The Characteristics of a Biometric

Helen van de Haar, Darelle van Greunen and Dalenca Pottas
Department of Information and Communication Technology
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
helen.vandehaar@nmmu.ac.za

***Abstract*— Biometric implementations have emerged as an improved solution in many spheres of life where security controls are necessary for authentication. However, not all human mannerisms and features can be used as a biometric measure. For example, the movement of an elbow will not satisfy the requirements for a useful biometric. There are a number of characteristics which are deemed important and that may be taken into account when choosing a human mannerism or feature to be used as a biometric for the purposes of identification. Some characteristics are more necessary than others. For example, the uniqueness of the fingerprint is more important than its acceptance as an identification mechanism by the public at large. One can find a number of these suggested characteristics in the literature and place them into various categories. The primary category will be its inherent nature but there may also be a technical and a procedural category. Technical considerations are where the typical technical implementation of the biometric may add further characteristics to the biometric. Finally, there may be procedural actions that will further have an influence on the biometric implementation. A categorized technical or procedural characteristic should add quality to the original inherent characteristics for any particular biometric. If a biometric feature and its further implementation (technical and/or procedural) satisfy a certain subset of these categorized characteristics which are deemed more important, then this may constitute a better choice than that which appears to satisfy a different subset of characteristics. This paper looks at the characteristics found in the literature and attempts to categorize them as inherent, technical or procedural in nature. The paper will subsequently look at some of the more popular biometric features and their inherent characteristics that have been found in the literature. Readers of this paper will be able to select appropriate biometric features based on the characteristics that are identified in this paper.**

Keywords—biometrics; characteristics; iris; fingerprint; face; voice; inherent; technical; procedural;

I. INTRODUCTION

Biometrics is a word that means “life” and “to measure” [1]. A biometric cannot be displaced from the person that it identifies because a biometric is a physical or behavioral feature of an individual. Biometrics are seen as a solution to password problems such as the tendency to lose known passwords, forget them or have them leaked to others. Therefore, biometric samples are seen to be more efficient and reliable than passwords for authentication or identification [1], [2]. One can use a single biometric called a single modal biometric solution such as fingerprints only, or a multi-modal solution using two or more biometrics [3]. For example, using fingerprints, iris scans and a facial photograph together, can be a multi-modal solution.

Not all human features are usable as a biometric. Various authors have indicated required characteristics for a biometric to be considered usable. This paper begins by describing these characteristics that are found in the literature. The characteristics are categorized in this paper as being inherent, technical or procedural in nature. After categorization, some of the more popular biometrics will be described in terms of their inherent characteristics. Readers of this paper may be assisted in their choice from the various sets of characteristics and from the suggested biometrics.

The paper will first discuss the categorization of the characteristics. Thereafter it will look at the popularity of the various biometric features. Some of the more popular biometric features will be taken further by looking at how they satisfy some of the suggested characteristics.

II. CHARACTERISTICS OF A BIOMETRIC

This section suggests a categorization of the various biometric characteristics that are found in the literature. Three categories are suggested: inherent, technical and procedural. The inherent category will comprise the characteristics that are seen as inherently part of the biometric itself. The technical category is for those characteristics that are added due to the particular implementation of the biometric. The procedural category is for those characteristics which are not inherent, and not part of the implementation, but involve procedural choices that are made regarding the implementation of the biometric.

Any biometric feature does not need to have all the characteristics in order to be useful as an identification feature.

A. Inherent Characteristics

According to many authors, when one uses a biometric to identify a person, there are four basic inherent characteristics that should be present. These are collectability (the ability to measure or extract the biometric element from the subject), universality (all subjects should have this biometric), uniqueness (each subject should have his/her own distinctive version of this element which is not duplicated in another subject) and permanence (this element should remain the same over time i.e. it is lifelong) [1], [2], [3], [4], [5], [6], [7], [8].

There are also ethical and political concerns [7]. Some authors therefore add to the suggested four characteristics above, by stating that a good biometric should be acceptable to the public who should therefore have no objections in providing their biometric samples [1], [2]. Reasons for non-acceptance may be that some of the biometric features require contact with the subject and can be seen to be intrusive. The public may also be concerned about having their biometrics captured and used for other purposes than originally intended or for which they did not originally provide informed consent [6], [9].

