[c] Department of Cyber and Computer Sciences, The Citadel Military College of South Carolina, 171 Moultrie Street, Charleston, SC, 29409, USA

ARTICLE INFO

Keywords:
Biometric authentication
Deep learning
Healthcare
Periocular biometrics

ABSTRACT

A vast amount of growth has taken place in the field of biometrics and in the healthcare industry. Biometrics provides the ability to identify individuals based on their physical and behavioral characteristics. The fusion of biometrics and information systems in the healthcare environment has provided a new approach to determine the identity of patients. In this paper, we investigate the biometric system and the authentication process using periocular biometrics specifically. We integrate this approach with the healthcare system to provide an advanced method to identify the patients securely. We propose a new technique that fuses the use of periocular biometrics and the electronic master patient index in healthcare information systems to identify humans in the healthcare environment. A comparative analysis of different periocular biometric recognition methods is conducted and assessed against various traditional and deep learning-based methods in our research study.

1. Introduction

Over the past decade, biometrics has evolved into an extremely popular field of study. A vast amount of interest and extensive research has led to the development of biometric data as a result. Biometrics, in the simplest definition, is the measurement of a human being using the physical and behavioral characteristics. It enables a human to be identified and authenticated through a set of recognizable and verifiable biometric data [1], such as face, fingerprint, iris, and voice data (which are classified as physiological characteristics [2]). These biometric identifiers are the distinctive, measurable characteristics that are used to label and describe individuals [3]. Behavioral biometrics are used to identify humans through their unique interactions with technology and devices. In the early stage, biometric applications, and devices appear to be consuming the entire world [4]. The global biometric market is expected to grow from 10.60 billion USD in 2016 to an estimated 41.39 billion USD by 2025, a 17.06% compound annual growth rate from 2017 to 2025 [4].

People go to hospitals and clinics, where various forms of physical identification are provided to a medical professional to determine the identity of the individual seeking medical attention. In emergency situations, where the individual is unconscious or unresponsive and without any form of identification, the medical professional will identify the person as Jane Doe or John Doe until their identity is established. In this situation, having a biometric system that can identify an individual based on the periocular region of their face would enable medical practitioners to identify the unconscious individual more rapidly. In smartphone technology, additional sensors and security features have been incorporated in the device to effectively authenticate an individual. This allows the individual to have access to their smartphone without a password or personal identification number (PIN).

In this research, we investigate the use of biometrics, in particular periocular biometrics, in conjunction with healthcare information systems. (The periocular region is the facial region in close proximity to the eyes [5].) We begin our research study by providing an overview of biometric systems. Next, periocular biometrics is explored to give more detailed information concerning biometrics. A deeper analysis is provided concerning how modules operate in the biometric system, with explanations of the enrollment, identification, and verification processes. The periocular region would be a suitable biometric for smartphones to use to authenticate individuals also. The periocular biometric indicates that it is not a biometric that is easily impersonated. Afterwards, we

* Corresponding author.
** Corresponding authors.
E-mail addresses: jcmason@aggies.ncat.edu (J. Mason), daver@uwec.edu (R. Dave), chatterjee.prosenjit@citadel.edu (P. Chatterjee), iallen@ncat.edu (I. Graham-Allen), esterlin@ncat.edu (A. Esterline), kroy@ncat.edu (K. Roy).

https://doi.org/10.1016/j.array.2020.100042
Received 16 May 2020; Received in revised form 3 August 2020; Accepted 3 September 2020
Available online 11 September 2020

provide an overview of how the healthcare information system is structured and explain how patients interact with the healthcare system.

After assessing biometric and healthcare systems, this research illustrates how a biometric system will capture the periocular biometrics of a patient in the healthcare environment. The biometric information will then be enrolled in the patient biometrics identification system. This information will then be connected and associated with the patient's enterprise master patient index (EMPI), which is a unique identifier used in the healthcare information system to identify every patient. As patients seek additional medical treatment, the biometric systems will be used to identify them and present their medical history, insurance information, and any other relevant information. To the authors' knowledge, there is no technology in existence providing this capability to patients in the healthcare system.

The remainder of this paper is organized as follows. In the next section, an overview of a biometric system is presented, and an analysis of periocular biometrics is given indicating the advantages for this type of biometrics. Section 3 discusses biometric system functionality pertaining to the system modes and modules. It also includes the biometric system performance in terms of True Positive Rate (TPR), False Positive Rate (FPR), False Acceptance Rate (FAR) and False Rejection Rate (FRR). The overview of the healthcare system is discussed in Section 4. This section also gives the explanation of the master plan index (MPI) and the EMPI as they relate to the Health Information Management System (HIMS). Information pertaining to the patient arrival and registration process is assessed, and the functionality of HIMS is presented in Section 4 also. Section 5 presents the literature review which provides information about biometrics, healthcare systems, and security concerns. Section 6 explores our proposed approach for the healthcare system with the integration of biometrics. Lastly, Section 7 concludes with the summarization of our research and provides insights for our future work.

2. Biometric Systems

Seven factors have been identified for assessing the suitability of any trait/characteristic for biometric authentication. Four of the factors are related to the human physiological characteristics and the remaining three are for constructing a biometric system based on human characteristics. The factors include universality, uniqueness, permanence, measurability, performance, acceptability, and circumvention [6]. Jain et al. explains these characteristics as follows [6]:

- Universality indicates that every person possesses the characteristic.
- Uniqueness means that the characteristic should be sufficiently different to distinguish one individual from the other.
- Permanence implies that the characteristic is not varying over time.
- Measurability (or collectability) is the measurement of the trait/characteristic should be able to be measured easily.
- Performance relates to the accuracy of the system based on operational requirements.
- Acceptability indicates the comfort individuals will have using their biometric characteristics that are captured and assessed by the system.
- Circumvention relates to the ease with which a characteristic might be imitated using fraudulent means.

We assess periocular biometrics for identification in this research. The authors are aware of the integration of biometric features in smartphone technology as they are used to assist with the identification of an individual. In the next section, an overview of periocular biometrics is introduced.

2.1. Periocular Biometrics

Periocular biometrics is one of the most distinctive subsets of biometric information of an individual and it can be used to assist with building a robust biometric authentication system. This form of biometric authentication system is good for desktop/laptop computers, smartphones, and tablets as these devices are less affected by PINs, or screen lock patterns for authentication purposes, swipe screen, password, and fingerprint. The periocular region includes the eyes, eyelids, eyelashes, eyebrows, irises, and tear ducts. The important aspect of the inclusion of the periocular region in a biometric authentication system is that this region of the human face remains almost unchanged with aging, typically. Also, human irises are unique to each individual, and the iris of the left eye is different from the right eye of any individual. Therefore, mimicking the iris is quite impossible for the imposter attempting to attack the biometric-based authentication system. Some other advantages of using periocular biometric information includes that it may lack information on the iris (as sometimes prominent iris features cannot be captured due to an uncontrolled environment) or other parts of the region under consideration and still provide the highest accurate classification during biometric authentication. As the periocular region contains sufficient sets of biometric features, the feature set extraction from the original images becomes feasible, and the subsequent training and validation during testing becomes robust and highly accurate. Previous research [7,8] shows that periocular biometrics can provide accurate methods of authentication.

3. Biometric System Functionality

In the following two subsections, the discussion is centered on the functionality of system modes and modules in the biometric system.

3.1. System Modes

There are two modes of authentication in a system where biometrics are used for authentication. The modes are enrollment and verification (or authentication). In the enrollment mode, a user's biometric information is captured by a biometric reader and stored in a template within the database. The stored template contains the user's identity to enable authentication. Once the user has been enrolled in the system, the biometric information is detected by the biometric sensor and related to the information that is stored in the database during the time of enrollment [9]. The transactions with this information need to be executed in a secure manner. During the verification mode, the user's biometric information is captured by the sensor, where a one-to-one evaluation is conducted with the biometric template from the database to make a determination (or verification) of whether the user is in fact the person who they claim [10]. In the verification process, there are three steps that must take place, which are [10]: 1) models, also referred to as reference models, are created for all the users in the system and stored in a model database; 2) some samples are matched with the reference models in order to produce the genuine and impostor scores and to compare with the threshold; and 3) testing process is conducted. In the verification mode, 'positive recognition' is used often, "where the aim is to prevent multiple people from using the same identity" [2]. In the identification mode, the user's biometric information is captured by the sensor; however, in contrast to the verification mode, a one-to-many evaluation is performed with the biometric templates from the database to establish the identity of a user who is unknown [10]. During the evaluation, if the system successfully identifies the user based on the biometric template in the database, where the assessment is within a previously set threshold, then a match is found. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who he/she (implicitly or explicitly) denies to be" [2]. These three modes of the biometric system are illustrated in Fig. 1.

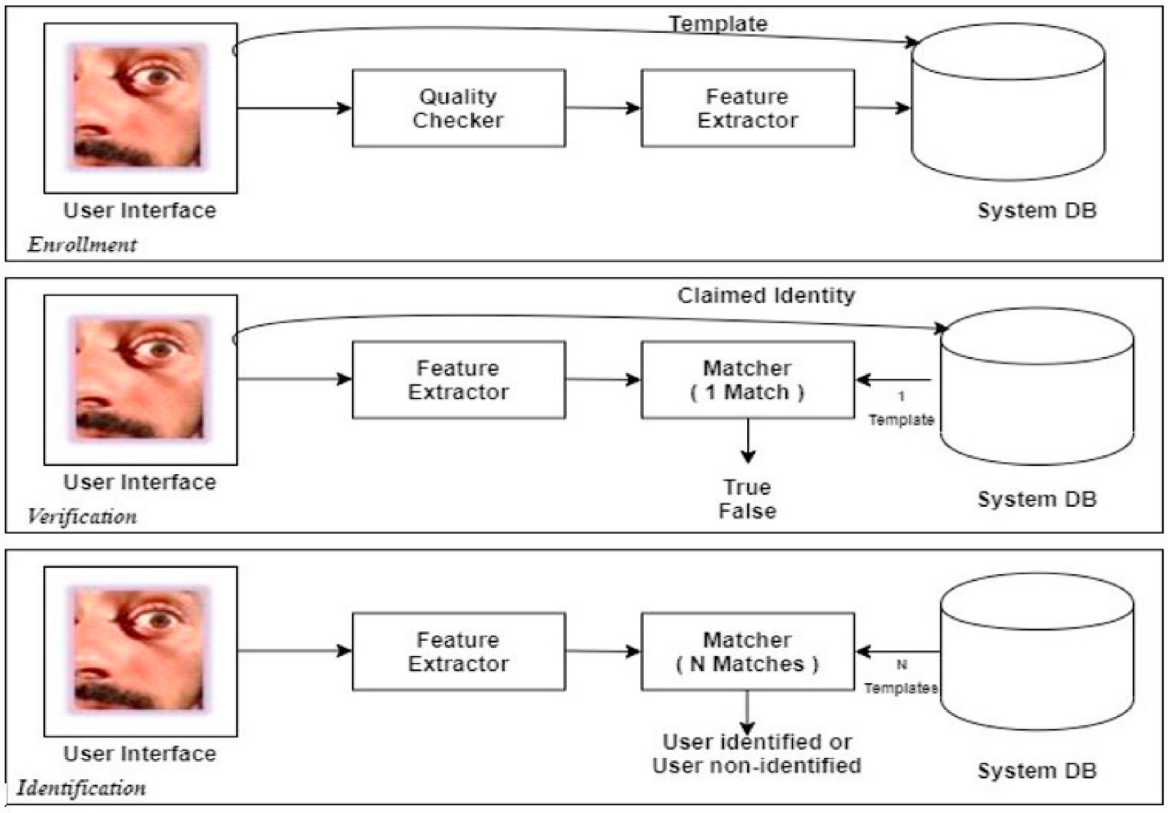


Fig. 1. Different modes of the biometric system.

