I.J. Information Technology and Computer Science, **2016, 4, 42-51**
Published Online April 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2016.04.06

Biometric Verification, Security Concerns and Related Issues - A Comprehensive Study

Sheela Shankar
Department of Electronics & Communication Engg, KLE Dr. M. S. Sheshgiri CET, Belgaum, India

V.R Udupi
Department of Electronics and Communication Engg, Gogte Institute of Technology, Belgaum, India

Rahul Dasharath Gavas
Department of Computer Science and Engineering, KLE Dr. M.S. Sheshgiri CET, Belgaum, India

Abstract—There has been many attempts to make authentication processes more robust. Biometric techniques are one among them. Biometrics is unique to an individual and hence their usage can overcome most of the issues in conventional authentication process. This paper makes a scrutinizing study of the existing biometric techniques, their usage and limitations pertaining to their deployment in real time cases. It also deals with the motivation behind adapting biometrics in present day scenarios. The paper also makes an attempt to throw light on the technical and security related issues pertaining to biometric systems.

Index Terms—Authentication, Biometric Systems, Biometric Techniques, Security.

I. Introduction

In modern society, the issues pertaining to the usurpation of identity are at the heart of numerous concerns. Proving one’s identity is of paramount importance in many real time applications.

The approaches used to establish a unique identity, follow a broad nomenclature:

1) *Something-you-are:* applies to the bodily characteristics that are unique identification of a person. Such features that are unique to an individual are termed as biometric traits.
2) *Something-you-know*: as the name implies, it is the secret information that is known only to the user. PIN numbers and passwords are the most appropriate examples to substantiate this.
3) *Something-you-have*: can be items or objects to validate the identity of a person. Examples include keys, passport, ATM cards, etc.

The first approach is advantageous over the rest due to many reasons. Currently, authentication is carried out through passwords [1], user ids, magstripe magnetic cards, PIN numbers, etc. on a large basis. In spite of their mass acceptance, they are vulnerable to certain liabilities. They can be lost, shared or can be forgotten owing to human memory. They can also be easily acquired or disclosed by direct covert observation. Keeping same passwords for all the accounts can be easy to remember, but is prone to security related issues. At the same time, frequently modifying the passwords can assure security to some extent; but remembering all of them becomes cumbersome. Hence these methods invoke the issue of “repudiation” and are prejudicial. Though, secure encryption techniques impart a high degree of security to credit card based transactions, the method fails to identify whether the right credit card owner is carrying out the transactions, especially in online applications. Altogether, the combined use of mere passwords and user id’s cannot be relied upon and alternative approaches are very crucial in this regard.

Owing to the vulnerabilities posed by, “*Something you have*”, and “*Something you know*”, approaches; biometric based methods have emerged since biometric identifiers are inimitable aspects conceptually. Hence they are being viewed as panacea in the field of authentication.

The rest of the paper is organized as follows. Section 2 deals with a brief introduction to biometric systems. Section 3 elaborates the various biometric techniques available and their comparison. The vulnerabilities faced by them are also discussed. Their applications are given in Section 4. The threats to biometric systems are discussed in Section 5. An introduction of assessing the error rates and the distortions among biometric techniques are given in Section 6 and 7 respectively. The compression and encryption of biometric signals are discussed in Section 8. Finally the paper concludes in Section 9.

II. Towards Biometric Approach

Biometrics is a science of application of statistical means to the measurements of biological entities. It bestows true user authentication [27]. It deals with recognizing an individual based on his physiological or behavioural traits. Behavioural biometric can be speech, signature, gait and keystroke analysis, whereas physiological biometric uses ear, face, voice, finger-print, hand veins, finger geometry, hand geometry, palms, iris matching and recently neuro-signals are used in this regard [2]. A biometric based system should satisfy the following criterion for mass- acceptance [3]:

Permanence: Non-changeability of the attributes with respect to time.

Circumvention: The ease with the system evades.

Uniqueness: The feature should be distinct between all users.

Collectability: Assessment and measurement of features should be feasible and less complex.

Measurability: Deals with acquiring and digitizing the biometric characteristic using suitable devices without causing inconvenience to anyone.

Universality: The feature should be inherent in all the users who access the system.

Acceptability: the system should be accepted by users and they must be well acquainted with it.

Fig. 1 represents a general model of biometric systems. Firstly, the input acquisition and digitizing of the chosen biometric takes place. Examples include a microphone, fingerprint scanner, EEG device and a camera in case of speech, finger-print, neuro-signals and face based authentication respectively. This phase embeds A/D converters. The second phase comprises of converting the signal from crude to system desirable format. It involves the elimination of artifacts and later on processing it by subjecting it to some normalization. The third stage includes extraction of useful features from the digitized data, known as identification of "landmarks" in the data. In the fourth phase, the system eliminates well-known and fixed variations (which are often stored in a repository for reference) since they are commonly encountered. Therefore, this stage is called as "template generator". And then, the newly created pattern is compared against the stored templates which are distinctive to an individual. Thus the system can match a specific set of physiological or behavioural features to recognize an individual. The output with respect to a genuine individual and an impostor in a general biometric system are as shown in Fig. 1.