Beynon-Davies [10] includes three of the main inherent characteristics described above, i.e. universality, uniqueness and permanence, but replaces collectability with a similar description called indispensability meaning that the identifier is always available when required. Added to this is exclusivity which means that the particular identifier is sufficient in itself for unique identification [10]. Indeed the current trend towards multi-modal biometrics means that this characteristic is not always necessary.

Bhatnagar et al [11] agree with some of the basic requirements and also dictate universality, uniqueness (distinctiveness) and permanence. They add acceptability as a fourth necessary characteristic [11]. Deriche [12] adds collectability to these four.

Table I lists the inherent characteristics that were found in the literature and were discussed in this section.

TABLE I. CHARACTERISTICS OF A BIOMETRIC – INHERENT

Authors	Collectable	Universal	Unique	Permanent	Acceptable
Ashok et al [1]	√	√	√	√	√
Beynon-Davies [10]		√	√	√	
Bhatnagar et al [11]		√	√	√	√
Birgale and Kokare [4]	√	√	√	√	
Chandra et al [6]	√	√	√	√	
Deriche [12]	√	√	√	√	√
Elumalai and Kannan [3]	√	√	√	√	√
Gaddam and Lal [13]			√		
Gokulkumari and Lakshmi [2]	√	√	√	√	√
Hosein [14]					√
Lalithamani and Soman [15]				√	
Lyon [9]					√
Manivannan and Padma [6]	√	√	√	√	√
Mordini and Massari [7]	√	√	√	√	
Őzkaya and Sağiroğlu [16]			√		
Sağiroğlu and Őzkaya [8]	√	√	√	√	

B. Technical Characteristics

Other characteristics which are probably more relevant to the various technical implementations are explained here.

Performance depends on the efficiency and accuracy of the extraction and matching of the biometric. The manner in which the biometric is calculated should also not influence its performance [2], [3], [6], [12], [13], [15], [16].

A cancellable biometric is one where the template may be generated from the extracted data, and then encrypted or processed further. If it is compromised in any way, then one should be able to therefore generate a new fresh template to replace the compromised version, perhaps by adding another authentication factor. One can, for example, encrypt the cancellable biometric template in order to provide an irrevocable, unique and effective final key [13], [15], [17].

One-way transformation is another characteristic that is seen to be of importance in the literature. When using one-way transformation, one should not be able to invert the computation used in the biometric template [13], [15], [17].

A final suggested technical characteristic may be that biometric authentication systems should also have live detection mechanisms to avoid illegal access attempts [18]. It is very important to ensure live-ness detection when taking fingerprint images for the purposes of identification to circumvent fake fingertips made from silicon or other means. The human typically has sweat glands that end up at the pores on the surface of the skin and sweating through these pores shows that there is life in the finger [19], [20].

Table II lists the technical characteristics that were found in the literature and were discussed in this section.

TABLE II. CHARACTERISTICS OF A BIOMETRIC - TECHNICAL

Authors	Cancellable	Live-ness	One-Way Transform	Performance
Bayly et al [18]		√		
Chen and Chen [17]	√		√	
Deriche [12]				√
Elumalai and Kannan [3]				√
Gaddam and Lal [13]	√		√	√
Gokulkumari and Lakshmi [2]				√
Lalithamani and Soman [15]	√		√	√
Manivannan and Padma [6]				√
Manivanan et al [19]		√		
Marcel [20]		√		
Ozkaya and Sağiroğlu [16]				√

C. Procedural Characteristics

The final category of characteristics that is discussed here is the procedural characteristics that may be added to the chosen biometric(s).

Where there is a bi- or multi-modal biometric solution, one can apply circumvention, where a different biometric can be used if the first one is not able to be extracted from a particular subject [3], [6]. Obviously the alternative biometric features would have had to be captured as well.

Diversity is when the biometric can be used for more than one purpose or application [13], [15]. Instead of having more than one biometric system, one can use the same system for a number of applications. Perhaps a country's identification mechanism can also be used by the crime control unit for catching criminals. There may be, however, some ethical considerations that should be taken care of.

Reusability is where one should be able to revoke and reissue the biometric, perhaps for the purpose of conciliation [13], [15].

These procedural characteristics are listed in Table III.

The next section discusses the proliferation of various biometric features with the purpose of identifying some of the more popular biometrics.

III. Proliferation of Biometric Features

This section discusses the proliferation of biometric features in terms of performance and acceptability since 2005.

