The Advantages and Disadvantages of Biometrics in Forensic Investigations

Name

Institution

Contents

This research study evaluates the advantages and disadvantages of biometric technologies within forensic investigations. There is widespread reliance on existing biometric techniques such as fingerprints and DNA samples to identify the suspect when a crime has been committed, however, such methods have their shortcomings an in particular the invasive manner in which such evidence is collected from the suspect. Researchers have proposed mechanisms by which biometric identification data can be obtained from the general population which can be stored in databased and used to identify or verify the identity of potential suspects. Clear privacy concerns arise from the collection of such data in relation to the general population as well as data protection issues. The main focus of this research will be on the main advantages and shortcomings of particular biometric techniques, including facial recognition, gait analysis and ear recognition as well as modification and advancements of existing techniques.

Chapter 1: Introduction to Biometrics for Forensic Examinations

1.1 Background

Biometric techniques have played an important role within the context of criminal and civil legal investigations for identification or authentication of perpetrators and for the provision of evidence within a court of law (Tistarelli and Champod, 2017). The difficulties presented by the reliability of witness identification has paved the way for recognition of identification techniques based upon biometric features. Such technologies have been used from as early as the turn of the nineteenth century, when Bertillon created standardised descriptive techniques that enabled the description and photographic documentation of faces and later created Anthropometry, the standardised measurement of selected features of the human body (Tistarelli and Champod, 2017). The development of fingerprinting identification systems, replaced Anthropometry shortly afterwards (Tistarelli and Champod, 2017).

Biometric identification refers to the process of verifying the identify an individual based upon her or his distinguishing physiological or behavioural characteristics. Physiological biometrics include finger prints or hand geometry are physical characteristics that are measured at a given point in time. Behavioural biometrics include the signature or voice, and consist of the way some form of behaviour is carried out; these persist over time (Bolle et al., 2013). Examples of

physiological biometrics that are in common use at this time include: face, fingerprint, hand geometry and iris. The signature and voice are behavioural biometrics that are also currently in frequent use (Bolle et al., 2013). There are a number of other physiological biometric identifiers that are currently in early stages of development, or used less frequently including: DNA, ear shape, odour, retina, skin reflectance and thermogram. Developmental uses of behavioural biometric identification include gait, keystroke and lip motion (Bolle et al., 2013). Each method has its own advantages and shortcomings and can be used in varying real-world applications.

Forensic science is currently facing a number of challenges in relation to the requirement to detect crime and identify the perpetrators of crime. The insufficiency of available evidence often creates challenges for the forensic investigator, including the need to locate a small piece of biological or physical evidence that is hidden within a chaotic crime scene; for example a small portion of a fingerprint, concealed handwriting or shoe print (Saini and Kapoor, 2016). Since most criminals attempt to conceal their crimes, some become incredibly adept at creating skilled forgeries; forensic examiners constantly need to seek new methods to find evidence despite such deception (Saini and Kapoor, 2016). Traditional methods of criminal identification and verification can involve very time consuming procedures, however, the detection of crime is also a very time sensitive process and evidence can be quickly destroyed, the faster a perpetrator can be identified, the more easily evidence and be maintained to secure a conviction. Finally, crime detection can involve many non-standard procedures; this poses great challenges in the face of the limitations of the cognitive ability of human forensic expertise (Saini and Kapoor, 2016). Hence the development of biometric technologies to address these challenges are great imperatives for the efficient and effective detection of criminal activity.

1.2 Aims and Objectives

The aims of the research study are to evaluate the advantages and disadvantages of the use of biometric technologies and its application within forensic investigations. The following objectives will be pursued:

- The evaluation of current trends and recent research into biometric identification and verification systems and their applications within forensic examinations;

- The consideration of specific advantages that can be introduced into the detection and prosecution in criminal courts of offenders through the use of biometric techniques
- The highlighting of the particular challenges that biometric technologies bring to the realm of forensic investigations and the adducing of reliable evidence in court

1.3 Methodology

The research study adopts a qualitative methodology, which emphasises an inductive approach in that theoretical ideas about the advantages and disadvantage of biometrics in forensic investigations are derived from the research rather than being formed prior to the collection of data (Bryman, 2016). In order to gain insight into these issues the research involves a secondary analysis of existing research studies which are available in academic texts, conference papers and academic journals. The choice of secondary methods is based on the fact that it enables the researcher to review an extensive range of various biometric technologies and methods within a single study, gives more time for the researcher to evaluate and interpret the data (Bryman, 2016) and draw comparisons about the relative weights of the various methods. A search was carried out of the relevant academic journal databases, which was largely restricted to English language publications and to research conducted between 2008 and 2018, although earlier studies are considered to provide historical context. The restriction to publications from the past ten years is based on the fact that biometrics is a fast moving field of technology and that the most recent research indicates the current state-of-the-art that is available for use within forensic investigations. Databases such as ACM Digital Library, IEEE Xplore, SCOPUS, and ProQuest, were searched using terms such as ‘biometrics’, ‘identification’, ‘authentication’, ‘forensic investigation’, ‘gait analysis’ and ‘facial recognition’.

1.4 Subsequent Chapters

Chapter 2 outlines and evaluates the advantages of biometric technologies in forensic investigations. It highlights the current biometric techniques and their particular benefits which they can bring to the field of digital forensics and their application in legal cases in providing sufficient reliable evidence to secure convictions against perpetrators of crime.

Chapter 3 considers the disadvantages and challenges of the use of biometric techniques within forensic investigations include shortcomings inherent within the technologies themselves and ethical and civil liberties considerations of the capturing of biometric data without the subject's consent. While shortcomings exist, this chapter also highlights some of the advances in methodologies that have been introduced to address the challenges inherent within biometric technologies.

Chapter 4 will bring together conclusions regarding the relative merits and shortcomings of biometric systems for forensic requirements as well as recommendations on variations that can be made to current techniques in order to address current limitations.

Chapter 2: Advantages of the use of Biometric Technologies in Forensic Examinations

The attacks on the World Trade Centre, New York of September 11, 2001 led to calls for developments of biometrics for security purposes to achieve more consistency across techniques worldwide (Norris-Jones and Marsh, 2009). However, while the public have been assured that biometric development would lead to the enhancement of national security, a number of concerns exist regarding the implications of advancement in such securities on technical, legal and ethical grounds (Norris-Jones and Marsh, 2009). Biometric systems such as forensic DNA databases have proven to promise significant benefits, but provides certain risks to civil rights protections (Smith, 2018). This Chapter focuses primarily upon the advantages of biometric technologies, with the risks and potential costs being reserved for Chapter 3.

