2022

Identification and Security Implications of Biometrics

Kathryn Boggs

Eastern Kentucky University

Recommended Citation

Boggs, Kathryn, "Identification and Security Implications of Biometrics" (2022). *Online Theses and Dissertations*. 688.
https://encompass.eku.edu/etd/688

IDENTIFICATION AND SECURITY IMPLICATIONS OF BIOMETRICS

BY

KATHRYN BOGGS

THESIS APPROVED:

____
Chair, Advisory Committee

VCalles
____
Member, Advisory Committee

____
Member, Advisory Committee

Ry K. Baggett
____
Dean, Graduate School

STATEMENT OF PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a Master of Science degree at Eastern Kentucky University, I agree that the Library shall make it available to borrowers under rules of the Library. Brief quotations from this document are allowable without special permission, provided that accurate acknowledgements of the source are made. Permission for extensive quotation from or reproduction of this document may be granted by my major professor. In [his/her] absence, by the Head of Interlibrary Services when, in the opinion of either, the proposed use of the material is for scholarly purposes. Any copying or use of the material in this document for financial gain shall not be allowed without my written permission.

Signature:

Kathryn Boggs

Kathryn Boggs

Date: 10/24/2022

IDENTIFICATION AND SECURITY IMPLICATIONS OF BIOMETRICS

BY

KATHRYN BOGGS

Submitted to the Faculty of the Graduate School of
Eastern Kentucky University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

2022

ACKNOWLEDGEMENTS

Thank you to the wonderful academics that participated in the completion of this thesis, Dr. Kristie Blevins, Ph.D., Dr. Victoria Collins, Ph.D., and Dr. Bill McClanahan, Ph.D., of Eastern Kentucky University, and Dr. Dennis Rodriguez, Ph.D., of Indiana University South Bend.

ABSTRACT

The usage of biometrics has become more frequent over the past couple of decades, notably due to technological advancements. Evolving technology in the field of biometrics has also led to increased accuracy of associated software, which have provided the opportunity to use a multitude of different human characteristics for identification and/or verification purposes. The current study assessed the usage of biometrics in casinos, hospitals, and law enforcement agencies using a survey methodology. Results indicated that privacy concerns related to the use of biometrics may not be as prevalent as indicated in the literature. Additionally, results indicated that the utilization of biometrics has led to increased accuracy in identification and verification processes, led to enhanced security, and would be highly recommended to other institutions. Information obtained from the literature notes the racial bias in facial recognition technologies due to algorithmic development based solely upon features of Caucasian individuals. Efforts need to be made to create facial recognition algorithms that are more racially and ethnically diverse.

TABLE OF CONTENTS

INTRODUCTION

Biometrics refers to the physiological and behavioral characteristics of human beings that are used throughout identification and verification processes. In contemporary society, biometric technology is used daily, whether by using biometrics to unlock a smart device or laptop, using certain applications on smart devices (i.e., banking applications, fitness applications, payment applications, etc.), security systems, or while carrying out employment duties. Researchers estimate that about 5 billion people use cellular phones, and approximately 3.2 billion people use smart phones (Estrela et al., 2021). Social media websites also utilize biometric technology. Specifically, Facebook uses facial recognition technology when suggesting other people that a user should "tag" in the photo with them (Norris, 2019). Additionally, Mann and Smith (2017) note that as of 2011, Facebook had approximately 100 billion photographs in its facial recognition database, and the rate of photo obtainment was estimated to increase by 6 billion photographs a month.

Prior to conducting the current study, the use of biometrics by law enforcement was known, notably due to the publicity afforded to the usage of biometrics by law enforcement agencies. Additionally, biometrics are often used in television crime shows featuring law enforcement agencies (i.e., Bones, CSI, NCIS, etc.), but the way in which the usage of biometrics is portrayed on television is purely fictional, hence why the current study focuses on the usage of biometrics in the real world. However, the utilization of biometrics in casinos and hospitals appear less often in the media.

The significance of the current study is that it concentrates on the usage of biometrics for identification and verification purposes in casinos, hospitals, and law enforcement agencies in real-life scenarios. Further, the realistic approach taken by the researcher addresses the issue highlighted in the literature maintaining that much of the research conducted on the topic of biometrics takes place in ideal conditions (Yang et al., 2019), often in a controlled environment that is less susceptible to outside influences.

Technology associated with biometrics has become increasingly advanced throughout the twenty-first century and is expected to increase in complexity throughout future years. However, as technology exponentially gains sophistication, the use of biometrics has raised some privacy concerns regarding how biometric data is stored and used by corporations and governmental entities.

The next section of this paper presents a literature review that conveys information regarding the various types of biometric characteristics, how they are classified, and how they are and can be used for identification purposes. Further, types of biometric systems and technologies and the associated modes of operation for identification and verification purposes are mentioned. Also noted is the utilization of biometrics on domestic and international levels and how biometrics are used by various institutions. The last portion of the literature review includes the research questions that the present study was based upon. Afterwards, there is a brief overview of the current study that describes the purpose of the study, followed by the methodology that details how the research was conducted. The following section presents the obtained results, which are subsequently interpreted in the discussion section, which also includes study limitations, implications for future research, and concluding remarks.

REVIEW OF THE LITERATURE

A literature review was conducted on the topic of biometrics to identify what types of biometric characteristics exist and how they are used for identification and security purposes. The literature review begins by defining what biometric characteristics are and how they are categorized, followed by a listing of biometric characteristics noted in the literature as traits that can be used for biometric identification. The biometric characteristics portion of the literature review also describes the types of requirements deemed necessary for use in processes of biometric identification and verification, with examples of how biometric characteristics are applied in different situations. Once biometric characteristics have been explained, the types of biometric systems are noted, followed by the modes of operation that differ between identification and verification tasks, and systems that differ by the number of biometric characteristics used for identification or verification purposes. Afterwards, system errors, vulnerabilities, and security measures are noted. Next the literature review illustrates the utilization of biometrics in contemporary times on a domestic and international basis, notably via information databases, law enforcement purposes, casinos, and cross-border travel. The final section of the literature review presents the research questions that the current study was based upon.

Biometric Characteristics

Biometric characteristics are frequently utilized to aid in processes of human identification and verification, as well as for enhancing security measures. For the purposes of this study, biometric characteristics identified in the literature are categorized in three different ways: (1) behavioral biometric characteristics, (2) physiological biometric characteristics, and (3) soft biometric characteristics. Physiological biometric characteristics are also referred to as “static” biometric characteristics because physiological traits usually do not change very much over time, and behavioral biometric characteristics are referred to as “dynamic” biometric characteristics because behavioral traits are more susceptible to change over the course of an individual’s life (Khan et al., 2020; Kopczewski & Smal, 2017). Biometric characteristics can also be categorized as “extrinsic”, meaning that the biometric trait is externally visible, existing outside of the body, and is susceptible to environmental factors, and “intrinsic”, meaning that the biometric traits are not externally visible and are better protected from environmental factors by existing within the human body (Alay & Al-Baity, 2020; Khan et al., 2020).

Behavioral biometric characteristics include gait (walking gait), keystroke dynamics, signature dynamics, and voice. Physiological biometric characteristics include body odor, deoxyribonucleic acid (DNA), ears, eyes, face, fingerprints, foot dynamics, hands, metabolic attributes, nails, neural analysis (neurological signals given off by neurons firing in the brain, analyzed using electroencephalography (EEG) and functional magnetic resonance imaging (fMRI), palm prints, skin patterns, smell, tongue, and vein patterns. Soft biometric characteristics consist of marks (birthmarks, freckles, moles), scars, and tattoos. (See Appendix A for biometric characteristic references).

Biometric characteristics are expected to adhere to four main requirements to be considered suitable for use in identification and verification processes: collectability, permanence, distinctiveness (uniqueness), and universality. The first requirement, collectability, dictates that a biometric characteristic must be able to be collected and measured in a quantitative manner (Asha & Chellappan, 2012; Blasco & Peris-Lopez, 2018; Dahia et al., 2020; Dantcheva et al., 2015; Jain & Kumar, 2010; Keyser et al., 2021; Khan et al., 2020; Mason et al., 2020; Moolla et al., 2021; Mordini & Massari, 2008; North-Samardzic, 2020; Pisani et al., 2019; Sanjekar & Patil, 2013; Yang et al., 2021). For example, a scanning algorithm is used to identify five specific features of the iris: (1) connective tissue strips; (2) circles; (3) signs; (4) freckles; and (5) crown. Additionally, the 266 patterns that can be found in the iris are simply the connective tissue strips that illustrate radial divisions within the iris and form such patterns (Aron & Manea, 2014).

The second requirement, permanence, mandates that a biometric characteristic must remain stable over time, meaning that it does not change (Asha & Chellappan, 2012; Blasco & Peris-Lopez, 2018; Dahia et al., 2020; Dantcheva et al., 2015; Jain & Kumar, 2010; Keyser et al., 2021; Khan et al., 2020; Mason et al., 2020; Moolla et al., 2021; Mordini & Massari, 2008; North-Samardzic, 2020; Pisani et al., 2019; Sanjekar & Patil, 2013; Yang et al., 2021). For example, the iris of the eye forms before birth, and the 266 patterns contained within the iris do not change over the course of a person's life (Ammour et al., 2020; Aron & Manea, 2014), which fulfils the permanence requirement.

The third requirement, distinctiveness (also referred to as uniqueness), requires that a biometric characteristic identified in one individual must not occur in another individual, meaning that no two people can have the exact same biometric characteristic (Asha & Chellappan, 2012; Blasco & Peris-Lopez, 2018; Dahia et al., 2020; Dantcheva et al., 2015; Jain & Kumar, 2010; Keyser et al., 2021; Khan et al., 2021; Mason et al., 2020; Moolla et al., 2021; Mordini & Massari, 2008; North-Samardzic, 2020; Pisani et al., 2019; Sanjekar & Patil, 2013; Yang et al., 2021). For example, the 266 different patterns found in the iris of the eye are unique to every individual, even between identical twins, who share 100% of their DNA (Aron & Manea, 2014; Gomez, 2019). Of note, identical twins also have different fingerprints (Dahia et al., 2020; Yang et al., 2021), finger-vein patterns (Yang et al., 2021), palm prints (Liu et al., 2015), and tongue patterns (Sivakumar et al., 2018).

The fourth requirement, universality, states that a biometric characteristic should be possessed by most, if not all, individuals (Asha & Chellappan, 2012; Blasco & Peris-Lopez, 2018; Dahia et al., 2020; Dantcheva et al., 2015; Jain & Kumar, 2010; Keyser et al., 2021; Khan et al., 2021; Mason et al., 2020; Moolla et al., 2021; Mordini & Massari, 2008; North-Samardzic, 2020; Pisani et al., 2019; Sanjekar & Patil, 2013; Yang et al., 2021). For example, most human beings have eyes, and the iris exists within each eye, hence it meets the requirement for being applicable to essentially all individuals.

One well-known application of biometrics is the use of facial recognition software and technology. Facial recognition processes utilize the spatial relationships of facial features such as the eyes, nose, lips, chin, and the appearance of the face (Jain & Kumar, 2010). Spatial relationships of the face are discerned by how far apart a person's eyes are, the appearance of their cheek bones, the appearance of their jaw line, and the appearance of their chin (Tot et al., 2021). The accuracy of facial recognition is affected by factors such as age, facial expression, disease, weather conditions, the intensity of light, and the angle of the sensor (Wlodarczyk, 2012). All facial recognition systems operate using algorithms created to be representative of a specific face (Mann & Smith, 2017), and there are different algorithms utilized in identification and verification processes (Jacquet & Champod, 2020).