3.2. System Modules

There are four important mechanisms within the biometric system [9] that are distributed through five modules. The first module is the biometric sensor, where the biometric information of a user is captured. This is the interface between the real world and the biometric system. In our research, we are capturing biometric information related to the user's periocular region. All the required pre-processing of the image is conducted in the next module. The third module is the feature extractor. This is the module where the biometric information captured by the sensor is processed to extract feature values. This includes removing artifacts introduced by the sensor, enhancing the input, or even conducting normalization if necessary. The fourth module is where the matching is conducted. The feature values are evaluated in comparison to the values contained within the biometric template to compute a matching score. This is a critical module, where the correct features of the periocular area are extracted in the optimal manner. An image of specific attributes is used to create a biometric template. The biometric template [11] is a numeric template that is a binary representation of specific points in the periocular region of the face. The fifth module is where the decision making occurs. This is where the user's identity is established or a claimed identity is accepted or rejected based on the information from the previous module [9]. Fig. 2(a) is an illustration of how the modules flow in a biometric system.

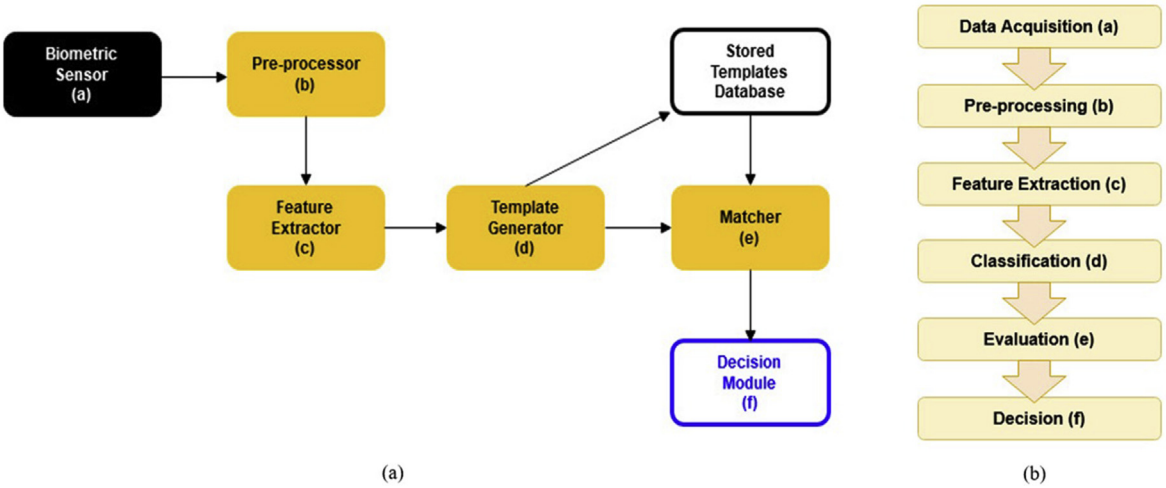


Fig. 2. (a) Diagram of the biometric system modules. (b) Classification steps for the biometric authentication.

3.3. Biometric System Performance

A biometric-based authentication system is a fundamentally complex system and its overall system performance depends on the hardware configurations, the software used, the tools selected, the hardware compatibility, the behavior and response time, and external factors that have direct impact on the input sensors connected to the system. In reality, high end system performance using a biometric authentication system is possible under controlled environments. In contrast, an uncontrolled environment adversely impacts the input sensors and reduces the system's performance. For example, periocular images taken in a low-light background will reduce the matching accuracy of the test objects during the validation process. The performance measurements of a biometric system are closely tied to the FAR and FRR. Ideally, for both FAR and FRR, the values are expected to be zero, i.e., the biometric authentication system should accept all genuine users and reject all the imposter attacks on the biometric authentication system. Also, by their very nature, FAR and FRR are inversely proportional. Fig. 2(b) provides the steps in biometric classification for authentication.

4. Healthcare Systems

The aim of a healthcare system is to take care of the health of the population in all possible ways considering the available resources and competing needs. Healthcare systems are described as combining organizational and financial work delivered to people. Concerns include problems of access (for whom and to which services), expenses, and resources. Hospitals, clinics, and all other health organizations can differ in various environments. Healthcare systems are complex and there are many types of operations that exist in the healthcare environment that we need to know related to healthcare systems and their providers. An examination of healthcare systems includes the consideration of the ways in which a system addresses commonly held values. From a technical perspective, indexes have been created in the information system to track information for patients using the MPIs and EMPIs. The next section will provide an overview of the health information management system.

4.1. Health Information Management System

In 2009, the United States Government created the American Reinvestment & Recovery Act (ARRA) to modernize the infrastructure of the United States of America, which included the "Health Information Technology for Economic and Clinical Health (HITECH) Act" [12,13]. The concept of the electronic health records (EHRs) was included in the HITECH Act. HITECH proposed the meaningful use of interoperable EHRs throughout the United States healthcare delivery system as a critical national goal [12]. The United States Congress decided not to define "meaningful use" in the law, however they allowed the Department of Health and Human Services to complete this action [14], which was done in 2010. The concept of "meaningful use" rested on the following five pillars [12]: 1) improving quality, safety, efficiency, and reducing health disparities; 2) engage patients and families in their health; 3) improve care coordination; 4) improve population and public health; and 5) ensure adequate privacy and security protection for personal health information.

It is important to understand that EHRs are more than a digitized version of paper charts and other records that healthcare providers must maintain for patients [14]. The implementation of EHRs creates a reduction in the amount of paperwork that exists in the healthcare industry. Large sums of money were not invested to merely digitize patient medical records. Policy makers view EHRs as the core of an emerging health information technology infrastructure that will improve the nation's healthcare system and the health of Americans [14].

The HIMS functions in the role of maintaining the structure and organization of information in healthcare and for the health of the patient. There are various components of HIMS that are responsible for different parts of capturing information about the patient as it relates to healthcare, such as the electronic medical records (EMRs), MPI, EMPI, and EHR. This research focuses on MPI and EMPI, which are discussed in the following sub-sections.

4.1.1. Master Patient Index

When a person undergoes a visit to any healthcare facility, such as the clinic, hospital, etc., to receive any form of treatment, demographic information is captured about the patient, as illustrated in Fig. 3. This information is captured in the MPI. A MPI is an index that is maintained separately from the medical record [15]. It has two main functions, where it ensures the registration data of a patient is clean and that redundant records do not exist, as well as linking patient records that are present across various Patient Registration Systems (PRS) [16]. As data is entered in the PRS it is supplied to the MPI in real-time. Some of the common information that is captured is as follows [17], patient information (which includes medical record number, first and last name, address, phone number, social security number, etc.), visit information (which contains location, date of the visit, account number), insurance information, providers, and related people (such as emergency, guarantor, and physician contact information). The information within a MPI is an extremely important component in the accuracy of patient information, such as identification of allergies, medication lists, and prior visits [17]. According to the HIMS standard, MPI is a valuable reference for basic demographic information and resident activity within one source [15].

4.1.2. Enterprise Master Patient Index

Industry efforts like health information exchange (HIE) and the Nationwide Health Information Network define EMPI as the combination of MPIs of two or more organizations [17]. When coupled with the benefits of cloud computing, an EMPI that is continuously maintained and updated can enhance the scalability and performance of the patient matching engine [18]. The patient matching engine is a component of an EMPI that can classify different database records as they are related to the same patient, which is depicted in Fig. 3.

The functionality of the EMPI expands more than just matching patient records. Once an EMPI exists, it has the ability to synchronize PRSs, locate history about patients outside of the EMR, prevents interfaces in the system from creating duplicate records, as well as raise alerts when patients are present in the hospital or healthcare facility [16].

4.2. Hospital Registration and Information Systems

Various healthcare locations have different registration processes when a patient arrives for the first time. When a new patient arrives at the hospital for the first time [19], the patient signs in by completing registration forms given by the receptionist(s) at the front desk of the healthcenter facility where treatment is being acquired. Once the registration form is completed and submitted, the patient provides their health insurance identification card to the receptionist to have it copied and have the information on it stored in the healthcare system. The front office verifies the health insurance information of the patient on the payer's website. Once the verification process is completed, the front office collects or mails the co-pay fees and issues the receipt of the transaction to patient. The front office creates a new medial chart for the patient and then notifies the back office of a new patient arrival. This process is presented in Fig. 4.

The focus of a hospital information system (HIS) is the integration of various capabilities and benefits. A HIS is also called the clinical data framework, which is intended to deal with the clinical, authoritative, and money related parts of a medical facility. Once a patient is enrolled in the HIS, all the information of that patient goes to the HIS database, which supplies information for the Patient Management System (PMS). A HIS provides the ability to manage clinical information thus allowing the professional staff to better manage appointments and billing for the

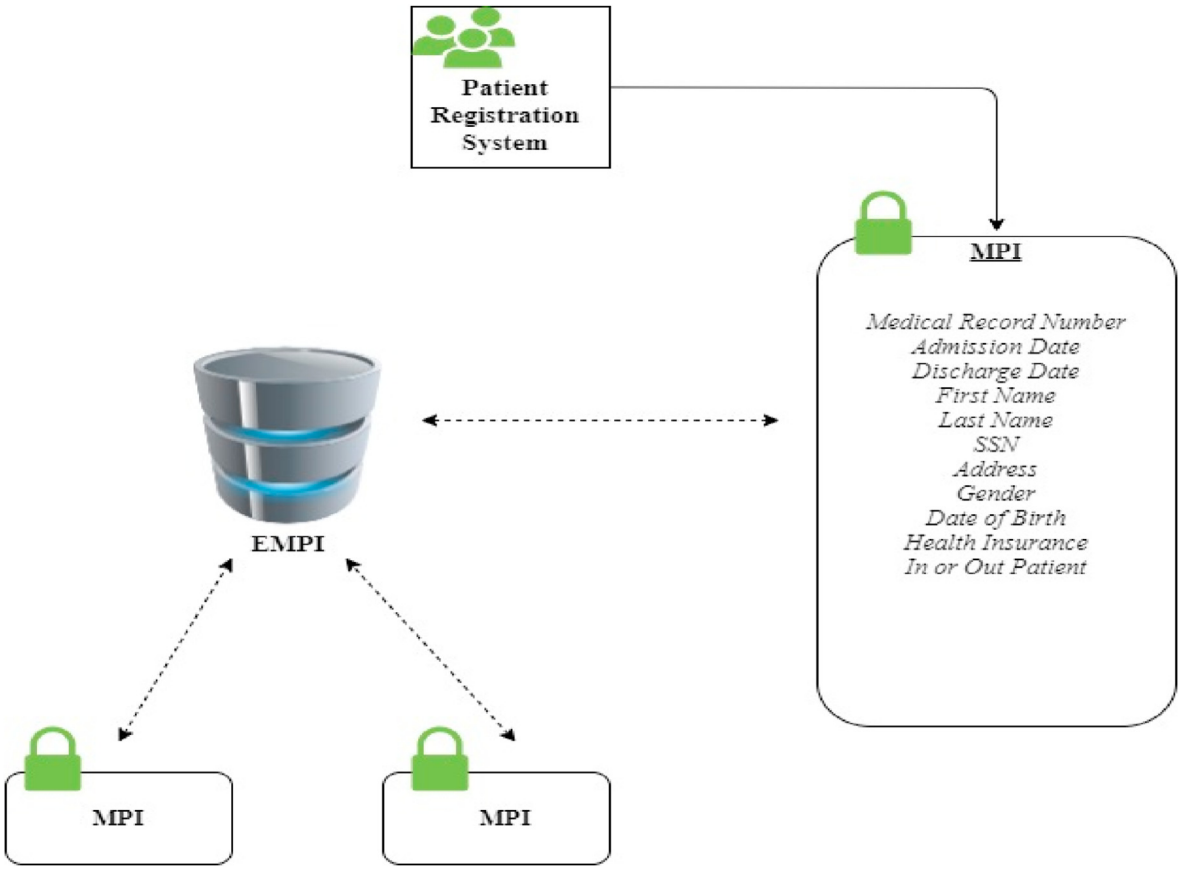


Fig. 3. Classifying different records as they related to the same patient.