2.1 Current Uses of Biometric Technologies

Biometric technologies have advantages as identification and authentication methods; rather than traditional identification measures centred upon a card, token or key that can be replicated or stolen, biometrics allow the identification based upon who the person is (Delac and Grgic, 2004). These technologies offer advantages over traditional authentication and identification mechanisms, including improved security features, fast and user-friendly authentication and access control as well as the ability of encrypting sensitive information (Flores Zuniga et al., 2010). The risks inherent within use of non-biometric recognition methods which is limited to what the subject knows or possesses are largely mitigated when biometric recognition systems

are employed. Biometric recognition systems are able to provide protection from theft or loss of access data, as well as convenience of us since access data does not been to be remembered or carried (Barbosa et al., 2016).

Several human characteristics have been studied in biometric applications and can be divided into separate categories depending on the area of human body that is involved. This method of categorisation includes (i) attributes of the hand (including finger prints and hand geometry) (ii) attributes of the eye region (e.g retina, iris), and (iii) attributes of the facial region (e.g. ear or face). Further characteristics include those related to chemical-medical attributes, (e.g. DNA, odour, bone) or to behavioural attributes (e.g electronic signature, gait) (Benzaoui et al., 2017). The various modalities of biometrics offer varying degrees of reliability. While DNA, the iris and the fingerprint are considered to be highly reliable in providing authentication and identification of a human subject, they require the cooperation of the subject. This has led researchers to focus on other areas, such as the face and the ear, since they do not require cooperation from the data subject (Benzaoui et al., 2017). Although regarded by researchers as an advantage of such techniques, this in itself however can lead to concerns over infringements into personal privacy which is discussed in Chapter 3.

The uses of biometric technologies are extensive. Criminal suspects have been successfully identified in airports or other public places through the use of surveillance cameras and the matching of facial characteristics with database images. Biometrics systems are thus used for the purposes of identification, where a person's identity can be verified without their awareness or approval(Bhatia, 2013). The scanning of people in a crowd can lead to the determination of an individual's identity by matching facial images with those in a security database. Biometrics are also used for verification purposes, to verify a particular identity based upon those who have permitted access to an area of a building, through a retina scans(Bhatia, 2013).

Biometric technologies can bring great advantages within the realm of forensic investigations. An example is the potential impact of a universal DNA database, which would include a collection of DNA profiles and associated information that can be used to identify suspects in criminal investigations. National DNA databases are held in both the United Kingdom and the United States (Smith, 2018). In August 2018, the US National DNA Index System (NDIS)

contained approximately 13.5 million profiles of convicted offenders and almost 900,000 crime scene profiles(Federal Bureau of Investigation, 2018). The United Kingdom's National NDA Database (NDNAD) is the largest in the world as a proportion of its population, with over 6 million offender profiles and over 550,000 crime scene profile records, as of 31 March 2017(Home Office, 2018). The benefits of DNA databases and associated technologies in forensic investigations is their ability to enable the more efficient investigation and prosecution of crime; it is argued that a universal database would remove the requirement for mass DNA screenings and theoretically act as a deterrent to individuals committing crimes due to much better detection rates and the difficulties this present to perpetrators in avoiding detection(Smith, 2018). The storage of personal data also carries civil liberties consequences however, which will be discussed in Chapter 3.

2.2 Biometrics for Facial Recognition

A popular method for identification which is non-invasive is facial recognition, which has a variety of potential uses both within the realms of forensic investigations and elsewhere. Mobile devices contain various types of private and commercially sensitive data and hence it is in the user's interests to ensure both confidentiality and integrity of the data that is stored and made accessible via such devices(Au and Choo, 2016). Biometric technologies therefore offer certain advantages over traditional methods such as pin numbers, which can be obtained through various nefarious means leading to potential intruder access to the device. Face biometrics have attracted significant attention as a potential technology that can provide secure access to mobile devices (Rattani and Derakhshani, 2018), since almost all smartphones have RGB cameras which are suitable for capturing facial images. However, traditional face biometrics may not be executable on mobile hardware due to the limited computing power and memory storage within mobile devices (Rattani and Derakhshani, 2018).

Despite the existence of various biometric techniques, such as finger prints, iris scan and hand geometry, face recognition is the most efficient and widely used (Chihaoui et al., 2016). Facial recognition is achieved through a three stage process illustrated in figure 1.

Figure 1: Face recognition process(Chihaoui et al., 2016)

Facial recognition systems start with the detection of the face in an image; in general, the system can decide if an image contains a face or not. The system then detects the location of one or more faces in an image (Chihaoui et al., 2016). This stage can become more difficult where there are additional complicating features in the image, such as facial expressions (smiling, surprise), orientation and other features such as glasses or facial hair. All of these features create obstacles to accurate facial detection (Chihaoui et al., 2016). After detecting the face in the image, then next stage is to extract the features of the face, or the features vectors known as the signature of the detected face. Authentication involves the comparison of a face with another in order to approve the requested identity; identification requires the face to be compared with several other faces to locate the correct face between among several possibilities (Chihaoui et al., 2016).

There many different approaches to facial recognition. Global approaches represent the face as a matrix of pixels, which is transformed into pixel vectors so that they can be manipulated. Such approaches are sensitive to variations such as lighting, posture, expression and orientation. Furthermore within an image of a face, there are other objects in the background; linear and non-linear approaches are therefore used in order to isolate just the facial image (Chihaoui et al., 2016). Depending on the type of classification system used features can be local features such as lines or facial features such as eyes, nose and mouth. Feature extraction is critical to animation and recognition of facial expressions (Kumar et al., 2014). Research into these areas therefore has developed to overcome the various disadvantages and provided improved techniques to improve rates or recognition.

Facial detection strategies can be divided into knowledge based methods, feature based methods, image-based methods and template matching methods. The knowledge-based methods have the advantage of being relatively simple as they calculate the parameters of human facial features and their relationships; this works well with frontal facial images. Feature based methods can be

further divided into low-level analysis, feature analysis and active shape models. From these Point Distributed Models, which are active shape models have particularly good detection rates (95%) (Kumar et al., 2014). Images based methods include the use of neural networks, which can be used to optimise performance by training multiple networks independently and then using their outputs combined with various arbitration methods(Kumar et al., 2014). The advantage of various methods being available is that this improves the chances of finding mechanisms to overcome particular obstacles to recognition that depend upon specific circumstances. A combination of methods can be used to fit particular requirements.

The final stage of facial biometrics is the recognition phase which can include holistic matching methods, one of the most widely based applications being Eigen pictures, which are based on principle component analysis(Kumar et al., 2014). Feature-based (structural) matching methods involve the feeding of local features (eye, mouth, nose) with local statistics, such as geometry or appearance and fed into a structural classifier. A hybrid method which combines the two previous approaches presents the most advantages, through the use of local features and the whole face region to recognise the face thus providing the greatest rates of recognition amongst these methods(Kumar et al., 2014).

