ON BIOMETRIC MODALITIES: A DETAILED REVIEW OF THE BIOMETRIC TECHNIQUES FOR SECURITY AND AUTHENTICATION

[1]Javed AkhtarUnar, [2]Abdul Wahid Memon, [2]Umair Ali Khan, [3]Ehsan Ali,
{[1]Department of Information Technology, [2]Department of Computer Systems Engineering, [3]Department of Electronic Engineering}
Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah.
email: jawedunar@yahoo.com,awam@quest.edu.pk, umair.khan@quest.edu.pk, ehsan.ali@quest.edu.pk

ABSTRACT

Reliable identification is the need of the modern networked society to grant access to different resources to genuine personnel. The lacunae of traditional identification systems paved the way to find alternatives. As an alternative, biometrics, which is the science of establishing human identity, based on the physical or behavioral characteristics offer several advantages. A number of biometric characteristics have been identified and tested during recent decades. This paper provides an in-depth analysis of the existing biometric systems along with their advantages and limitations. Besides, we also discuss soft biometrics and multi-modal biometric systems in detail and identify the scenarios and metrics which play pivotal role in the successful implementation and accuracy of biometrics technology. For comparative analysis of biometrics modalities, we identify two different sets of features and provide a qualitative comparison of different modalities.

Index terms - biometrics, modalities, authentication, verification

I. INTRODUCTION

Numerous attacks on public, government and private properties portrayed a chaotic scenario and questioned the effectiveness of surveillance systems. In order to cope with the existence of ever increasing number of these systems, a wide variety of approaches have been utilized. The existing security systems usually rely on the cryptographic methods requiring the masses to remember a secret text (password) or keep something with them (token, card) or a combination of both to prove their identity. As a result, the individuals are flooded with passwords and tokens to prove their identity to these systems in order to gain access to different resources such as access control, computer logins, checking e-mails, making bank transactions, border control, welfare disbursements, etc. However, the following problems challenge the authenticity of such systems: (i) forgetting the password/token, (ii) losing card, (iii) divulging the password to an unauthorized person, (iv) number of passwords to be remembered, (v) number of cards to carry, and (vi) ascertaining the identify of a user by the machine. As an alternative solution, the researchers have proposed the idea of human recognition with their physiological or behavioral attributes known as "Biometrics". In general, biometrics refers to the statistical analysis of biological data [1].However, in computer science, it refers to the automatic human recognition through their unique physiological (e.g., fingerprint, face, iris, etc.) or behavioral attributes (e.g., voice, signature, gait, etc.) [2][3][4][5]. Although, not the perfect solution, biometric recognition offers attempts to address many of the aforementioned challenges in the way that these attributes are part of the human body and represent the remarkable capability of humans to recognize each other. Eventually, this idea motivated French anthropologist Alphonse Bertillon to develop the first ever recognition system based on the scientific measurements of an individual's bony parts such as left middle finger, skull width, trunk, cubit, foot length along with eye color, hair color, side and front view photographs. However, the efficacy of the system was seriously challenged when the populated readings showed the identical measurements amongst several individuals. Despite its failure, the system proved a motivating and inspiring factor for Sir Galton to develop an elementary fingerprint recognition system based on the findings of HenryFaulds and William James describing the uniqueness and permanence of fingerprints in 1880. Subsequently, New York State Prison Department inaugurated the system in 1913 and it was adopted as the first fingerprint recognition system in United States.

Any physical or behavioral attribute can qualify for being a biometric trait unless it satisfies the following seven factors
i) Universality: possessed by all humans,
ii) Distinctiveness:distinguishable amongst the population,
iii) Permanence:invariance over a period of time,
iv) Collectability:easily collectible in terms of acquisition, digitization and feature extraction with convenience,
v) Performance: imposed constraints to collection must be realistic and guarantee higher accuracy as well as availability of resources to collect that attribute,
vi) Acceptability:the willingness of population to submit

that attribute to the recognition system, and vii) Circumvention: hard to imitate or mimicked incase of fraudulent attack against the recognition system [3]. Several distinctive characteristics have been identified and tested for recognition. Figure 1 shows the up-to-date nomenclature of these characteristic.

This paper provides an in-depth, critical analysis of the biometric technology along with the merits and demerits of each biometric technique used till date. We highlight the set of features which serve as the criteria for successful implementation and usability of a biometric technique.

The paper is structured as follows. Section I provides basic information consisting of composition, classification, operational scenarios, errors and certain tradeoffs related to biometric systems. In section II, we discuss different biometric modalities along with their salient points, feature sets, matching techniques, advantages and limitations. In addition, section III sheds light on the limitations of mono-modal biometric systems and the need for multi-modal systems.