Facial recognition algorithms are less accurate when used to identify people of ethnic or racial minority status, especially for African American women (The PEW Charitable Trusts, 2020). The Congressional Research Service (2020) reported concurring results, noting that individuals of Asian and African American descent experience a higher false-positive rate during facial recognition processes. The disparities in facial recognition accuracy are attributed to the methods of facial recognition algorithm development. Most of the facial recognition algorithms currently used were developed and tested based on the demographic traits of Caucasian individuals, which are subsequently less accurate when utilized for identifying persons of differing races and ethnicities (Congressional Research Service, 2020; Jacquet & Champod, 2020; Keyser et al., 2021).

A study regarding the security of facial recognition applications on smartphones was conducted by Galterio et al. (2018) using both IOS (Apple) and Android devices. Five applications were selected for examination: (1) FaceLock (Eigenface software; Android devices only); (2) AppLock (Face metric software; Android devices only); (3) Luxand Face Recognition (Face metric software; Android and IOS devices); (4) True Key (Eigenface software; Android and IOS devices); and (5) BioID Facial Recognition (Face metric software; IOS devices only). While all of the applications are used for facial recognition to unlock devices, the Luxand Face Recognition application creates a facial recognition database which sets it apart from the other four applications. The authors concluded that the Luxand Facial Recognition application was the most secure for device security. Further, study results indicate that applications used for facial recognition on IOS devices are more secure than applications used for facial recognition on Android devices because facial recognition applications for Android were spoofed using a printed picture instead of an actual person, but IOS applications were not spoofed when presented with a printed picture (Galterio et al., 2018). Jeon, Jeong, Jee, Huang, Kim, Park, Kim, Wufuer, Jin, Kim, and Choi (2019), developed an Android-based mobile facial recognition application for use in hospital settings. While CT scans can be used for facial recognition and have a higher resolution, the mobile application exhibited 99.99% accuracy in patient verification (Jeon et al., 2019).

While facial recognition technology is relatively new dating back to the 1960s and 1970s (Norris, 2019), fingerprints are considered the oldest biometric characteristic used for identification, potentially dating back to the Babylonian period in 500 B.C. (Wlodarczyk, 2012). Each fingerprint has ridges, called minutiae points, that are unique to every individual and are used in the process of fingerprint recognition. Additionally, fingerprints are identifiable via examination of the papillary lines, the friction ridges of the fingers, which are classified into three categories: arch, beliefs, and loop (Aron & Manea, 2014). The fingerprint recognition process is categorized in three different ways: (1) minutiae-based; (2) non-minutiae-based; and (3) hybrid systems, which combine minutiae-based and non-minutiae-based characteristics (Kour et al., 2016). Fingerprints are one of the four types of friction ridge impressions, which also consist of footprints, palm prints, and toe prints (Meagher et al., 2014).

In addition to being one of the oldest methods, fingerprint recognition remains one of the most frequently used methods of biometric identification (Appati et al., 2015; Center for Global Development, 2021; Ceyhan, 2008). Automated Fingerprint Identification Systems (AFIS) were introduced into law enforcement practices in the 1960s (Jain et al., 2004). There are various types of fingerprint sensors that can be utilized for conducting fingerprint recognition, including: (1) optical fingerprint sensors, which examine fingerprints based upon the reflectance and/or transmittance of light; (2) capacitive fingerprint sensors, which measure the difference in capacity between a sensor plate and a finger; (3) thermal fingerprint readers, which operate through the use of a pyrodetector as a heat-sensitive element that measures temperature differences between the papillary lines of a finger; and (4) ultrasonic fingerprint readers, which evaluate fingerprints by transmitting an ultrasonic signal to the fingerprint which then reflects and deforms the ultrasonic wave, subsequently providing a distinct ultrasonic wave that can be analyzed (Adámek et al., 2015; Lalović & Bogdanoski, 2021; Langenderfer & Linnhoff, 2005; Moradoff, 2010).

Fingerprint recognition systems are vulnerable to error based upon distortion by factors such as the pressure of a finger on a fingerprint scanner, a rotated fingerprint, and having dirt and/or moisture on the finger being used in the fingerprint recognition process (Iloanusi & Ezema, 2017). Individuals with certain medical conditions such as leprosy and eczema can lose the ridge patterns on their fingers, and therefore such individuals cannot always be reliably identified using fingerprints (The PEW Charitable Trusts, 2020). In an experimental study, Tu, Yao, Zu, Liu, and Zhang (2020), proposed the usage of a fingerprint restoration algorithm based on a cubic Beizer curve, which is a parametric curve defined by four points, that was shown to be successful in regenerating missing fingerprint attributes (Tu et al., 2020). For enhanced security, Yang, Wang, Hu, Zheng, Chaudhry, Adi, and Valli (2018), created a finger-vein based bio-cryptosystem built for smart cards to better protect biometric data. This method is supported by additional research, which asserts that finger-vein authentication systems exhibit high levels of security and low levels of error rates (Mohsin et al., 2020).

Modern technology has made it possible to use human eyes for biometric identification, notably the iris and retina, however the iris is used more frequently than the retina due to scanning times and accuracy rates (Aron & Manea, 2014). The iris is the colored portion of the eye that surrounds the pupil and is considered a highly reliable biometric characteristic as the iris forms during the neonatal period before birth (Aron & Manea, 2014; Jain & Kumar, 2010). The iris is an intrinsic biometric characteristic because it is an internal part of the body and is protected by the cornea (Department of Homeland Security, 2015). The iris is responsible for expanding and contracting the retina to account for differences in levels of light intensity (Park et al., 2011). Irises are examined by using near-infrared light which enhances the appearance of the tissue structures in the iris which form distinct patterns (Department of Homeland Security, 2015), and there are 266 different patterns identified in irises (Aron & Manes, 2014). High accuracy rates attributed to using irises as biometric characteristics are that iris recognition is not affected by different colors of eyes (Department of Homeland Security, 2015), and is minimally affected by contact lenses or changes that occur throughout the aging process (Aron & Manea, 2014). Irises are very distinctive, as iris tissue patterns are different between an individual's left and right eyes (Mason et al., 2020; Sreeja et al., 2018). Additionally, iris colors and structural tissue patterns are different between the eyes of identical twins (Aron & Manea, 2014; Sreeja et al., 2018), who share 100% of their DNA (Aron & Manea, 2014; Gomez, 2019). Iris recognition technologies debuted in the 1990s (Liu et al., 2015), which is still a relatively new type of biometric identification when compared to methods of identification such as facial recognition and fingerprint scanning.

Although blood is the most common bodily fluid collected at crime scenes due to the amount of DNA contained within it, there are other types of bodily fluids that DNA can be extracted from for purposes of human identification. Utilizing metabolite biometrics, Hair, Mathis, Brunelle, Halámková, and Halámek (2018) found that sweat can be used to positively identify individuals in a more expedient manner than using blood. Using sweat molecules to obtain DNA could potentially be easier due to its noninvasiveness. In the study conducted by Hair et al. (2018), sweat samples were obtained from 25 participants using a BAND-AID brand non-stick pad, with athletic tape and a silicone band over the top to promote sweat production. Three specific compounds were used to positively identify and differentiate between individuals based upon the chemical composition of participants' sweat: lactate, urea, and glutamate. Although this method was effective at identifying persons, it is of limited use because the molecular compounds in a person's sweat change on a day-to-day basis, hence the DNA profiles cannot be stored in a database for future identification purposes (Hair et al., 2018). Due to changes in the chemical composition of an individual's sweat every twenty-four hours, metabolic attributes do not remain stable enough to fulfill the permanence requirement.

Sivakumar, Nair, Zacharias, Nair, and Joseph (2018) proposed the usage of tongue prints as biometric characteristics used to identify and differentiate between individuals. Human tongues are unique to each individual based upon the physiologic texture and geometric outline of the tongue, and can aid in the identification process via examining unique tongue features and characteristics. It is also noted that the tongue can be used to differentiate between identical twins, which adds to the legitimacy of using this feature as a biometric identifier. Additionally, the tongue is protected by the oral cavity and therefore deemed immune to forgery. Sivakumar et al. (2018) demonstrated that the accuracy of identification through the usage of tongue prints was approximately 97.05%, and the researchers encourage the implementation of a tongue image database for use in biometric testing (Sivakumar et al., 2018). However, because the tongue is an intrinsic biometric characteristic, obtaining tongue print samples would be considered invasive and not realistically suitable for identification and verification processes.

Alphonse Bertillion is credited with introducing human ears into identification processes (Chorás, 2005; Chowdhury et al., 2018). Human ears go through a stretching process when children are young and the form of the ear stabilizes around the age of 8 and remains the same until approximately 70 years when the ear begins stretching again due to age (Abaza et al., 2013). Further, the color composition throughout the ear is more evenly distributed than in the face, iris, or retina (Chorás, 2005).

While many biometric traits are physiological, the inclusion of other features (i.e., marks, scars, and tattoos), into identification and/or verification processes enhances accuracy rates of biometric systems by providing more detailed information that is used throughout the search for the template associated with a certain individual (Asha & Chellappan, 2012), as the use of marks, scars, and tattoos in conjunction with additional biometric characteristics exhibits a high degree of distinctiveness (Dantcheva et al., 2015; Nixon et al., 2015). Some researchers assert that soft biometric traits fulfill the requirements of permanence and distinctiveness (Abdelwhab & Viriri, 2018), however, other researchers maintain that soft biometric characteristics do not fulfill the requirements of permanence and distinctiveness (Aron & Manea, 2014; Jain et al., 2004; Jain & Kumar, 2010; Langenderfer & Linnhoff, 2005). While there are differing arguments as to which requirements are met, the traits that are classified as soft biometric characteristics remain similar, consisting of marks, scars, and tattoos (Abdelwhab & Viriri, 2018; Caplova et al., 2018; Dantcheva et al., 2015; Jain & Ross, 2015; Nixon et al., 2015).

Further, using soft biometrics such as marks, scars, and tattoos is an effective method to use when identifying both living and deceased individuals. Notable benefits associated with tattoos are that their visibility is not eroded by early decomposition, and previously removed or modified tattoos can be viewed via radiographic examination (Caplova et al., 2018). Also, tattoo ink goes deep enough under the skin that the tattoo pigments can withstand severe skin burns (Jain & Ross, 2015). When there is discolored skin on a deceased person, applying hydrogen peroxide with a three-percent concentration will make the tattoo visible, however, this method will destroy the tattoo and all associated pigmentation. Upon examining tattoos with colored ink, infrared imaging was found to be useful for viewing tattoos with green and black colors, while red ink colors were not as visible (Caplova et al., 2018).

A study conducted by Sauerwein et al. (2017) focused on the effects of decomposition on biometric traits including fingers, faces, and irises. The main factor leading to decomposition was temperature, where higher temperatures in the spring and summer led to faster decomposition, and lower temperatures in the winter slowed decomposition. Overall, fingerprints were the most reliable biometric trait, remaining intact longer than irises and facial features. The spring trial showed that biometric traits were intact for an average of four days, the summer trial showed that biometric traits were intact for an average of three days, and the winter trial showed that biometric traits were intact for an average of 28 days (Sauerwein et al., 2017). Regarding the identification of both antemortem and postmortem individuals, biometric data from fingerprints, DNA, and dental records are deemed to be the most reliable (Caplova et al., 2018).

Biometric Systems

Systems and technologies identified in the literature that are utilized in biometric identification and verification processes include computerized tomography (CT) scan, electrocardiogram (ECG/EKG), electroencephalogram (EEG), eye scanners, facial recognition, fingerprint scanners, finger-vein scanners, functional magnetic resonance imaging (fMRI), magnetic resonance imaging (MRI), and palm print scanners. (See Appendix B for biometric system references).