The most common techniques for facial recognition are currently 2-dimentional (2D) techniques, however, the most recent advances in this area are 2-dimentional (3D) techniques which have been found to offer great support for improving recognition performance. Researches have demonstrated that 3D depth maps provide a more robust face representation, which is less affected by changes in lighting than 2D images (Maria and Nappi, 2014). 3D models are built using range data or a polygonal mesh, retains much more information about the complex geometry of the face than 2D models. A whole head model can be created by taking several scans from various viewpoints to create a global representation of the whole head as opposed to a 2D image of just the face.

The most popular way is to create a 3D polygonal mesh, which consists of a list of vertices connected by edges. Despite their asserted robustness however, 3D models can be computationally expensive; moreover, 3D sensors are still affected by a strong light source or reflective surfaces (Maria and Nappi, 2014). Moreover, 3D images cannot be acquired without

the subjects cooperation and require accurate calibration and synchronisation of all the elements of the system; this cannot be achieved in a uncontrolled setting in the way that 2D facial images are acquired (Maria and Nappi, 2014). The relative weaknesses of these methods is that they are not suitable for use in forensic investigations at present, due to the complexities of creating the 3D images.

2.3 The Benefits of Facial Biometrics in Forensic Investigations

While fingerprint recognition techniques have been used for decades in digital forensics, facial recognition techniques provide more benefits. Facial recognition techniques have benefits in that facial images are easier to obtain than fingerprints. No human participation is required, all that is needed is a suitable camper system to capture the person's identity (Lohiya and Shah, 2015). Police officers can easily be equipped with computers and tablets to enable quick searches of an individual against existing criminal records. Images are available through extensive quantities of video footage from CCTV cameras which may be analysed manually in which suspects faces are available. Automatic facial recognition techniques therefore improve this process (Lohiya and Shah, 2015). Since digital cameras which have the capacity to record both still images and videos are ubiquitous within society, videos and images obtained pay an important role in the investigation and prosecution of crime (Srinivas et al., 2016).

In forensic applications facial comparisons are carried out for a number of purposes, including the gathering of intelligence data, screening and access control, and forensic identification. Since automatic processes for facial comparison do not conform to a single standard practice, forensic facial comparisons are frequently performed manually (Srinivas et al., 2016). At present automated facial recognition processes are accurate under controlled circumstances, they have yet to achieve a level of reliability and repeatability that make them suitable for forensic identification purposes. While expert evidence of manual comparisons is therefore routinely accepted as evidence in multiple United States federal and state courts (Spaun and Bruegge, 2008), automatic recognition does not yet provide sufficient reliability to be used in this way. Various research studies have therefore been established in order to overcome the lack of reliability in the current facial recognition systems within forensic use.

Facial features used in forensic facial comparison can be distinguished as either class characteristics of individual characteristics. The former are shares by a number of persons within a group, including the overall facial shape, shape of the ears, eyes, mouth or nose and the existence of facial hair(Srinivas et al., 2016). Srinivas et al (2016) have proposed an improved multi-scale facial mark system in which facial marks are detected automatically and a semi-automatic facial mark system that integrated human knowledge with the improved multi-scale facial mark system. The results of their study who that geometric distributions of facial mark patterns can be used to distinguish between individuals for the purposes of forensic investigations. A combination of an automated system with human knowledge was shown to improve performance. Future research in this field seeks to distinguish the classification of transient and permanent marks(Srinivas et al., 2016) which is necessary if facial recognition data is going to have reliability over time at the identification of suspects.

2.4 Gait and Ear Biometrics

Biometrics for the gait and ear are a smaller research field than established biometrics like facial recognition and finger prints, but the former are more directly amenable to forensic use. Gait has been used in a number of successful criminal convictions in the UK (Nixon et al., 2010). Early studies on ear and gait biometrics began in the 1990s, however, some of the early studies were carried out on very small databases of samples. There are a number of advantages of using gait and ear biometrics in forensic investigations. Gait is an emergent biometric which is defined as the manner of locomotion, or the way of walking (Nixon et al., 2010). There are a large number of studies that have shown the advantages of gait biometrics(Nixon et al., 2006) few are concerned with the use of gait for identification within forensics.

2.5 The Advantages of Ear Biometrics in Forensic Investigations

There are also major advantages of ears biometrics for forensic deployment, this they ear ages more gradually than the human face of gait. Since the ear is part of the disaster identification system, it may be possible to match suspects even after a considerable passage of time, or despite considerable natural disguise such as hair growth(Nixon et al., 2010). While earlier biometric modalities need complete user permission and cooperation, later modalities can be used without

knowledge of the subjects the sensors are able to capture images at a distance (Sarangi et al., 2018). Images of ears can be captures using a low resolution camera in a similar way to the face and does not require considerable cooperation by the subject (Sarangi et al., 2018).

An ear recognition system can be described of three basic stages: ear normalisation, feature extraction and classification. The ear image must initially be normalised to a standard size and direction according to the long axis of the outer ear contour. The long axis is calculated by establishing the two points which have the longest distance on the ear contour and sketching a line that crosses through them (Yuan and Mu, 2014). The second and third stages are to represent the ear with its appropriate feature extraction and classification, an area where there has been significant academic research (Masaoud et al., 2013). In real world applications of ear biometrics the greatest challenge is finding an efficient descriptor to represent and model the human ear which can be affected by varying lighting levels, pose variation, noise and occlusion (Benzaoui et al., 2014). In this respect local descriptors representing features in small local image patches have been proven to be more effective in real-world conditions that global image descriptors that are derived from the entire ear image(Benzaoui et al., 2014).

2.6 The Advantages of Gait Biometrics in Forensic Investigations

Gait recognition has particular advantages in that is has the potential to overcome many of the major limitations of other biometric techniques such as face, iris and fingerprint recognition, which can be obtain from many crime scenes. Larsen and Simonsen (2008) have established the usefulness of gait analysis in forensic investigations, in being able to identify a bank robber my matching surveillance from the crime scene against images of a potential suspect. The evidence was later used in court and assisted in the securing of a conviction against the suspect (Larsen et al., 2008). A real life case in the UK of a burglar who was apprehended by the police due to the distinctive way in which he walked, which was analysed and identified by a podiatrist (Bouchrika et al., 2011). The gait of the perpetrator was captured on CCTV images. Through gait analysis of the surveillance images and a posture assessment the podiatrist was able to confirm a significant similarity between the individual captured on the images and police suspect. Faced with this evidence against him, the suspect pleaded guilty to the crime (Bouchrika et al., 2011).