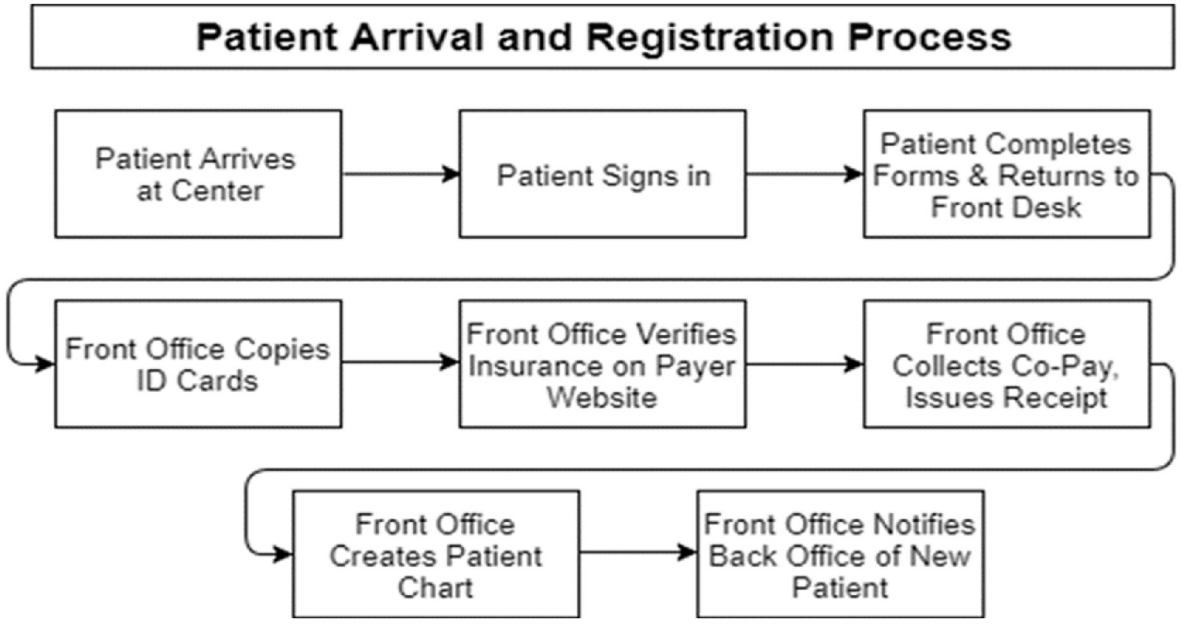


Fig. 4. The arrival and registration process for a new patient seeking medical attention at a healthcare location.

patients [20]. All the information received by the PMS goes to the Patient Information database, where it refreshes the electronic records of the patients. Once an electronic record gets refreshed, the information of the patient via the MPI in the database is refreshed simultaneously. Fig. 5 provides an illustration of how the HIS connects to the PMS.

5. Related Work

Patient records are viable for patient care, but incomplete patient records or wrong information in a patient's record can lead to prescribing the wrong prescriptions and misdiagnosis. The issue of security is oftentimes a concern when it comes to confidentiality of medical

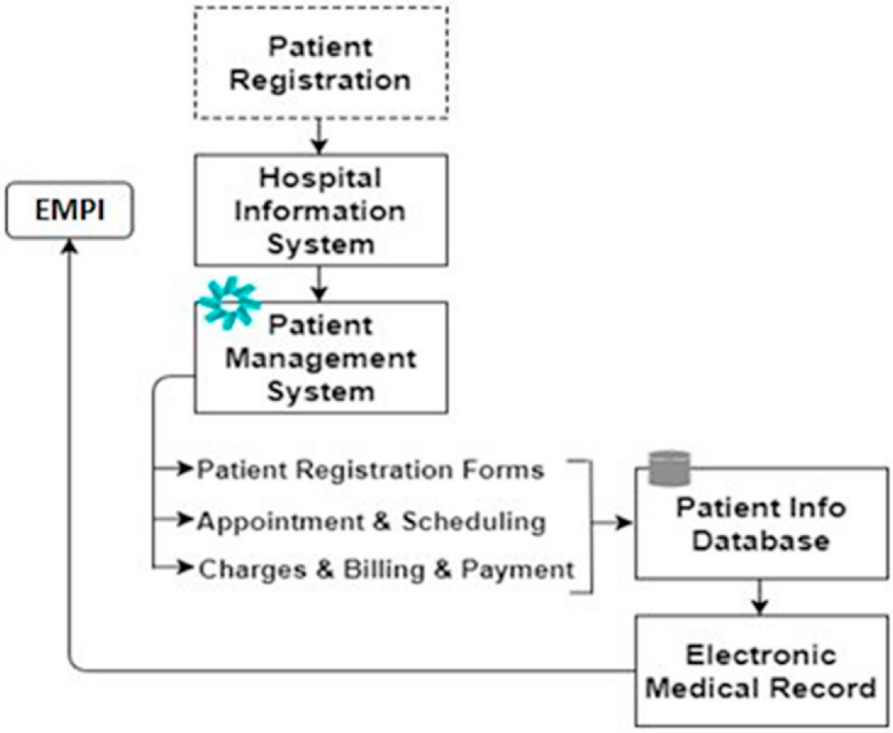


Fig. 5. Patient registration in the HIS for the PMS.

information [21]. HIMS is comprised of systems that automate the process to collect patient information, which eliminates bulky paperwork in hospitals and addresses the shortage of healthcare personnel [22]. Consequently, a health management system with integrated fingerprint biometrics could provide some level of security for patients and healthcare professionals, as it has been shown in Ref. [23]. Patients want to have assurance that the privacy of their records are well kept [24]. With the advent of Information Communication Technologies (ICT), researchers are working on ways of using ICT to deliver healthcare services at low costs. This has led to the development of the Telemedicine, Ehealth, and Wellness (TEW) systems. Besides, the application of ICT to remotely collect and disseminate information in a sensitive domain like healthcare, raises a number of security related issues. Therefore, in Ref. [25] they have investigated a number of TEW systems and have analyzed their technologies and security implementations. Patient records that are misrepresented or not well stored have a negative consequence resulting in prescribing the wrong prescriptions for patients. The evolution of advanced technology through biometric authentication provides security and privacy in the healthcare system.

The research in Ref. [26] implemented a HIMS, called CareMed, which utilizes two-factor authentication practices, specifically password and/or PIN and fingerprint biometrics. The security is incorporated in the system to secure patient health records that are contained within the system as it is used by healthcare providers. The authors of [27] developed Gellos HMS, which is an HMS using Unified Modeling Language (UML), Visual Basic.Net, and a Microsoft Access database. Gellos HMS provides access to the administrator, patient registration process, the doctor, and the nurse modules. Multi-factor authentication is incorporated into the system, where fingerprint biometrics and passwords and/or PINs are used.

In [28], the authors focused on how to preserve patient records with biometrics identification in health management systems. The main functionalities of the design and implementation of the system were achieved with UML and Visual Basic.Net. The client application provides access to patient records implemented with Microsoft Access. A dual authentication technique using a PIN and biometrics was utilized for the purpose of securing the system. Unlike normal authentication processes invoked by a user to access the network, biosensors with healthcare applications normally need to be validated automatically, followed by data transmission to the remote server without any explicit request.

A novel tri-factor user authentication protocol with mutual access is proposed in Ref. [29]. In a tri-factor authentication scenario, a smart card is physically issued to the user who first registers to a system. Each user possesses a smart card for later login and authentication. Integrated Pulmonary Index (IPI) patterns are used for biometrics authentication because body sensor networks have ability to collect IPI patterns and transmit it to MGW (Management at Gateway) network to form final authentication. IPI is an index which uses information from capnography and pulse oximetry to provide a single value that describes the patient's respiratory status [29]. The question was raised by the researchers, "how can we provide an effective form of authentication that is supremely accurate, fast, and convenient, operates on multiple devices, platforms and software?" The best solution to these kinds of problems is the use of biometric techniques for authentication. The authors identified there are lots of biometric methods that have been used for authentication practices in hospitals already.

In [30], the authors reviewed the different biometric techniques used in healthcare systems such as palm vein scanning, fingerprint identification systems, proximity authentication, right patient model and bio key. As more hospitals and healthcare systems migrate to computerized physician order entry and electronic health records, and more HIEs are built to coordinate care across networks, there is a great need to effectively manage data integrity to ensure it is kept free from corruption, modification, or unauthorized access [31]. Healthcare can only be effective if the right care is provided to the right patient, using the right patient information [32].

The performance of combining the use of online signature and voice biometrics in order to perform robust user authentication is analyzed in Ref. [33]. Signatures are verified using the dynamic programming technique of string matching. Voice is verified using a commercial off the shelf, software development kit. In order to improve the authentication performance, they combine information from both the online signature

and voice biometrics.

In [34], the authors propose a template protection scheme as random rectangular hashing to strengthen the multimodal biometric system. The performance of the proposed template protection scheme is measured using the fingerprint FVC2004 and PolyU palmprint databases. A biometric system automatically recognizes the person based on his/her physiological or behavior characteristics [35].

An understanding of the utilization, attitudes, and concerns of healthcare consumers and providers regarding biometrics is presented in Ref. [36]. Data was analyzed from a survey of 324 adult subjects, including 167 healthcare consumers and 157 healthcare providers. Healthcare providers were found more accepting of biometric technologies than consumers. Feelings about the potential uses and limitations of biometrics were found to be more differentiated among providers than consumers. Based on the findings, the authors suggest the need for additional research into the types of biometrics adopted in diverse healthcare settings and into the nature of innovators or early adopters. Some of the practical implications were if biometrics is to gain acceptance, there seems to be a need for different promotion strategies for providers and consumers. Identity is important when it is weak. The human body lies at the heart of all strategies for identity management. Secure identification is critical in the healthcare system, both to control logic access to centralized archives of digitized patients' data, to limit physical access to buildings and hospital wards, and to authenticate medical and social support. There is also an increasing need to identify patients with a high degree of certainty. Thereby, future works on biometrics technology will include DNA (Deoxyribo Nucleic Acid) analysis, neural wave analysis, and skin luminescence [37].

