ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 14, Issue, 02, pp. 64930-64937, February, 2024
https://doi.org/10.37118/ijdr.27834.02.2024

REVIEW ARTICLE OPEN ACCESS

BIOMETRICS IN HEALTHCARE AS A TECHNOLOGICAL CONTRIBUTION TO MITIGATE PATIENT IDENTIFICATION ERRORS: A REVIEW

***Zahraa. A. Bahman**

Department of Diagnostic Imaging, Amiri Hospital, Kuwait

ARTICLE INFO

Article History:
Received 17th January, 2024
Received in revised form
26th January, 2024
Accepted 06th February, 2024
Published online 28th February, 2024

Key Words:
Biometrics, Misidentification,
Healthcare, Contactless Biometrics.

****Corresponding author: Zahraa. A. Bahman***

ABSTRACT

Biometrics are becoming essential and have been recommended as a technological method for identification due to its ability to provide unique verification of a person. Biometrics use physiological characteristics of the human's body which were chosen because they usually do not change over a lifetime and cannot be duplicated or forgotten. Different biometrics technologies have proven to be applicable to solve the problems of duplicated patients' records and assure a correct identity. This research would make contribution in relation to solutions for patient identification methods within the healthcare sector, by expanding the knowledge base of biometric technology as an identification system that have been used in healthcare sector worldwide. Also, pointing out the patient misidentification issue within hospitals. The research may have influence on the awareness to the importance of proper identification and to the biometric use in the healthcare sector.

Citation*: *Zahraa A. Bahman, 2024. *"Biometrics in Healthcare as a Technological Contribution to mitigate Patient Identification Errors: A Review". International Journal of Development Research*, 14, (02), 64930-64937.

INTRODUCTION

Healthcare providers aim to deliver good care and health services to patients. This can be achieved by providing the right care to the right patient, through using the correct information about him/her. Most healthcare providers use manual processes for patient identification which often results in identification errors that are carried out through the entire service according to the report of Imprivata [1]. Patient identification errors could imperil patient's safety. Therefore, "identifying patients correctly" is the goal number one of the international patient safety goals set by the Joint commission International (JCI) [2], which is a nonprofitable organization as a global leader for healthcare quality and patient safety. Healthcare services, diagnosis and treatment are not a simple process. Minor inaccuracy can lead to major mistakes, especially that healthcare providers base their services on the given information and available data such as medical history, allergy lists and medications. Any mismatch of these data with the treated patients can lead to serious impact on patient's health [3]. As suggested actions by the collaborating Centre for Patient Safety Solutions of the World Health Organization (WHO) [4], Member States should consider specific strategies some of which are: to provide clear guidelinesto identify patients who do not carry proper identification and for distinguishing the identity of patients who carry the same name. Also, non-verbal approaches to identify unconscious or confused patients should be evolved and used.

In addition to motivatethe participation of patients in all stages of the process. Thus, proper patient identification is highly important in healthcare. Patient identity check plays an essential role in improving the safety measures in healthcare delivery in any country. Thus, having an appropriate patient identification system within the healthcare organizations is important, and it became a must in most countries all over the world. Today, there are several methods for patient identification implemented worldwide. The most common ones are Unique Patient Identifier, algorithm approaches, referential matching software, biometrics, radio frequency identification device (RFID) systems and hybrid models. However, no current identification method yet has been known to have a 100% matching rate [5,6]. This research presents literature review from previous studies on identification errors in healthcare beside a comparison of different biometric technologies and their implementation in public and healthcare sector. In addition to a review of related works of biometric implementation in healthcare.

METHODOLOGY

Literature review to learn the current research state in implementing biometric technology. The main purpose of the literature review is to provide a proper context for the study based on previous research. This literature will review some evidence of medical errors due to patient misidentification, in addition to different types of biometric techniques used worldwide for the identification and their implementation in healthcare. The strategy in the literature review involved a comprehensive approach to gain information that could

help to review other researchregarding biometrics and its use in healthcare. The investigation of information in the literature was done by reviewing several types of references such as books, journal articles, academic studies, and government publications. Most of which were available on the internet. Information was retrieved mainly from the Kuwait University Library database, google scholar search engine, IEEE Explore, ResearchGate, PubMed, Sage, ScienceDirect, Social Science Research Network, SpringerLink, in addition to Master and Ph. D thesis reports. The main searched keywords that have been used in the search were: Biometric, patient misidentification, biometric in healthcare, acceptance of biometric, fingerprint, iris, palm vein recognition, biometric implementation in healthcare. The main objectives of the research are to provide in depth knowledge and understanding the importance of proper patient identification and medical errors as consequences of patient mis identification. Also, to provide context of different types of biometric techniques used worldwide for the identification and their implementation in healthcare.

LITERATURE REVIEW

Patient Identification Errors

The Emergency Care Research Institute (ECRI) which is specialized in patient care research, indicates that around 13% of identification errors happen during patient registration. Additionally, ECRI analysts reported that patient identification issues are common in healthcare, and it is significantly affecting patient safety and financial implication. Research showed that 7 -10 % of patients are misidentified during medical record searches and around 6 percent of them had been affected negatively [7]. WHO, has mentioned that the National Patient Safety Agency in the United Kingdom reported several incidents associated with missing or incorrect information on wristbands. Likewise, the U.S. Department of Veterans Affairs' National Center for Patient Safety had marked more than 100 incidents related to patient misidentification from the period 2000 to 2003 [4]. Three essential requirementsare needed to identify patients with a high degree of certainty [8]. First is reducing medical errors. Second is reducing risks of fraud. And third is improving capacity to react to medical emergencies. Different countries reported an estimation around 10-16% of hospitalized patients encounter an adverse incident related to clinical care, with a mortality rate of 5-8% in these patients. A survey of medical errors by Europeans revealed that nearly 78% of citizens classify medical errors as critical issue in their countries. Patient misidentification is one of the major causes of such errors. Therefore, accurate means of identifying patients and staff is a pivotal step for reducing medical errors. Examples about the consequences of patient misidentification are summarized below:

a) Duplicated Medical Records [1].
- The American Health Information Management Association (AHIMA) reported that duplicated medical records rated between an average of 8-12 % of which 40% had blank or default values in one of the key data fields.
- A study done at John Hopkins Hospital revealed that 92% of the errors that resulted in duplicated medical records were caused by inpatient registration mistakes.