All biometric systems are developed for purposes of either identification or verification, and biometric systems need to be tailored to their intended usage. Identification systems function via the use of a 1:N (one-to-many) matching system, whereby biometric data is compared to all users in a system, and verification systems function via the use of a 1:1 (one-to-one) matching system, whereby biometric data is compared to an identity already on file (Abdelwhab & Viriri, 2018; Ammour et al., 2020; Asha & Chellappan, 2012; Down & Sands, 2004; Kour et al., 2016; Wlodarczyk, 2012; Xiao, 2007). Biometric systems frequently operate in three phases: enrollment, template creation, and a matching process (Asha & Chellappan, 2012). Upon first interacting with a biometric system an individual goes through the process of enrollment, which is when a person's biometric data (i.e., facial image; fingerprint), are obtained and prepared for entry into a database. To begin, features are extracted from the biometric data collected to create a template that stores algorithmic representations of the individual's biometric data. Lastly, the matching process is exemplified when an individual is required to present a previously enrolled biometric characteristic to a biometric system during identification and/or verification processes to see if the individual's biometric data matches the template that was created of it (Abdelwhab & Viriri, 2018; Ammour et al., 2020; Asha & Chellappan, 2012; Blasco & Peris-Lopez, 2018; Choudhury & Rabbani, 2020; Dahia et al., 2020; Galterio et al., 2018; Jekova et al., 2018; Kausar, 2021; Langenderfer & Linnhoff, 2005; Mason et al., 2020; Mishra, 2010; Moradoff, 2010; Niculescu & Coman, 2017; Ozkaya & Sagiroglu, 2010; Petermann et al., 2006; Pisani et al., 2019; Siwicki, 2018; Wayman et al., 2005; Xiao, 2007; Yang et al., 2019; Yang et al., 2021).

There are two types of biometric systems: unimodal and multimodal. Unimodal systems use one biometric characteristic for recognition, and multimodal systems use multiple biometric characteristics for recognition (Dantcheva et al., 2020; Ryu et al., 2021). Multimodal biometric systems are often more secure, reliable, and accurate as opposed to unimodal systems due to the usage of multiple traits instead of just one (Asha & Chellappan, 2012; Down & Sands, 2004; Larbi & Taleb, 2018; Mishra, 2010; Sanjekar & Patil, 2013). However, unimodal biometric systems may be preferred in some situations because multimodal biometric systems are highly complex, user participation is more demanding, and the associated expenses are high (Bhilare et al., 2020; Ryu et al., 2021).

In preparation for using a multimodal biometric system, the biometric characteristics chosen are compiled and transformed through a process of fusion. There are five different types of fusion referenced in the biometrics literature: (1) sensor-level fusion; (2) feature-level fusion; (3) score-level fusion (also known as match-score fusion); (4) rank-level fusion; and (5) decision-level fusion.

When conducting the sensor-level fusion process, raw biometric data obtained from one or multiple sensors is collected and immediately fused together prior to the feature extraction process (Aggarwal & Jindal, 2012; Jain et al., 2006; Krishnakumari & Savitha, 2017; Larbi & Taleb, 2018; Ma et al., 2020; Mishra, 2010; Sahoo et al., 2012; Singh et al., 2019; Srivastava, 2017). Further, Sahoo et al. (2012) note three subtypes of sensor-level fusion: (1) single sensor-multiple instances; (2) intra class-multiple sensors; and (3) inter-class multiple sensors.

Feature-level fusion is conducted by obtaining biometric data from multiple sensors and features are extracted separately from each trait. Afterwards, all of the extracted features are consolidated into a single feature (Aggarwal & Jindal, 2012; Alay & Al-Baity, 2020; Jain et al., 2006; Krishnakumari & Savitha, 2017; Larbi & Taleb, 2018; Ma et al., 2020; Mishra, 2010; Ross & Jain, 2003; Sahoo et al., 2012; Singh et al., 2019; Srivastava, 2017). Researchers note the importance of making sure that the sensors used for collecting biometric data are compatible so that the features extracted are fused properly (Srivastava, 2017).

In the process of score-level fusion (also known as match-score-level fusion), matching algorithms are applied to biometric data and a match score is output for each biometric trait. The match score for each trait represents the degree of similarity between an individual's presented trait and the template created of the same trait. The match scores for each of the traits are then combined to create a single match score (Aggarwal & Jindal, 2012; Alay & Al-Baity, 2020; Jain et al., 2006; Krishnakumari & Savitha, 2017; Larbi & Taleb, 2018; Ma et al., 2020; Mishra, 2010; Ross & Jain, 2003; Sahoo et al., 2012; Singh et al., 2019; Srivastava, 2017).

Rank-level fusion is frequently used when a biometric system is operating in identification mode. Test patterns input to the system render an output of ranks applied to each identity in the database. Afterwards, the ranks output by the system are then merged to represent a unanimous rank for each identity in the database (Aggarwal & Jindal, 2012; Jain et al., 2006; Ma et al., 2020; Sahoo et al., 2012; Singh et al., 2019). Additionally, Aggarwal and Jindal (2012) mention that no normalization process needs to be applied to rank-level data because the ranks that are output by multiple biometric systems are already compatible.

Throughout the decision-level fusion process, all the presented biometric traits are pre-classified separately from one another. Afterwards, the biometric traits are collected (i.e., facial image; fingerprint), and features are extracted from each of the obtained samples. From there, based upon the features extracted from biometric traits, a decision is rendered to either accept or reject the validity of a person’s identity (Alay & Al-Baity, 2020; Jain et al., 2006; Krishnakumari & Savitha, 2017; Larbi & Taleb, 2018; Ma et al., 2020; Mishra, 2010; Ross & Jain, 2003; Singh et al., 2019; Srivastava, 2017). Furthermore, Singh et al. (2019) noted that the commonly used fusion algorithm at the decision-level is majority voting, a process in which each of the biometric traits selected for use in the multimodal system are separately analyzed and a decision is made regarding the authenticity of the individual in question. Essentially, each trait is either “accepted” meaning that the individual is who they claim to be, or “rejected” meaning that the individual is not who they claim to be. After a decision is made for each of the presented biometric traits, the majority of the “accepts” or “rejects” renders the final decision whether to accept or reject the individual’s claim of identity. For example, if three traits are used in a biometric system and two of them are accepted, the system accepts the claimed identity as valid. In contrast, if two traits are rejected then the system rejects the claimed identity as invalid.

Biometric system performance is assessed based upon system error rates. The two most common types of failure rates associated with biometric systems are false acceptance rate (FAR) and false rejection rate (FRR) (Asha & Chellappan, 2012). False acceptance rate, otherwise known as a type-II error, refers to the number of times a user who should be rejected is accepted by the system (Appati et al., 2021; Baig & Eskeland, 2021; Dahia et al., 2020; Down & Sands, 2004; Lagou & Chondrokoukis, 2011; Mann & Smith, 2017; Yang et al., 2021). False rejection rate, otherwise referred to as a type-I error, refers to the number of times a user who should be accepted by the system is rejected (Appati et al., 2021; Baig & Eskeland, 2021; Dahia et al., 2020; Down &

Sands, 2004; Lagou & Chondrokoukis, 2011; Mann & Smith, 2017; Yang et al., 2021). Because the FAR and FRR have an inverse relationship, the FAR should increase while FRR decreases, or vice versa (Down & Sands, 2004; Yang et al., 2021). If the FAR and the FRR have the same value, it is referred to as the equal error rate (EER), or crossover rate (Down & Sands, 2004; Yang et al., 2021). Biometric identification and verification systems are not 100% accurate because they are based on algorithms that represent specific biometric characteristics which are stored as templates in a biometric system (Mann & Smith, 2017). Generally, the recognition accuracy is dependent upon the image quality and matching algorithms (Yang et al., 2019).

Biometric systems are vulnerable to spoofing attacks, where an illegitimate user presents a false biometric characteristic in effort to convince the system that the user is legitimate (Lagou & Chondrokoukis, 2011; Xiao, 2007). For example, fingerprints can be spoofed by using materials such as gelatin, granulated plastic, latex, modeling clay, Play-Doh, and silicone (Adámek et al., 2015; Salvi et al., 2021; Singh & Singh, 2012). Faces can be spoofed by wearing a latex face mask or presenting a high-resolution photo of an individual's face (Salvi et al., 2021; Singh & Singh, 2012). Additionally, irises can also be spoofed by presenting a high-resolution photo of an individual's eye (Singh & Singh, 2012). One countermeasure against spoofing attacks is liveness detection, whereby a system attempts to differentiate between a live human and a material copy (Staunch et al., 2020). Liveness detection can be conducted through the usage of bodily signals such as pulse, temperature, and light reflectance (Xiao, 2007; Yang et al., 2019). An additional countermeasure against spoofing attacks is the implementation of a multimodal biometric system as using more than one biometric characteristic enhances system security (Xiao, 2007), and multimodal biometric systems are less sensitive to environmental influences (Ryu et al., 2021). An additional vulnerability of biometric systems is function creep, which describes the incidence where biometric data that was collected in one instance for a specific purpose is subsequently used for a different or unintended purpose without an individual's consent (Mann & Smith, 2017; Mordini & Massari, 2008).

Cancelable biometric systems offer enhanced security by transforming biometric templates in an irreversible way by utilizing non-invertible transformations during the enrollment process (Baig & Eskeland, 2021; Kausar et al., 2021; Mohsin et al., 2020; Yang et al., 2018; Yang et al., 2019). Biometric cryptosystems are also used to bolster security by way of creating biometric templates with cryptographic keys (Baig & Eskeland, 2021; Soltane et al., 2017; Yang et al., 2019).

Utilization of Biometrics

Biometrics are utilized on a domestic and international level. The Automated Fingerprint Identification System (AFIS) was first developed for the Federal Bureau of Investigation (FBI) in the 1960s and implemented in the 1970s based upon research conducted by the National Institute of Standards and Technology (NIST) (Eze & Chijioke, 2016). AFIS technologies are used globally in forensic and law enforcement practices (Jain & Kumar, 2010). The European Dactyloscopic System database (Eurodac) is the European Union's (EU) biometric database of fingerprints, which was created in 1997, implemented in 2002 (Ceyhan, 2008), and began operating in 2003 (Lyon, 2008). Eurodac was initially created to store fingerprints of individuals seeking asylum in a member state of the EU, was later made available to law enforcement agencies within the EU and is now utilized on an international scale (Amelung, 2021).

In contemporary travel settings, a biometric passport is now required to travel internationally (Choudhury & Rabbani, 2020). Biometric passports are based on guidelines set by the International Civil Aviation Organization (ICAO) that designate facial recognition as the international standard for usage in biometric passports, also referred to as “e-passports” (Choudhury & Rabbani, 2020; Mann & Smith, 2017). Biometrics are also utilized to increase efficiency in border crossing. At least 20 countries within the EU use Automated Border Control (ABC) systems, otherwise referred to as “biometric e-gates” (Leese, 2018). Although ABC systems may be more convenient for border crossing, an associated issue is that, for the 20 countries that use biometric e-gates, there are approximately 17 different companies that provide the equipment and technology necessary to operate ABC systems. However, each of the companies involved create systems that operate utilizing various technologies, and such a wide variety of systems and technologies are frequently incompatible and differ in accuracy and reliability (Leese, 2018).

Bank transactions can now be done using mobile applications on smart devices, which have incorporated the use of biometrics for security purposes (i.e., fingerprint scanning for account access). Banking institutions have also implemented biometric technology into regular transactions internationally, such as facial recognition, fingerprint scanning, and voice authentication (Keyser et al., 2021).