Gait is defined as “the manner of locomotion characterised by consecutive periods of loading and unloading the limbs” (Bouchrika, 2016, p. 310). The rhythmic pattern of human gait follows an established pattern, consisting of repeated cycles; characterised in two phases: the stance phase and the swing phase. Thus human gait is made up of four main sub-tasks that together constitute a walking pattern (Bouchrika, 2016). The typical gait biometric system is comprised to two components: (i) a hardware system that acquires data, usually a single CCTV camera or distributed network of cameras and (ii) the software system that is capable of recognition and processing of data. The software system for gait biometrics is established through a three stage process: (i) subject detection, (ii) feature extraction and (iii) data classification. Various classification techniques are used in vision-based systems for gait recognition, including K-Nearest Neighbour Classifier (KNN) as the most popular, Support Vector Machines and Neural Networks. The advantage of KNN is its simplicity and fast computation (Bouchrika, 2016). Gait analysis provides advantages in situations where a perpetrators face is obscured or veiled and CCTV footage is deemed unusable for direct recognition and in situations where other methods of identification such as DNA or fingerprints are unavailable(Bouchrika, 2016).

2.7 Summary

From this chapter it has been observed that biometric techniques can offer various advantages to the realm of forensic investigations and in detection and prosecution of criminal activity. The use of automated methods such as facial recognition greatly increases the speed of recognition which can be a long process when carried out through human cognitive processes. Such evidence can also be more reliable in court, scientific demonstrations of identification are often more reliable than witness testimony which can often prove extremely unreliable(Choo, 2018). While there are many biometric methods, the focus has been upon facial recognition, gait and ear biometrics. All three of these methods are of value within forensic investigations due to the ability to obtain biometric information from subjects without their participation. These techniques therefore overcome the shortcomings of the most commonly used techniques (DNA and fingerprints) in that data can be obtained from the subject in a non-invasive manner. These mechanisms of identification and authentication have also proved reliable, nevertheless due to various constraints that will be discussed in the next chapter, their wide scale adoption has not yet been achieved.

Chapter 3: Disadvantages and Challenges in using Biometric Technologies in Forensics

There are a number of disadvantages and challenges in implement biometric technologies for forensic investigations. Each technology has its own disadvantages and the use of biometrics themselves have challenges that are related to the nature of their use. Furthermore, important regulations that exist within the EU put significant restrictions upon the storage and processing of personal data that prevents the acquisition and storage of biometric data about individuals without their consent.

3.1 The Shortcomings of Biometrics as Forensic Evidence

There are challenges of facial biometrics for identification and authentication purposes within forensic investigations. Due to the nature of changes in the face and expression over time as well as other challenges such as varying illuminations, poor contrast and non-cooperation by subjects these technologies lead to limited recognition performances (Sarangi et al., 2018). Facial recognition in many instances has proved unreliable for visual surveillance systems; this is due to the fact that those who are committing crimes have become well aware of the fact that CCTV is frequently in operation in many areas and therefore disguise or hide their faces. Furthermore video data that is captured may be too low resolution in order to reliably identify the perpetrator from their facial characteristics(Bouchrika et al., 2011). A significant shortcoming of video image data of facial figures in security applications is that facial features may not be recovered from a distance, even when using night vision capacities (Kale et al., 2002).

Gait analysis also has a number of shortcomings that would enable defence counsel to challenge its reliability as evidence in court. In comparison to well-established methods used in biometrics such as fingerprints and DNA, gait analysis may be influenced by a variety of external covariate factors which can impact upon the gate pattern and thus render evidence unreliable (Bouchrika, 2016). These factors include psychological variations such as state of anxiety and medical conditions or those related to appearance such as footwear and clothing. Environmental factors can also affect the credibility of evidence such as lighting conditions and viewpoint (Bouchrika, 2016).

3.2 Privacy and Biometric Data Protection

The right to respect for a private life is an important human rights protection incorporated within Article 8 European Convention on Human Rights 1950 (ECHR). It is the foundation of protections against the collection and use of personal data. Ethical and legal considerations with regards to biometric data usage is directly related to the right of protection of personal data (Deliversky and Deliverska, 2018). The lack of transparency and lawfulness of the processing of personal data can lead to physical, tangible and intangible damages; the processing of images can lead to identity theft, discrimination or identity fraud, leading to serious economic or social consequences(Deliversky and Deliverska, 2018). Evidence that has been obtained by unlawful means can also be subject to challenge when adduced in court and therefore may be unreliable in securing a conviction. Researches in the field of biometric technologies appear to regard the ability to obtain biometric data by non-invasive means (and without the requirement to obtain consent from the data subject) as a benefit in biometric techniques. This aspect does however raise privacy and ethical concerns about the collection of such data.

Development of new technologies in the area of biometrics pose similar challenges to those posed by human genetics databases (Sutrop, 2010). While on the one hand biometric technology is coveted as a mechanism with which to address the perceived need for increased security, it is also feared that without sufficiently stringent regulations that there is a risk of abusing fundamental rights to human dignity and privacy(Tomovo, 2009). No biometric data is totally accurate, even a common DNA analysis does not have a 100% reliability. However, in many uses within criminal investigations its accuracy is critical. Ethical problems arise in the application of biometrics and communication technologies which involve the transfer or personal data about individuals (Cosmi et al., 2009). “Function creep” is a particular problem that related to the application of biometrics. This occurs where the original purpose for which the data collection is justified is overreached and the biometric data is used for various other purposes (Cosmi et al., 2009).

Three separate aspects of biometric technologies and their application to forensic investigations give rise to separate ethical or legal concerns. The first is the taking of the biometric sample from the individual through image capture, current uses such as fingerprints and iris scan are regarded by researchers as disadvantageous due to their invasive nature (and the requirement to obtain consent from the data subject) (Benzaoui et al., 2017). The second stage is the extraction of data

from the sample, to create a biometric template. The final stage is the storage of the image or template in a database, which may be stored locally on hardware within the organisation, or externally at an unknown location within the cloud (Tomovo, 2009). Since biometric data is derived from the human body there are understandably areas of resistance based upon individual, religious or socio-cultural differences. Fair processing of personal data requires that the data subject be informed of the storage of data; the data controller also has responsibility to establish a certain degree of accuracy of the system. Hence there is a need within the various cultural, social and religious contexts for the right balance to be achieved between security needs for identification and verification and legal and ethical requirements for data protection (Tomovo, 2009).

3.3 Data Protection and the Storage of Biometric Data

The EU General Data Protection Regulation 2016/679 (GDPR) came into force in 2018, and creates new regulations for the collection, storage and retention of biometric data. The Regulation introduces several categories of personal data which related to physical, behavioural and physiological characteristics to which different regimes apply (Kindt, 2018). The GDPR introduces a complex set of laws which regulates the collection, storage and retention of biometric data, which also enables EU Member States some discretion as to adopt or modify existing legal rules. This has led to a lack of clarity on the legal requirements surrounding the processing of personal biometric data (Kindt, 2018).