b) Wrong Procedure Performed
- In 2014, a confusion between two patients' surname happened, when the treating physician provided the wrong patients information over the phone to the surgeon that resulted in heart surgery on a wrong patient [9].

c) Medication Error
- In a Swedish study, 60 errors were identified over a period of 12 years involving cytotoxic drug administration and 8.3% involved wrong-patient administration [7].

d) Unnecessary Radiation Exposure
- In a study at two large academic hospitals, it was found that 0.004% of radiology reports were done for wrong patients [7].

e) Blood Transfusion Reaction and Laboratory Errors [7].
- 16 hospitals shared centralized database revealed 16 instances of specimen mismatches of which 50% were due to patient misidentification
- Various institutions reported that 11.6% to 36% of clinical laboratory errors were related to patient ID errors.

Obtaining a higher rate of proper patient identification is one of the quality improvements goals in all healthcare systems. WHO has published an article about solutions for patient safety to ensure correct patient identification in healthcare [4]. It mainly emphasized on suggestions like:

- The responsibility of healthcare professionals to specify the identity of patients and apply the healthcare service to the accurate patient using at least two identifiers (name and date of birth). While having a clear protocol for identifying patients in the healthcare system, it is rather important to engage patients in the process.
- Continuous training and follow up of the performance of the protocol will improve its effectiveness.
- The education of patients about identification procedures will play a crucial role in obtaining their cooperation.

Biometric in Public

A biometric system is basically a pattern recognition method that recognizes an individual based on features originated from a certain physiological or behavioural trait that the person possesses.Biometric are also defined as the automated measurements of physiological or behavioral characteristics that are used to authenticate, determine, or confirm the identity of a person [10]. The use of biometrics was limited to forensic applications for a very long time. However, it has been largely used these days due to the ability to process and store its data digitally using modern computers. This technological advancement boosted the opportunity for a wider spectrum of biometrics uses. For example, passports, ID cards and driving licenses which improved waiting time at check points and border control. Biometrics provide a challenging solution to increase security needs, as it bases authentication on aspects that are specific to everyone. However, biometrics is only one element of a larger scale system which may involve:

- Special sensors to capture/scan a biometric reading.
- Transmission of this data from the sensor to a computer
- A well-defined database to store the biometrics data.
- Decision making and resulting action.

Therefore, Biometrics solutions should be considered as an entire system design rather than a single device. The Public Private Analytic Exchange Program reported that biometrics-based authentication system was provided for the Indian government's Aadhaar system, where 1.1 billion Indian citizens were biometrically captured with either contactless fingerprint or iris recognition to establish identity for the purpose of government benefits. Four billion authentication transactions have taken place since the program started. The system verifies the identity of a citizen with 92 percent accuracy, and it is expected to rise to 95 percent as stated officially by the Indian government [11]. Biometrics have been used to identify patients in emergencies, where many patients arrive without sufficient identification documents [8]. Such emergencies include natural disasters, technological disasters, major transportation accidents and acts of terrorism. In emergency, rapid medical diagnosis and treatment is substantial, where patients should be properly identified once arrived. Also, it was mentioned that combining biometrics and biomedical data into a single portable sensor may provide quick positive identification of casualties with reliable treatment. It should be always considered that the possibility of enrolling patients may be difficult in case of pain, injuries, and burns. Any failure to enrol a patient in an identification scheme should not delay the emergence treatment. Historically, biometrics were used since the second century by a Chinese emperor for authenticating specific seals with a fingerprint. In the 19th century, Bertillon, who was a police officer and biometric researcher, used biometrics in a scientific policing to

identify reoffending criminals. In 1901 and 1902, the Metropolitan Police in U.K and the French police respectively started to use biometrics for identification. In 1942, the Federal Bureau of Investigation (FBI) in the USA also started using biometrics [12]. Lately, biometrics became one of the biggest predilections in individual identifications, and it was claimed to be better than current established authentication methods [13].

Recently, biometric technologies have had radical impact on various areas such as smartphones, law enforcement, public security, borders and migration control, military, commercial applications, and financial services.

- **Law enforcement biometrics** are used to support law enforcement agencies which include criminal ID solutions like Automated Fingerprint Identification Systems (AFIS) that search, store and retrieve fingerprint data and related records. Also, live face recognition in crowd which is the ability to identify faces in crowded places is being used in cities and airports in many countries, as in China where there are about 170 million CCTV cameras that use facial recognition technology combined with real tracking to pick individuals out of crowds [14].
- **Border and migration control**: There are no doubt that many countries have adopted many secured identification methods since the terrorist's attack of September 11th, 2001, in the United States. Managing the security and identification have become a top priority in many countries for border control [15]. Therefore, the best technology to achieve this target is continuously being searched forFingerprints and cameras for face recognition are widely used in airports to identify travelers. The European Union has implemented EURODAC, the first multinational biometric system in the world which serves more than 32 nations, used for asylum seekers based on their fingerprints [12]. Biometric passports, also known as e-Passport represent a combination between paper and electronic passport that uses biometrics data to authenticate the traveler's identity [16]. At the international airport of Frankfurt, Hong Kong, and neighboring Macao their residents are being issued with a chip card that contains biometric data to assist the acceleration of border-crossing procedures. Kuwait Airport uses fingerprint as biometric technology mechanism to accurately identify individuals and to overcome security issues such as illegal immigrants, terrorism and identity duplication fraud that challenge the authorities in the State of Kuwait [15]. The study addressed the effectiveness of biometric in job performanceand it considered fingerprint to be the best and most effective modality used in controlling the borders.
- **Military**: It is not well known how biometric is being used in defense agencies due to the sensitivity of sharing this information to public. The USA military started in 2004 to collect and analyze biometrics of faces, irises, DNA, and fingerprints. More than 7.4 million identities are available in their database mostly from the military operations in Iraq and Afghanistan [12]. The Department of Defense (DOD) had arrested or murdered around 1,700 individuals in the period from 2008- 2017 based on biometrics and forensic matches. DOD used biometrics to maintain several military processes, such as targeting, force protection, and humanitarian assistance [17].