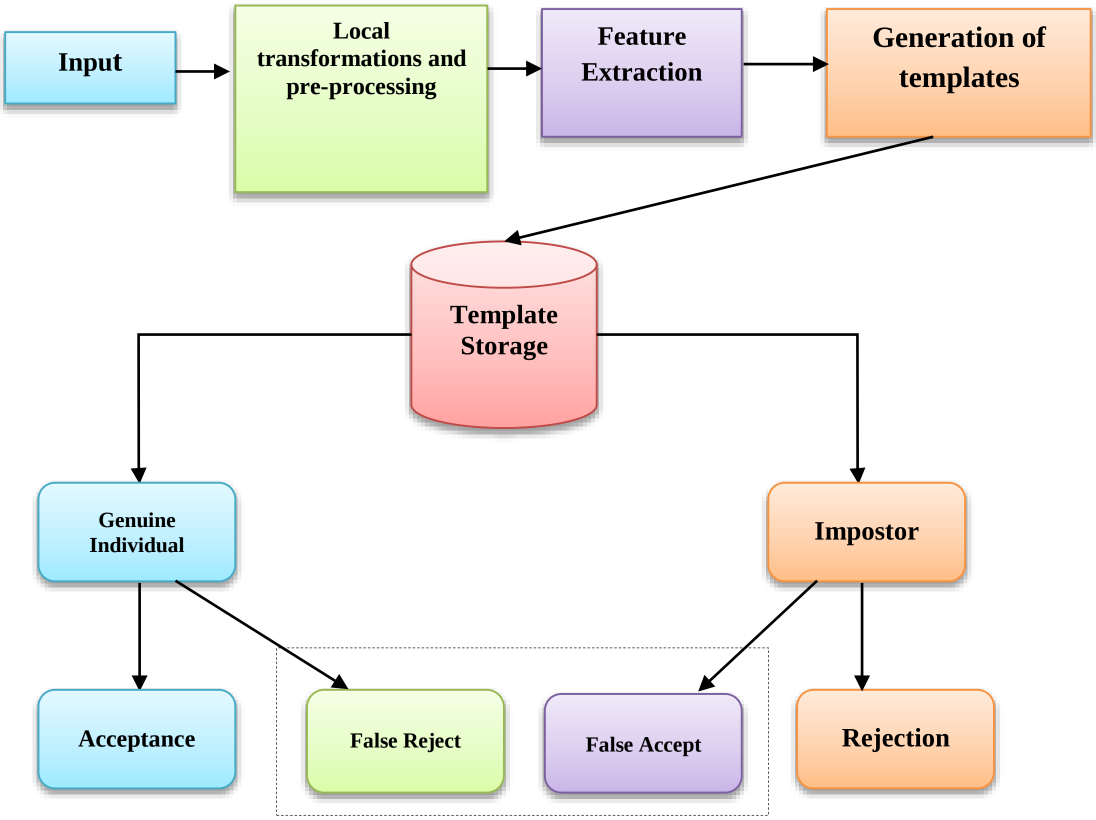

Fig.1. Typical Biometric Setup.

III. Biometric Techniques

There are assortments of biometric characteristics which are used in a wide range of applications. Fig. 2 gives a bird's eye view of them. Every biometric trait comes with its own weaknesses and strengths and the type of application determines its choice. These techniques have surfaced from time and time. Almost any behavioural trait or anatomical feature might be deemed a candidate for an operable biometric. Nevertheless, we have to place such ideas in perspective and align them with the apparent requisite. A brief outlook of the commonly used biometrics is as given below:

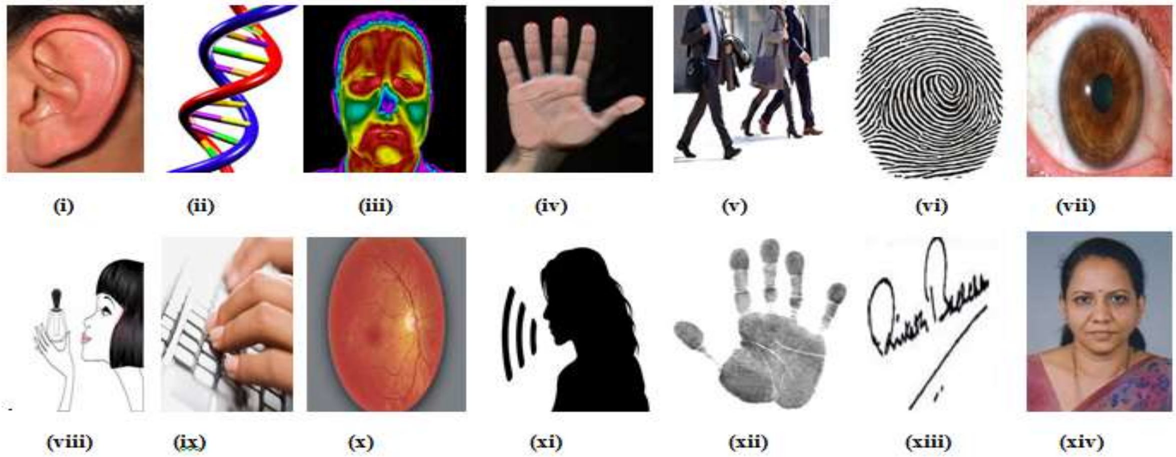

Fig.2. Examples of Biometric Techniques: (i) Ear (ii) DNA (iii) Facial Thermo gram (iv) Hand and finger geometry (v) Gait (vi) Fingerprint (vii) Iris (viii) Odour (ix) Keystrokes (x) Retinal Scan (xi) Voice (xii) Palm Print (xiii) Signature (xiv) Face

3.1. Ear

Human ear can also be used as a biometric as per the findings of Iannarelli in his attempts to identify a person based on his ear [4]. Recent progresses made in this domain include the works of Hurley et al. [5], etc. It has been found that the structure of the cartilaginous tissue of the pinna and the shape of the ear are distinct for an individual. The recognition process basically deals with matching the distance of specific points on the pinna from a landmark location on the ear [6].