Biometrics has been implemented in several fields, such as smartphone technology from un/locking smartphones using fingerprint data or facial recognition technology, boarding flights and clearing customs using facial recognition or fingerprint data. However, there are several concerns that have been raised regarding biometrics. If someone's biometric data is compromised, it is not possible to get another one. In 2015, 5.6 million individuals' fingerprints were stolen in a massive breach from the Office of Personnel Management (OPM) [38]. OPM stated that [38], "The ability to misuse fingerprint data is limited. However, this probability could change over time as technology evolves."

In [39], a conceptual framework for biometrics in healthcare is presented, which consists of four main areas, such as (1) identifying basic elements; (2) examining important processes with special attention to the digital signature process; (3) reviewing relevant biometrics technologies; and (4) presenting a set of criteria and tradeoffs for evaluating the applicability of biometrics elements.

The essential components of biometrics technologies, along with multi-biometrics fusion for healthcare systems are presented in Ref. [40]. There are critical points in the biometric system when biometric data is classified as a 'high risk'. They are when the biometric data is enrolled in the biometric system as well as when the biometric data is updated [41]. There is a possibility the data could get altered with fraudulent data. For example, companies are producing applications that require biometric data to access an application. A company like Wells Fargo says that it will not store the original images of the biometric data that is used in the authentication process, however the data will be encrypted [42]. Nonetheless, there have been several instances where biometric hacking has occurred on a large scale.

Some additional security concerns are that a biometric sensor could be fooled and the accuracy of the sensor. If the biometric data of a biometric system is compromised, it is not possible to reverse the damage that has been done. Some vital privacy concerns are present when considering biometrics as a form of identification. In Refs. [43] several privacy concerns are identified as 1) any collection of data could eventually get hacked; 2) biometrics may become so commonplace that people become complacent; 3) the data stored in a biometric database may be more vulnerable than any other kind of data; 4) some pieces of your physical identity can be duplicated; 5) laws governing biometrics are a work in progress, which means your rights might be different from state to state. The researchers are aware of these security concerns and will be taken into consideration when designing and implementing the biometric system.

6. Proposed Periocular Authentication Module

We propose utilizing periocular biometrics to identify patients in the hospital/healthcare information systems instead of using a physical device for identification. The periocular biometric enables giving more attention in biometric authentication systems. The periocular is the area surrounding the eye. Nowadays, most mobile devices (e.g., tablets and smartphones) have a camera, which we use to acquire periocular images non-invasively. The periocular image is suitable when the camera is not detailed enough for an iris acquisition. In addition to being resilient to camera quality, the periocular biometric is not as affected by certain factors as is the facial biometric. Such factors include facial pose, changes in expression, and occlusion of the face. The authentication module can be replaced and used for other biometrics including the face, fingerprint, and iris.

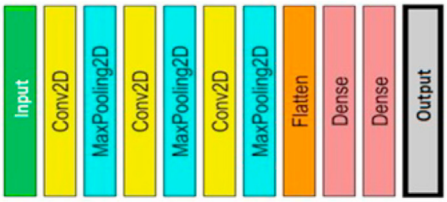
Biometric authentication systems incorporate classification techniques to distinguish the real person from imposters. Deep learning techniques have played a pivotal role in biometric-based authentication systems recently [44]. In this paper, we propose a deep learning-based method to classify the biometric data generated by the patients enrolled in the healthcare authentication system. During the enrollment process, biometric information from the patient is collected through sensors and image capturing tools installed by the hospital. The enrolled image samples will then be trained using a Convolutional Neural Network (CNN) [44]. Through the use of a CNN, a pre-trained neural network can be deployed, which can reduce the amount of training and processing time.

This research develops a deep CNN [45] to train and test the periocular samples from the patients. Inspired by the AlexNet proposed and implemented by Krizhevsky, A. et al. [45], we implemented a multiclass CNN, denoted as "modified AlexNet". We select our input image datasets under controlled environments, for the real time enrollment, training, testing and accuracy validation. The modified AlexNet (Fig. 6(a)) has a total of 3 discrete convolution 2D layers, 3 Max Pooling 2D Layers, 1 Flatten layer, and 2 Dense 2D layers. We use the sigmoid function instead of soft-max approach for faster classification and validation. Also, we use Binary Cross Entropy, Adam Optimizer with a learning rate of 0.01. In Fig. 6 (b), we show the main components of the modified AlexNet. We modified the traditional AlexNet to make the model applicable to periocular authentication. Also, the modified AlexNet works well for sparse training data.

6.1. Enterprise Master Patient Index

Previously, in Section 4, we discussed how current information systems (HIS, MPI, etc.) operate in the healthcare environment. We are proposing our biometric system, which uses periocular biometric information read by the biometric sensors to identify patients. The biometric system will retain its original functionality. The biometric modes of enrollment, identification, and verification will operate as previously discussed; see Section 4 for more information. Additional components of our system will be placed where the biometric template that is stored in the system database links to the patient's index in EMPI, as seen in Fig. 7.

The EMPI will connect with the information systems to locate various EMRs and information of the patient within the HIS. This will reduce the amount of work for the front desk receptionist when interacting with patients as they arrive. This will also assist nurses, doctors, medical examiners, and others in identifying patients, especially when looking up their medical histories. Patients can be identified with their unique EMPI from different clinical, financial, and administrative systems. The biometric information will be stored in the cloud in a database. Fig. 8



(a) The CNN structure implemented for the periocular biometric authentication system

Block 1	Conv2D: Filter Size	32x32	Block 2	Conv2D: Filter Size	64x64	Block 3	Conv2D: Filter Size	128x128	Dense Layer	Flatten Layer	1
	Kernel: Size	3x3		Kernel: Size	3x3		Kernel: Size	3x3		Dense Layer: Filter Size	128
	Activation Method	ReLU		Activation Method	ReLU		Activation Method	ReLU		Dense Layer: Filter Size	128
	Max-Pool Layer, Pool Size: 2x2, Strides: 2x2			Max-Pool Layer, Pool Size: 2x2, Strides: 2x2			Max-Pool Layer, Pool Size: 2x2, Strides: 2x2			Activation Method	ReLU
										Sigmoid Activation Binary Cross Entropy, Adam Optimizer, Learning Rate 0.01	

(b) Convolutional Neural Network Architecture of our modified AlexNet. (ReLU: Rectifier Linear Unit)

Fig. 6. (a) The CNN structure implemented for the periocular biometric authentication system. (b) Convolutional Neural Network Architecture of our modified AlexNet. (ReLU: Rectifier Linear Unit).

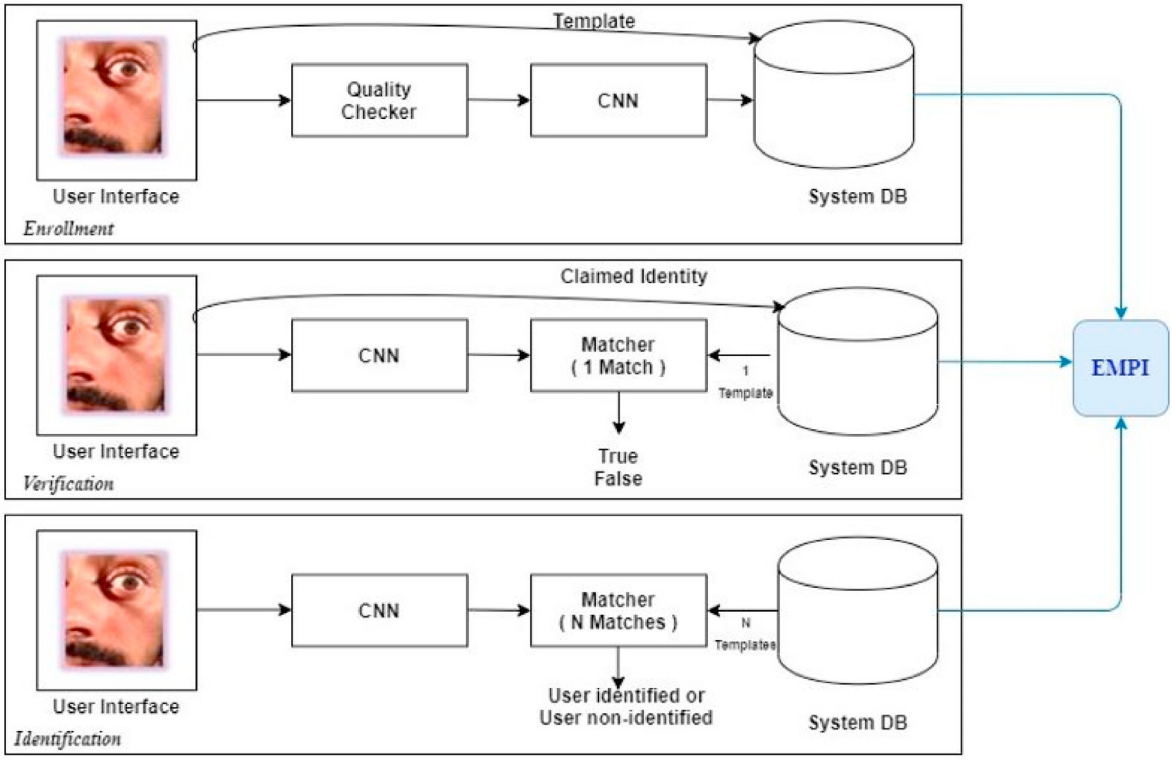


Fig. 7. The patient's periocular biometric information gets coupled with the EMPI system.

illustrates the process of how a patient's biometric information flows through the process and is connected to their EMPI.

6.2. Architecture

In any generic architecture for health organizations, patients must register first to continue with system services. Our proposed architecture is based on the scenario where a patient is not registered in the HIS. The process begins with the patient's periocular biometric data being captured and stored in the cloud for the first time using biometric technology. Fig. 9 is a depiction of the sequence of how the biometric authentication system captures the patient's periocular biometrics.