Biometric Technologies

Different biometric technologies functionalities and their advantages and disadvantage are reviewed.

Fingerprints: Fingerprint is the oldest biometric technique used for authentication. It has been used since 1896 specifically for identification of criminals. The concept is based on the fingertips with corrugated skin that have ridges lines from one side of the finger [26]. Fingerprint recognition affords accuracy for both verification and Identification. Biometric method is popular because of its compactness and low cost. On the other hand, the sensor is usually not capable of capturing acceptable quality images for people with very dry, burned, wet skin or with cut on the fingertips [13]. There are some challenges in the fingerprint identification of new-borns, elderly, and individuals with damaged fingerprints due to manual labour [27]. To prevent the omission of services to these individuals, some strategies were suggested such as linking a new-born's record to the fingerprints of their authorised guardians, registering multiple fingerprints for manual laborers and elderly people to rise the matching accuracy, and using other identifiers as a backup such as their name or location.

Fingerprint scanning has become the most widely used due to the availability of portable, low-cost technologies [28]and the high sensitivity and specificity for verification[29]. Although, twins might have identical DNA structure, but they do not share the same fingerprints. Others also have reported that fingerprinting is a feasible technology for verifications [30]. With the vast innovations in technologies, multispectral imaging of fingerprints made it possible to acquire images of not only the surface but also the subsurface features of the skin which results in enhanced image of the fingerprint under different operational circumstances. Multiple colour images from different polarizations and angles are acquired to capture many different properties of the finger that made it possible to capture images when there is moisture, contaminants or even poor contact between the finger and the sensor. Studies showed that multispectral imaging is reliable in spoof detection, where it can identify live human fingerprint and reject fake ones [31]. Recently, there is a high tendency toward contactless fingerprint technology (CFT), which differs from the contact-based fingerprint in that it directly captures fingerprint images without physical contact to the sensor. Whereas contact-based fingerprint needs direct physical contact with a sensor and relies on physical medium, such as paper, ink, or plate to capture a fingerprint image. CFT is considered the third generation of fingerprint techniques after the ink based which capture the tops of fingerprint ridges on paper after pressure is applied, and optic based which capture light reflected from the tops of fingerprints on a plate to capture fingerprint images. Contactless fingerprint has some advantages such as faster capture times and more hygienic. Also, it captures three dimensional images of users' fingerprints directly. On the other hand, contact based fingerprint systems depends on users pressing their three-dimensional fingers on two dimensional surfaces which causes some distortion in the captured image. CFT reduces this problem and provides better fingerprint image. With all mentioned advantages of contactless fingerprint technology, it is still an emerging technology in its infancy stage [11].

Palm Vein Recognition: It is a recent biometric technology that uses unique characteristics of the vein to identify an individual. This technology focuses on the veins of the hands where each finger has veins connected directly with the heart and has its own physical traits. The recognition system captures images of the vein patterns by applying infrared light transmitted through the hand and captured by a camera that records the vein patterns. This method has a high level of security which can protect information. Also, the level of accuracy has a high degree of reliability with low cost of equipment and installation. Furthermore, it takes shorter time than other methods which increases the acceptance [12]. The scanning process is fast, and identification is accurate. The scanner is easily sanitized with antibacterial wipes [32]. In Japan, palm vein recognition is used to access ATM and banking services, and it is used for physical access of hospitals and universities [33]. The Sapporo Hospital in Japan also implemented palm vein recognition for patient authentication in the medical record system. Patients, who need to go through an operation, register their palm vein patterns prior to the operation. On the day of the operation, the palm vein is scanned from the patient and compared to the registered one to confirm the identity of the operated patient [24].

Facial Recognition: This system is the most familiar biometric method for identifying people from still photograph images of their faces or active and changing images [33]. It measures the unique patterns of a person's face by comparing and analysing facial

contours to verify the identity. The technique employs an overall analysis of the facial image and breakdown into several specific components such as the eyes, eyebrows, nose, lips, and chin. General functioning of facial recognition includes face detection, face analysis, image conversion into data and last finding the matched data [34]. Facial recognition unlike other biometric technologies, it does not require any physical contact with a device and patients can be recognized even if they are unconscious [35]. Research using Microsoft Kinect V2 sensor for patient verification demonstrated that facial features could be used and implemented for patient verification. Many Untied State healthcare organizations had already implemented facial recognition as a mean of identification to improve patient identity and health data safety. Augusta, Georgia-based University Health Care System is one of those who identify patients and retrieve relevant medical record within the organization's EHR system using photo/facial biometrics [36].