3.2. DNA

Biometrics based on Deoxyribonucleic acid (DNA) could be the most exact form of identifying an individual [18]. Every human being is characterised by his/her own individual map for every cell made, and this map or ‘blueprint’ is present in every cell. Since DNA is the arrangement that states who we are intellectually and physically unless a person has an identical twin, it is not probable that any other individual will be composed of the same precise set of genes. DNA is collected from many sources like hair, mouth swabs, finger nails, blood, saliva, straws, blood stains and any other source that has been attached to the body at some time. The technique suffers from high cost and slow procedures involved in the process. This technique finds wide acceptance in criminal trials like forensic applications for uniquely identifying an individual.

3.3. Facial, hand, and hand vein infrared thermogram

Like a regular (visible spectrum) photograph, infrared camera can be used to capture the pattern of heat radiated by human body in an unobtrusive way. These patterns have been found to be a characteristic feature of an individual [19]. A non-invasive thermogram-based system does not require contact, but image acquisition is challenging in uncontrolled environments, where heat emanating surfaces (e.g., vehicle exhaust pipes and room heaters) are present in the vicinity of the body. A similar technology using near infrared imaging is used to scan the back of a clenched fist to determine hand vein structure. This method is best suitable for covert recognition. However the major factor inhibiting its usage is the cost of the thermogram equipment.

3.4. Hand and finger geometry

Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its size of palm, shape and lengths and widths of the fingers [7, 8]. Such systems have been installed on a large scale on commercial basis, since the technique is inexpensive, less complex and relatively easy to use. The presences of environmental factors like weather or individual anomalies like dry skin do not pose any hindrance on the accuracy of this methodology. However hand geometry is not invariant during the growth period of children. A person’s jewellery (like rings) or limitations in dexterity (e.g., from arthritis) causes serious challenges in extracting the correct hand geometry information. Since the hand geometry is not very distinctive feature, the technique is not recommended and cannot be scaled up when the population is large. The physical size of a hand geometry-based system is considerably large and hence it cannot be embedded in certain portable devices like laptops. There are verification systems which are based on measurements of only a few fingers, typically the index and the middle, instead of the entire hand. These devices are much smaller than those that are used for hand geometry, but still much larger than those used in some other biometrics like fingerprint, face, voice.

3.5. Gait

The works of Cutting and Kozlowski on perception experiments based on light point displays [9] have paved the way for usage of gait for recognition process. They found that recognition on the manner of walking (gait) is possible. The early attempts towards gait recognition in computer vision can be attributed to Niyogi and Adelson in the early 1990s [10]. Gait is a complex spatio-temporal biometric and is the peculiar way in which a person walks. Though not distinctive, but it is sufficiently discriminatory to render recognition in low-security applications [11]. Gait is a behavioural biometric and may not remain invariant, especially over a long period of time, due to major injuries involving joints or brain, inebriety or due to fluctuations in body weight. This technique may be an acceptable biometric since the acquisition of gait is similar to acquiring a facial picture. Such systems use video –sequence footage of a walking person to assess different movements of each articulate joint. Hence these are computationally expensive and input intensive [12, 13].

3.6. Fingerprint

Graphical patterns of valleys and ridges on the surface of finger tips are called fingerprints which uniquely characterise an individual. One kind of widely-used features is called *minutiae*, which is usually defined as the ridge ending and the ridge bifurcation. Minutiae-based fingerprint representation techniques are widely in use. The barriers faced in extraction of minutiae are the variations in pressure, large displacements, noise, etc. [20].

3.7. Iris

Usage of iris in recognition process is considered to be one of the efficient means of biometric modalities [21]. The reasons attributed to this are 1) iris is accessible and protected; 2) iris is rich in texture and this texture has many degrees of freedom; 3) the iris texture is thought to be stable throughout a person’s life span, barring catastrophic injury, or illness; 4) iris can be accessed easily in a non-contact manner from moderate distances; 5) the fraction of the population that cannot present an iris due to congenital defect or injury such as aniridia is considerably less.

3.8. Odour

The underlying principle behind the body odour biometrics is that every human smell is unique [22]. The capturing of smell is facilitated by sensors from non-intrusive body parts like the back of the hand. Mastiff Electronic Systems has been carrying out rigorous work on the methods of capturing a person’s smell. Every human smell is composed of chemicals known as volatiles which are extracted by the system and converts them into a template. The usage of body odour triggers some of the privacy concerns since the body odour carries a considerable amount of sensitive personal information. Some activities or diseases can be detected by analysing the body odour.

3.9. Keystroke

This technique deals with assessing the keystroke patterns produced during typing which has been found to be a unique biometric signature [14]. Hence these patterns can be used like a digital signature to verify the identity of computer locally at a certain workstation or remotely over the Internet. Recognition through keystroke analysis can boost the username and password security model by evaluating the manner in which these strings are typed. There is no requirement of any additional hardware since all computers are equipped with a keyboard. This technique takes in to account the patterns of timing that occurs as result of a typist pressing different keys on the keyboard. This typing pattern gives several unique features. One such factor is the keystroke latency (KL) indicating the time between pressing two consecutive keys. Another feature is the key hold-down time (KD) which is the amount of time that a particular key is held down. This technique is beneficial in e-mail, internet banking, user account protection, etc. and many other computer based applications. Through this model, the users can reuse the same login credentials for multiple accounts, thereby simplifying security requirements.