Next, a patient index number will be generated and associated to the biometric data of the patient. The generated patient index becomes the EMPI. A registered patient will allow the scanning of their periocular biometric data by the biometric sensor technology, which will check the associated patient index, using the EMPI, for the patient's biometric information and records in the HIS. At this point in the process, the patient will be able to access all of the appropriate services without wasting any additional time for data matching. In our architecture, we include verification, identification, and enrollment processes using the CNN architecture, which secures and matches the data. We are using these strategies because they create a strong, robust, and secure architecture to match periocular biometric data with the EMPI of the particular patient,

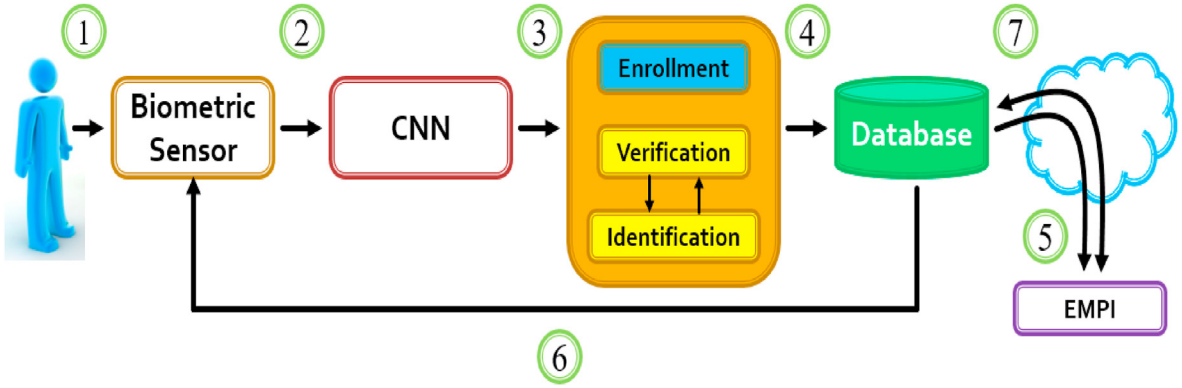


Fig. 8. Patient biometric information is coupled with their EMPI.

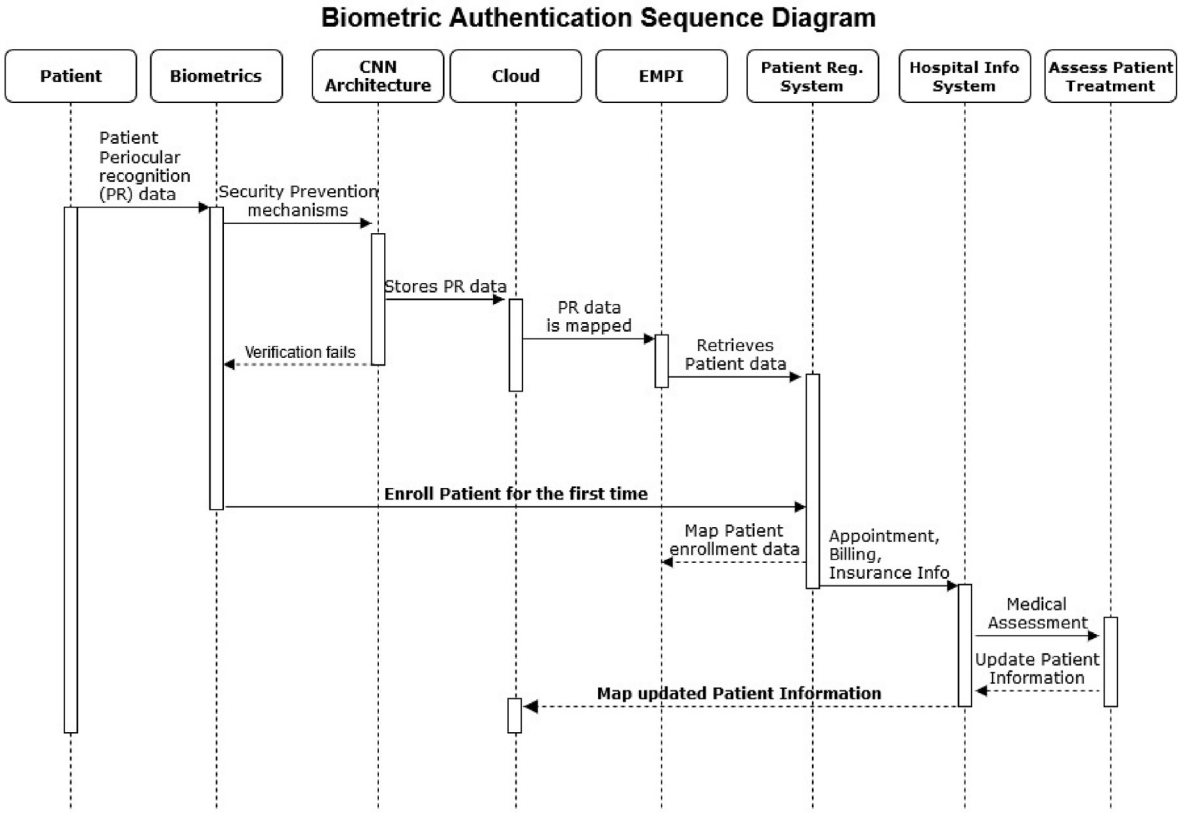


Fig. 9. Sequence diagram for the biometric authentication system.

which gives high accuracy for the matching phase. In summary, the system will serve the purpose of securely matching a patient's periocular biometric data to get the patient's EMPI. Once the patient's data is matched, the newly registered or already registered patient will have an appointment processed by the front desk personnel, who will pass all the required information to the nurse. The nurse will forward all the medical information of the patient to the doctor. After the completion of the appointment, all the charges for lab services and the pharmacy are updated in the HIS, which directly connects with the EMPI, as we have shown previously. Thus, the new information is added and updated in the patient's record. Whenever the patient comes for the next appointment, their periocular biometric data will be matched with the updated EMPI in a secured manner, as shown in Fig. 10.

6.3. *Results for Periocular Biometric Authentication*

We implemented a prototype framework based on periocular biometric data. We used the Biometric and Image Processing Lab (BIPLab) Mobile Iris CHallenge Evaluation – Part I (MICHE-I) [46] periocular dataset, which contains color periocular image datasets that are collected using Apple iPhone5 and Samsung Galaxy S4 smartphones, where the subjects are about 10 cm away from the device. The pixel resolution of the Apple iPhone 5 and Samsung Galaxy S4 are of high quality.

The Apple iPhone5 has a resolution of 960 × 1280, and the Samsung Galaxy S4 has a resolution of 1080 × 1920. For the Apple iPhone5 datasets, the images were taken from the FaceTime HD (front) camera of 1.2 megapixels (MP). For the Samsung Galaxy S4 datasets, the images were taken from the CMOS (front) camera of 2.0 MP. The dataset

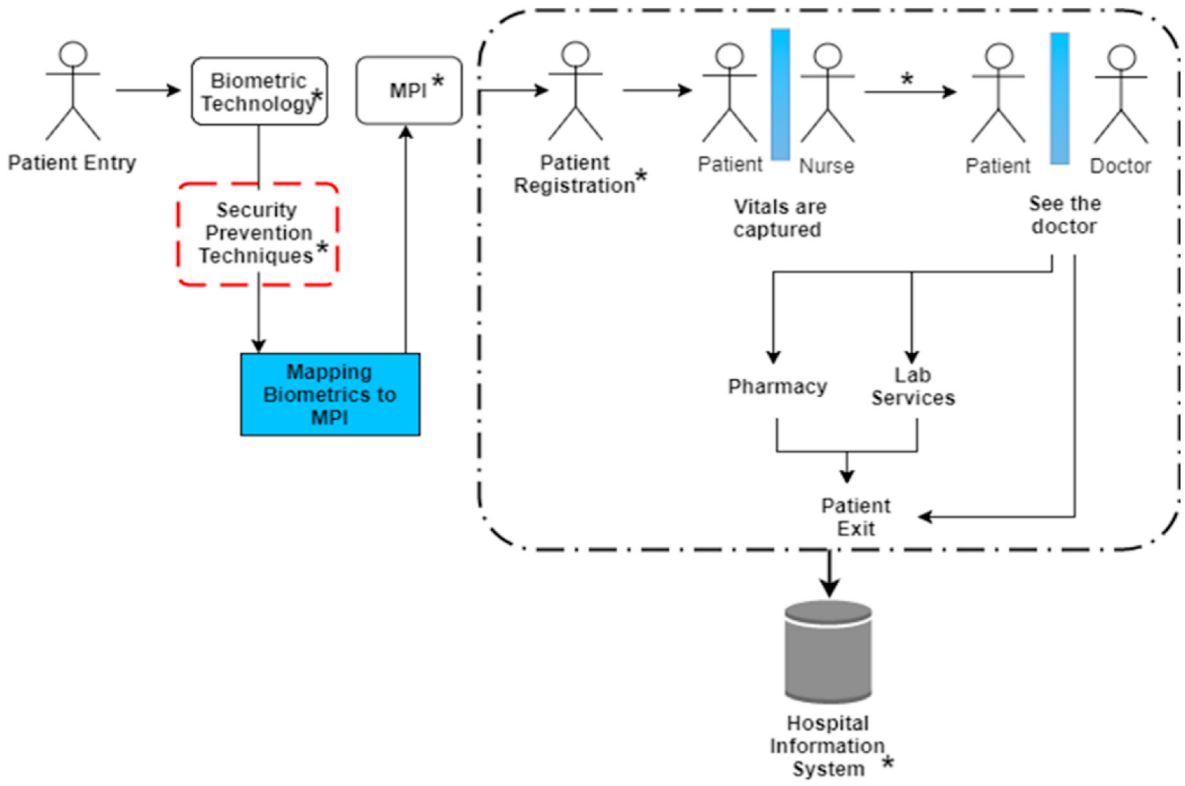


Fig. 10. Patient process using the biometric system and how the information is added in the HIS.

contains 75 classes of periocular image sets per person. Each class has 16 images of the same person. In total, we used 1200 images taken from the Apple iPhone 5, and 1200 images taken from the Samsung Galaxy S4 smartphones.

This research applies the multiclass CNNs for identification of each individual, and their successive validation and testing. We applied the modified AlexNet on the BIPLab MICHE-I [46] periocular dataset for experimental evaluation. The modified AlexNet is lighter in its layer structure and is much faster than the traditional AlexNet, as proposed in Refs. [45]. The training pattern of the CNNs varies depending on the time and the memory availability of the CPUs/GPUs. To conduct a realistic experiment, we ran our CNN architecture on the BIPLab MICHE-I datasets [46] for multiple times, observed the performances and minute variations, and recorded the results.

Figs. 11 and 12 are the experimental results for the classifications on the BIPLab MICHE-I Apple iPhone 5 periocular image dataset. We achieved significant training accuracy and validation accuracy even though 75 training classes were used. As the training goes on, the training loss decreases, as expected, but the validation loss fluctuates due to overfitting. The validation loss did not go below 46.59%, where we needed to adjust the early stopping range to a negative value to complete the validation. After 20 iterations, we achieved a training accuracy of 88.44%, a validation accuracy of 93.33%, and a test accuracy of 88.75%. We achieved a precision of 0.92, recall of 0.89, and the f1-score of 0.89.

Figs. 13 and 14 are the experimental results for the multiclass classifications on the BIPLab MICHE-I Samsung Galaxy S4 periocular image dataset. We achieved significant training and validation accuracies even though 75 training classes were used. We noticed that the training loss decreased as expected as the training progressed, but the validation loss fluctuated again due to the overfitting. The validation loss did not reduce below 46.59%, where we adjusted the early stopping range to a negative value to complete the validation. After 20 iterations, we achieved a training accuracy of 90.31, a validation accuracy of 93.65% before the overfitting started, and a test accuracy of 88.36%. We achieved a precision of 0.93, recall of 0.88, and the f1-score of 0.89.