Retention of biometric data of individuals who have not been convicted of a criminal offence is one of the biggest legal difficulties, an issue that has been subjected to successful legal challenge. For example, in the UK in *S & Marper v United Kingdom* [2008] ECHR 1581, the police had retained DNA samples of individuals who had been arrested but had later been acquitted, or who had had the charges against them dropped. The European Court on Human Rights (ECtHR) found the retention of their DNA evidence to be a violation of their right to privacy under Article 8 ECHR (Sampson, 2018). Furthermore, the indefinite retention of biometric samples including DNA evidence and fingerprints of data subjects was successfully challenged in *R (on the application of GC & C)* v *The Commissioner of Police of the Metropolis* [2011] UKSC 21, except for in exceptional circumstances.

However, despite these findings the police have also been criticised for failing to retain sufficient evidence on dangerous offenders such as Ian Huntley, who was convicted in 2003 of the murder of two 10-year-old girls in the Bichard Report (Bichard, 2004). Hence the public consider that law enforcement authorities should have access to all available data on those who may have committed serious criminal offences, yet still value their own privacy when it comes to the sharing of personal data. The critical issue therefore is how to achieve the correct balance between the needs of law enforcement agencies to detect those responsible of serious crimes and the needs of the public to keep their own personal data private and protected from misuse.

3.4 Overcoming Privacy Concerns: Transient Biometrics

In general, it is considered that biometric description should be universal and permanent. The universality condition implies that it can be derived from the great majority of members of the population, while permanency indicates that the biometric signature should maintain its consistency over time(Bouchrika, 2016). These permanent characteristics offer advantages over traditional identification or verification methods such as passwords, pin numbers, driving licences of passports since they cannot be stolen or forgotten. However, there are a number of privacy concerns within permanent methods of identification, in particular those that can be obtained in an unobtrusive manner and without the knowledge or consent of the owner. As a result, transient biometric methods have been proposed (Barbosa et al., 2016)

Transient biometrics can be distinguished from cancellable biometrics in that the latter, the biometric data is protected via an irreversible transform, whereas in the former, the biometric data themselves have only temporary recognition value(Barbosa et al., 2016). It is a relatively new concept for biometric recognition and are distinct from traditional biometric recognition systems that concentrate on biometric characteristics that are as constant as possible (e.g. eye retina). These traditional forms of biometric give accuracy over time, but there is resistance to their use for non-critical applications due to the risk of their misuse (Barbosa et al., 2013). Particularly due to the development of the concept of the “right to be forgotten” within EU member states legal systems, the need to create biometric characteristics that have a transient lifetime. One option for a transient biometric that has been presented is the fingernail, having a life span of approximately two months (Barbosa et al., 2013).

The use of the fingernail images as biometric data has been the topic of a number of research studies. A system which acquires the image of the nail bed, uses the groves of the nail bed to create a pattern for recognition purposes (Kumar et al., 2014). The nail bed can be used for such purposes since the skin under the nail bed is unique for each person(Krstic, 1991). Exploration of the nail bed surface can be carried out through segmenting the five fingernails as regions of interest (ROI) from a hand image using a contour segmentation algorithm. Difficulties arise using the method due to bias with respect to a subject's skin tone. The electric signature is then created using the Haar wavelet and Independent component analysis (ICA) (Kumar et al., 2014). This methodology leads to high recognition rates but the researchers did not evaluate the effective of finger nail growth on recognition rates – so no longitudinal analysis is carried out (Barbosa et al., 2016).

Barbosa et al (2016) also present a method for transient biometrics through the use of finger nail data. The input image is converted to grayscale for the object-detection algorithm. The authors objective was to identify a subject by comparing a biometric signature against a dataset of previously connected samples. Their solution therefore includes three phases: image segmentation of the nail bed of the right index finger that is isolated from other surrounding features, and pre-processing; the extraction of a biometric signature from the image and finally the method for matching the nail-bed signature with the previously acquired data(Barbosa et al., 2016). This method exploits texture features which are extracted from finger nail images. This mechanism therefore creates a transient means of biometric identification through data that changes over time. Such a solution may help overcome the problem of user's reluctance to providing recognition data and fulfil the requirements of "the right to be forgotten", which may be used in day to day applications. It was found that identification performance was high within a week of taking the images, but degraded considerably after a two month period (Barbosa et al., 2016).

3.5 Reliability of Biometric Methods and Systems

Biometrics has been promoted as the "magic bullet" that will solve the problem of the real and urgent need to accurately identify people on the internet, especially since many financial crimes

and other crimes of deception are committed online (Keenan, 2015). However, there are greater requirements for multi-factor authentication requirements to ensure security. Businesses and the public however, have been reluctant to adopt biometric technologies, one reason being that the include identifiers such as fingerprints or retinal scans that cannot be changed. Furthermore, like all technology biometric technologies can be subject to exploitation. For example the iPhone 5 and the iPhone 6's Touch ID sensor is capable of being hacked through obtaining an excellent copy of the user's fingerprint (Keenan, 2015).

Biometric technologies all have error rates, such as iris-based biometrics systems failing to uniquely identify the traveller, resulting in the arbitrary refusal of passengers from aircraft. This therefore gives rise to risks relating to border security (Keenan, 2015). Iris scanning has seen only limited adoption, while the reliability is good, with only a small chance of false positives. Replicated irises are hard to create as the scans involve a significant amount of detail (Thompson, 2018). Despite the efficiencies of this system there take up has not been great, due to concerns that have been raised about hygiene and accessibility. Share iris scanning equipment can become unhygienic unless cleaned after each use. This type of technology is also inaccurate for individuals with certain medical conditions, such as diabetes which can lead to an alteration of the appearance of the eye over time (Thompson, 2018). Fingerprints of those who work in hard manual jobs can also be eroded over time (Nigam et al., 2015).

3.6 Overcoming Reliability Issues with Soft Biometrics

After decades of research into individual biometric modalities by numerous researchers, it has been observed that none of the individual modalities can be completely reliable all of the time. To address these issues therefore, researchers have proposed multi-modal fusion of selection of biometric modalities to increase the possibility of recognition (Ross et al., 2006). Multi-modal biometric recognition systems necessarily are more complex to introduce and therefore likely to be costlier. Multi-model systems can also include multiple aspects of the same feature. While face biometrics have achieved satisfactory results in controlled environments, various factors such as expression, pose and occlusion limit the practical application of this technology in practical situations. Recent advances in facial biometric technologies includes the use of complementing facial recognition systems with facial soft biometric traits (Arigbabu et al.,

2015). Soft biometrics have been defined as “physical or behavioural characteristics which provide detailed descriptions of humans” (Arigbabu et al., 2015, p. 513).

Research work into soft biometrics has been carried out largely within the areas of machine learning and computer vision. Soft biometrics has largely focused on three categories: face, body and accessory-related attributes (Dantcheva et al., 2011).