3.10. Retinal Scans

The textures in the retinal vasculature are highly unusual characteristic of an individual and each eye. It is not easy to replicate or modify the retinal vasculature and hence it is claimed to be the most secure biometric [23]. During the data acquisition phase, the subject is required to peep into an eye-piece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged. This phase requires cooperation of the user, entails contact with the eyepiece and requires a conscious effort on the part of the user. These factors have caused an adverse effect on the public acceptability of retinal biometric.

3.11. Voice

This technique analyses the voice of the user in order to store a voice print that is later used for recognition [24]. The aim of speech recognition is to find ‘what principle’ has been spoken while the aim of the speaker verification is ‘who’ told that. Speaker verification emphasizes on the vocal features that yield speech and not on the sound or the pronunciation of the speech itself. The vocal qualities depend on the dimensions of the mouth, vocal tract, nasal cavities and the other speech processing mechanisms inherent in the human body. These characteristics of human speech are unique to an individual unlike the behavioural part which is subjected to change on account of emotional state, medical conditions (like colds, throat infection, etc.), age, etc. The obstacle in this system is that the speech features are sensitive to a number of factors like the background noise. Speaker recognition is most suitable in phone-based applications but the voice signal over phone is usually degraded in quality by the communication channel and the microphone.

3.12. Palm print

Patterns of valleys and ridges are found in the palms of the human hand like the fingerprints [25]. Palm prints are expected to be more unique than the fingerprints as the area of the palm is larger than the area of the finger. The palm print scanners are more expensive and bulkier than the fingerprint sensors because they have to scan a larger area. Human palms also consist of additional distinguishing features such as wrinkles and principal lines that can be captured even with a lower resolution scanner, which would be cheaper. When using a high-resolution palm print scanner, all the features of the palm such as hand geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be collected to build a very effective biometric system.

3.13. Signature

The manner of signing is also found to be a unique trait of an individual. It requires contact with the writing instrument and an effort on the part of the user. This technique is accepted by the government, commercial and legal transactions as a method of recognition. Signatures are a behavioural biometric that are subject to changes over a period of time and are influenced by emotional and physical conditions of the signatories. Signatures of some subjects vary significantly to such an extent that successive signature impressions vary. Professional impostors produce exact fake signatures, thereby creating false acceptance.

3.14. Face

Face recognition basically deals with acquiring a static or dynamic (video) face image and comparing it for recognition process. The face image is subjected to extraction of features. Face recognition suffers from major shortcomings like variations in illumination, pose, gender, expressions, age, occlusions, etc. [26]. Popular face databases are available which serve as benchmarks to test the robustness of any face recognition algorithms. This technique finds tremendous applications in Mugshot, surveillance, etc.

Another possible biometric might be using the neuro-signals generated as a result of various human activities in the brain. Though Electroencephalography (EEG) based systems have been used exclusively in Brain Computer Interface (BCI) systems, their usage in terms of biometric has yet not been explored much due to the higher degree of complexity and non- repeatability in the neuro-signals. Also, the data capture methodology is quite complex when compared to the rest of the biometrics. However, current BCI applications are been run by using low-cost, portable EEG devices [29, 30].

3.15. Comparison of Various Biometrics Techniques

A brief comparison of the above biometric techniques based is provided in Table 1 on the basis of their accuracy, cost and convenience. Similarly, their comparison with respect to the biometrics traits mentioned in Section 2 is given in Table 2.

IV. Applications

Biometrics approach is more suitable in applications like prison security and identification of criminals. Nevertheless, it is also convenient to be used in E-Commerce, access control and E-Banking domains. Notable applications of biometrics include national ID, attendance and time, driver and voter registration, immigration checkpoints and welfare disbursement. Knowledge –based authentication (*Something you know*) for data access especially in remote login has been replaced by biometric systems. On similar grounds, the token-based authentication popular in physical access control are substituted by biometrics.

Table 1. Comparisons of various biometric techniques based on their accuracy, cost and convenience

Rank	Accuracy	Cost	Convenience
1	DNA	Voice	Voice
2	Iris	Signature	Face
3	Retina	Finger	Signature
4	Finger	Face	Finger
5	Face	Iris	Iris
6	Signature	Retina	Retina
7	Voice	DNA	DNA

Table 2. Comparison of biometrics based on the properties discussed in Section 1.1.

Trait	Circumvention	Permanence	Acceptability	Uniqueness	Universality	Collectability	Measurability
Face	Low	Medium	High	High	High	High	High
Fingerprint	High	Medium	Medium	High	Medium	Medium	High
Ear	Low	High	High	High	Medium	High	High
Iris	Low	Medium	Low	High	Medium	Low	High
Palm Print	Medium	Medium	Medium	Medium	Medium	Medium	High
Signature	High	Medium	Medium	High	Low	Medium	High
Voice	High	Medium	High	Medium	High	High	High
Gait	Low	Medium	High	Medium	High	High	Medium
Keystrokes	Medium	Medium	High	Medium	Medium	Medium	Medium