Casinos were one of the first institutions to utilize technologies associated with video surveillance for security purposes during the 1960s and 1970s. For example, Harrah's Las Vegas Hotel and Casino retains all biometric data and has information dating back to 1995 (Norris, 2019). While 24-hour surveillance is mandatory for casinos, there are currently no jurisdiction mandates for facial recognition technologies (Ma, 2016). Legislation has been passed in some states, such as Ohio, mandating that casinos are actors of the state, subsequently creating casino control commissions to supervise casinos and their adherence to the guidelines proposed by the commission (Norris, 2019).

Law enforcement agencies often utilize biometric characteristics and technologies such as DNA, facial recognition, fingerprint scans, iris scans, and palm print scans. Additionally, facial recognition is primarily used by law enforcement agencies for 1:N (one-to-many) matching identification processes (Congressional Research Service, 2020). Some facial recognition systems have been incorporating marks, scars, and tattoos into the algorithmic processes of identification (Choudhury & Rabbani, 2020). Law enforcement agencies use soft biometric characteristics like marks, scars, and tattoos when advertising descriptions of missing and/or unidentified individuals, and for advertising descriptions of wanted criminal offenders in attempt to locate them (Dantcheva et al., 2015).

Additional examples of current biometric initiatives include the Five Country Conference (FCC) Protocol, between the United States, Canada, the United Kingdom, New Zealand, and Australia, which is a collaborative effort to share biometric data on an international scale (The PEW Charitable Trusts, 2020). Another example is India's Aadhaar program, which is a multimodal biometric identification program that has registered over 1.2 billion people and utilizes fingerprints, iris scans, digital photographs, and demographic information (The PEW Charitable Trusts, 2020). In the United States, the Federal Bureau of Investigation (FBI) created the Next Generation Identification (NGI) program, which includes the use of fingerprints, facial features, iris features, and palm features (Yang et al., 2019).

A concern regarding the utilization of biometrics is the potential violation of privacy and civil rights (Aron & Manea, 2014; Mann & Smith, 2017). An additional privacy concern is the maintenance and storage of biometric data (Langenderfer & Linnhoff, 2005). Some countries that are implementing biometric programs have not yet created legal frameworks that address privacy rights (Center for Global Development, 2021). In the United States, Illinois was the first state to enact legislation regarding the use of biometric data. In 2008 the Biometric Information Privacy Act (BIPA) went into effect, which limits the use of individuals' biometric data without first obtaining consent from the person. BIPA set guidelines for the disclosure, protection, and retention of biometric data, and also set requirements for punishments imposed upon anyone that misuses biometric data (Jackson, 2020). Exemptions to the use of biometric data under BIPA without a person's consent apply if biometric data is required for financial or lawful purposes or is required for issuing a warrant or subpoena (Krishan & Mostafavi, 2018; Norris, 2019). States that subsequently enacted legislation reminiscent of BIPA in Illinois were Texas in 2009 and Washington in 2017 (Krishan & Mostafavi, 2018; Norris, 2019). In the European Union, the General Data Protection Regulation (GDPR) was implemented in 2018, which strictly limits the usage of and access to the personal data of individuals, which includes biometric data, and is considered the most stringent legislation to date regarding the usage of biometrics (Proton Technologies AG, 2022).

Research Questions

In the present study, exploratory research was conducted to assess the identification and security implications of biometrics used in casinos, hospitals, and law enforcement agencies located in Indiana and Kentucky. A survey methodology was used to gather information on what types of biometric characteristics and technologies are used in each of the three institutions and the frequency with which biometrics are used. The survey also inquired about how employees at each of the institutions perceive the utilization of biometrics.

The researcher intends to assess the identification and security implications of biometrics utilized in casinos, hospitals, and law enforcement agencies located in Indiana and Kentucky by answering the following questions:

1. Are biometrics utilized in the sample population of casinos, hospitals, and law enforcement agencies? If so, how often?
2. When an employee at one of the three institutions is utilizing biometric data and technology, what biometric characteristics are used most often in their employment position? How frequently are biometrics used in their employment position?
3. What biometric characteristics are used most often in the three institutions? Is there a difference between the biometric characteristics used in the institution versus those used in specific employment positions?

4. What types of biometric systems and technologies are used in the three institutions? Are the biometric systems unimodal, multimodal, or both?
5. How is biometric data stored and protected? Is the data secured? Is the data encrypted? Do all employees have access to biometric data? Is biometric data stored on-site? Are there guidelines for the acquisition, storage, and use of biometric data?
6. How do employees at the three institutions perceive biometrics? Has identification become more accurate with the use of biometrics? Does the utilization of biometrics provide enhanced security at the institutions? Would the usage of biometrics be recommended to other institutions? How much concern is there regarding privacy?

METHODOLOGY

A literature review was conducted on the topic of biometrics to ascertain necessary information for creating a survey. After reviewing the biometrics literature relevant to the study, consisting of 126 articles, a 20-question survey was created with the intention of conducting exploratory research assessing the identification and security implications of biometrics utilized in casinos, hospitals, and law enforcement agencies in Indiana and Kentucky. Eligible participants included any person employed in a casino, hospital, or law enforcement agency located in the seven chosen locations for both Indiana and Kentucky. A total of 68 institutions that consisted of casinos, hospitals, and law enforcement agencies were contacted via telephone and e-mail to request participation in the survey. For distribution purposes, the online platform Survey Monkey was used.

A stratified sampling method was utilized in effort to ensure sample representativeness. Furthermore, locations in each state were chosen as representative samples of each state based upon geographical location and population size. Population sizes were obtained from the United States Census Bureau as of April 2020. Seven locations in Indiana, United States, that were identified as a representative sample of the state, which included: (1) Bloomington (population size 79,168); (2) Evansville (population size 117,298); (3) Fort Wayne (population size 263,886); (4) Indianapolis (population size 887,642); (5) Lafayette (population size 70,783); (6) Muncie (population size 65,194); and (7) South Bend (population size 103,453). Additionally, seven locations in Kentucky, United States, were identified as a representative sample of the state, which included: (1) Bowling Green (population size 72,294); (2) Covington (population size 40,961); (3) Frankfort (population size 28,602); (4) Lexington/Fayette County (population size 322,570); (5) Louisville/Jefferson County (population size 782,909); (6) Pike County (population size 58,669); and (7) Richmond (population size 34,585).

The survey began by asking participants whether they were employed at a casino, hospital, or law enforcement agency. Next, participants were asked what location in Indiana or Kentucky they were employed at. Afterwards, participants were asked if biometrics were utilized in the institution at which they were employed. Next, using a five-point scale, participants were asked how often biometrics were used in the institution at which the participant was employed. Answer choices ranged from never, rarely, somewhat often, often, to frequently.

Subsequently, participants were asked what biometric characteristics are used most often in the *institution* at which they were employed. 24 answer choices were provided that consisted of behavioral, physiological, and soft biometric characteristics which included: (1) body odor; (2) DNA; (3) ears; (4) eyes; (5) face; (6) fingerprints; (7) foot dynamics; (8) hands; (9) metabolic attributes; (10) nails; (11) neural analysis; (12) palm prints; (13) piercings; (14) scars; (15) skin patterns; (16) smell; (17) tattoos; (18) tongue; (19) vein patterns; (20) gait (walking gait); (21) keystroke dynamics; (22) signature dynamics; (23) voice; and (24) other. While there was no literature found that cited piercings as a soft biometric characteristic, it was included in the survey response options to assess whether piercings have been used for identification purposes.

Participants were then asked if biometrics were utilized in their *specific employment position.* From there, further inquiry was made regarding how often biometric characteristics are used in the respondent's specific employment position. Answer choices consisted of a five-point scale ranging from never, rarely, somewhat often, often, to frequently. Afterwards, participants were asked what biometric characteristics were used most often in their *specific employment position.* Answer choices provided consisted of 24 behavioral, physiological, and soft biometric characteristics which included: (1) body odor; (2) DNA; (3) ears; (4) eyes; (5) face; (6) fingerprints; (7) foot dynamics; (8) hands; (9) metabolic attributes; (10) nails; (11) neural analysis; (12) palm prints; (13) piercings; (14) scars; (15) skin patterns; (16) smell; (17) tattoos; (18) tongue; (19) vein patterns; (20) gait (walking gait); (21) keystroke dynamics; (22) signature dynamics; (23) voice; and (24) other.

Next, participants were asked what types of biometric systems/technologies were utilized in the institution at which they were employed. Answer choices consisted of: (1) computerized tomography (CT) scan; (2) electrocardiogram (ECG/EKG); (3) electroencephalogram (EEG); (4) eye scanners; (5) facial recognition; (6) fingerprint scanners; (7) finger-vein scanners; (8) functional magnetic resonance imaging (fMRI); (9) magnetic resonance imaging (MRI); (10) palm print scanners; and (11) other.

Afterwards, participants were asked if the institution at which they were employed utilized unimodal biometric systems (one biometric characteristic), multimodal biometric systems (multiple biometric characteristics), or both unimodal and multimodal systems. Next, participants were asked how biometric data is stored and protected in the institution at which they were employed. Answer choices consisted of: (1) back-up server; (2) cloud server; (3) cryptosystem; and (4) other.

Participants were then asked if the usage of biometrics has increased the accuracy of identification. Further, participants were asked if the use of biometrics provided enhanced security. Subsequently, participants were asked if they would recommend the use of biometrics to other institutions. From there, participants were asked if they were concerned about privacy with biometrics. Afterwards, participants were asked if the institution at which they were employed stored biometric data on site. Next, participants were asked if biometric data was secured in the institution at which they were employed. This led to posing the question as to whether biometric data at the institution was encrypted or not encrypted. Subsequently, participants were asked if all employees had access to biometric data at the institution where the respondent was employed. Finally, participants were asked if the institution at which they were employed provided proposed guidelines for the acquisition, storage, and use of biometric data.

RESULTS

A total of 68 casinos, hospitals, and law enforcement agencies were contacted to request participation in the survey. Subsequently, 15 individuals participated in the survey, which rendered a 22% response rate. Of the 68 casinos, hospitals, and law enforcement agencies surveyed, 80% of respondents were hospital employees, 13.3% of respondents were casino employees, and 6.7% of respondents were employed at a law enforcement agency. Regarding locations in Indiana and Kentucky, 80% of respondents were from South Bend, Indiana, 6.7% of respondents were from Louisville, Kentucky, 6.7% or respondents were from Richmond, Kentucky, and 6.7% responded “other” for their location. Of the 15 participants, 60% noted that biometrics are utilized in the institution at which they were employed, and 40% noted that biometrics are not utilized in the institution at which they were employed. When asked about the frequency with which biometrics are utilized in the *institution* at which they were employed, 33.3% responded “never”, 13.3% responded “rarely”, 6.7% responded “somewhat often”, and 46.7% responded “frequently”.

When asked what biometric characteristics are used most often in the *institution* at which participants were employed, the top two results were fingerprints (26.7%) and gait (26.7%), followed by eyes (20%) and tattoos (20%). Of note, piercings were selected as being used by 6.7% of participants. The following table depicts the results from question 5 (what biometric characteristics are used most often in the institution?).