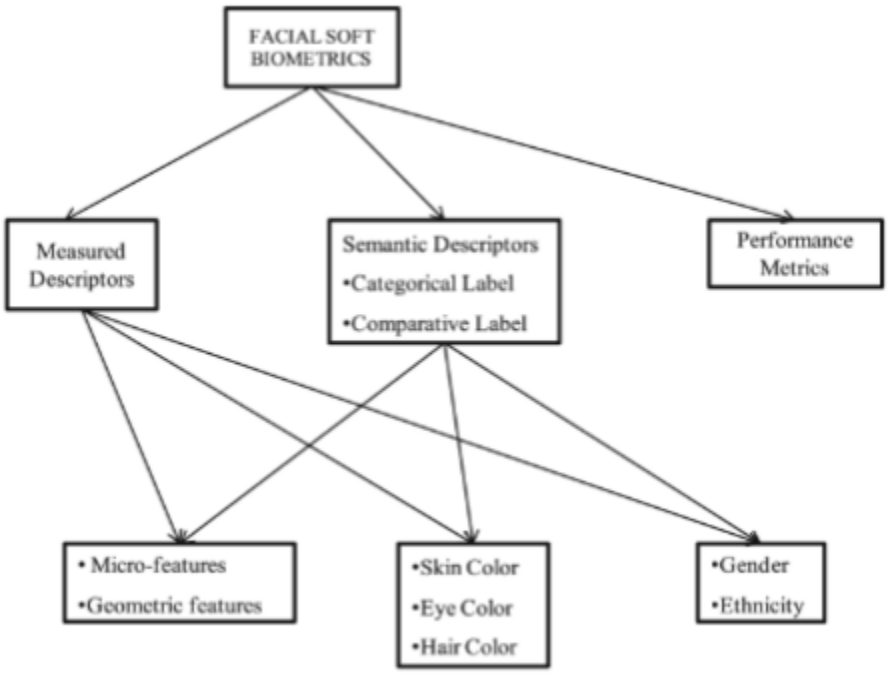

Figure 1: Categorisation of Soft Biometric Methods (Arigbabu et al., 2015)

Current research into facial soft biometrics has either extracted features as measured descriptors or semantic descriptors. Research into facial features is carried out with the same aim in soft biometrics as in traditional biometrics. The purposes is to extract prominent facial features with significant identifying and/or discriminating capabilities (Arigbabu et al., 2015). The methods of both forms of biometric research remains the same, however, soft biometrics focuses upon different facial traits to traditional biometrics. Traditional biometrics has been developed through the use of low-resolution images and therefore has overlooked the possibilities of extracting other discriminating micro-features of the facial image (Lin and Tang, 2006).

Argibabu et al (2015) have used high-resolution images and extracted micro-features, facial colour features, gender and ethnicity, showing several key benefits to complement the performance of conventional facial recognition system. The researchers show that microscopic marks on the facial image become critical to facial identification where the facial image is captured off-frontal pose or limited by occlusion (Arigbabu et al., 2015). Since the system does not require a reference image to perform recognition, this mechanism can be highly beneficial in forensic investigations to identify criminal suspects. Furthermore, these additional techniques remove the difficulties inherent within facial biometric techniques due to expression, occlusion and pose. At the same time the requirement for human subject compliance is diminished(Arigbabu et al., 2015), which depending on the point of view may be an advantage or disadvantage of this method.

3.7 Challenges of Presenting Biometric Forensic Evidence in Court

Forensic investigations using biometric evidence will eventually need to produce evidence that is sufficiently reliable to lead to a conviction in court. While there are undoubtedly advantages in the production of biometric forensic evidence, studies have also illustrated various shortcomings. During the criminal trial, jurors will be presented with multiple forms of evidence from both sides in the trial that is contradictory by nature(Maeder et al., 2017). A large number of studies have shown that jurors perceive DNA evidence to be strong forms of evidence, e.g. (Lieberman et al., 2008). Unfortunately, it is not always the case the DNA evidence is infallible as the lay juror without scientific understanding might consider it to be.

There are a number of possible difficulties with DNA samples and deficiencies in the laboratory processing, analysis techniques, quality control and possible environmental contaminants (Lieberman et al., 2008). Lieberman et al (2008) also discovered that jurors were unable to discern the impact of reliable conditions and correct accreditations for the lab upon the reliability of DNA evidence. DNA and other biometric evidence therefore produces a risk that jurors are unable to sufficiently discern whether it is reliable evidence upon which to convict a defendant and that undue weight might be given to scientific evidence when the conditions under which the evidence has been collected has given risks to errors.

3.8 Summary

This chapter has raised the main privacy and data protection concerns that arise from proposals to obtain identification evidence from general members of the public through the creation of facial image, or other biometric identification mechanisms databases. Furthermore some of the obstacles to reliability of such methods has been considered as well as proposals of new mechanisms to overcome these difficulties, such as the use of soft biometrics.

4.0 Conclusion

The above analysis has considered a number of advantages and disadvantages of the use of biometrics in forensic investigations. While there are clear technical advantages of biometric approaches to forensic investigations, there are challenges as implicit within all technology that have prevented obstacles to the wide scale adoption of biometric techniques within forensic investigations and in the provision of evidence in court. Biometric technologies in general provide advantages over traditional identification methods in that they are based upon who the person is and their inherent characteristics as opposed to something they own or can remember (token, key card or password). Characteristics that exist within the human body, such as iris, retina, fingerprint or facial image are much harder to replicate than a password or a key card.

Common uses of biometrics in forensic investigations currently include the use of DNA sequences and fingerprints. Scholars have argued that a national DNA database which obtains peoples DNA as a prerequisite of citizenship would lead to the improved detection of crime and act as a deterrent. Issues of privacy however and the potential for misuse of such information lead to significant resistance against such a collection. Fingerprint and DNA methods while being long standing methods of being used as proof of crimes require invasive methods for their collection and hence, only those who have already been convicted of crimes have this information stored in a database, which limits the detection of crime to existing offenders. A further difficulty with DNA evidence is the fact that studies have shown that jurors have difficulties in discerning reliable DNA evidence from unreliable evidence and as such appear to place too high a probative value on such evidence.

To circumvent the difficulties inherent within the collection of DNA and fingerprint evidence, less invasive methods have been developed such as facial recognition techniques and gait or ear analysis. Facial images, gait and the shape of the ear can all be obtained through photographic imagery which can be acquired without the subject's knowledge or consent. This is considered to be a significant advantage of such methods by researchers, but also subjects these techniques to significant concerns regarding privacy particularly the collection and storage of data about human subjects to which they neither consent nor have knowledge of. When compared to well established methods such as DNA or fingerprints, gait analysis is considered to be impacted by a number of external covariate factors that affect the pattern of the gait and thus undermine its credibility as evidence(Bouchrika, 2016). The probability of recognition can be impacted by factors such as clothing, footwear, or psychological factors such as the state of anxiety or certain medical conditions. Like facial images, gait images are also affected by lighting and viewpoint.