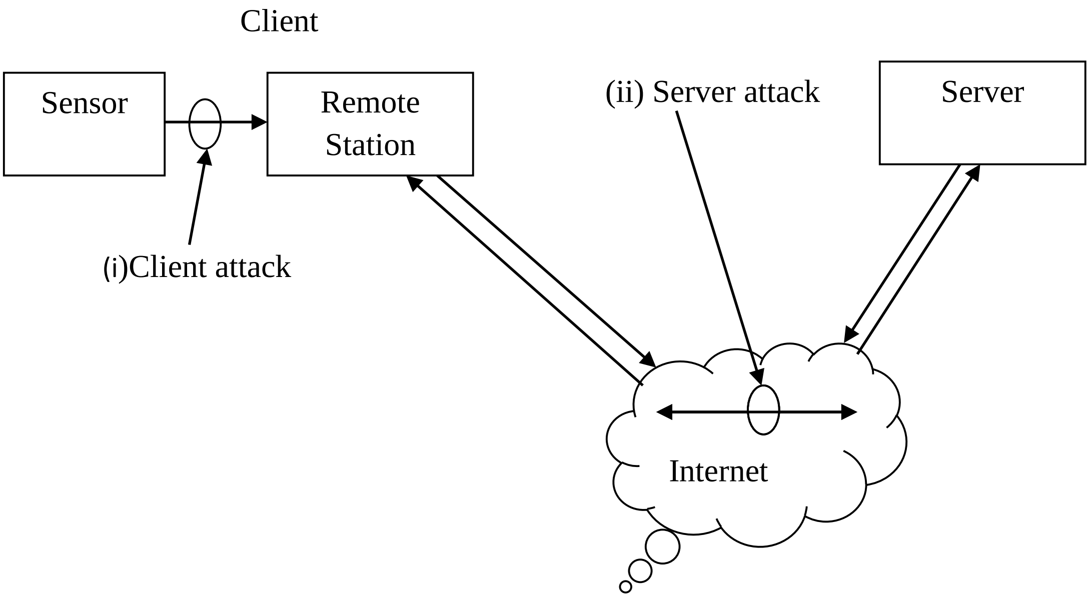

Fig.3. Indication of the Biometric Specific Attacks in a Biometric Based System.

V. Threats to Biometric Systems

A large number of attacks are prevalent on both traditional and biometrics based authentication systems. There are various sources of attack, both on traditional and biometrics authentication systems. Schneier [15] mentions some of the abuses that are common to biometrics authentication systems. Fig. 3 shows the two major types of attacks specific to biometric systems. They are as follows: 1) Brute-force attack at the client (sensor) or at the server, which is similar to a brute-force attack in traditional systems of authentication, which deals with enumerating all the possible passwords. In case of biometrics system, it involves enumerating all possible templates or biometric signals. 2) Resubmission of a formerly attained signal at the client, a recorded signal is replayed to the system, bypassing the sensor. Examples here include the presentation of a copy of a fingerprint image, recorded audio signal or facial image from a speaker. It is evident from Fig. 3 that it is possible to attack both the client (i) and the server (ii) in the above mentioned ways.

Presentation of fake biometrics at the sensor is another type of attack. In this mode of attack, a replica of a biometrics is presented to the system, for instance, a forged copy of a signature, a fake finger, or a face mask. Detection of fake finger can be achieved at the sensor by sensing the finger conductivity or pulse. Similar attempts are still required to identify other types of fake biometrics. In case of face recognition, when the processing power increases, software algorithms will be able to perceive such attacks by processing video rather than single still images.

5.1. Privacy and security concerns

The major drawback of biometric authentication systems is vulnerable to replay attacks. Pre-recorded templates or signals could be sent deceitfully to such systems in order to gain access. Biometric authentication system requires signals that are unique to a person. This creates an issue of privacy. There are chances that once acquired; these signals could be used for various other purposes without the consent of the user.

A password based system has only two possible results, the password either matches or it does not. But in case of biometrics systems, the decision of acceptance or rejection of a subject is based on the degree of match. Hence chances of committing errors by the system are high and hence proper adjustments between the error rates must be balanced. Additional trepidations rather than the security of the transactions are caused when biometrics are deployed on a large scale like the credit cards. One major issue is the privacy. Such systems require the images of body parts like iris, fingers, face, etc. along with the name, date of birth of the subject; which are primarily stored in some database in a digital format. Hence the fear of sharing of such information is a major cause of concern among the general public. The public is insecure with the fact that their private data is stored in a central repository. There are chances of such databases getting misused or could be shared, thereby violating the privacy of the user. The public is worried as their biometric data could be used for testing against repositories used by law enforcement agencies, to seek information regarding any criminal affairs. One of the unique property of biometric is that it cannot be changed and its invariance with time. Perhaps this might be a largest liability as well. In case of credit card being hacked, the bank issues a new card but it is not possible with biometric systems, i.e. a person has only one face, five fingers on each hand. Many security protocols for biometric systems have been identified, for instance the one using seismic waves as in [28].

VI. Error Rates

In general the error rate of a pattern recognition system and in particular an automated biometric system is dependent on several factors. The performance of the system is characterized by the underlying algorithms and the quality of the input and enrolled biometrics signals. Though most of the biometrics systems store a compact representation or a template of the signal, it is also feasible to store the original sample itself. In both the cases, the signals as well as their templates are patterns for the working algorithms, i.e. the pattern P is a sample S(β) of the biometric β, or it is a template that represents S(β). In this case, β can be regarded as uniquely related to an individual. Hence, β ≡ID (individual) is the identity of an individual, which can uniquely identify a person. Formulation in terms of hypothesis testing can be used for authenticating a person. Let the stored biometric template be pattern P'= S(β') and the one under test be a pattern P = S(β). In terms of hypothesis testing, we have