Iris Recognition: Iris is the thin circular diaphragm that lies between the cornea and lens of the human eye which is the coloured area surrounding the pupil [37]. Iris recognition is one of the most popular types of biometric technology which identifies the unique patterns of individual's iris. There are two steps in this method enrolment, and verification. In the enrolment step, a picture of the eyes is taken with both ordinary and infrared light. The photographs are then analysed by a computer and identifies more than 200 unique features which are then turned into digits called iris code that is stored in a computer database. The second step which is the verification, to check the identity, needs the eyes to be scanned then the computer will process the image and extracts the iris code and compare it with the stored data [37].The main advantages of iris scanning are the high accuracy and low chance of false positive. On the other hand, some of the disadvantages are that it can be affected by the change of the pupil size, relatively expensive method and requires proper alignment and positioning. In 2002, the University ofSouthern Alabama Medical Centre (USAMC) has developed the iris technology which became the first acute care facility to implement Iris recognition for user authentication to access the system [38]. Some technology leading companies like Google and Samsung have used iris technology in several ways. Google's data centre has been provided with iris recognition technology to verify the identity of their employees to control the access [39]. Smartphones were not away from the biometric technology where the iris recognition was available on Samsung as the first smartphone which gives users the ability to verify financial transactions with 'Selfie Pay' by iris verification. Also, iris recognition was used to unlock screen of Samsung mobile smartphone [40].

Biometric Process

The general steps and processes of how biometrics work [42; 43] is illustrated as shown in diagram 1.

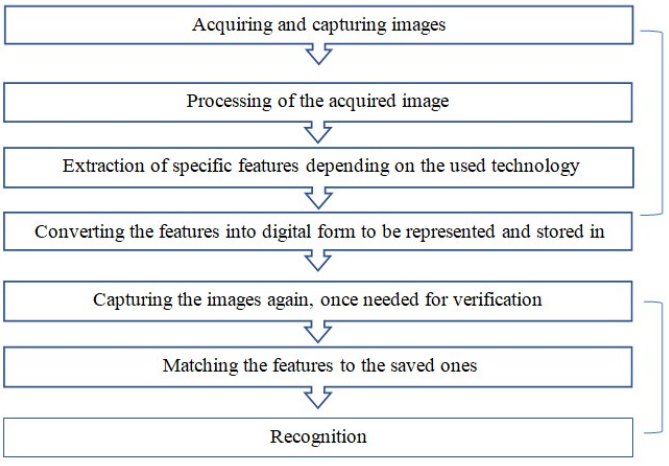

Diagram 1. Two stages, enrolment, and verification with several steps in each stage

Seven requirements' criteria to assess biometric technologies must be available to decide the suitability and to determine whether the biometric factor can be used or not [43], such requirements are:

1. Universality, biometric should be possessed by many people.
2. Uniqueness, should be unique and different for everyone.
3. Permanence, should be constant, not changed over time.
4. Collectability should be possible to collect.
5. Performance should achieve high accuracy and a low error rate.
6. Acceptability should be accepted by the public.
7. Difficult to fraud, should be difficult and costly to fool the system.

A comparison of some biometric technologies regarding the mentioned requirements are listed in Table 1. based on the reviewed literatures [13;42;44], It is noticeable that the most biometric technology that meets the requirements is fingerprint.

Table 1. Comparison of different biometrics

Biometric Technology	Fingerprint	Palm vein	Facial recognition	Iris recognition
Universality	M	M	H	H
Uniqueness	H	M	L	H
Permanence	H	M	M	H
Collectability	M	M	H	M
Performance	H	M	L	H
Acceptability	M	M	H	L
Circumventing	H	H	L	H
H: High / M: Moderate / L: Low				

A survey was done in 2018 by the Center of identity at the University of Texas at Austin showed that 58% of the participants felt very comfortable with the technology of fingerprint while 33% were happy with other forms of biometric technologies [44]. Another research [45] reported that iris has the highest level of security among the four mentioned biometric technologies followed by the fingerprint. The report also mentioned that iris is an expensive technology when compared to others.

Biometrics Advantages and Disadvantages

In summarizing several reviewed studies, [47;48; 49;50;51] regarding the advantages and disadvantages of biometric, Table 2 demonstrates the main points.

Contactless Biometrics

The National Institute of Standards and Technology (NIST) [51], reported that contactless biometric technology is expected to be in high demand due to the hygiene concern especially after the pandemic of Corona Virus COVID-19 which erupted in December 2019 in China and continued to spread all over the world resulting in high mortality rates and millions of people got infected as announced by the WHO in their daily reports. One of the advised precautions of WHO was to reduce contact and maintain high hygiene. Therefore, many countries paused the use of contact-based biometrics as precaution as the disease is known to spread through shared contact with surfaces contaminated with the virus. In Kuwait, like some other countries, employee's attendance fingerprint was halted during the pandemic, so other means of proving attendance were used. That brings the importance of contactless biometrics where reducing the number of things people need to touch is highly recommended. Many public and private organizations used contactless biometrics for authentication and identification[52]. Major International Airports such as Heathrow, Orlando, Los Angeles, and some others had witnessed significant development in touchless biometric technology [53]. According to the Market Research Report[54], it is expected that the market size of the contactless biometric technology will hit $18.6 globally by 2026 with a radically reduced time consumption for less intrusive biometric validation devices. In addition, it will lead to less rigidities and higher pleasant and satisfied staff. Contactless biometric

technologies are being adopted recently by governments around the world to act swiftly to the crisis of COVID-19. This is expected to increase the demand for contactless technologies.

Biometric in healthcare

The step of healthcare organizations toward Electronic Health Record (EHR) has motivated the need of reliable authentication system to access patient records. Biometrics such as fingerprint, face, iris, hand geometry, palm print, voice and signature are widely utilized in diverse fields by now. The health sector is not excluded from this technological breakthrough. Given that patients' medical records are frequently being accessed for better healthcare provision, there is an imperative need to adopt better form of authentication that allows secure, accurate and timely identification instead of using nonbiometric methods that have many drawbacks [18, 19]. Biometric technology adoption in healthcare is making progress within the field, as healthcare providers are pressured to reduce fraud, maintain secure and easy access to medical records, facilities, and equipment, reduce costs and to facilitate the management of confidential medical records and patients' identification. [20, 21] Biometric in healthcare is mainly used for authentication, access control, encrypting health data, identifying patients, and verifying the identity of a patient. The study [21] pointed out the main advantages of using biometrics in healthcare over other traditional security methods.