Various facial recognition techniques have been developed and have been successfully used to identify and verify individual images; however, despite extensive research in the area, automated processes are still to achieve sufficient reliability and repeatability for their use in forensic identifications. Visual surveillance mechanisms have been easily circumvented by those who are planning to commit crimes, their pervasive nature means that offenders will take steps to conceal their faces from the cameras and avoid detection. While biometric detection systems have shown to prove unreliable under certain conditions, there is constant innovation in the area of biometric technologies that seeks to overcome the difficulties of existing applications.

Soft biometrics has been introduced as a mechanism to overcome the shortcomings of existing facial recognition techniques. Soft biometrics takes advantages of high resolution images and relies upon micro-features in the face to complement conventional facial recognition systems and increase reliability. These techniques however, still fail to overcome the difficulties that arise where the face is obscured by the suspect. 3D techniques are also used to overcome some of the shortcomings inherent within 2D facial techniques, in that they create a model that represents the whole head as opposed to merely the face. Despite the advancements provided in such techniques they are not however suitable for forensic methods due to the complexities of creating 3D images and the high computational cost of carrying out the recognition process.

Finally, transient biometric methods have been proposed as a mechanism for overcoming the difficulties of privacy and data protection which provide significant legal obstacles to the successful use of biometric technologies within crime detection. Transient technologies use biometric data that has only temporary recognition value. The use of images of the fingernail has been proposed as one form of biometric data, in which the groves of the nail bed create a pattern for recognition purposes. The identification performance of such methods have been found to be good within a week of taking the images, but changes in the appearance of the nail bed mean that the ability to achieve recognition from this part of the human body degrades considerably over a period of two months.

There is a vast amount of research into the area of biometric technologies and their application in forensic investigations. At present however there are many difficulties in using such evidence to secure convictions in legal cases and the main methods that are still in use are fingerprint and DNA methods. As computational power and techniques improve and the resolution of camera images increases however, it seems clear that many benefits could be derived in forensic investigations through the application of a wider range of biometric techniques.

Bibliography

i. Legal Cases

S & Marper v United Kingdom [2008] ECHR 1581

R (on the application of GC & C) v The Commissioner of Police of the Metropolis [2011] UKSC 21

ii. Legislation

EU General Data Protection Regulation 2016/679

iii. Journal Articles/ Books/ Online Sources

Arigbabu, O.A., Ahmad, S.M.S., Adnan, W.A.W., Yussof, S., 2015. Recent advances in facial soft biometrics. The Visual Computer 31, 513–525. https://doi.org/10.1007/s00371-014-0990-x

Au, M.H., Choo, R., 2016. Mobile Security and Privacy: Advances, Challenges and Future Research Directions. Syngress.

Barbosa, I.B., Theoharis, T., Abdallah, A.E., 2016. On the Use of Fingernail Images As Transient Biometric Identifiers. Mach. Vision Appl. 27, 65–76. https://doi.org/10.1007/s00138-015-0721-y

Barbosa, I.B., Theoharis, T., Schellewald, C., Athwal, C., 2013. Transient biometrics using finger nails, in: 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS). Presented at the 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), pp. 1–6. https://doi.org/10.1109/BTAS.2013.6712730

Benzaoui, A., Adjabi, I., Boukrouche, A., 2017. Experiments and improvements of ear recognition based on local texture descriptors. Optical Engineering 56, 043109. https://doi.org/10.1117/1.OE.56.4.043109

Benzaoui, A., Hadid, A., Boukrouche, A., 2014. Ear biometric recognition using local texture descriptors. Journal of Electronic Imaging 23, 053008. https://doi.org/10.1117/1.JEI.23.5.053008

Bhatia, R., 2013. Biometrics and Face Recognition Techniques. International Journal of Advanced Research in Computer Science and Software Engineering 3, 93–99.

Bichard, M., 2004. The Bichard Inquiry: Report (No. HC 653). The Stationary Office, London.

Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., Senior, A.W., 2013. Guide to Biometrics. Springer Science & Business Media.

Bouchrika, I., 2016. Evidence Evaluation of Gait Biometrics for Forensic Investigation, in: Hassanien, A.E., Fouad, M.M., Manaf, A.A., Zamani, M., Ahmad, R., Kacprzyk, J. (Eds.), Multimedia Forensics and Security: Foundations, Innovations, and Applications. Springer, Cham, Switzerland, pp. 307–326.

Bouchrika, I., Goffredo, M., Carter, J., Nixon, M., 2011. On Using Gait in Forensic Biometrics. Journal of Forensic Sciences 56, 882–889. https://doi.org/10.1111/j.1556-4029.2011.01793.x

Bryman, A., 2016. Social Research Methods. Oxford University Press, Oxford.

Chihaoui, M., Elkefi, A., Bellil, W., Ben Amar, C., Chihaoui, M., Elkefi, A., Bellil, W., Ben Amar, C., 2016. A Survey of 2D Face Recognition Techniques. Computers 5, 21. https://doi.org/10.3390/computers5040021

Choo, A., 2018. Evidence, 5 edition. ed. Oxford University Press, Oxford, United Kingdom.

Cosmi, E.V., Meloni, P., Marzano, S., Sacco, R., 2009. Ethical and Legal Aspects of Biometrics, in: Mordini, E., Green, M. (Eds.), Identity, Security and Democracy: The Wider Social and Ethical Implications of Automated Systems for Human Identification. IOS Press, Amsterdam, Netherlands, pp. 111–114.

Dantcheva, A., Velardo, C., D'Angelo, A., Dugelay, J.-L., 2011. Bag of soft biometrics for person identification. Multimed Tools Appl 51, 739–777. https://doi.org/10.1007/s11042-010-0635-7

Delac, K., Grgic, M., 2004. A Survey of Biometric Recognition Methods, in: 46th International Symposium Electronics in Marine. Presented at the ELMAR-2004, Zadar, Croatia.

Deliversky, J., Deliverska, M., 2018. Ethical and Legal Considerations in Biometric Data Usage—Bulgarian Perspective. Front Public Health 6. https://doi.org/10.3389/fpubh.2018.00025

Federal Bureau of Investigation, 2018. CODIS - NDIS Statistics [WWW Document]. Federal Bureau of Investigation. URL https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics (accessed 9.24.18).

Flores Zuniga, A.E., Win, K.T., Susilo, W., 2010. Biometrics for Electronic Health Records. Journal of Medical Systems 34, 975–983. https://doi.org/10.1007/s10916-009-9313-6

Home Office, 2018. National DNA Database annual report, 2016 to 2017 [WWW Document]. GOV.UK. URL https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/724596/040718_new_CCS0518718592_National_DNA_Database_Strategy_Board_AR_2016-17_updates_NEW.pdf (accessed 9.24.18).