$$H_0:\beta=\beta'\text{,the claimed identity is correct.} \quad (1)$$

$$H_1: \beta \neq \beta'\text{, the claimed identity is incorrect.} \quad (2)$$

To evaluate the similarity between patterns P and P', some similarity measure,

$$s=\mathrm{Sim}(P,P')=\mathrm{Sim}(S(\beta), S(\beta')) \quad (3)$$

And then the decision of a match is made based on a threshold T. H_0 is decided if s≥T and H_1 is decided if s<T. In case of expression (1), deciding H_0 when H_1 is true, results in the false acceptance of a person. This is termed as false positive. Conversely, deciding H_1 when H_0 is true rejects an individual incorrectly. Such a false reject is also called a false negative. The False Reject Rate (FRR) and False Accept Rate (FAR) together depict the error rate (accuracy) of a biometric recognition system. The FRR and FAR are closely correlated variables and depend largely on the decision threshold T, which is depicted in Fig.4. The distribution to the right is of scores from genuine users whereas the distribution on the left is of scores from intruders. The decision threshold T is indicative of the trade-off, between FRR and FAR. Thus FAR and FRR can be defined as follows:

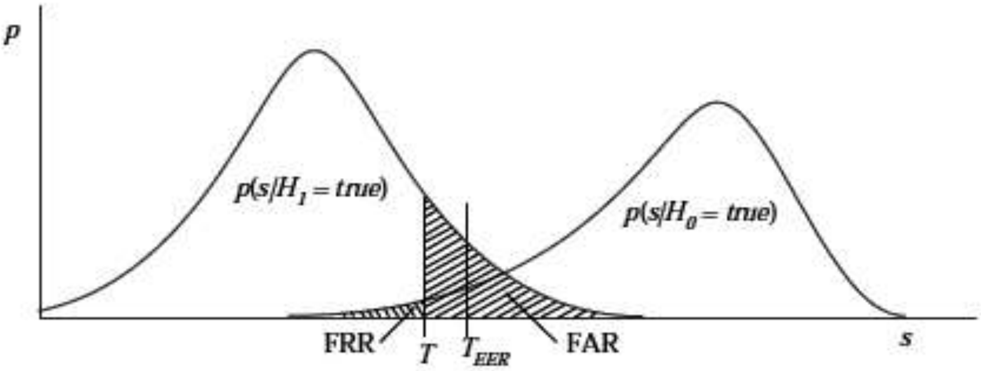

Fig.4. Two Types of Error Rates: FAR and FRR in Biometric Systems.

$$\mathrm{FAR}=\frac{Number\ of\ Imposters\ Accepted\ X\ 100}{Total\ Number\ of\ Imposter\ Comparisons}\% \quad (4)$$

$$\mathrm{FRR}=\frac{Number\ of\ Genuine\ Persons\ Rejected\ X\ 100}{Total\ Number\ of\ Genuine\ Comparisons}\% \quad (5)$$

The error rates are a function of the match/non-match decision threshold. The relationship of these two errors is represented by plotting FRR against FAR along with the threshold T (as free variable). Such a plot is termed as the receiver operator characteristics (ROCs) curve.

Fig. 5 shows an example of an ROC curve. Improvement of one of the error rates is possible only at the expense of the other. An attempt to lower one kind of error culminates in increase of another. Based on the needs of an application, the operating point of a system can be drifted to a low FRR or a low FAR. The equal error point T_{EER} is used rarely.

Genuine Acceptance Rate (GAR) is a measure of the acceptance of genuine candidates and is given by,

$$\mathrm{GAR} = (100 - \mathrm{FRR})\ \% \quad (6)$$

Area under the ROC curve (AUC) is defined as a scalar quantity which tells the probability that a classifier gives a higher match score to a randomly selected genuine sample than to a randomly selected impostor sample. Commonly, for a better interpretation, the Error under the ROC Curve (EUC) is used and is defined as follows:

$$\mathrm{EUC} = (100 - \mathrm{AUC})\ \% \quad (7)$$

Another system performance issue is known as the “fail to enroll” rate [16]. This measure deals with the percentage of subjects that cannot be enrolled due to their poor biometric signals or since their signals are too noisy to match. By any means if such subjects are identified and removed from using the system, then both FAR and FRR can be enhanced.

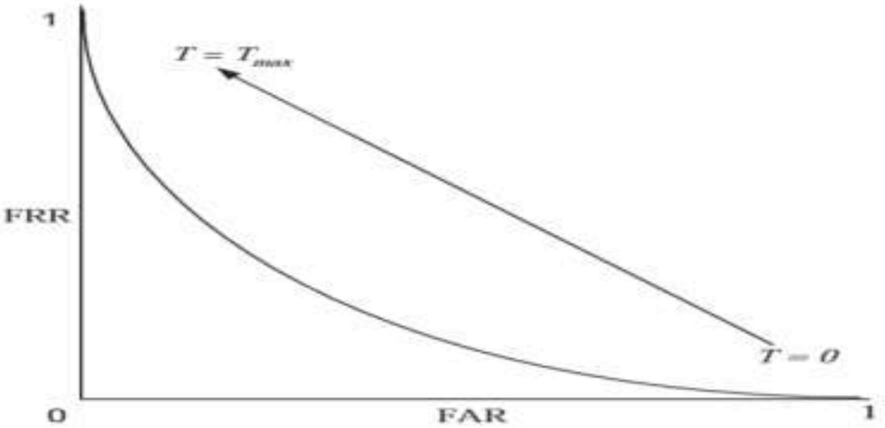

Fig.5. ROC curve showing the relationship between FAR and FRR as a function of decision threshold T

The enrollees in biometric systems can be classified in terms of animals in the zoo, as formulated by Doddington [17], well-known as the "Doddington's zoo". Though the classification was designed particularly for voice recognition, but it can be applied to other biometrics as well. The classification is as follows:

- **Goats:** is the group of persons that are difficult to authenticate. This class of subjects generates majority of false rejects.
- **Sheep:** Authentication systems perform practically well for such subjects and these constitute the major portion of the population.
- **Wolves:** This class belongs to subjects who are good at imitating other subjects, i.e. their biometric are likely to be accepted as that of another person. This class creates lots of false accepts and are successful intruders to the system.
- **Lambs:** These classes of people are the ones who are easy to imitate. They contribute to false accepts because a randomly chosen person from the total population is highly likely to be authenticated (though erroneously) as one of the lambs.