Some of which are simple user authentication, limited or controlled access rights to the health data, accurate identification for remote access to the health data, security and accessibility of the HER and health information encryption. Additionally, biometric in healthcare is more protected against medical identity theft, accountable of user operations, user-friendliness, and faster verification. The reduced registration time is considered as additional benefit of biometrics for patients and healthcare provider [19]. Biometrics also help in eliminating medical errors before a patient goes through any medical investigation. Scanning the patient's fingerprint or iris would enables healthcare staff to ensure the accurate identification of a patient before surgery or any medical

Table 2. Advantages and disadvantages of biometric technologies

	Fingerprint	Palm Vein recognition	Facial recognition	Iris
Advantages	-High Reliability - Robust - Highly Distinctive - Proven Accuracy - User Convenience - Uniqueness -Stable over time - Ease of use - Low cost - Low power consumption	- Difficult to spoof because of the need for constant flow of blood - Unique	- Efficient - High Acceptance - Ease to use - Low cost of implementation	-Uniqueness - Robust - Highly Distinctive -Widespread of iris scanners - Ease of use and flexible operating devices
Disadvantages	-Injury can affect - Dry skin can cause difficulties	- Vein pattern could change over the lifetime - Can be affected by temperature, humidity, and other factors	- Changes over lifetime - Vulnerable to manipulation by surgery - Not unique among twins -Religious or Cultural inhibitions	- High Cost - Processor is complex - Relatively new - Not accurate when wearing glasses or eye lenses -Affected with diabetes

Table 3. Applications of different biometric technologies in healthcare

Author	Country / Name of Entity	Biometric Technique	Reason of application	Main findings and impact
[57]	Kenya / Kenyatta National Hospital	Iris scan	Patient identification in routine HIV services	15457 scans were conducted. Results showed that it was feasible, acceptable and can be effectively linked to electronic medical records. 99% of patients agreed to use the technology, 86% were correctly recognized in repeated visits.
[58]	Ghana / Kintampo Health Research Centre	Fingerprint identification	To link community data with hospital data in rural areas	Total of 27662 visitors were linked to resident individuals with over 65% were successfully identified and linked
[59]	USA / University of Pittsburgh Medical Center	Fingerprint	To reduce patient registration time, reduce fraud, and reduce duplicate medical records	More than 50,000 patients participated. Most patients were eager to use the solution due to convenience and security reasons. better maintenance of consistent care
[60]	Viet Nam / National institute of Hygiene and Epidemiology	Fingerprint recognition	To verify patient identity and avoid misclassification for vaccine trial of cholera disease	153 volunteers were involved, study showed that the fingerprint technology was easy to use and proved that it can be effectively used in vaccine trial. Also, some fear of abusing their fingerprints was reported
[61]	Papua New Guinea /New Tribes Mission Medical Clinic	Fingerprint and photo	To identify patients seeking healthcare who cannot sign their name or if names change overtime	The system dramatically reduced the time required for accurate identification of patients
[62,25]	Turkey / Turkish National health system – Social Security institution	Palm vein authentication	To increase the efficiency of healthcare system and provide simpler access to healthcare facilities and prevent billing fraud	More than 10.000 units were used. Resulted in fast registration process, highly secured authentication, high user acceptance
[63]	USA / Mount Sina Hospital, a member of Hospital Insurance Company (HIC)	Palm Vein recognition	To ensure positive patient identification for radiation oncology	Reduced the number of medical errors to zero. Also, it led other hospitals within the HIC program to plan for expanding the use of the technology in emergency departments.
[64]	USA / Harris Health system in multiple hospitals	Palm Vein recognition	To avoid confusion of patient medical records	Helped in identifying people who intentionally presented wrong identification also in patients who were too injured to identify themselves

procedures. Besides, having a biometric system support would assist in identifying many of the anonymous patients in the emergency unit [22]. Biometrics have undoubtedly great potentials in healthcare by improving the information security, having impact in cost reductions, improved accessibility, and increased quality of care [23]. The fingerprint authentication is currently used for patient registration in the U.S. to help reduce medical errors and solve the problem of patient misidentification. Biometric authentication was implemented at patient registration locations to increase productivity and improve patient satisfaction. In traditional patient registration, the patient would provide identity proof and insurance via multipledocuments which is tiring and time-consuming system.Therefore, this traditional process was replaced at many of the registration counterswith an advanced biometricsystem for authentication that streamlined the patient check-in procedure. In the registration process, patients would simply provide their name and date of birth and would then place their registered fingerprint on the sensor to prove their identity. Consequently, this solution confirms that the patient is linked to his/her medical record, thus correct insurance information can be assured, and the proper care can be delivered [24]. Biometric technologies are spreading continuously in new application areas. One of these areas is healthcare. Many healthcare entities have applied some biometric means, some of which were reviewed and listed in Table 3. As of early 2011 only three healthcare systems have implemented a biometric system to aid in the identification of patients. The first was BayCare Health System in Tampa, Florida, second is the Carolinas HealthCare System in Charlotte, North Carolina and the third is ValleyCare HealthCare System in Pleasanton, California. In 2012 Broadlawns Medical Center in Iowa started using a biometric system [55].

Conventional identification processes are not reliable any more due to the human errors during registration and dishonest patients who present wrong or fake identity. Therefore, the BayCare Health System in Tampa, Florida had implemented biometric technologies such as vein recognition to help in the patient identification process at registration [56]. Several reviewed literatures revealed that biometric technologies are increasingly being used to identify patients in the US. An example of biometric implementation in healthcare is the Palm vein authentication that was implemented in Carolinas HealthCare System (CHS) in the United States [24] which accurately register patient information and confirm that the appropriate medical treatment is provided to the correct person, while also providing privacy and saving medical records from identity theft and insurance fraud. More than 1000 medical staff in the Royal Hampshire County Hospital in the United States need daily access for up to 15 different healthcare applications. These staff members had to memorize every unique combination for logging into the different applications. Introducing biometrics for authentication had saved their time without the need to remember passwords. The staff only needed to log in once to complete their regular activities [18].