A. Performance

Regarding the characteristic of performance, when the UK Passport Service did trials with biometrics in 2005, they found that face recognition had a success rate of 69%, fingerprints 81% and iris recognition systems 96%, the latter being the preferred biometric for both men and women [21]. This is shown in Figure 1.

TABLE III. CHARACTERISTICS OF A BIOMETRIC - PROCEDURAL

Authors	Circumvention	Diversity	Reusability
Elumalai and Kannan [3]	√		
Gaddam and Lal [13]		√	√
Lalithamani and Soman [15]		√	√
Manivannan and Padma [6]	√		

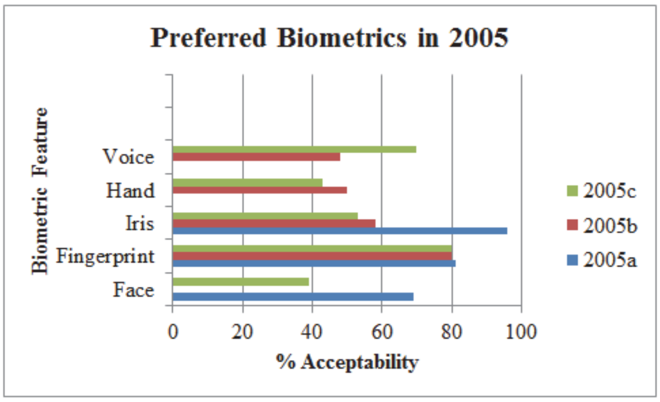

Fig. 1. Preferred Biometrics in 2005

Another survey in 2005 indicated that the fingerprint and iris were seen to have a very high accuracy rating, followed by the voice and face with simply a high measure and the keystroke was given a medium measure of accuracy rating [22].

Later in 2007, in the United Kingdom, a survey viewed the fingerprint and iris as being extra reliable with hand and face being simply reliable [23].

Resource usage may also affect performance. The size of the template that is stored may vary depending on the biometric method. Speaker recognition uses the most storage space (between 10000 and 20000 bytes). Perhaps fingerprint (between 250 and 1000 bytes) and iris recognition (512 bytes) methods are reasonably sized. Face recognition requires either 84 or 1300 bytes [24].

B. Acceptability

The second characteristic discussed further is that of acceptability.

Another USA survey in 2005 showed that 80% of people found fingerprinting to be most acceptable as a biometric, followed by iris recognition (58%), hand geometry (50%) and speaker verification (48%) [25].

The order of market share in 2005 for the above was as follows: fingerprint recognition 47-49%; face recognition 10-12%; hand geometry 10-12%; iris recognition 8-10%; voice verification 5-6%; and signature recognition 1-2% [24]. This is shown in Figure 2.

The usage of biometrics in a mobile context was also listed in a survey in 2005, indicating that the public was willing to use the following biometrics for mobile applications [22]: fingerprint (80%); voice (70%), hand geometry (43%); face (39%); iris (53%) and keystroke dynamics (27%). They viewed the face, keystroke and voice as non-intrusive [22].

An international consumer survey in 2006 found that 70% of consumers worldwide would be comfortable with biometrics to combat crime such as fraud and identity theft [26]. The public therefore seems reasonably willing to accept biometric technology.

Later in 2007 in the United Kingdom, a survey showed the following usage of biometrics [23]: signature 38%, fingerprint 16%, keystroke dynamics 11%, voice 10%, hand 7% and face 4%. All these biometrics were viewed by the public as being extra comfortable [23].

In 2011 the Unisys Security Index reported that 53% of United States citizens would accept using biometrics to gain access to servers and 21% were even willing to submit to biometrics for their social media access [27]. Also in 2011, a global forecast by RNCOS Industrial Research Solutions revealed that the face, fingerprint and iris would consume about 84% of the global biometric market by 2012 [28]. It seems, therefore, that the trend for face, fingerprint and iris is to maintain its hold on the market and it has grown from about 80% to 84% since 2005. This is also shown in Figure 2.

In a 2011 report on biometric systems used for grant payouts such as pensions, various countries are shown to be using biometrics. Fingerprints are used by Malawi, South Africa, India, Ghana, Namibia, Botswana, Kenya, Nigeria, Iraq, Philippines, Bolivia and Mexico. Iris is used by Indonesia and the DRC. Pakistan and Afghanistan use both iris and fingerprints [29]. Again this shows increased widespread acceptance of biometrics for identification.