A feasible technique to distinguish the two types of false accepts is to think of wolves causing "active false accepts", and lambs causing "passive false accepts". This means, for a closed world (all subjects enrolled) both the types of false accepts are fixed numbers. A significant higher FAR could be resulted due to the wolves by actively attacking such systems with un-enrolled wolves.

- **Chameleons:** This class belongs to the subjects that are both easy to imitate and are good at imitating others. They are a source of active false accepts when being authenticated and a source of passive false accepts when enrolled.

VII. Distortions to Biometric Signals

This section makes an outlook on the distortion which is most often non-invertible with respect to raw biometric signal while being acquired by the sensor. This leads to storage of incorrect information of the person under consideration. In case of face recognition systems, a morphed version of a face image might be enrolled. This could be achieved in many ways. For instance, a regular point pattern on the face image could be overlapped. The morphed image is then acquired by arbitrarily disturbing this point pattern in a structured manner. Hence a person could be enrolled with such a morphed image. The system often goes unaware of such image morphing. However this could result in a right person not getting authenticated. This is a common scenario in face recognition systems. It is to be noted that in order to apply the same image morphing for each authentication; the face image needs to be transformed into a canonical position before the distortion. This could be achieved by aligning intrinsic points in the face image, like the intra-eye segment in a face.

VIII. Compression and Encryption

Biometric signals differ considerably from the compression of the signal done using standard image compression techniques. A signal loses its spatial domain characteristics like geometric proximity due to compression of the signal, i.e. two points in the original uncompressed signal are unlikely to remain at a comparable distance in the compressed domain. However, after decoding the original signal is either approximately or perfectly restored if the compression is lossy. However in most of the biometric signals, the local geometry of the signal is retained. In case of encryption, the goal is to recover the original signal at the culmination of secure transmission of data. More often, most of the existing biometric systems cannot authenticate encrypted or compressed signals. Hence proper selection of these methodologies is of paramount importance.

IX. Conclusion

Each biometric technique comes with its own merits and demerits and usage of only one can be vulnerable in high security applications. Attempts to amalgamate two or more techniques are vital in this regard. But in cases where security is of marginal concern, comprising with only one biometric can be acceptable. This should make sure that the selection of a particular biometric technique is in good agreement to the application domain.

REFERENCES

[1] Yang, Wen-Her, and Shiuh-Pyng Shieh. "Password authentication schemes with smart cards." *Computers & Security* 18, no. 8 (1999): 727-733.

[2] Yeom, Seul-Ki, Heung-Il Suk, and Seong-Whan Lee. "Person authentication from neural activity of face-specific visual self-representation." *Pattern Recognition* 46, no. 4 (2013): 1159-1169.

[3] Jain, A. K., Ross, A., & Prabhakar, S. 2004. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14, 4–20.

[4] Iannarelli, A. "Ear Identification, Forensic Identification series, Fremont."*Paramont Publishing, Calif, ISBN* 10 (1989): 0962317802.

[5] Hurley, David J., Mark S. Nixon, and John N. Carter. "Force field energy functionals for image feature extraction." *Image and Vision computing* 20, no. 5 (2002): 311-317.

[6] Nanni, Loris, and Alessandra Lumini. "A multi-matcher for ear authentication." *Pattern Recognition Letters* 28, no. 16 (2007): 2219-2226.

[7] Han, Chin-Chuan, Hsu-Liang Cheng, Chih-Lung Lin, and Kuo-Chin Fan. "Personal authentication using palm-print features." *Pattern Recognition* 36, no. 2 (2003): 371-381.

[8] Han, Chin-Chuan. "A hand-based personal authentication using a coarse-to-fine strategy." *Image and Vision Computing* 22, no. 11 (2004): 909-918.

[9] J.E. Cutting and L.T. Kozlowski, "Recognition of friends by their walk", Bull.of the Psychonomic Soc., vol. 9, pp. 353-356, 1977.

[10] Niyogi, Sourabh A., and Edward H. Adelson. "Analysing gait with spatiotemporal surfaces." In *Motion of Non-Rigid and Articulated Objects, 1994, Proceedings of the 1994 IEEE Workshop on*, pp. 64-69. IEEE, 1994.

[11] Xin Zhang and GuoliangFan, "Dual gait generative models for human motion estimation from a single camera", IEEE Transactions on Systems, Man, And Cybernetics—Part B: Cybernetics, vol. 40, no. 4, pp. 1034-1049, Aug. 2010.

[12] Konstantinos Moustakas, Dimitrios Tzovaras, and Georgios Stavropoulos, "Gait recognition using geometric features and soft biometrics", IEEE Signal Processing Letters, vol. 17, no. 4, pp. 367-370, Apr. 2010.