Table 1				
Characteristic	**Selected**	**Percentage**	**Not selected**	**Percentage**
Body odor	0	0%	15	100%
DNA	1	6.7%	14	93.3%
Ears	0	0%	15	100%
Eyes	3	20%	12	80%
Face	1	6.7%	14	93.3%
Fingerprints	4	26.7%	11	73.3%
Foot dynamics	0	0%	15	100%
Hands	2	13.3%	13	86.7%
Metabolic attributes	1	6.7%	14	93.3%
Nails	1	6.7%	14	93.3%
Neural analysis	1	6.7%	14	93.3%
Palm prints	1	6.7%	14	93.3%
Piercings	1	6.7%	14	93.3%
Scars	2	13.3%	13	86.7%
Skin patterns	1	6.7%	14	93.3%
Smell	0	0%	15	100%
Tattoos	3	20%	12	80%
Tongue	0	0%	15	100%
Vein patterns	1	6.7%	14	93.3%
Gait (walking gait)	4	26.7%	11	73.3%
Keystroke dynamics	0	0%	15	100%
Signature dynamics	0	0%	15	100%
Voice	2	13.3%	13	86.7%

When asked if biometrics are utilized in their *specific employment position*, 26.7% of respondents indicated “yes”, and 73.3% of respondents indicated “no”. Inquiry as to the frequency with which biometrics were utilized in a participant’s *specific employment position*, 53.3% responded “never”, 20% responded “rarely”, 6.7% responded “somewhat often”, 13.3% responded “often”, and 6.7% responded “frequently”. Regarding what biometric characteristics are utilized most often in a participant’s *specific employment position*, the top two results were fingerprints (20%) and gait (20%), followed by eyes (13.3%) and tattoos (13.3%). The following table depicts the results from question 8 (what biometric characteristics are used most often in your employment position?).

Table 2

Characteristic	**Selected**	**Percentage**	**Not selected**	**Percentage**
Body odor	0	0%	15	100%
DNA	0	0%	15	100%
Ears	0	0%	15	100%
Eyes	2	13.3%	13	86.7%
Face	0	0%	15	100%
Fingerprints	3	20%	12	80%
Foot dynamics	0	0%	15	100%
Hands	1	6.7%	14	93.3%
Metabolic attributes	1	6.7%	14	93.3%
Nails	0	0%	15	100%
Neural analysis	1	6.7%	14	93.3%
Palm prints	0	0%	15	100%
Piercings	1	6.7%	14	93.3%
Scars	1	6.7%	14	93.3%
Skin patterns	0	0%	15	100%
Smell	0	0%	15	100%
Tattoos	2	13.3%	13	86.7%
Tongue	0	0%	15	100%
Vein patterns	1	6.7%	14	93.3%
Gait (walking gait)	3	20%	12	80%
Keystroke dynamics	0	0%	15	100%
Signature dynamics	0	0%	15	100%
Voice	1	6.7%	14	93.3%

When asked about the types of biometric systems and technologies utilized in the institutions at which participants were employed, the two most selected answers were CT scans (53.3%) and MRI (53.3%), followed by ECG (40%), EKG (40%), EEG (26.7%), fingerprint scanners (26.7%), and eye scanners (20%). The following table depicts the results from question 9 (what kinds/types of biometric systems/technologies are utilized in this institution?).

Table 3				
System/Technology	**Selected**	**Percentage**	**Not selected**	**Percentage**
CT scans	8	53.3%	7	46.7%
ECG	6	40%	9	60%
EEG	4	26.7%	11	73.3%
EKG	6	40%	9	60%
Eye scanners	3	20%	12	80%
Facial recognition	1	6.7%	14	93.3%
Fingerprint scanners	4	26.7%	11	73.3%
Finger-vein scanners	0	0%	15	100%
fMRI	1	6.7%	14	93.3%
MRI	8	53.3%	7	46.7%
Palm print scanners	2	13.3%	13	86.7%

Participants were asked about the types of biometric systems utilized in the institutions at which they were employed, subsequently, 40% of participants indicated that their employment institution utilizes unimodal biometric systems, 20% of participants indicated that their employment institution utilizes multimodal biometric systems, and 40% of participants indicated that their employment institution utilizes both unimodal and multimodal biometric systems. When asked how biometric data is stored and protected in the institutions at which they were employed, 46.7% of participants cited the use of a cloud server, 33.3% of participants cited the use of a cryptosystem, 26.7% of participants cited the use of a back-up server, and 13.3% of participants indicated that they did not know how biometric data is stored and protected. The following table depicts the results of question 11 (how is biometric data stored and protected?).

Table 4				
Storage/protection	**Selected**	**Percentage**	**Not selected**	**Percentage**
Back-up server	4	26.7%	11	73.3%
Cloud server	7	46.7%	8	53.3%
Cryptosystem	5	33.3%	10	66.7%
Other “don’t know”	2	13.3%	13	86.7%

When asked if biometrics has increased the accuracy of identification, 72.7% of participants responded “yes”, while 27.3% of participants responded “no”. Further, when asked if the use of biometrics has provided enhanced security, 72.7% of participants responded “yes”, and 27.3% of participants responded “no”. Inquiry as to whether participants would recommend the usage of biometrics to other institutions, 91.7% responded “yes”, and 8.3% responded “no”. Regarding privacy concerns about biometrics, 33.3% of participants noted that they were concerned about privacy with biometrics, whereas 66.7% of participants noted that they were not concerned about privacy with biometrics.

For security assessments, participants were asked if the institution at which they were employed stored biometric data on site- 50% of respondents selected “yes”, and 50% of respondents selected “no”. When asked if biometric data was secured, 88.9% of participants responded “secured” and 11.1% of participants responded with “not secured”. Inquiry as to whether biometric data was encrypted or not encrypted resulted in 66.7% of participants indicating that biometric data is encrypted, and 33.3% of participants indicating that biometric data is not encrypted. When asked if all employees have access to biometric data at the participant’s institution of employment, 20% responded that yes, all employees have access to biometric data, and 80% responded that no, all employees do not have access to biometric data. When asked if the institutions at which participants were employed had proposed guidelines for the acquisition, storage, and use of biometric data, 60% of participants indicated that yes, there are proposed guidelines, and 40% of participants indicated that no, there are not proposed guidelines.

DISCUSSION

The biometrics literature indicates that the most frequently utilized biometric characteristics for identification and verification are mainly physiological, specifically the characteristics associated with an individual's face, fingerprints, and eyes (Godi & Rao, 2019; Jain et al., 2006; Luo et al., 2018). Results of the current study indicate that the two most commonly utilized biometric characteristics in the institutions at which participants were employed were fingerprints and gait (walking gait). This is consistent with the literature noting that fingerprints are one of the most utilized biometric characteristics. However, this is also inconsistent with the literature, as gait (walking gait) is not referenced as one of the most frequently used biometric characteristics. While piercings were selected by 6.7% of participants as having been used for identification purposes, the sample size of the current study was not large enough to determine the generalizability of using piercings as a biometric characteristic.

Hospitals may be more likely to use CT, ECG/EKG, EEG, fMRI, and MRI scans for identification purposes as opposed to casinos and law enforcement agencies because the equipment required to conduct these types of scans is usually already available in a hospital, whereas casinos and law enforcement agencies would need to find access to the necessary equipment elsewhere. This is demonstrated by the results of the current study in which 80% of participants were hospital employees, and the two most selected technologies used for biometric identification purposes were CT and MRI scans.

The biometrics literature mentions privacy as being one of the major concerns associated with the use of biometrics. Conversely, results of the current study indicate that only about 1/3 of respondents were concerned about privacy regarding biometrics. The lack of concern about privacy by respondents could be attributable to having prior knowledge and interaction with biometric systems. However, it may also be attributable to not having prior knowledge and/or interaction with biometric systems, as respondents noted that while biometrics are used frequently in the institutions at which they were employed, biometrics were not frequently utilized in the respondents' specific employment positions. Overall, participants signaled that the usage of biometrics has increased the accuracy of identification and has provided enhanced security. Additionally, most of the study participants indicated that they would recommend the use of biometrics to other institutions.

Racial disparities associated with facial recognition technologies are tied to the creation and development of algorithms used to conduct facial recognition processes. Most of the algorithms currently in use were designed based upon the specific traits of Caucasian individuals, which differ from the specific traits of individuals of ethnic and/or racial minorities. Therefore, facial recognition technologies are less accurate when used to identify persons of minority status, notably by way of producing false positive rates (Congressional Research Service, 2020; Jacquet & Champod, 2020; Keyser et al., 2021; The PEW Charitable Trusts, 2020). This leads the researcher to contend that facial recognition algorithms need to be made more diverse to account for variations in demographic traits. Doing such should theoretically lessen the racial biases in facial recognition algorithms and provide more accurate results. Additionally, the recency with which empirical research was conducted that highlighted racial disparities in facial recognition algorithms indicates that by drawing attention to the issue, subsequent efforts to develop facial recognition algorithms that are based on a variety of ethnic and racial qualities is the logical next step for the development of facial recognition algorithms, especially because facial recognition technologies are often used in highly diverse societies, such as the United Kingdom and the United States.

Limitations

The current study encountered a limitation of institutions being reluctant or unable to discuss the topic of biometrics. Additionally, the study was limited due to a small sample size, therefore the results are not generalizable to either of the states the survey was conducted in. Further, the results are also not generalizable to casinos, hospitals, or law enforcement agencies, as 80% of survey respondents were hospital employees.

Implications for Future Research

Regarding the usage of unimodal and multimodal biometric systems, future research could investigate the types of multimodal biometric systems used in casinos, hospitals, and law enforcement agencies (i.e., traits selected, types of fusion used). Additionally, if an institution uses both unimodal and multimodal biometric systems, further inquiry could be made as to why both types of systems are used, and if there are specific instances when unimodal biometric systems would be chosen for use as opposed to multimodal biometric systems. Similar research could be conducted on the use of biometric systems by technology companies and corporations such as Amazon, Apple, Google, Microsoft, Samsung, etc., as well as the use of biometric systems by banks (i.e., mobile applications, payment cards, security features).

Conclusion

The current study evaluated the usage of biometrics in casinos, hospitals, and law enforcement agencies. A survey methodology was used to gain insight as to what types of biometric characteristics were used in the three institutions and what types of technologies were used to examine biometric characteristics. Results indicated that the most used biometric characteristics were fingerprints and gait, and the most used technologies were CT and MRI scans, however, this may be attributable to 80% of survey participants being hospital employees,

A major identification implication was noted from the biometrics literature regarding racial disparities associated with facial recognition algorithms. Dedicated efforts need to be made to create facial recognition algorithms based upon the features of individuals of ethnic and/or minority groups as opposed to solely being developed based upon the features of Caucasian individuals.

References

Abaza, A., Ross, A., Hebert, C., Harrison, M. A. F., & Nixon, M. S. (2013). A survey on ear biometrics. *ACM Computing Surveys, 45*(2:22), 2-35.

Abdelwhab, A., & Viriri, S. (2018). A Survey on Soft Biometrics for Human Identification. In J. Yang, D. S. Park, S. Yoon, Y. Chen, & C. Zhang (Eds.), *Machine learning and biometrics.* IntechOpen.

Adámek, M., Matýsek, M., & Neumann, P. (2015). Security of biometric systems. *Procedia Engineering*, 169-176.

Aggarwal, S., & Jindal, N. (2012). Multimodal biometric system using fusions. *International Journal of Advanced Research in Computer Science, 3*(5), 264-268.

Agrafioti, F., Bui, F. M., & Hatzinakos, D. (2011). Medical biometrics in mobile health monitoring. *Security and Communication Networks*, *4*, 525-539.

Alay, N., & Al-Baity, H. H. (2020). Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits. *Sensors, 20*(5523), 1-17.

Ameer, A. M., & Jose, M. V. (2021). Biometric authentication based medical data management in cloud systems. *Ilkogrentim Online- Elementary Education Online, 20*(5), 1766-1773.