By 2012, the Unisys Security Index reported that 50% of Australians did not accept face technology for social media access such as Facebook, but that 95% of them would accept biometric security for airport customs; 92% for security camera footage and 66% are already happy to have face recognition biometrics for staff in companies [30].

Looking at Figure 1 and Figure 2, it can be seen that the fingerprint and the iris are most popular with the latter gaining ground. Voice and face recognition are also well used. The next subsection will look at these four biometric features and discuss them in terms of some of the suggested characteristics.

IV. Inherent Characteristics of Biometric Features

This section examines the iris, fingerprint, face and voice biometrics in terms of their inherent characteristics as found in the literature, as well as their technical performance. A summary of these is found in Table IV.

A. Iris

Since 1997 there has been use of iris identification techniques. The iris is the textured coloured part of the eye. No two persons have the same iris. There are embryonic factors that influence a human iris development such that even identical twins are distinguishable [4]. The unique patterns in the iris are determined by the subject's DNA, which differ even between the left and the right eye of the same person and are constant throughout the lifetime of the person [31]. The iris is therefore seen to have an inherent unique characteristic.

Regarding performance, the iris patterns are often seen to be the most stable and reliable of the biometrics. It has been described as the best biometric for the most important data and is more accurate and reliable as an identification mechanism than fingerprints, face, retina, hand geometry, voice or signature patterns. Their error rates are lower in comparison to facial features, fingerprints, palm-prints, retina, hand-writing signature, DNA and gait [6], [31].

The segmentation of the iris itself must also be reliable otherwise there will be an effect on the performance of the iris as an identification mechanism. Most iris recognition systems depend on the subject standing less than two meters from the imaging device, and remaining motionless for three seconds. This will restrict the implementations of this biometric. Using a different iris capture technology, one can lock onto a person's eye and capture high-quality iris images from a distance of 18 metres. In a "stop and stare" approach, the user aligns his eye so that the iris segmentation is not degraded and becomes a circular shape. In an uncontrolled environment the iris may be non-elliptical which also makes extraction more difficult [32].

Actually only part of the iris image is required for correct identification [31]. If iris images are captured under controlled circumstances then one can better ensure high quality iris images by capturing a sequence of images and selecting the best one. The discarded ones usually are out of focus, or have blurring due to motion, or have eyelid or eyelash occlusion caused by blinking during the capture of the iris image [32]. One should also be careful to not expose the iris to too much light outdoors, as there will be contraction and dilation of the pupil. The iris is able to be captured regardless of the subject wearing glasses or color contacts, or having undergone laser surgery. There are more than 250 points of reference that are captured from the iris [5], [10], [24].

The iris is a contactless method of identification as well as one with high confidence levels which may make it more acceptable to the public.

Regarding the universality characteristic of the iris, the iris-scan technology does not work well with very dark irises [33]. The iris is also not stable until a child is about two years old thereby having an effect on its permanence characteristic [34].

B. Fingerprints

Fingerprints are the oldest biometric used for identification, dating back to 2200 BC. Fingerprints are lifelong, unique, stable, durable and convenient. They are also usually available, very reliable and highly accurate.

Regarding its acceptability as a biometric, it is very popular because it is convenient and efficient and is already widely used for access, for ATM authentication and for welfare hand-outs [2].

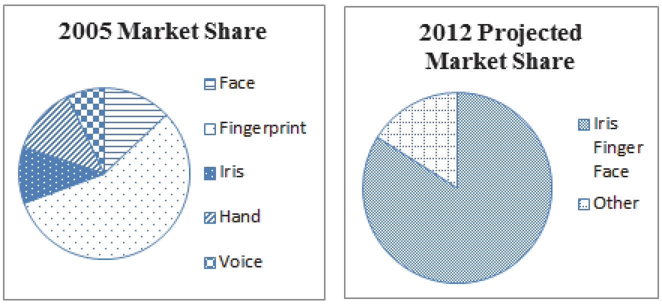

Fig. 2. Actual 2005 Market Share and 2012 Projected Market Share

The universal characteristic is affected by the fact that usually about 2% of tested fingerprints are unreadable perhaps due to harsh conditions, or perhaps because the scanners are not high quality [33]. Finger-scan technologies cannot read fingerprints well if the person is elderly or has been employed as a construction worker or artisan. There may be cultural or circumstantial issues and different populations may render different results [33]. Fingerprints can be affected by diseases of the skin and therefore should not always be used as a sole biometric method for identification in a universal context. Even childhood skin diseases will affect the adult skin.