CONCLUSION

This research would make contribution in relation to solutions for patient identification methods within the healthcare sector, by expanding the knowledge base of biometric technology as an identification system that have been used in healthcare sector worldwide. The lack of adopting operational principles and the limitation in processes and technologies has resulted in inaccurate patient identification. Missing patient's information and absence of their medical history has resulted in many incidents. Due to that, a secure and reliable system is needed to capture, store, and retrieve relevant patient data. The reliability depends on how to verify or identify a patient. Therefore, introducing reliable technological methods beside human involvement in patient registration that optimize accurate patient identification is essential to assure the identity of the patient being treated. Hence, biometric technologies could be a choice of identification. Biometric technologies are growing and spreading in many different areas and are widely used in our daily life. However, in healthcare, biometrics are not yet being highly adopted as in other sectors. Optimizing accurate patient identification using technological approaches such as biometrics are necessary to reduce the occurrence of patient's misidentification in hospitals. The most advantage of biometrics is that they are always carried with the individual because it is one of the unique characteristics within his body that is not vulnerable to loss or obliviousness. Despite some limitations as in any technology, most of the sites where biometrics were implemented or tested, showed public acceptance, and expected more improvement and feasibility regarding patient registration and identification. Biometric technologies can be supportive mechanism to mitigate the limitations of other identification methods. In healthcare, biometrics are expected to grow further in the coming years. There are several factors not covered in this research, need to be considered prior to implementing such technology such as the accuracy, security, privacy, and cost of biometric technology. Nowadays, biometric technologies have been improved in a way that it can provide increased accuracy with less price. Biometrics are being used for many high secure identification and personal verification solutions. Recent developments in biometric made it possible for fast, easy, and more accurate verification with cost savings. Biometric technology can add operational competence to the healthcare sector by increasing patient satisfaction when reducing medical errors and reduce expenses and fraud.

REFERENCES

Imprivata. 2015. Improving patient care with positive patient identification. Retrieved from https://healthsystemcio.com/whitepapers/PatientSecure-WhitePaper-Imprivata.pdf

Joint Commission International [JCI]. (n.d). International patient safety goals. Retrieved from https://www.jointcommissioninternational.org/en/standards/international-patient-safety-goals/

Kelly, S. (2016). The patient misidentification crisis. Retrieved from https://www.hcinnovationgroup.com/clinical-it/article/13007940/the-patient-misidentification-crisis

World Health Organization (WHO). (2007). Patient safety solutions. Retrieved from https://www.who.int/patientsafety/solutions/patientsafety/PS-Solution2.pdf

Riplinger, L., Piera-Jiménez, J., & Dooling, J. P. (2020). Patient identification techniques–approaches, implications, and findings. *Yearbook of Medical Informatics, 29*(1), 81-86. https://doi.org/10.1055/s-0040-1701984

Rudin, R. S., Hillestad, R., Ridgely, M. S., Qureshi, N. S., & Davis, J. S. (2019). Defining and evaluating patient-empowered approaches to improving record matching. *Rand Health Corporation, 8*(3), 3. https://doi.org/10.7249/rr2275

Emergency Care Research Institute (ECRI). (2016). Patient Identification Errors. *Health Technology Assesmsment Information Services, special report.* Retrieved from https://www.ecri.org/Resources/HIT/Patient%20ID/Patient_Identification_Evidence_Based_Literature_final.pdf

Mordini, E., & Ottolini, C. (2007). Body identification, biometrics and medicine: ethical and social considerations. *Annali-Istituto Superiore di Sanita, 43*(1), 51-60. https://www.researchgate.net/profile/Emilio-Mordini/publication/6300222_Body_identification_biometrics_and_medicine_Ethical_and_social_considerations/links/59ca2a2daca272bb0507572a/Body-identification-biometrics-and-medicine-Ethical-and-social-considerations.pdf

Jeon, B., Jeong, B., Jee, S., Huang, Y., Kim, Y., Park, G. H., Kim, J., Wufuer, M., Jin, X., Kim, S. W., & Choi, T. H. (2019).. A facial recognition mobile app for patient safety and biometric identification: design, development, and validation. *JMIR:Journal of Medical Internet Research. mHealth and uHealth, 7*(4), e11472. https://doi.org/10.2196/11472

Sayed, M., & Jradi, F. (2014). Biometrics: effectiveness and applications within the blended learning environment. *Computer Engineering and Intelligent Systems, 5*(5). https://www.iiste.org/Journals/index.php/CEIS/article/view/12806/13126

Ulicny, B., Brainovich, M., DeCaro, T., Furbee, J., Koder, R., McCloskey, L., . . . Hixenbaugh, J. (2017). *Risks and*

opportunities of contactless biometrics. Retrieved from https://www.researchgate.net/publication/339052601_Risks_and_Opportunities_of_Contactless_Biometrics_2017_Public_Private_Analytic_Exchange_Program

THALES. (2021). Biometrics: definition, use cases and latest news. Retrieved from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

Mali, K., & Bhattacharya, S. (2013). Comparative study of different biometric features.*International Journal of Advent Research in Computer and Electronics.* 2(7).