In the next level of our experiment, we focused on different feature extraction techniques and compared the performances. The image-based feature extraction can only be possible through the formation of feature

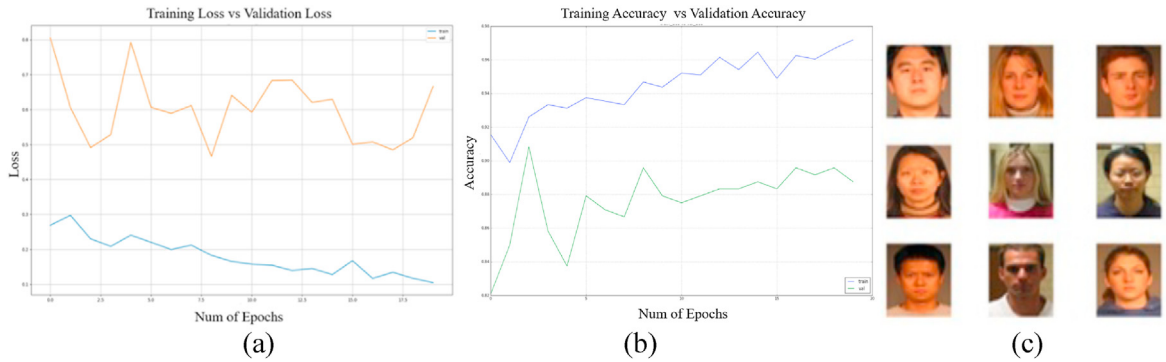


Fig. 11. (a) Training Loss vs. Validation Loss (b) Training Accuracy vs. Validation Accuracy (c) periocular images dataset.

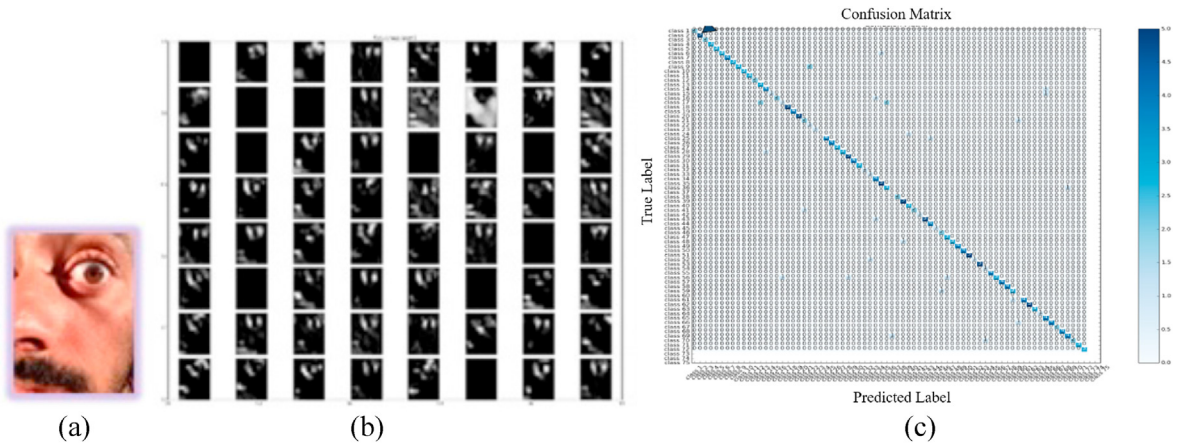


Fig. 12. Experimental study done on Apple iPhone 5 BIPLab MICHE-I dataset (a) Test Image from Subject Class (b) Internal Feature Map Layers distribution (c) Confusion Matrix showing that Class 2 got a high concentration level.

Fig. 13. (a) Training Loss vs. Validation Loss (b) Training Accuracy vs. Validation Accuracy.

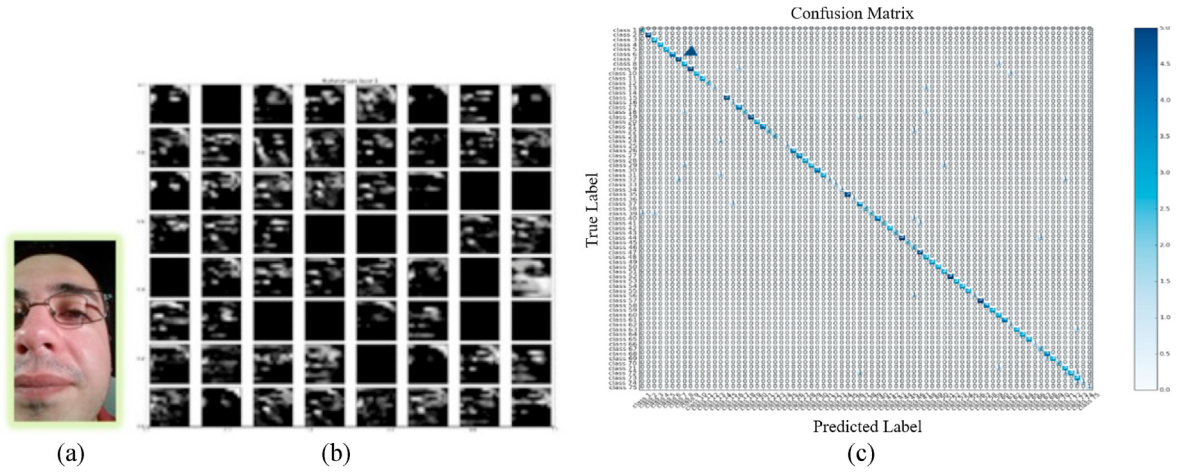


Fig. 14. Experimental study done on the Samsung Galaxy S4 BIPLab MICHE-I dataset (a) Test Image from Subject Class 7 (b) Internal Feature Map Layers distribution (c) Confusion Matrix showing Class 7 received a high concentration level.

vector sets during the training and enrollment steps, and the extracted features are matched during the recognition steps. There are several popular image feature extractions techniques available for periocular or face recognition [47–49]. In this research, we extracted local features, gradient features, and texture-based features from periocular images. To demonstrate the performance of the deep learning-based approaches and their effectiveness with the popular feature extraction methods, we applied three widely used feature extraction methods. Such methods

include the scale-invariant feature transform (SIFT) [47] for the local object features extraction, the histogram of oriented gradients (HOG) [48] for the gradient object detection, and the local binary pattern (LBP) [49] for the texture-based image feature extraction. Fig. 15 shows the feature elicitation approaches using SIFT, HOG, and LBP. Tables 1 and 2 show the comparative analysis of the approaches applied on Samsung Galaxy S4 and Apple iPhone 5 images.

The Receiver Operating Characteristic (ROC) curves show the verification performances on the iPhone 5 and Samsung Galaxy S4 datasets. The ROC curve shows the performances of the TPR vs FPR for both of the datasets, as demonstrated in Figs. 16 and 17. From Figs. 16 and 17, we see that the modified AlexNet shows a reasonable TPR of 98% of on both of the datasets. The ROC curves in Fig. 18 show the performance of FAR vs FRR. The average error rates for our proposed model is in the range of (3.2%–6.2%), as shown in Fig. 18. The test accuracy reported in this research for the modified AlexNet was significant, according to its deep network architecture. The training and validation processes are reasonably faster than the other approaches. The modified AlexNet used optimum CPU/GPU memory and efficiently handled high resolution color images with precision.

From Table 1, we found that SIFT produced a test accuracy of 83%, whereas the HOG and LBP produced the test accuracies of 80.03% and 85.01%, respectively on the Samsung Galaxy S4 periocular dataset during the time of recognition. We also observed that the execution time of HOG was lower than the SIFT and LBP approaches, as shown in Table 1. Furthermore, we feed the extracted features elicited from SIFT, HOG, and LBP to our modified AlexNet individually. We obtained classification accuracies of 85.21%, 82.78%, and 85.7% using the SIFT, HOG, and LBP with the modified AlexNet, respectively. We also found that the modified AlexNet alone received a highest accuracy of 88.36% on the Samsung Galaxy S4 dataset. The test losses are also shown in Table 1. Modified AlexNet achieved the lowest loss of 11.64%. We found from Table 1 that the modified AlexNet took the lowest computation effort of 1134.071 s.

Table 2 shows the results obtained based on the Apple iPhone 5 dataset. SIFT, HOG, and LBP achieved the accuracies of 80.49%, 89.5%, and 85%, respectively. We obtained the classification accuracies of 87.11%, 86.52%, and 88.14% using the SIFT, HOG, and LBP, respectively when applying with the modified AlexNet. The modified AlexNet alone achieved an accuracy of 88.4% on the Samsung Galaxy S4 dataset. Table 2 also represents the overall comparison of testing losses and computational efforts. The HOG obtained the lowest testing loss of 10.5%. It is observed from Table 2 that HOG outperformed the other approaches in terms of testing accuracy and loss; however, the modified AlexNet took the lowest computation time of 116.837 s.

Table 1
Comparison of different periocular recognitions technique and their individual contribution to the modified AlexNet. ***Dataset used: Samsung Galaxy S4.***

Image Recognizer/ Classifier	Test Accuracy (%)	Test Loss (%)	Time of Execution per cycle (Sec)
SIFT	83	17	203.476
HOG	80.03	19.97	129.332
LBP	85.01	14.99	156.589
SIFT + Modified AlexNet	85.21	14.79	306.228
HOG + Modified AlexNet	82.78	17.22	364.946
LBP + Modified AlexNet	85.7	14.3	201.158
Modified AlexNet	88.36	11.64	113.071

Table 2
Comparison of different periocular recognition techniques and their individual contribution to the modified AlexNet. ***Dataset used: Apple iPhone 5.***

Image Classifier	Test Accuracy (%)	Test Loss (%)	Time of Execution per cycle (Sec)
SIFT	80.49	19.51	203.968
HOG	89.5	10.5	128.402
LBP	85	15	156.593
SIFT + Modified AlexNet	87.11	12.89	307.054
HOG + Modified AlexNet	86.52	13.48	365.138
LBP + Modified AlexNet	88.14	11.86	196.706
Modified AlexNet	88.4	11.6	116.837

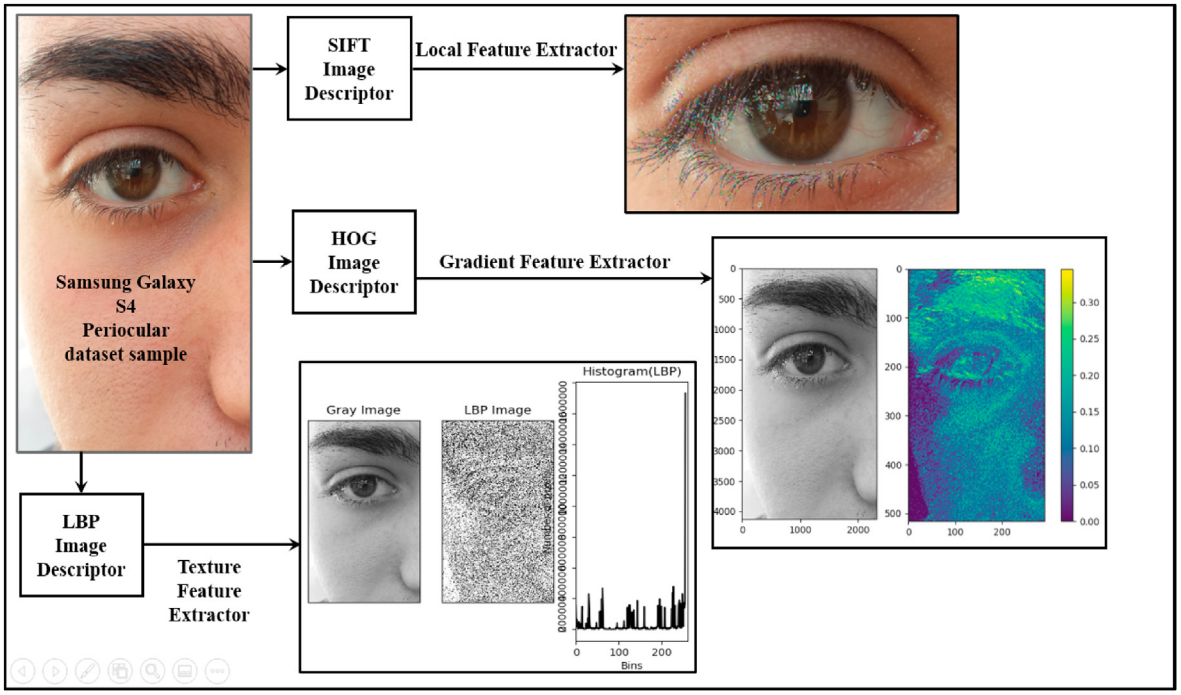


Fig. 15. Feature extraction using SIFT, HOG, and LBP on Samsung Galaxy S4 periocular dataset.