Looking at the permanence of fingerprinting, these systems are usually only for adult usage. It has been argued that very young children should not be used for fingerprinting due to the subsequent stretching of their fingers while they grow. Fingerprints are life-long unless there are cuts or bruises on the fingertips. It is suggested that baby fingerprints are too small but the ridges and furrows start to develop already in the womb [34].

Regarding the performance characteristic, fingerprinting is seen as being more accurate than hair, blood type or ear prints. The technology is easy to implement but it may be costly [6], [16]. Performance can be affected if a fingerprint itself is sweaty or dry or has some skin defect. Problems also include environmental temperatures, dirt, sweat, humidity or dryness. One may not place the finger at the same angle always and one may exert more pressure than at other instances thereby causing distortion. However, fingerprints can be taken in less than two minutes which provides for good performance [5]. There are about 35 points taken in a fingerprint [10].

C. Face Recognition

Face recognition uses those facial features that are not easily altered. Various features of the face, such as upper outlines of eye sockets, cheekbones and mounts are analyzed. Usually about 20 points are captured. The images are usually captured by video cameras and therefore this form of biometrics can be used for surveillance purposes [10], [35].

Looking at the performance characteristics of face recognition, some large databases have been used with face recognition, but the accuracy is not as good as with iris or fingerprint recognition [35]. One must also be aware that the face recognition is affected by light, pose, background scale, noise, face occlusion (by hairstyle and makeup) and facial expression. There are concerns, that to be successful, the face recognition identification should be done under controlled conditions. If the person is not facing the camera head-on, or is wearing glasses or caps, or there is a change in the light on the subject, then it is difficult to identify the person. The effect of these factors must be reduced in order to get the best performance [16].

Face biometrics are non-invasive and therefore easily accepted by users but it is costly. Face recognition is less intrusive i.e. it does not expect one to “press your face against a clean glass” for example. Rather, the technology can be used from a distance to recognize one’s face.

D. Voice Recognition

Each person’s voice is unique in that it has a pitch, a cadence and some inflection for its various phonemes. One can usually recognize a person on the other side of a phone instantly when that person begins to say “Hello”. Voice recognition is where a particular speaker may be identified. Speech recognition is where one analyses what the person is actually saying. This is the only biometric that uses acoustic data and can therefore work with public telephones [36]. One can capture voice samples even with smart phones or Personal Digital Assistants (PDAs) as long as there is a microphone.

Regarding the performance characteristic, voices can change over time due to emotions, health or age. They can also be distorted depending on the quality of the device that is capturing the voice [24], [36]. When using voice biometrics, some extractions are made from the speech stream and it is obviously more efficient if there is a larger amount of speech recording data captured with a good microphone and accompanied by noise cancellation [36]. The voiceprint must be strengthened to avoid security breaches. Voice biometrics takes up minimal space and is also non-invasive but there are problems with error rates [6]. However, a study in the UK proved that there was better performance using speaker verification than all other biometrics except for the iris [37]. Voice biometrics certainly reduces time spent on identification procedures but there must be no excessive background noise. Where a zone is particularly noisy, then voice biometrics may not be a good choice of a biometric to be used at that point. A different biometric will provide a more acceptable and efficient identification of the individual under these circumstances.

The iris, fingerprint, face and voice biometrics have been discussed in detail. Table IV shows a summary of some of the characteristics mentioned with reference to these four biometric samples. The rating of low, medium or high for each biometric element as suggested by Deriche [12] has been added to the table. The rating shows that the iris seems to be consistently high, except for the acceptability by the public which is rated as low [12]. One wonders whether this low acceptability rating may improve if the members of the public are brought to a better understanding of the iris sampling process.