Amelung, N. (2021). “Crimmigration control” across borders: The convergence of migration and crime control through transnational biometric databases. *Historical Social Research, 46*(3), 151-177.

Ammour, B., Boubchir, L., Bouden, T., & Ramandi, M. (2020). Face-iris multimodal biometric identification system. *Electronics, 9*(85), 1-18.

Appati, J. K., Nartey, P. K., Owusu, E., & Denwar, I. W. (2021). Implementation of a transform-minutiae fusion-based model for fingerprint recognition. *International Journal of Mathematics and Mathematical Sciences,* 1-12.

Aron, I., & Manea, A. C. (2014). Recognition of a person based on the characteristics of the iris and retina. *Bulletin of the Transilvania University of Braşov Series VII, 7*(56:1).

Asha, S., & Chellappan, C. (2012). Biometrics: An overview of the technology, issues and applications. *International Journal of Computer Applications, 39*(10), 35-52.

Baig, A. F., & Eskeland, S. (2021). Security, privacy, and usability in continuous authentication: A survey. *Sensors, 21*(5967), 1-26.

Barros, A., Resque, P., Almeida, J., Mota, R., Oliveira, H., Rosário, D., & Cerqueira, E. (2020). Data improvement model based on ECG biometric for user authentication and identification. *Sensors, 20*(2920), 1-18.

Bhatia, A., & Bhabha, J. (2017). India’s Aadhaar scheme and the promise of inclusive social protection. *Oxford Development Studies, 45*(1), 64-79.

Bhilare, S., Jaswal, G., Kanhangad, V., & Nigam, A. (2018). Single-sensor hand-vein multimodal biometric recognition using multiscale deep pyramidal approach. *Machine Vision and Applications, 29*, 1269-1286.

Blasco, J., & Peris-Lopez, P. (2018). On the feasibility of low-cost wearable sensors for multi-modal biometric verification. *Sensors, 18*(2782), 1-20.

Bokade, G. U., & Kanphade, R. D. (2019). Multimodal biometric authentication based on feature level fusion: A novel approach to improve genuine acceptance rate in case of accidental injuries to biometric traits. *The IUP Journal of Telecommunications, XI*(3), 26-42.

Caplova, Z., Obertova, Z., Gibelli, D. M., Angelis, D. D., Mazzarelli, D., Sforza, C., & Cattaneo, C. (2018). Personal identification of deceased persons: An overview of the current methods based on physical appearance. *Journal of Forensic Sciences, 63*(3), 662-669.

Center for Global Development. (2021). Biometrics FAQs. https://www.cgdev.org/page/biometrics-faqs, 1-5.

Ceyhan, A. (2008). Technologization of Security: Management of uncertainty and risk in the age of biometrics. *Surveillance & Society, 5*(2), 102-123.

Chorás, M. (2005). Ear biometrics based on geometrical feature extraction. *Electronic Letters on Computer Vision and Image Analysis, 5*(3), 84-95.

Choudhury, A. H., & Rabbani, M. M. A. (2020). Biometric passport for national security using multibiometrics and encrypted biometric data encoded in the QR code. *Journal of Applied Security Research, 15*(2), 199-229.

Chowdhury, D. P., Bakshi, S., Guo, G., & Sa, P. K. (2018). On applicability of tunable filter bank based feature for ear biometrics: A study from constrained to unconstrained. *Journal of Medical Systems, 42*(11), 1-20.

Congressional Research Service. (2020). Federal law enforcement use of facial recognition technology.

Crampton, J. W. (2019). Platform biometrics. *Surveillance & Society*, *17*(1/2), 54–62.

Dahia, G., Jesus, L., & Segundo, M. P. (2020). Continuous authentication using biometrics: An advanced review. *WIREs Data Mining and Knowledge Discovery, 10*(1365), 1-23.

Dantcheva, A., Velardo, C., D'Angelo, A., & Dugelay, J. (2010). Bag of soft biometrics for person identification: New trends and challenges. *Multimedia Tools and Applications, 51,* 739-777.

Dantcheva, A., Elia, P., & Ross, A. (2015). What else does your biometric data reveal? A survey on soft biometrics. *IEEE Transactions on Information Forensics and Security, 11*(3), 441-467.

Department of Homeland Security. (2015). Biometric systems application note. 1-17.

Down, M. P., & Sands, R. J. (2004). Biometrics: An overview of the technology, challenges and control considerations. *Information Systems Control Journal, 4*.

Essink, H. M., Knops, A., Lung, A. M. A. L., Van Der Meulen, C. N., Wouters, N. L., Van Der Molen, A. J., Veldkamp, W. J. H., & Termaat, M. F. (2020). Real-time person identification in a hospital setting: A systematic review. *Sensors, 20*(3937), 1-23.

Estrela, P. M. A. B., Albuquerque, R. O., Giozza, D. M. A. W. F., & Júnior, R. T. S. (2021). A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications. *Sensors, 21*(4212), 1-27.

Etter, L. P., Ragan, E. J., Campion, R., Martinez, D., & Gill, C. J. (2019). Ear biometrics for patient identification in global health: A field study to test the effectiveness of an image stabilization device in improving identification accuracy. *BMC Medical Informatics and Decision Making, 19*(144), 1-9.

Eze, S. G., & Chijioke, E. O. (2016). Public enlightenment on the acceptance of fingerprint biometric technology for administration in academic institutions and other organizations. *Journal of Education and Practice, 7*(28), 158-163.

Galterio, M. G., Shavit, S. A., & Hayajneh, T. (2018). A review of facial biometrics security for smart devices. *Computers, 7*(37), 1-11.

Godi, S., & Rao, K. R. (2019). Non-conventional biometrics using DOST features for secure cloud deployment. *International Journal of Knowledge-based and Intelligent Engineering Systems, 23,* 15-20.

Gomez, A. (2019). Twins. *The Tech Interactive*.

Haghighar, M., Zonouz, S., & Abdel-Mottaleb, M. (2013). Identification using encrypted biometrics. In: Wilson R., Hancock E., Bors A., Smith W. (Eds.) *Computer analysis of images and patterns.* CAIP 2013. Lecture Notes in Computer Science, vol 8048. Springer, Berlin, Heidelberg. 440-448.

Hair, M. E., Mathis, A. L., Brunelle, E. K., Halámková, L., & Halámek, J. (2018). Metabolite biometrics for the differentiation of individuals. *Analytical Chemistry, 90,* 5322-5328.

Hamoodi, Y. A. F., & Ramadhan, S. A. M. (2019). Identification of biometrics based on a classical mathematical methods in forensic medicine. *Indian Journal of Forensic Medicine & Toxicology, 13*(3), 265-275.

Iloanusi, O. N., & Ezema, C. A. (2017). A quantitative impact of fingerprint distortion on recognition performance. *Information Security Journal: A Global Perspective, 26*(6), 267-275.

Jackson, M. (2020). Opting out: Biometric information privacy and standing. *Duke Law & Technology Review, 18*(1), 293-305.

Jacquet, M., & Champod, C. (2020). Automated face recognition in forensic science: Review and perspectives. *Forensic Science International, 307*(110124), 1-14.

Jain, A. K., Dass, S. C., & Nandakumar, K. (2004). Soft biometric trait for personal recognition systems. *Proceedings of International Conference on Biometric Authentication, LNCS 3072,* 731-738.

Jain, A. K., Pankanti, S., Prabhakar, S., Hong, L., Ross, A., & Wayman, J. L. (2004). Biometrics: A grand challenge. *Proceedings of International Conference on Pattern Recognition.*

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security, 1*(2), 125-143.

Jain, A. K., & Kumar, A. (2010). Biometrics of next generation: An overview. *Second Generation Biometrics*.

Jain, A. K., & Ross, A. (2015). Bridging the gap: From biometrics to forensics. *Philosophical Transactions: Biological Sciences*, *370*(1674), 1–10.

Jekova, I., Krasteva, V., & Schmid, R. (2018). Human identification by cross-correlation and pattern matching of personalized heartbeat: Influence of ECG leads and reference database size. *Sensors, 18*(372), 1-20.

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 MHealth and UHealth*, *7*(4), 11472.

Kausar, F. (2021). Iris based cancelable biometric cryptosystem for secure healthcare smart cards. *Egyptian Informatics Journal, 22,* 447-453.

Keyser, A. D., Bart, Y., Gu, X., Liu, S. Q., Robinson, S. G., & Kannan, P. K. (2021). Opportunities and challenges of using biometrics for business: Developing a research agenda. *Journal of Business Research, 136*, 52-62.

Khan, S., Parkinson, S., Grant, L., Liu, N., & McGuire, S. (2020). Biometric systems utilising health data from wearable devices: Applications and future challenges in computer security. *ACM Computing Surveys, 53*(4), 85:1-29.

Kono, M., Miura, N., Fujii, T., Ohmura, K., Yoshifuji, H., Yukawa, N., Imura, Y., Nakashima, R., Ikeda, T., Umemura, S., Miyatake, T., & Mimori, T. (2015). Personal authentication analysis using finger-vein patterns in patients with connective tissue diseases – possible association with vascular disease and seasonal change. *PLOS One*, 1-11.

Kopczewski, M., & Smal, T. (2017). Possibilities for the use of biometric data in security systems. *Journal of Science of the Military Academy of Land Forces, 49*(4:186), 168-179.

Kour, J., Hanmandlu, M., & Ansari, A. Q. (2016). Biometrics in cyber security. *Defence Science Journal, 66*(6), 600-604.

Krishan, R., & Mostafavi, R. (2018). Biometric technology: Security and privacy concerns. *Journal of Internet Law*, 19-23.

Krishnakumari, Y., & Savitha, G. (2017). A review on unimodal and multimodal biometric. *International Journal of Innovative Science and Research Technology, 2*(5), 514-521.

Kumar, P., Saini, R., Kaur, B., Roy, P. P., & Scheme, E. (2019). Fusion of neuro-signals and dynamic signatures for person authentication. *Sensors, 19*(4641), 1-16.

Lagou, P., & Chondrokoukis, G. (2011). Choosing a biometric for nonrepudiation. *Information Security Journal: A Global Perspective, 20*, 17-24.

Lai, C. Q., Ibrahim, H., Abdullah, M. Z., Abdullah, J. M., Suandi, S. A., & Azman, A. (2019). Arrangements of resting state electroencephalography as the input to convolutional neural network for biometric identification. *Computational Intelligence and Neuroscience,* (7895924).

Lalović, K. G., & Bogdanoski, M. Z. (2021). Java gui application for comparing the levels of security – fingerprint vs. iris. *Military Technical Courier, 69*(3), 676-686.

Langenderfer, J., & Linnhoff, S. (2005). The emergence of biometrics and its effect on consumers. *The Journal of Consumer Affairs, 39*(2), 314-338.

Larbi, N., & Taleb, N. (2018). A robust multi-biometric system with compact code for iris and face. *International Journal on Electrical Engineering and Informatics, 10*(1), 1-13.

Leese, M. (2018). Standardizing security: The business case politics of borders. *Mobilities, 13*(2), 261-275.

Liu, C., Wang, J., Peng, C., & Shyu, J. Z. (2015). Evaluating and selecting the biometrics in network security. *Security and Communication Networks, 8,* 727-739.

Liu, S., Song. Y., Zhang, M., Zhao, J., Yang, S., & Hou, K. (2019). An identity authentication method combining liveness detection and face recognition. *Sensors, 19*(4733), 1-14.

Luo, Y., Cheung, S. S., Lazzeretti, R., Pignata, T., & Barni, M. (2018). Anonymous subject identification and privacy information management in video surveillance. *International Journal of Information Security, 17,* 261-278.

Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics, 22*(9), 499-508.

Ma, D. (2016). Employing popular emerging technologies in the regulation of commercial gaming is not always a winning strategy. *Albany Law Review, 79*(4), 1409-1432.

Ma, Y., Huang, Z., Wang, X., & Huang, K. (2020). An overview of multimodal biometrics using the face and ear. *Mathematical Problems in Engineering, 2020*, 1-17.

Mann, M., & Smith, M. (2017). Automated facial recognition technology: Recent developments and approaches to oversight. *UNSW Law Journal, 40*(1), 121-145.

Mason, J., Dave, R., Chatterjee, P., Graham-Allen, I., Esterline, A., & Roy, K. (2020). An investigation of biometric authentication in the healthcare environment. *Array, 8*(100042*),* 1-15.

Meagher, S., Dvornychenko, V., & Garris, M. (2014). Characterization of laten print "lights-out" modes for automated fingerprint identification systems. *Journal of Forensic Identification, 64*(3), 255-284.

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

Mishra, A. (2010). Multimodal biometrics it is: Need for future systems. *International Journal of Computer Applications, 3*(4), 28-33.

Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Ariffin, S. A. B., Alemran, A., Enaizan, O., Shareef, A. A., Jasim, A. N., Jalood, N. S., Baqer, M. J., Alamoodi, A. H., Almahdi, E. M., Albahri, A. S., Alsalem, M. A., Mohammed, K. I., Ameen, H. A., & Garfan, S. (2020). Finger vein biometrics: Taxonomy analysis, open challenges, future directions, and recommended solution for decentralised network architectures. *Digital Object Identifier, 8,* 9821-9845.

Moolla, Y., Kock, A. D., Mabuza-Hocquet, G., Ntshangase, C. S., Nelufule, N., & Khanyile, P. (2021). Biometric recognition of infants using fingerprint, iris, and ear biometrics. *Digital Object Identifier, 9*, 38269-38286.

Moradoff, N. (2010). Biometrics: Proliferation and constraints to emerging and new technologies. *Security Journal, 23*(4), 276-298.

Mordini, E., & Massari, S. (2008). Body, biometrics and identity. *Bioethics, 22*(9), 488-498.

Morosan, C. (2018). Information disclosure to biometric e-gates: The roles of perceived security, benefits, and emotions. *Journal of Travel Research, 57*(5), 644-657.

Nagwanshi, K. K., & Dubey, S. (2018). Statistical feature analysis of human footprint for personal identification using BigML and IBM Watson analytics. *Arabian Journal for Science & Engineering (Springer Science & Business Media B.V)*, *43*(6), 2703–271.

Niculescu, B. R., & Coman, C. (2017). NATO automated biometric identification system (NABIS). *MTA Review, XXVII*(2), 67-72.

Nixon, M. S., Correia, P. L., Nasrollahi, K., Moeslund, T. B., Hadid, A., & Tistarelli, M. (2015). On soft biometrics. 1-23.

Norris, S. (2019). "…And the eye in the sky is watching us all" – The privacy concerns of emerging technological advances in casino player tracking. *UNLV Gaming Law Journal, 9*(269), 269-291.

North-Samardzic, A. (2020). Biometric technology and ethics: Beyond security applications. *Journal of Business Ethics, 167,* 433-450.

Norval, A., & Prasopoulou, E. (2019). Seeing like a citizen: Exploring public views of biometrics. *Political Studies, 67*(20, 367-387.

Ozkaya, N., & Sagiroglu, S. (2010). Generating one biometric feature from another: Faces from fingerprints. *Sensors, 10,* 4206-4237.

Park, U., Jillela, R. R., Ross, A., & Jain, A. K. (2011). Periocular biometrics in the visible spectrum. *IEEE Transactions on Information Forensics and Security, 6*(1), 96-106.

Petermann, T., Sauter, A., & Scherz, C. (2006). Biometrics at the borders—the challenges of a political technology. *International Review of Law Computers & Technology, 20*(1&2), 149-166.

The PEW Charitable Trusts. (2020). Health care can learn from global use of biometrics.

Pisani, P. H., Mhenni, A., Giot, R., Cherrier, E., Poh, N., De Carvalho, A. C. P. D. L. F., Rosenberger, C., & Ben Amara, N. E. (2019). Adaptive biometric systems: Review and perspectives. *ACM Computing Surveys*, *52*(5), 1–38.

Proton Technologies AG. (2022). General data protection regulation. Gdpr.eu.

Ramos, M. S., Carvalho, J. M., Pinho, A. J., & Brás, S. (2021). On the impact of data acquisition protocol on ECG biometric identification. *Sensors, 21*(4645), 1-11.

Ross, A., & Jain, A. (2003). Information fusion in biometrics. *Pattern Recognition Letters, 45*(24), 2115-2125.

Ryu, R., Yeom, S., Kim, S., & Herbert, D. (2021). Continuous multimodal biometric authentication schemes: A systematic review. *Digital Object Identifier, 9*, 34541-34557.

Sahoo, S. K., Choubisa, T., & Prasanna, S. R. M. (2012). Multimodal biometric person authentication: A review. *IETE Technical Review, 29*(1), 54-75.

Salvi, R., Fuentealba, P., Henze, J., Bisgin, P., Sühn, T., Spiller, M., Burmann, A., Boese, A., Illanes, A., & Friebe, M. (2021). Vascular auscultation of carotid artery: Towards biometric identification and verification of individuals. *Sensors, 21*(6656), 1-17.

Sanjekar, P. S., & Patil, J. B. (2013). Overview of multimodal biometrics. *Signal & Image Processing: An International Journal, 4*(1), 57-64.

Sauerwein, K., Saul, T. B., Steadman, D. W., & Boehnen, C. B. (2017). The effect of decomposition on the efficacy of biometrics for positive identification. *Journal of Forensic Sciences, 62*(6), 1599-1602.

Singh, Y. N., & Singh, S. K. (2012). Challenges of biometrics: Evaluation of system attacks and defenses. *Journal of Information Assurance and Security, 7,* 207-221.

Singh, M., Singh, R., & Ross, A. (2019). A comprehensive overview of biometric fusion. *Information Fusion, 52*, 187-205.

Sivakumar, T. T., Nair, S. S., Zacharias, G. C., Nair, M. S., & Joseph, A. P. (2018). Identification of tongue print images for forensic science and biometric authentication. *Journal of Intelligent and Fuzzy Systems, 34,* 1421-1426.

Siwicki, B. (2018). Biometrics entering a new era in healthcare. *Healthcare IT News*, 1-8.

Sohn, J. W., Kim, H., Park, S. B., Lee, S., Monroe, J. I., Malone, T. B., Kinsella, T., Yao, M., Kunos, C., Lo, S. S., Shenk, R., & Machtay, M. (2020). Clinical study of using biometrics to identify patient and procedure. *Frontiers in Oncology, 10*(586232), 1-9.

Soltane, M., Messikh, L., & Zaoui, A. (2017). A review regarding the biometrics cryptography challenging design and strategies. *BRAIN – Broad Research in Artificial Intelligence and Neuroscience, 8*(4), 41-64.

Sreeja, V. S., Josephine, M. S., & Raja, V. J. (2018). Survey on biometric identification system. *International Journal of Pharmaceutical Research, 10*(4), 223-226.

Srivastava, N. (2017). Fusion levels in multimodal biometric systems—a review. *International Journal of Innovative Research in Science, Engineering and Technology, 6*(5), 8874-8878.

Staunch, M., Wodzinski, M., & Skalski, A. (2020). Contact-free multispectral identity verification system using palm veins and deep neural network. *Sensors, 20*(5695), 1-17.

Talreja, V., Ferrett, T., Valenti, M. C., & Ross, A. (2017). Biometrics-as-a-service: A framework to promote innovative biometric recognition in the cloud. *Distributed, Parallel, and Cluster Computing, arXiv:1710.09183.*

Tome, P., Vera-Rodriguez, R., Fierrez, J., & Ortega-Garcia, J. (2015). Facial soft biometric features for forensic face recognition. *Forensic Science International, 257*, 271-284.

Tot, I. A., Bajčetić, J. B., Jovanović, B. Ž., Trikoš, M. B., Bogićević, D. L., & Gajić, T. M. (2021). Biometric standards and methods. *Military Technical Courier, 69*(4), 963-977.

Tu, Y., Yao, Z., Xu, J., Liu, Y., & Zhang, Z. (2020). Fingerprint restoration using cubic Beizer curve. *BMC Bioinformatics, 21*(514), 1-19.

United States Census Bureau. (2020). 2020 census results. www.census.gov

Wayman, J., Jain, A., Maltoni, D., Maio, D. (2005). An introduction to biometric authentication systems. In: Wayman, J., Jain, A., Maltoni, D., Maio, D. (Eds.) *Biometric systems.* Springer, London. 1-20.

Wlodarczyk, R. (2012). Biometric features used for forensic identification of humans. *Internal Security*, 125-140.

Wu, W., Pirbhulal, S., & Li, G. (2020). Adaptive computing-based biometric security for intelligent medical applications. *Neural Computing and Applications, 32*, 11055-11064.

Xiao, Q. (2007). Biometrics – Technology, application, challenge, and computational intelligence solutions. *IEEE Computer Intelligence Magazine*, 5-25.

Yang, W., Wang, S., Hu, J., Zheng, G., Chaudhry, J., Adi, E., & Valli, C. (2018). Securing mobile healthcare data: A smart card based cancelable finger-vein bio-cryptosystem. *Digital Object Identifier*, *6*, 36939-36947.

Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. *Symmetry, 11*(141), 1-19.

Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2021). Biometrics for internet-of-things security: A review. *Sensors, 21*(6163), 1-26.

Yuan, J., & Yu, S. (2013). Efficient privacy-preserving biometric identification in cloud computing. *2013 Proceedings IEEE INFOCOM,* 2652-2660.

Zhang, Y., Chen, Z., Chen, W., & Li, H. (2019). Unobtrusive and continuous BCG-based human identification using a microbend fiber sensor. *Digital Object Identifier, 7*, 72518-72527.

Zheng, W., Lee, D., & Xia, J. (2021). Photoacoustic tomography of fingerprint and underlying vasculature for improved biometric identification. *Scientific Reports, 11*(17536).

Zhu, L., Zhang, C., Xu, C., Liu, X., & Huang, C. (2018). An efficient and privacy-preserving biometric identification scheme in cloud computing. *IEEE Access, 6,* 19025-19033.