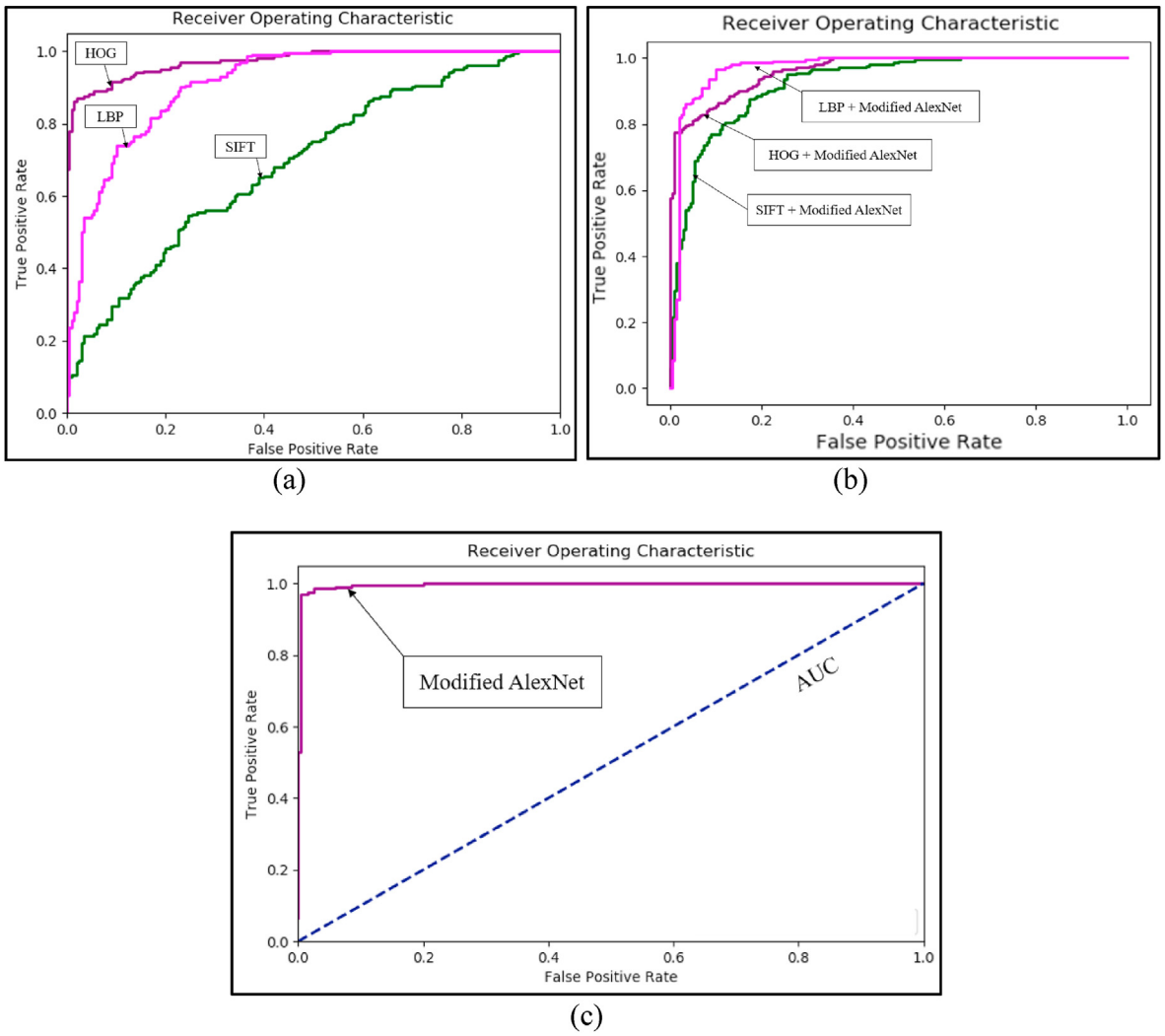


Fig. 16. (a) ROC for the SIFT, HOG, and LBP, (b) ROC for the SIFT + modified AlexNet, HOG + modified AlexNet, and LBP + modified AlexNet, and (c) ROC for the modifed AlexNet.

7. Conclusion & Future Work

A human can be identified through the measurements of their body. We refer to these measurements as biometrics. The integration of biometric data and the physical world offers society biometric applications and devices.

We propose a biometric system for the healthcare environment. Our biometric system presents a novel approach in identifying patients, both new and registered, in healthcare information systems. This form of biometric authentication is also very applicable for desktop/laptop computers, smartphones, and tablets. We propose capturing the periocular biometrics of each patient with their knowledge and consent. The periocular region is the area of the face that includes the eyes, eyelids, eyelashes, eyebrows, and irises. Periocular biometrics are unique to each individual. We propose linking an individual's biometric data with their EMPI, which is the identifier used in healthcare information systems to locate electronic healthcare records. The EMPI is unique to each patient. Our newly introduced system will assist with protecting data and reduce computation time relating to patients. We have conducted tests using the BIPLab MICHE-I dataset of our proposed system implemented as a prototype framework. The prototype framework utilized multiclass CNNs, specifically, a modified version of AlexNet, to test the accuracy of identifying the patient for each periocular biometric image captured on a smartphone; the TPR achieved approximately 98%. We also compare the performances of the deep neural network architectures with the traditional and widely used feature extraction approaches, including SIFT, HOG, and LBP.

Our future work consists of investigating how to incorporate our periocular biometrics authentication system for employees of healthcare and hospital systems, such as doctors, nurses, physicians, and surgeons, etc. We plan to implement the appropriate physical devices and software to capture the periocular data. Then we plan to have volunteers between the ages of 18–60 years assist with generating our own dataset for our proposed system. We will continue using the modified AlexNet CNN machine learning approach to get a better understanding of possible implementations of our proposed biometric system. We plan to investigate the appropriate mechanisms to use to integrate and incorporate the biometric technology into the healthcare information system.

CRediT author statement

Janelle Mason: Conceptualization, Methodology, Validation, Writing – Original draft preparation & Reviewing and Editing. Rushit Dave: Methodology, Writing- Original draft preparation. Prosenjit Chatterjee: Visualization, Methodology (Periocular Recognition Implementation), Writing – Original draft preparation & Reviewing and Editing. Ieschecia Graham-Allen: Conceptualization. Albert Esterline: Validation. Kaushik Roy: Conceptualization (Biometrics in health information system), Methodology (Biometric Part), Writing, Editing and Overall Supervision.

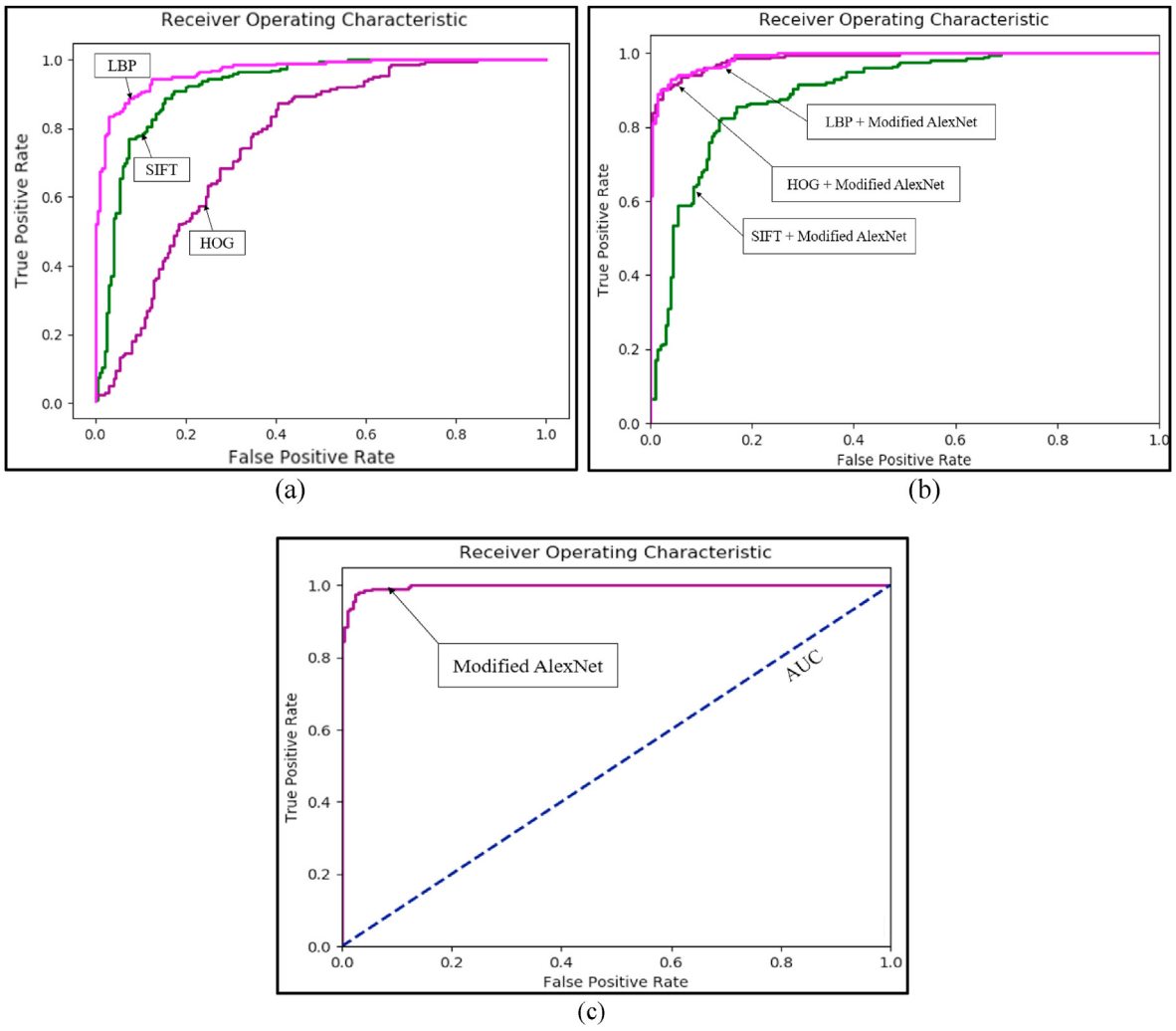


Fig. 17. (a) ROC for the SIFT, HOG, and LBP, (b) ROC for the SIFT + modified AlexNet, HOG + modified AlexNet, and LBP + modified AlexNet, and (c) ROC for the modifed AlexNet.