TABLE IV. BIOMETRIC CHARACTERISTICS

Characteristic	**Biometric**	**Rating [12]**	**Detail**
Collectable	Iris	Medium	
	Fingerprint	Medium	Fingerprints are usually readily available.
	Face	High	
	Voice	Medium	Can be captured with smartphones, PDAs and computer microphones.
Universal	Iris	High	Can capture through glasses and contacts. 1 in 10000 persons have unsuitable irises.
	Fingerprint	Medium	Only 2% of fingerprints are unreadable. Only 1 in 1000 fingers is

Character -istic	**Biometric**	**Rating [12]**	**Detail**
			unreadable.
	Face	High	
	Voice	Medium	
Unique	Iris	High	Embryonic factors influence the human iris. Even identical twins are distinguishable. Even left and right eye differ.
	Finger-print	High	The fingerprint is unique and immutable.
	Face	Low	
	Voice	Low	Unique pitch, cadence and inflection.
Permanent	Iris	High	Permanent from the age of 8 months. Stable after 2 years old. Constant throughout the lifetime.
	Finger-print	High	The fingerprint is lifelong, durable. Furrows develop in womb. Not read well if the subject is elderly.
	Face	Medium	No age restrictions.
	Voice	Low	
Acceptable	Iris	Low	Contactless method.
	Finger-print	Medium	Widely acceptable.
	Face	High	Non-invasive, less intrusive.
	Voice	High	Voiceprint capture is non-invasive.
Performs well	Iris	High	Stable. More reliable (more reliable than fingerprint, face, retina, hand geometry, voice and signature. High accuracy rates. Best biometric for important data. Lower error rates than fingerprints, palms, retina, handwriting, DNA and gait. There are high confidence levels. Only part of the iris is necessary. Collection of iris is fast and accurate. Short time needed to perform the matches.
	Finger-print	High	It is convenient, stable, efficient and reliable. It is highly accurate, more than hair, blood type or ear prints. It is an easy technology to implement. Can capture in less than 2 minutes.
	Face	Low	Accuracy of face recognition is not as good as iris or fingerprint recognition.
	Voice	Low	Voiceprints require minimal space. Speaker recognition is second best in performance, after the iris.

V. Applying Biometrics and Characteristics

An application example is given here to further demonstrate the use of biometric characteristics. Suppose the scenario is to choose a biometric solution for the elderly to receive social welfare grants. Looking at the inherent characteristics in Table I, one would ideally prefer a collectable, unique, universal, permanent biometric that is acceptable to the elderly. Matching this to Table IV, one sees that the fingerprint is not read well if the subject is elderly, therefore it does not satisfy the permanence characteristic requirement for this application. The iris, however, remains constant throughout the lifetime. Looking at the universality characteristic, one sees that 1 in 10000 persons have unreadable irises, and 1 in 1000 fingerprints are unreadable. Perhaps a bi-modal biometric solution is applicable where both fingerprint and iris samples are collected to ensure a better chance of universality.

One can add technical characteristics to this implementation. For example, to circumvent claims for grants from fraudsters who collect money on behalf of family members who have passed away, one can implement checks for live-ness. To increase performance, the implementation can be of such a nature that only efficient sensors are used for fast data capture, providing good clear images under controlled circumstances. Looking at performance in terms of preventing errors where persons are erroneously identified, one can ensure higher thresholds of correctness and choose appropriate algorithms that are used through the various stages of an implementation. For example, the extraction of a biometric sample may have functions added for noise cancellation. Other stages where performance can be improved may be to use efficient algorithms to speed up the matching process against the database templates, or to encrypt the biometric keys for security enhancement.

Procedural characteristics may be added as well. Circumvention is already able to be applied such that if an elderly person's fingerprints are unreadable, then his/her iris may be accepted as an alternative biometric for identification. Applying diversity, one may wish to use the biometric database also for health services to the elderly.

This subsection used a fictitious implementation in order to demonstrate the choice of appropriate characteristics for an example biometric implementation.

VI. Conclusion

Various literature sources have described one or more inherent characteristics that a biometric feature should have if it is to be used for identification purposes. Some of the more important ones are that the feature must be unique and permanent (life-long). Others may be seen to be of lesser importance, such as being acceptable to the public and the performance thereof. There are even characteristics that are added on during the particular technical or procedural implementation of the biometric as an identification mechanism. An example of a technical characteristic is one-way transformation. A procedural implementation requirement may be that of diversity. A particular biometric feature and its implementation may satisfy a number of characteristics, as has also been seen in the examined literature. It may therefore be useful to first make decisions on which characteristics are important before making decisions on which biometric feature(s) to use and how to proceed with the complete implementation.