Cuthbertson, A. (2019). China Invents Super Surveillance Camera That Can Spot Your Face from a Crowd of Thousands. Retrieved from https://www.independent.co.uk/service/contact-us-759589.html

Al-Alawi, A. I., Al-Faresi, R. K. E., & Abdel-Razek, R. H. (2016). Evaluating the Effectiveness of Biometric Technologies in Controlling the Border Ports of the State of Kuwait. *Journal of E-Government Studies and Best Practices, 2016*, 1-20. https://doi.org/10.5171/2016.542264

Atanasiu, A., & Mihailescu, M. I. (2010). *Biometric passports (ePassports).* Paper presented at the 2010 8th International conference on communications. https://doi.org/10.1109/iccomm.2010.5509095

Government Accountability Office. (2017). Dod biometrics and forensics *Progress made in establishing long-term deployable capabilities, but further actions are needed.* Retrieved from https://www.gao.gov/assets/690/687207.pdf

Gold, S. (2010). Healthcare biometrics—defending patients and their data. *Biometric Technology Today, 2010*(7), 9-11. https://doi.org/10.1016/s0969-4765(10)70145-4

Ogbodo, I. (2020). Exploring access to ehr by emergency patients using multimodal biometrics. *International Journal of Latest Technology in Engineering, Management & Applied Science, IX*(IV), 44-50. https://www.researchgate.net/profile/Ifeoma-Ogbodo/publication/341294524_Exploring_Access_to_EHR_by_Emergency_Patients_Using_Multimodal_Biometrics/links/5eb96f8c92851cd50da96c0d/Exploring-Access-to-EHR-by-Emergency-Patients-Using-Multimodal-Biometrics.pdf

Marohn, D. (2006). Biometrics in healthcare. *Biometric Technology Today, 14*(9), 9-11. https://doi.org/10.1016/s0969-4765 (06) 70592-6

Zuniga, A. E. F., Win, K. T., & Susilo, W. (2010). Biometrics for electronic health records. *Journal of Medical Systems,* 34(5), 975-983. https://doi.org/10.1007/s10916-009-9313-6

Messmer, E. (2004). Healthcare looks to biometrics. Retrieved from https://www.networkworld.com/article/2327706/healthcare-looks-to-biometrics.html

Chandra, A., Durand, R., & Weaver, S. (2008). The uses and potential of biometrics in health care: Are consumers and providers ready for it? *International Journal of Pharmaceutical and Healthcare Marketing, 2*(1), 22-34. https://doi.org/10.1108/17506 1208108 65406

Biometric Update. (2017). Biometrics in Healthcare. Retrieved from https://www.biometricupdate.com/wp-content/uploads/2017/04 /special-report-global-biometric-healthcare.pdf

Uhl, A., Busch, C., Marcel, S., & Veldhuis, R. (2020). *Handbook of vascular biometrics*: Springer Nature. https://doi.org/10.1007/978-3-030-27731-4

Yun, Y.W., (2002) "The '123' of Biometric Technology." Biometrics Working Group of Security & Privacy Standards Technical Committee, 80 - 96, retrieved from pdfs.semanticscholar.org/b2f5/39d1face23a018b8e2824a898a8fee3ac77c.pdf.

Storisteanu, D. M. L., Norman, T. L., Grigore, A., & Norman, T. L. (2015). Biometric fingerprint system to enable rapid and accurate identification of beneficiaries. *Global Health: Science and Practice, 3*(1), 135-137. https://doi.org/10.9745/ghsp-d-15-00010

Seidlein, L., Vu, D. T., Dang, D. A., Do, G. C., Puri, M., Gupta, V., Park, J. K., Ali, M., Deen, J., Lopez, A. L., Shin, S. H., & Clemens, J. (2007). Using a fingerprint recognition system in a vaccine trial to avoid misclassification. *Bulletin of the World Health Organization*, *85*(1), 64-67. https://doi.org/10.2471/BLT.06.031070

Wall, K. M., Kilembe, W., Inambao, M., Chen, Y. N., Mchoongo, M., Kimaru, L., . . . Fulton, T. R. (2015). Implementation of an electronic fingerprint-linked data collection system: a feasibility and acceptability study among Zambian female sex workers. *Globalization and Health, 11*(1), 1-11. https://doi.org/10.1186/s12992-015-0114-z

Harichund, C., Haripersad, K., & Ramjee, G. (2013). Participant verification: prevention of co-enrolment in clinical trials in South Africa. *SAMJ: South African Medical Journal, 103*(7), 491-493. https://doi.org/10.7196/samj.6674

Rowe, R. K., Nixon, K. A., & Butler, P. W. (2008). Multispectral fingerprint image acquisition. In *Advances in Biometrics* (pp. 3-23). London: Springer. https://doi.org/10.1007/978-1-84628-921-7_1

Manimekalai, S. (2014). A study on biometric for single sign on health care security system. *International Journal of Computer Science and Mobile Computing, 3*(6), 79-87.

Jaiswal, S., Bhadauria, S. S., & Jadon, R. S. (2011). Biometric: case study. *Journal of Global Research in Computer Science, 2*(10), 19-48.

Panda Security. (2019). The complete guide to facial recognition technology. https://www.pandasecurity.com/en/mediacenter/panda-security/facial-recognition-technology/

Silverstein, E., & Snyder, M. (2017). Implementation of facial recognition with Microsoft Kinect v2 sensor for patient verification. *Medical physics, 44*(6), 2391-2399. https://doi.org/10.1002/mp.12241

Cidon, D. (2018). Making IT better: how biometrics can cure healthcare. *Biometric Technology Today, 2018*(7), 5-8. https://doi.org/10.1016/s0969-4765(18)30094-8

Mir, A., Rubab, S., & Jhat, Z. (2011). Biometrics verification: a literature survey. *International Journal of Computing and ICT Research, 5*(2), 67-80.