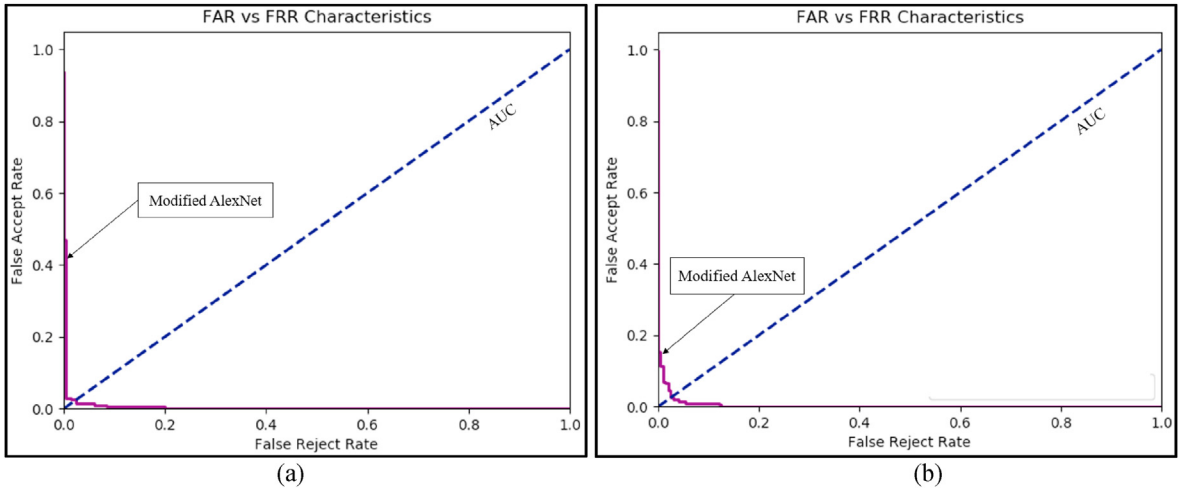


Fig. 18. Precision vs Recall graph for the implemented modified AlexNet on (a) Samsung Galaxy S4 dataset (b) Apple iPhone 5 dataset. **AUC = Area Under Curve.*

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This work is partially supported by NSF under the grant CNS 1900187 and partially supported by the U. S. Department of Education under the Title III Historically Black Graduate Institutions Grant. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NSF and the U. S. Department of Education.

References

[1] Thales Group. Biometrics: authentication and identification (2018). https://www.gemalto.com/govt/inspired/biometrics; 2018, July 05.
[2] Ross A, Nandakumar K, Jain AK. Introduction to multibiometrics. In: Handbook of biometrics. Boston, MA: Springer; 2008. p. 271–92.
[3] Jain A, Hong L, Pankanti S. Biometric identification. Commun ACM 2000;43(2):90–8.
[4] Thakkar D. Global biometrics market analysis: trends and future prospects. https://www.bayometric.com/global-biometric-market-analysis/; 2017, October 23.
[5] Kumari P, Seeja KR. Periocular biometrics: a survey. Journal of King Saud University-Computer and Information Sciences; 2019.
[6] Jain AK, Bolle R, Pankanti S, editors. Biometrics: personal identification in networked society. Kluwer Academic Publications; 1999, ISBN 978-0-7923-8345-1.
[7] Dellana R, Roy K. October). Data augmentation in CNN-based periocular authentication. In: 2016 6th international conference on information communication and management (ICICM). IEEE; 2016. p. 141–5.
[8] Jenkins J, Shelton J, Roy K. October). A comparison of genetic based extraction methods for periocular recognition. In: 2016 6th international conference on information communication and management (ICICM). IEEE; 2016. p. 309–13.
[9] Ross A, Jain A. Information fusion in biometrics. Pattern Recogn Lett 2003;24(13):2115–25.
[10] Sahoo SK, Choubisa T, Prasanna SM. Multimodal biometric person authentication: a review. IETE Tech Rev 2012;29(1):54–75.
[11] Avisian Staff. What's behind the biometric template? Mathematical templates enhance privacy and usability of biometric systems. https://www.secureidnews.com/news-item/whats-behind-the-biometric-template/; 2011, May 18.
[12] Centers for Disease Control and Prevention. Introduction | meaningful use | CDC. https://www.cdc.gov/ehrmeaningfuluse/introduction.html; 2019, September 09.
[13] 42 CFR Parts 412. Medicare and medicaid programs; electronic health record incentive program; proposed rule. In: Part II department of health and human services. Federal register, vol. 75; 2010, January 13. p. 1843–2011. 8, https://www.cms.gov/Regulations-and-Guidance/Legislation/Recovery/downloads/CMS-2009-0117-0002.pdf.
[14] Ferris N. 'Meaningful use' of electronic health records. https://www.healthaffairs.org/do/10.1377/hpb20100824.587990/full/; 2010, August 24.
[15] AHIMA Long Term Care Task Force. AHIMA's long-term care health information practice and documentation guidelines - practice guidelines for LTC health information and record systems. http://bok.ahima.org/Pages/Long%20Term%20Care%20Guidelines%20TOC/Practice%20Guidelines; 2013, January 1.
[16] Prosch L. What is master patient index?. https://www.thinkoccam.com/what-is-master-patient-index/; 2017, Aug 27.
[17] Wiedemann, L. A. "Fundamentals for Building a Master Patient Index." Enterprise Master Patient Index (Updated) Available at:http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048389.hcsp.
[18] Nalbandian G. MPI vs. EMPI: comparing patient matching value and performance for the healthcare enterprise. https://nextgate.com/2018/05/mpi-vs-empi-patient-matching-value/; 2018, May 07.
[19] Ayers A. Urgent care association of America. http://www.alanayersurgentcare.com/Linked_Files/UCAOA_Length_of_Stay_2009_03_13.pdf; 2009, March 13.
[20] Vegoda PR. Introduction to hospital information systems. Int J Clin Monit Comput 1987;4(2):105–9.
[21] Mogli G. Role of Biometrics in healthcare privacy and security management system. Sri Lanka Journal of Bio-Medical Informatics 2012;2(4).
[22] Ikhu-Omoregbe NA, Azeta AA. Design and deployment of a mobile-based medical alert system. In: E-healthcare systems and wireless communications: current and future challenges. IGI Global; 2012. p. 210–9.
[23] Jhaveri H, Sanghavi D. Biometric security system and its applications in healthcare. Int J Tech Res Appl 2014;2(6):15–20.
[24] Bazin A. Biometrics for patient identification—a US case study. ID World Abu Dhabi; 2012. p. 18–9.
[25] Mirembe DP. Design of a secure framework for the implementation of telemedicine, eHealth, and wellness services. 2006.
[26] Azeta AA, Iboroma DOA, Azeta VI, Igbekele EO, Fatinikun DO, Ekpunobi E. Implementing a medical record system with biometrics authentication in E-health. In: 2017 IEEE AFRICON. IEEE; 2017, September. p. 979–83.
[27] Azeta AA, Omoregbe NA, Misra S, Iboroma DOA, Igbekele EO, Fatinikun DO, Ekpunobi E, Azeta VI. Preserving patient records with biometrics identification in e-Health systems. In: Data, engineering and applications. Singapore: Springer; 2019. p. 181–91.
[28] Díaz-Palacios JR, Romo-Aledo VJ, Chinaei AH. March). Biometric access control for e-health records in pre-hospital care. In: Proceedings of the joint EDBT/ICDT 2013 workshops; 2013. p. 169–73.
[29] He CG, Bao SD, Li Y. A novel tri-factor mutual authentication with biometrics for body sensor networks in healthcare applications. Int J Smart Sens Intell Syst 2013;6(3).
[30] Manimekalai S. A study on biometric for single sign on health care security system. Int J Comput Sci Mobile Comput 2014;3(6):79–87.
[31] Spence B. Hospitals can finally put a finger on biometrics. http://www.securityinfowatch.com/article/10473265/hospitals-can-finally-put-a-fingeron-biometrics; 2011, November 4.
[32] Trader J. Why healthcare should evaluate biometrics for patient identification. 2012.
[33] Krawczyk S, Jain AK. Securing electronic medical records using biometric authentication. In: International conference on audio-and video-based biometric person authentication. Berlin, Heidelberg: Springer; 2005, July. p. 1110–9.
[34] Gudavalli M, Kumar DS, Raju SV. Integrated biometric template security using random rectangular hashing. Global J Comput Sci Technol 2014;14(7):32–8.
[35] Jain AK, Flynn P, Ross AA, editors. Handbook of biometrics. Springer Science & Business Media; 2007.
[36] Chandra A, Durand R, Weaver S. The uses and potential of biometrics in health care. Int J Pharmaceut Healthc Market 2008;2(1):22–34.
[37] Duquenoy P, George C, Kimppa K. Ethical, legal, and social issues in medical informatics. 2008.
[38] Pepitone J. OPM hack: 5.6 million fingerprints (not 1.1 million) were stolen. https://www.nbcnews.com/tech/security/opm-5-6-million-fingerprints-not-1-1-million-were-n432281; 2015, September 20.
[39] Mitra S, Gofman M, editors. Biometrics in a data driven world: trends, technologies, and challenges. CRC Press; 2016.
[40] Rakshit RD, Kisku DR. Biometric technologies in healthcare biometrics. In: Design and implementation of healthcare biometric systems. IGI Global; 2019. p. 1–28.
[41] Fauscette M. Biometrics are coming & so are security concerns. https://www.darkreading.com/endpoint/biometrics-are-coming-and-so-are-security-concerns/a/d-id/1331536; 2018, April 20.
[42] Scottile C. As biometric scanning use grows, so does security risk. https://www.nbcnews.com/mach/mach/biometric-scanning-use-grows-so-do-security-risks-ncna593161; 2016, July 24.
[43] (n.d.) Van der Kleut J. Biometrics and biometric data: what is it and is it secure? https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html.
[44] Goodfellow I, Bengio Y, Courville A, Bengio Y. Deep learning 2016;1.
[45] Krizhevsky A, Sutskever I, Hinton EG. Imagenet classification with deep convolutional neural networks 2017;60(6):84–90. June 2017.
[46] Marsico MD, Nappi M, Riccio D, Wechsler H. Mobile Iris Challenge Evaluation k(MICHE), biometric iris dataset protocols. Pattern Recogn Lett 2015:17–23. 2015.
[47] Lowe D. BObject recognition from local scale-invariant features. In: Proc. 7th int. Conf. Computer vision; 1999. p. 1150–7. Kerkyra, Greece.
[48] Dalal N, Triggs B, Schmid C. May). Human detection using oriented histograms of flow and appearance. In: European conference on computer vision. Berlin, Heidelberg: Springer; 2006. p. 428–41.
[49] Silva C, Bouwmans T, Frélicot C. An extended center-symmetric local binary pattern for background modeling and subtraction in videos. 2015, March.