REFERENCES

[1] J. Ashok, V. Shivashankar and P.V.G.S. Mudiraj. (2010). An overview of Biometrics. *International Journal on Computer Science and Engineering*. [Online]. *2(7),* pp. 2402-2408. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=58663718&site=ehost-live

[2] G. Gokulkumari and A. Lakshmi. (2010). Study of effects and perceptual analysis in implementing biometric authentication. *European Journal of Scientific Research.* [Online]. *61(2),* pp. 242-254. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=70240505&site=ehost-live

[3] E. Elumalai and M. Kannan. (2011). Multimodal authentication for high end security. *International Journal on Computer Science and Engineering.* [Online]. *3(2),* pp. 687-692. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=69584227&site=ehost-live

[4] L. Birgale and M. Kokare. (2009). A survey on iris recognition. *The IUP Journal of Electrical & Electronics Engineering.* [Online]. *11(4),* pp. 7-25. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=44622039&site=ehost-live

[5] A. Chandra, R. Durand and S. Weaver. (2008). The uses and potential of biometrics in health care: Are consumers and providers ready for it? *International Journal of Pharmaceutical and Healthcare Marketing.* [Online]. *2(1),* pp. 22-34. Available: http://www.emeraldinsight.com/journals.htm?articleid=1718605

[6] S. Manivannan and E. Padma. (2011). Comparative and analysis of biometric systems. *International Journal on Computer Science and Engineering.* [Online]. *3(5),* pp. 2156-2162. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=69620864&site=ehost-live

[7] E. Mordini and S. Massari. (2008). Body, biometrics and identity. *Bioethics.* [Online]. *22(9),* pp. 488-498. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=34740981&site=ehost-live

[8] S. Sağiroğlu and N. Özkaya. (2009). An intelligent face features generation system from fingerprints. *Turkish Journal of Electrical Engineering and Computer Sciences.* [Online]. *17(2),* pp. 183-203. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=44335243&site=ehost-live

[9] D. Lyon. (2008). Biometrics, identification and surveillance. *Bioethics.* [Online]. *22(9),* pp. 499-508. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=34740984&site=ehost-live

[10] P. Beynon-Davies. (2007). Personal identity management and electronic government: The case of the national identity card in the UK. *Journal of Enterprise Information Management.* [Online]. *20(3),* pp. 244-270. Available: http://www.emeraldinsight.com/journals.htm?articleid=1602474

[11] J.R. Bhatnagar, B. Lall and R.K. Patney. (2010). Performance issues in biometric authentication based on information theoretic concepts: a review. *IETE Technical Review.* [Online]. *27(4),* pp. 273-285. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=51893552&site=ehost-live

[12] M.A. Deriche. (2008). Trends and challenges in mono and multi biometrics. *Image Processing Theory, Tools and Applications, 2008. First Workshop on 23-26 November 2008.* [Online]. pp. 1-9. Available: http://dx.doi.org/10.1109/IPTA.2008.4743801

[13] S.V.K. Gaddam and M. Lal. (2011). Development of bio-crypto key from fingerprint using cancellable templates. *International Journal on Computer Science and Engineering.* [Online]. *3(2),* pp. 775-783. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=69584218&site=ehost-live

[14] I. Hosein. (2004). The sources of laws: Policy dynamics in a digital and terrorized world. *The Information Society.* [Online]. 20, pp. 187-199. Available: http://www.tandfonline.com/doi/abs/10.1080/01972240490456854

[15] N. Lalithamani and K.P. Soman. (2009). Irrevocable cryptographic key generation from cancelable fingerprint templates: An enhanced and effective scheme. *European Journal of Scientific Research.* [Online]. *31(3).* pp. 372-387. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=44066115&site=ehost-live

[16] N. Özkaya and S. Sağiroğlu. (2010). Generating one biometric feature from another: Faces from fingerprints. *Sensors.* [Online]. *10(2),* pp. 4206-4237. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=51203480&site=ehost-live

[17] H. Chen and H. Chen. (2010). A hybrid scheme for securing fingerprint templates. *International Journal of Information Security.* [Online]. *9(5),* pp. 353-361. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=54325824&site=ehost-live

[18] D. Bayly, M. Castro, A. Arakala, J. Jeffers and K. Horadam. (2009). Fractional biometrics: Safeguarding privacy in biometric applications. *International Journal of Information Security.* [Online]. *9(1),* pp. 69-82. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=47728632&site=ehost-live

[19] N. Manivanan, S. Memon and W. Balachandran. (2010). Automatic detection of active sweat pores of fingerprint using highpass and correlation filtering. *Electronics Letters.* [Online]. *46(18),* pp. 1268-1269. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=53422077&site=ehost-live