Mogli, G. (2012). Role of Biometrics in healthcare privacy and security management system. *Sri Lanka Journal of Bio-Medical Informatics, 2*(4), 156-165. https://doi.org/10.4038/sljbmi.v2i4.2245

Google Workspace (2013). Security and data protection in a Google data center. Retrieved from https://www.youtube.com/watch?v=cLory3qLoY8

Lee, J. (2017). Samsung Galaxy S8 to feature Princeton Identity iris technology for Mastercard selfie pay. Retrieved from https://www.biometricupdate.com/201703/samsung-galaxy-s8-to-feature-princeton-identity-iris-technology-for-mastercard-selfie-pay

Segun, O. F., & Olawale, F. B. (2017). Healthcare data breaches: Biometric technology to the rescue. *International Research Journal of Engineering and Technology, 4*(11), 946-950.

Sinha, G. R. (2019). *Advances in Biometrics*: Springer, Cham. https://doi.org/10.1007/978-3-030-30436-2

Jain, A. K., Bolle, R., & Pankanti, S. (2006). *Biometrics: personal identification in networked society* (Vol. 479): Springer Science & Business Media.https://doi.org/10.1007/978-0-387-32659-7

Joy, K. (2019). Biometrics in healthcare: How it keeps patients and data safe. Retrieved from https://healthtechmagazine.net/article/2019/12/biometrics-healthcare-how-it-keeps-patients-and-data-safe-perfcon

Shaheed, K., Liu, H., Yang, G., Qureshi, I., Gou, J., & Yin, Y. (2018). A systematic review of finger vein recognition techniques. *Information, 9*(213), https://doi.org/10.3390/info9090213

Arunkumar, C., & Deepanayaki, M. (2018). Pros & Cons of Various Bio-Metric Authentication Systems *International Journal of Scientific & Engineering Research, 9*(4), 104-108. https://www.ijser.org/researchpaper/Pros-Cons-of-Various-Bio-Metric-Authentication-Systems.pdf

Kavitha, S., & Sripriya, P. (2018). A review on palm vein biometrics. International *Journal of Engineering and. Technology,* 7, 407-409. https://doi.org/10.14419/ijet.v7i3.6.16013

Alsaadi, I., (2015) "physiological biometric authentication systems, advantages, disadvantages and future development: a review".

International journal of scientific & technology research, vol 4 (12). ISSN 2277-8616

Kumar, S., & Walia, E. (2011). Analysis of various biometric techniques. *International Journal of Computer Science and Information Technologies, 2*(4), 1595-1597. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.227.7148&rep=rep1&type=pdf

Das, R. (2016). Vein Pattern Recognition. Retrieved from https://resources.infosecinstitute.com/topic/newest-biometric-technology-vein-pattern-recognition/

National Institute of Standards and Technology (NIST). (2020). NIST study measures performance accuracy of contactless finger printing tech. Retrieved from https://www.nist.gov/news-events/news/2020/05/nist-study-measures-performance-accuracy-contactless-fingerprinting-tech

Murad, M. (2020). Epidemics like coronavirus are putting a spotlight on contactless biometrics. Retrieved from https://www.biometricupdate.com/202002/epidemics-like-coronavirus-are-putting-a-spotlight-on-contactless-biometrics

Stickland, J. (2020). Covid-19: Contactless biometrics in the spotlight. Retrieved from https://www.biometricupdate.com/202005/covid-19-contactless-biometrics-in-the-spotlight

KbvResearch. (2020). Contactless biometrics technology market size. Retrieved from https://www.kbvresearch.com/contactless-biometrics-technology-market/

Hansen, N. (2012). Palm scanners enhance patient safety. Iowa's Broadlawns Medical Center integrated the biometric system with its registration process. *Health Manage Technology. 2012* Aug;33(8):12. PMID: 22946211

Mag, H. (2010). Biometric technology verifies patients' identity. Retrieved from https://www.hcinnovationgroup.com/home/article/13002101/biometric-technology-verifies-patients-identity

Gimbel, E. (2019). How biometric technologies improve healthcare operations. https://healthtechmagazine.net/article/2019/12/how-biometric-technologies-improve-healthcare-operations

SonLa Study Group. Using a fingerprint recognition system in a vaccine trial to avoid misclassification. Bull World Health Organ. 2007 Jan;85(1):64-7. doi: 10.2471/blt.06.031070. PMID: 17242760; PMCID: PMC2636211.

Fulcrum Biometrics. (2021). Biometric ID system helps clinic in new guinea efficiently manage services and medical records. Retrieved fromhttps://www.fulcrumbiometrics.com/v/vspfiles/assets/images/downloads/fulcrum_new_tribes_case_study.pdf

Bengs, T. (2012). Case study: Healthcare in Turkey. An increase in efficiency in healthcare through process optimization and the use of robust, forgery-proof authentication systems.

Slisz, R. (2017). HIC hospitals reduce medical errors with new palm-vein scanning initiative.

White, E. B., Meyer, A. J., Ggita, J. M., Babirye, D., Mark, D., Ayakaka, I., . . . Davis, J. L. (2018). Feasibility, acceptability, and adoption of digital fingerprinting during contact investigation for tuberculosis in Kampala, Uganda: a parallel-convergent mixed-methods analysis. Journal of Medical Internet Research, 20(11), e11541. https://doi.org/10.2196/11541

Anne, N., Dunbar, M. D., Abuna, F., Simpson, P., Macharia, P., Betz, B., . . . Carey, F. (2020). Feasibility and acceptability of an iris biometric system for unique patient identification in routine HIV services in Kenya. *International Journal of Medical Informatics, 133*, 104006. https://doi.org/10.1016/j.ijmedinf.2019.104006

Odei-Lartey, E. O., Boateng, D., Danso, S., Kwarteng, A., Abokyi, L., Amenga-Etego, S., . . . Owusu-Agyei, S. (2016). The application of a biometric identification technique for linking community and hospital data in rural Ghana. *Global Health Action, 9*(1), 29854. https://doi.org/10.3402/gha.v9.29854

****