Kale, A., Rajagopalan, A.N., Cuntoor, N., Kruger, V., 2002. Gait-based recognition of humans using continuous HMMs, in: Proceedings of Fifth IEEE International Conference on Automatic Face Gesture Recognition. Presented at the Fifth IEEE International Conference on Automatic Face Gesture Recognition, IEEE, Washington, DC, USA, pp. 336–341. https://doi.org/10.1109/AFGR.2002.1004176

Keenan, T.P., 2015. Hidden Risks of Biometric Identifiers and How to Avoid Them, in: Black Hat USA 2015. Canadian Global Affairs Institute, University of Calgary, pp. 1–13.

Kindt, E.J., 2018. Having yes, using no? About the new legal regime for biometric data. Computer Law & Security Review 34, 523–538. https://doi.org/10.1016/j.clsr.2017.11.004

Krstic, R.V., 1991. Human Microscopic Anatomy: An Atlas for Students of Medicine and Biology. Springer Science & Business Media.

Kumar, A., Garg, S., Hanmandlu, M., 2014. Biometric authentication using finger nail plates. Expert Systems with Applications 41, 373–386. https://doi.org/10.1016/j.eswa.2013.07.057

Larsen, P.K., Simonsen, E.B., Lynnerup, N., 2008. Gait analysis in forensic medicine*. J. Forensic Sci. 53, 1149–1153. https://doi.org/10.1111/j.1556-4029.2008.00807.x

Lieberman, J.D., Carrell, C.A., Miethe, T.D., Krauss, D.A., 2008. Gold versus platinum: Do jurors recognize the superiority and limitations of DNA evidence compared to other types of forensic evidence? Psychology, Public Policy, and Law 14, 27–62.

Lin, D., Tang, X., 2006. Recognize High Resolution Faces: From Macrocosm to Microcosm, in: Proceedings of the 2006 IEEE Computer Society Conference on Computer Vision and Pattern

Recognition - Volume 2, CVPR '06. IEEE Computer Society, Washington, DC, USA, pp. 1355–1362. https://doi.org/10.1109/CVPR.2006.243

Lohiya, R., Shah, P., 2015. Face Recognition Techniques: A Survey for Forensic Applications. International Journal of Advanced Research in Computer Engineering & Technology 4, 1540–1546.

Maeder, E.M., Ewanation, L.A., Monnink, J., 2017. Jurors' Perceptions of Evidence: The Relative Influence of DNA and Eyewitness Testimony when Presented by Opposing Parties. Journal of Police and Criminal Psychology 32, 33–42. https://doi.org/10.1007/s11896-016-9194-9

Maria, D.M., Nappi, M., 2014. Face Recognition in Adverse Conditions: A Look at Achieved Advancements, in: Maria, D.M. (Ed.), Face Recognition in Adverse Conditions. IGI Global, Washington DC.

Masaoud, K., Algabary, S., Omar, K., Nordin, M.J., Huda, S.A.S.N., 2013. A Review Paper on Ear Recognition Techniques: Models, Algorithms and Methods. Australian Journal of Basic and Applied Sciences 7, 411–421.

Nigam, I., Vatsa, M., Singh, R., 2015. Ocular biometrics: A survey of modalities and fusion approaches. Information Fusion 26, 1–35. https://doi.org/10.1016/j.inffus.2015.03.005

Nixon, M.S., Bouchrika, I., Arbab-Zavar, B., Carter, J.N., 2010. On use of biometrics in forensics: Gait and ear, in: 2010 18th European Signal Processing Conference. Presented at the 2010 18th European Signal Processing Conference, pp. 1655–1659.

Nixon, M.S., Tan, T., Chellappa, R., 2006. Human Identification Based on Gait. Springer Science & Business Media, New York.

Norris-Jones, L., Marsh, S., 2009. An investigation into the technical, legal and ethical issues associated with biometrics in the UK (application to biometrics module for computing programmes). International Journal of Electronic Security and Digital Forensics 2, 206. https://doi.org/10.1504/IJESDF.2009.024904

Rattani, A., Derakhshani, R., 2018. A Survey Of mobile face biometrics. Computers & Electrical Engineering 72, 39–52. https://doi.org/10.1016/j.compeleceng.2018.09.005

Ross, A.A., Nandakumar, K., Jain, A.K., 2006. Handbook of Multibiometrics. Springer Science & Business Media, New York.

Saini, M., Kapoor, A.K., 2016. Biometrics in Forensic Identification: Applications and Challenges. Journal of Forensic Medicine 1, 1–6. https://doi.org/10.4172/2472-1026.1000108

Sampson, F., 2018. The ATHENA equation – balancing the efficacy of citizens' response with the reality of citizens' rights around data protection. The Police Journal 91, 205–223. https://doi.org/10.1177/0032258X17701321

Sarangi, P.P., Mishra, B.S.P., Dehuri, S., 2018. Fusion of PHOG and LDP local descriptors for kernel-based ear biometric recognition. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-018-6489-0

Smith, M., 2018. Universal forensic DNA databases: Balancing the costs and benefits. Alternative Law Journal 43, 131–135. https://doi.org/10.1177/1037969X18765222

Spaun, N.A., Bruegge, R.W.V., 2008. Forensic Identification of People from Images and Video, in: 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems. Presented at the 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems, pp. 1–4. https://doi.org/10.1109/BTAS.2008.4699363

Srinivas, N., Flynn, P.J., Vorder Bruegge, R.W., 2016. Human Identification Using Automatic and Semi-Automatically Detected Facial Marks. Journal of Forensic Sciences 61, S117–S130. https://doi.org/10.1111/1556-4029.12923

Sutrop, M., 2010. Ethical Issues in Governing Biometric Technologies, in: Proceedings of the Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, ICEB'10. Springer-Verlag, Berlin, Heidelberg, pp. 102–114. https://doi.org/10.1007/978-3-642-12595-9_14

Thompson, E., 2018. Understanding the Strengths and Weaknesses of Biometrics [WWW Document]. Infosecurity Magazine. URL https://www.infosecurity-magazine.com:443/opinions/strengths-weaknesses-biometrics/ (accessed 9.26.18).

Tistarelli, M., Champod, C., 2017. Biometric Technologies for Forensic Science and Policing: State of the Art, in: Tistarelli, M., Champod, C. (Eds.), Handbook of Biometrics for Forensic Science. Springer, Cham, Switzerland.

Tomovo, S., 2009. Ethical and Legal Aspects of Biometrics, in: Mordini, E., Green, M. (Eds.), Identity, Security and Democracy: The Wider Social and Ethical Implications of Automated Systems for Human Identification. IOS Press, Amsterdam, Netherlands, pp. 111–114.

Yuan, L., Mu, Z., 2014. Ear Recognition Based on Gabor Features and KFDA. The Scientific World Journal 1–12. https://doi.org/10.1155/2014/702076