[20] S. Marcel. (2013). BEAT – biometrics evaluation and testing. *Biometric technology today.* [Online]. *2013(1),* pp. 5-7. Available: http://dx.doi.org/10.1016/S0969-4765(13)70014-6

[21] Unknown author. (2005). Biometric bytes: Breaking news from the biometrics industry. *Card Technology Today.* [Online]. *17(6),* p. 8. Available: http://www.sciencedirect.com/science/article/pii/S0965259005703248

[22] N.L. Clarke and S.M. Furnell. (2005). Authentication of users on mobile telephones – A survey of attitudes and practices. *Computers & Security.* [Online]. *24(7),* pp. 519-527. Available: http://dx.doi.org/10.1016/j.cose.2005.08.003

[23] S. Furnell and K. Evangelatos. (2007). Public awareness and perceptions of biometrics. *Computer Fraud & Security.* [Online]. *1(2007),* pp. 8-13. Available: http://dx.doi.org/10.1016/S1361-3723(07)70006-4

[24] Department of the Treasury. (2005). *The use of technology to combat identity theft.* [Online]. Available: http://communitybooks.worldebooklibrary.org/Members/Government_Library/United_States_Department_of_the_Treasury/biometrics_study.pdf

[25] Unknown author. (2005). Biometric bytes: Breaking news from the biometrics industry. *Card Technology Today.* [Online]. *17(10),* p. 8. Available: http://www.sciencedirect.com/science/article/pii/S0965259005703868

[26] M. Cohn. (2007). Biometrics: Key to securing consumer trust. *Biometric Technology Today.* [Online]. *15(3),* pp. 8-9. Available: http://dx.doi.org/10.1016/S0969-4765(07)70082-6

[27] T. Caldwell. (2011). Comment. *Biometric Technology Today.* [Online]. *2011(10).* p. 12. Available: http://www.sciencedirect.com/science/article/pii/S0969476512700206

[28] RNCOS Industrial Research Solutions. (2012). *Global biometric forecast to 2012.* [Online]. Available: http://www.rncos.com/Report/IM140.htm

[29] A. Gelb and C. Decker. (2011). *Cash at your fingertips: Biometric technology for transfers in resource-rich countries*. [Online]. Available: http://papers.ssrn.com/so13/papers.cfm?abstract_id=1888376

[30] Unknown author. (2012). Australians oppose facial recognition in social media. *Biometric Technology Today.* [Online]. *2012(12).* p. 12. Available: http://dx.doi.org/10.1016/S0969-4765(12)70134-0

[31] C.D. Htwe, and W. Htay. (2011). Performance evaluation of iris region detection and localization for biometric identification system. *World Academy of Science, Engineering and Technology.* [Online]. *75,* pp. 229-232. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=60801476&site=ehost-live

[32] K. Roy and P. Bhattacharya. (2010). Improvement of iris recognition performance using region-based active contours, genetic algorithms and SVMs. *International Journal of Pattern Recognition.* [Online]. *24(8),* pp. 1209-1236. Available: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=57141438&site=ehost-live

[33] H. Murray. (2007). Monstrous play in negative spaces: Illegible bodies and the cultural construction of biometric technology. *The Communication Review.* [Online]. *10(4),* pp. 347-365. Available: http://dx.doi.org/10.1080/10714420701715415

[34] W. Jia, H-Y. Cai, J. Gui, R-X. Hu, Y-K. Lei and X-F. Wang. (2012). Newborn footprint recognition using orientation feature. *Neural Computing and Applications.* [Online]. *21(8),* pp. 1855-1863. Available: http://0-link.springer.com.wam.seals.ac.za/article/10.1007%2Fs00521-011-0530-9

[35] K.A. Rhodes. (2004). *Aviation security. Challenges in using biometric technologies.* [Online]. Available: http://communitybooks.worldebooklibrary.org/Members/Government_Library/Government_Accountability_Office/d04785t.pdf

[36] J. Markowitz. (2000). Voice biometrics. *Communications of the ACM.* [Online]. *43(9),* pp. 66-73. Available: http://web.ebscohost.com/ehost/detail?sid=41c4e797-c340-4892-80d4-108e0edac300%40sessionmgr14&vid=1&hid=24&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=11941838

[37] J. Markowitz. (2001). Speaker verification. *Biometric Technology Today.* [Online]. *9(7),* pp. 9-11. Available: http://dx.doi.org/10.1016/S0969-4765(01)00820-7