APPENDICIES

Appendix A: Biometric Characteristic References

Body odor	(Langenderfer & Linnhoff, 2005; Mordini & Massari, 2008; Wlodarczyk, 2012).
Deoxyribonucleic acid (DNA)	(Caplova et al., 2018; Haghigar et al., 2013; Hamoodi & Ramadhan, 2019; Jacquet & Champod, 2020; Jain & Kumar, 2010; Keyser et al., 2021; Krishan & Mostafavi, 2018; Langenderfer & Linnhoff, 2005; Niculescu & Coman, 2017; Sreeja et al., 2018; Wlodarczyk, 2012).
Ears	(Abaza et al., 2013; Chorás, 2005; Choudhury et al., 2018; Etter et al., 2019; Kour et al., 2016; Langenderfer & Linnhoff, 2005; Mir et al., 2011; Moolla et al., 2021; Moradoff, 2010; Mordini & Massari, 2008; Ozkaya & Sagiroglu, 2010; Ryu et al., 2021; Tome et al., 2015; Wlodarczyk, 2012).
Eyes	(Alay & Al-Baity, 2020; Ameer & Jose, 2021; Ammour et al., 2020; Asha & Chellappan, 2012; Bhatia & Bhabha, 2017; Bokade & Kanphade, 2019; Crampton, 2019; Down & Sands, 2004; Essink et al., 2020; Godi & Rao, 2019; Haghigar et al., 2013; Jain et al., 2004; Jain et al., 2006; Jain & Kumar, 2010; Keyser et al., 2021; Kono et al., 2015; Kour et al., 2016; Krishan & Mostafavi, 2018; Lagou & Chondrokoukis, 2011; Lai et al., 2019; Langenderfer & Linnhoff, 2005; Liu et al., 2019; Luo et al., 2018; Lyon, 2008; Mohsin et al., 2020; Moolla et al., 2021; Moradoff, 2010; Mordini & Massari, 2008; Nagwashi & Dubey, 2018; Niculescu & Coman, 2017; Ozkaya & Sagiroglu, 2010; Ryu et al., 2021; Salvi et al., 2021; Sanjekar & Patil, 2013; Soltane et al., 2017; Sreeja et al., 2018; Talreja et al., 2017; Wlodarczyk, 2012; Xiao, 2007; Yang et al., 2018; Yang et al., 2019; Yang et al., 2021; Yuan & Yu, 2013; Zheng, 2021; Zhu et al., 2018).
Face	(Alay & Al-Baity, 2020; Ammour et al., 2020; Asha & Chellappan, 2012; Bokade & Kanphade, 2019; Crampton, 2019; Down & Sands, 2004; Essink et al., 2020; Godi & Rao, 2019; Haghigar et al., 2013; Hamoodi & Ramadhan, 2019; Jacquet & Champod, 2020; Jain et al., 2004; Jain et al., 2006; Jain

	& Kumar, 2010; Keyser et al., 2021; Kono et al., 2015; Kour et al., 2016; Krishan & Mostafavi, 2018; Lagou & Chondrokoukis, 2011; Langenderfer & Linnhoff, 2005; Luo et al., 2018; Lyon, 2008; Mishra, 2010; Mohsin et al., 2020; Moradoff, 2010; Mordini & Massari, 2008; Morosan, 2018; Niculescu & Coman, 2017; Norval & Prasopoulou, 2019; Ozkaya & Sagiroglu, 2010; Ryu et al., 2021; Salvi et al., 2021; Sanjekar & Patil, 2013; Soltane et al., 2017; Sreeja et al., 2018; Talreja et al., 2017; Tome et al., 2015; Wlodarczyk, 2012; Xiao, 2007; Yang et al., 2018; Yang et al., 2019; Yang et al., 2021; Yuan & Yu, 2013; Zheng, 2021; Zhu et al., 2018).
Fingerprints	(Alay & Al-Baity, 2020; Ammour et al., 2020; Appati et al., 2021; Asha & Chellappan, 2012; Bhatia & Bhabha, 2017; Bhilare et al., 2018; Bokade & Kanphade, 2019; Caplova et al., 2018; Ceyhan, 2008; Down & Sands, 2004; Essink et al., 2020; Godi & Rao, 2019; Haghigar et al., 2013; Jacquet & Champod, 2020; Jain et al., 2004; Jain et al., 2006; Jain & Kumar, 2010; Keyser et al., 2021; Kono et al., 2015; Kour et al., 2016; Lagou & Chondrokouski, 2011; Lai et al., 2019; Langenderfer & Linnhoff, 2005; Liu et al., 2019; Luo et al., 2018; Lyon, 2008; Meagher et al., 2014; Mohsin et al., 2020; Moolla et al., 2021; Moradoff, 2010; Mordini & Massari, 2008; Morosan, 2018; Nagwashi & Dubey, 2018; Niculescu & Coman, 2017; Norval & Prasopoulou, 2019; Ozkaya & Sagiroglu, 2010; Pisani et al., 2019; Ryu et al., 2021; Salvi et al.,. 2021; Sanjekar & Patil, 2013; Soltane et al., 2017; Sreeja et al., 2018; Talreja et al., 2017; Tu et al., 2020; Wlodarczyk, 2012; Xiao, 2007; Yang et al., 2018; Yang et al., 2021; Yuan & Yu, 2013; Zheng, 2021; Zhu et al., 2018).
Foot dynamics	(Meagher et al., 2014; Moradoff, 2010; Mordini & Massari, 2008; Nagwashi & Dubey, 2018).
Gait (walking gait)	(Ammour et al., 2020; Bokade & Kanphade, 2019; Crampton, 2019; Jain et al., 2004; Keyser et al., 2021; Kour et al., 2016; Krishan & Mostafavi, 2018; Lai et al., 2019; Mishra, 2010; Mohsin et al., 2020; Niculescu & Coman, 2017; Ryu et al., 2021;

	Salvi et al., 2021; Sanjekar & Patil, 2013; Talreja et al., 2017).
Hands	(Ameer & Jose, 2021; Asha & Chellappan, 2012; Bhilare et al., 2018; Bokade & Kanphade, 2019; Down & Sands, 2004; Jain et al., 2004; Jain et al., 2006; Jain & Kumar, 2010; Keyser et al., 2021; Kono et al., 2015; Kour et al., 2016; Langenderfer & Linnhoff, 2005; Liu et al., 2019; Mohsin et al., 2020; Moradoff, 2010; Mordini & Massari, 2008; Ozkaya & Sagiroglu, 2010; Wlodarczyk, 2012; Xiao, 2007).
Keystroke dynamics	(Ammour et al., 2020; Bokade & Kanphade, 2019; Down & Sands, 2004; Jain et al., 2004; Jain et al., 2006; Jain & Kumar, 2010; Keyser et al., 2021; Kour et al., 2016; Morosan, 2018; Niculescu & Coman, 2017; Ryu et al., 2021; Salvi et al., 2021; Soltane et al., 2017; Xiao, 2007; Yang et al., 2021).
Marks (birthmarks, freckles, moles)	(Dantcheva et al., 2015; Keyser et al., 2021; Nixon et al., 2015).
Metabolic attributes	(Hair et al., 2018).
Nails	(Wlodarczyk, 2012).
Neural analysis (neurological signals given off by neurons firing in the brain, analyzed using electroencephalography (EEG) and functional magnetic resonance imaging (fMRI)	(Keyser et al., 2021; Kumar et al., 2019; Lai et al., 2019).
Palm prints	(Ammour et al., 2020; Asha & Chellappan, 2012; Bhilare et al., 2018; Bokade & Kanphade, 2019; Crampton, 2019; Godi & Rao, 2019; Jain et al., 2004; Jain & Kumar, 2010; Kour et al., 2016; Lai et al., 2019; Langenderfer & Linnhoff, 2005; Luo et al., 2018; Meagher et al., 2014; Nagwashi & Dubey, 2018; Niculescu & Coman, 2017; Ryu et al., 2021; Sanjekar & Patil, 2013; Soltane et al., 2017; Sreeja et al., 2018; Yang et al., 2021; Zheng, 2021).
Scars	(Abdelwhab & Viriri, 2018; Caplova et al., 2018; Dantcheva et al., 2015; Jacquet & Champod, 2020; Nixon et al., 2015; Ryu et al., 2021; Tome et al., 2015).
Signature dynamics	(Alay & Al-Baity, 2020; Ameer & Jose, 2021; Ammour et al., 2020; Bokade & Kanphade, 2019; Down & Sands, 2004; Hamoodi & Ramadhan, 2019; Jacquet & Champod, 2020; Jain et al., 2004; Jain et al., 2006; Jain & Kumar, 2010; Kour et al., 2016; Lai et al., 2019; Luo et al., 2018;

	Mishra, 2010; Pisani et al., 2019; Salvi et al., 2021; Sanjekar & Patil, 2013; Soltane et al., 2017; Sreeja et al., 2018; Xiao, 2007; Yang et al., 2021).
Skin patterns	(Crampton, 2019; Mordini & Massari, 2008).
Smell	(Wlodarczyk, 2012).
Tattoos	(Abdelwhab & Viriri, 2018; Caplova et al., 2018; Dantcheva et al., 2015; Jain & Ross, 2015; Keyser et al., 2021; Nixon et al., 2015).
Tongue	(Sivakumar et al., 2018).
Vein patterns	(Alay & Al-Baity, 2020; Bhilare et al., 2018; Keyser et al., 2021; Kono et al., 2015; Krishan & Mostafavi, 2018; Langenderfer & Linnhoff, 2005; Moradoff, 2010; Morosan, 2018; Niculescu & Coman, 2017; Ryu et al., 2021; Sreeja et al., 2018; Staunch et al., 2020; Wlodarczyk, 2012).
Voice	(Alay & Al-Baity, 2020; Ameer & Jose, 2021; Bokade & Kanphade, 2019; Down & Sands, 2004; Haghigar et al., 2013; Jain et al., 2004; Jain et al., 2006; Jain & Kumar, 2010; Keyser et al., 2021; Krishan & Mostafavi, 2018; Lagou & Chondrokouski, 2011; Lai et al., 2019; Luo et al., 2018; Mishra, 2010; Mohsin et al., 2020; Morosan, 2018; Nagwashi & Dubey, 2018; Niculescu & Coman, 2017; Ozkaya & Sagiroglu, 2010; Pisani et al., 2019; Salvi et al., 2021; Sanjekar & Patil, 2013; Soltane et al., 2017; Sreeja et al., 2018; Talreja et al., 2017; Xiao, 2007; Yang et al., 2018; Yang et al., 2019; Yang et al., 2021).

Appendix B: Biometric System References

Computerized tomography (CT) scan	(Jeon et al., 2019).
Electrocardiogram (ECG/EKG)	(Agrafioti et al., 2011; Barros et al., 2020; Blasco & Peris-Lopez, 2018; Jekova et al., 2018; Mir et al., 2011; North-Samardzic, 2020; Ramos et al., 2021; Salvi et al., 2021; Wu et al., 2020; Zhang et al., 2019).
Electroencephalogram (EEG)	(Barros et al., 2020; Kumar et al., 2019; Lai et al., 2019; Mir et al., 2011; North-Samardzic, 2020).
Eye scanners	(Alay & Al-Baity, 2020; Bhatia & Bhabha, 2017; Jain & Kumar, 2010; Krishan & Mostafavi, 2018; Lagou & Chondrokoukis, 2011; Liu et al., 2019; Soltane et al., 2017).
Facial recognition	(Alay & Al-Baity, 2020; Ameer & Jose, 2021; Essink et al., 2020; Galterio et al., 2018; Jacquet & Champod, 2020; Jain & Kumar, 2010; Jeon et al., 2019; Krishan & Mostafavi, 2018; Liu et al., 2019; Ryu et al., 2021; Soltane et al., 2017; Wlodarczyk, 2012; Xiao, 2007).
Fingerprint scanners	(Alay & Al-Baity, 2020; Ameer & Jose, 2021; Appati et al., 2021; Bhatia & Bhabha, 2017; Ilousani & Ezema 2017; Jain & Kumar, 2010; Lalović & Bogdanoski, 2021; Langenderfer & Linnhoff, 2005; Liu et al., 2019; Meagher et al., 2014; Moradoff, 2010; Sohn et al., 2020; Soltane et al., 2017; Tu et al., 2020; Yang et al., 2019; Zheng, 2021).
Finger-vein scanners	(Bhilare et al., 2018; Jain & Kumar, 2010; Krishan & Mostafavi, 2018; Mohsin et al., 2020; Yang et al., 2018).
Functional magnetic resonance imaging (fMRI)	(Lai et al., 2019).
Magnetic resonance imaging (MRI)	(Caplova et al., 2018; North-Samardzic, 2020).
Palm print scanners	(Bhilare et al., 2018; Jain & Kumar, 2010).