[13] Zongyi Liu and SudeepSarkar, "Improved gait recognition by gait dynamics normalization", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 6, pp. 863-876, Jun. 2006.

[14] Monrose, Fabian, and Aviel D. Rubin. "Keystroke dynamics as a biometric for authentication." *Future Generation computer systems* 16, no. 4 (2000): 351-359.

[15] B. Schneier, The uses and abuses of biometrics, Commun. ACM 42 (8) (1999) 136.

[16] Maio, Dario, Davide Maltoni, Raffaele Cappelli, James L. Wayman, and Anil K. Jain. "FVC2000: Fingerprint verification competition." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 24, no. 3 (2002): 402-412.

[17] Doddington, George, Walter Liggett, Alvin Martin, Mark Przybocki, and Douglas Reynolds. *Sheep, goats, lambs and wolves: A statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation*. NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD, 1998.

[18] Ortega-Garcia, Javier, Josef Bigun, Douglas Reynolds, and Joaquin Gonzalez-Rodriguez. "Authentication gets personal with biometrics." *Signal Processing Magazine, IEEE* 21, no. 2 (2004): 50-62.

[19] Rodwell, P. M., S. M. Furnell, and Paul L. Reynolds. "A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head." *Computers & Security* 26, no. 7 (2007): 468-478.

[20] Ross, Arun, Anil Jain, and James Reisman. "A hybrid fingerprint matcher." *Pattern Recognition* 36, no. 7 (2003): 1661-1673.

[21] Wildes, Richard P., Jane C. Asmuth, Gilbert L. Green, Steven C. Hsu, Raymond J. Kolczynski, James R. Matey, and Sterling E. McBride. "A machine-vision system for iris recognition." *Machine vision and Applications* 9, no. 1 (1996): 1-8.

[22] Gibbs, Martin D. "Biometrics: body odor authentication perception and acceptance." *ACM SIGCAS Computers and Society* 40, no. 4 (2010): 16-24.

[23] Liu, Simon, and Mark Silverman. "A practical guide to biometric security technology." *IT Professional* 3, no. 1 (2001): 27-32.

[24] Varga, Andrew, and Herman JM Steeneken. "Assessment for automatic speech recognition: II. NOISEX-92: A database and an experiment to study the effect of additive noise on speech recognition systems." *Speech communication* 12, no. 3 (1993): 247-251.

[25] Han, Chin-Chuan, Hsu-Liang Cheng, Chih-Lung Lin, and Kuo-Chin Fan. "Personal authentication using palm-print features." *Pattern Recognition* 36, no. 2 (2003): 371-381.

[26] Zhao, Wenyi, Rama Chellappa, P. Jonathon Phillips, and Azriel Rosenfeld. "Face recognition: A literature survey." *Acm Computing Surveys (CSUR)* 35, no. 4 (2003): 399-458.

[27] Bolle, Ruud M., Jonathan H. Connell, and Nalini K. Ratha. "Biometric perils and patches." *Pattern Recognition* 35, no. 12 (2002): 2727-2738.

[28] Shankar, Sheela, and V. R. Udupi. "A Dynamic Security Protocol for Face Recognition Systems Using Seismic Waves." (2015).

[29] Navalyal, Geeta U., and Rahul D. Gavas. "A dynamic attention assessment and enhancement tool using computer graphics." *Human-centric Computing and Information Sciences* 4.1 (2014): 1-7.

[30] Geeta, N., and Rahul Dasharath Gavas. "Enhanced Learning with Abacus and its Analysis Using BCI Technology." *International Journal of Modern Education and Computer Science (IJMECS)* 6.9 (2014): 22.

Authors' Profiles

Prof. Sheela Shankar has completed her Bachelor of Engineering in Electronics and Communication from BIET, Davangere, Karnataka. She has pursued her Masters in Electronics and Control Engineering from Birla Institute of Technology and Science, Pilani. Currently she is working as an associate professor in the department of Electronics and Communication Engineering, KLE

Dr.M.S.Sheshgiri College of Engineering and Technology, Belgaum, Karnataka, India. Her areas of research includes image processing, communication engineering and control engineering.

Dr. V. R. Udupi did his bachelor’s degree in Electronics and communication Engg. from Mysore University in 1984 and pursued his master’s degree in Electronics Engineering with computer applications as specialization from Shivaji University, Kolhapur, Maharashtra state, in 1989. He has completed his doctoral degree in Electrical Engineering from Shivaji University, Kolhapur, Maharashtra state, in 2003. His field of interests includes signal processing, Image processing, cryptography, and knowledge based systems. Currently he is working as a professor in Electronic and communication department of Gogte institute of Technology, Belgaum, Karnataka state. He has published more than 42 technical papers in national and international conferences and 08 articles in journals. He is a life member of ISOI, SSI, CSI, BMESI, and ISTE.

Mr. Rahul Dasharath Gavas has completed his Bachelor of Engineering in Computer Science and Engineering from KLE Dr. M.S Sheshagriri College of Engineering and Technology, Belgaum, Karnataka, India. He is currently working in TCS Innovation Labs, Kolkata. His areas of interest include Brain-Computer Interface, Computer Graphics, Biological Signal Processing and Software Engineering.

How to cite this paper: Sheela Shankar, V.R Udupi, Rahul Dasharath Gavas,"Biometric Verification, Security Concerns and Related Issues - A Comprehensive Study", International Journal of Information Technology and Computer Science(IJITCS), Vol.8, No.4, pp.42-51, 2016. DOI: 10.5815/ijitcs.2016.04.06