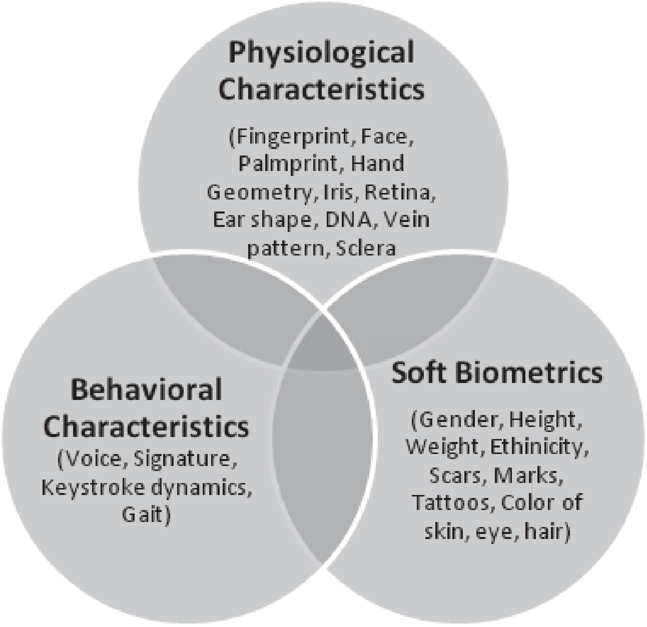
Physiological Characteristics
(Fingerprint, Face, Palmprint, Hand Geometry, Iris, Retina, Ear shape, DNA, Vein pattern, Sclera
Behavioral Characteristics
(Voice, Signature, Keystroke dynamics, Gait)
Soft Biometrics
(Gender, Height, Weight, Ethinicity, Scars, Marks, Tattoos, Color of skin, eye, hair)

Figure 1: Different Biometric Modalities

Section IV provides a comparative analysis of the biometric modalities with our identified sets of features. Section V concludes the paper.

2. BIOMETRIC SYSTEMS

A biometric system comprises offour modules: i) image acquisition module, (ii) feature extraction module to process the acquired biometric image and to extract the salient or discriminatory features, iii) matcher module to match the features obtained from the probe image with the features of gallery images in order to obtain a match score, (iv) an embedded decision making module to verify or to reject the claimed identification from the user based on the match score, and iv) a database module for storing the digital representation of acquired biometric samples (called templates) during enrolment phase.

The accuracy of a biometric system is heavily data-dependent and influenced by several other factors such as i) quality of biometric trait, ii) composition of target user population, iii) size of the database, iv) time interval, v) variation in the operating environment, and vi) robustness of algorithms. Besides these factors, the following factors also affect the accuracy of a biometric system[9][3][7][8]:(i) False Match Rate (FMR)whichrefers to the percentage measurement of invalid matches, (ii) False Reject Rate (FRR)whichis the measure of times (in percentage) the system recognizes an authorized user as an impostor, and (iii) Equal Error Rate (ERR)whichrefers to the point where FMR and FRR are equal and refers to a trade-off between the false accepts and rejects rates.

3. BIOMETRIC MODALITIES

This section discusses various physical and behavioral biometric modalities in terms of operation, feature extraction and matching algorithms.

3.1. Fingerprints

The unique texture of ridges and valleys present on the fingertips is believed to be unique for every human being even for identical twins and its consistency over entire life time. This makes fingerprint texture a suitable choice for human identification [3][5][8]. A fingerprint image contains the ridge bifurcations (minutiae points) used for recognition purpose and the ridge flow which helps in classifying fingerprints into one of the five categories, namely arch, tented arch, left loop, right loop and whorl [7][11]. A typical fingerprint image may contain 30-40 minutiae points [12]. A fingerprint recognition system may be classified as the one that uses the minutiae points for feature matching or the one that uses the pattern matching techniques [5][14]. High recognition rate, higher acceptability, low cost and portable sensors are the major objectives to design a fingerprint recognition system. On the contrary, the accuracy of these systems is affected by distorted images, physical contact with the sensors, natural image contaminants such as dead cells of finger, scars, cuts, wet and dry skin [3][5][7][8].

3.2. Face Recognition Systems

Amongst all the biometric modalities, face is the most natural trait that provides the basis for automated face recognition systems [8]. However, the nonlinear structure of human face makes it a complex pattern recognition problem and an active area of research in computer vision [16]. The automated face recognition consists of image acquisition, feature extraction and feature matching phases. An automated face recognition system may employone of two approaches:(i) a feature based approach which computes the geometrical relationships amongst various key features from certain region of face such as distance between the eyes, mouth, side of the nose [17][18], or (ii) a holistic approach which uses the entire face image for performing the recognition task [19]. Categorically, automated face recognition systems can be divided in 2D or 3D systems. A 3D system based on the modeling of facial features as local and global curvatures presents more detailed information of facial geometry as compared to 2D system [16][17]. The most prominent 2D face recognition techniques include Principal Component Analysis (PCA), Fisher Discriminant Analysis (FDA), Self Organizing Map and Convolutional Network, Template Matching, Line Edge Maps (LEMs), Elastic Bunch Graph Matching (EBGM), Directional Corner Point (DCP) and Local Binary Patterns (LBP) [16] [17]. Although, none of these algorithms can guarantee a high recognition rate in a 2D system as the their performance may be drastically affected by illumination variations, pose variations, age variations, and occlusions [16][17]. In contrast, 3D face recognition approaches offer more robustness against the illumination and pose variations [16][20]. Some of the 3D face recognition techniques include Iterative Closest Point (ICP), Curvature based Segmentation approaches, and viewpoint-invariant technique [16].

3.3. Retina Recognition

The blood vessel pattern present on retina of human eye is unique [23]. In addition, the vasculature pattern of retina is the most secure biometric signature for two reasons; one that the retina is well protected and the other that forging the retinal vascular pattern is almost impossible [24]. A retina based identification system acquires the retinal vascular image through projecting an infrared light on the surface of retina due to the faster absorption of infrared light by the blood vessels as compared to the surrounding tissues. Subsequently, the acquired image is further processed and matched with the already enrolled pattern to establish the identity [25]. The feature extraction and matching techniques are based either on landmarks or on circular region of interest [23]. The landmark-based approaches consider the position and bifurcations of blood vessels [26]. Whereas, the area of reference based approaches consider the position of a reference point such as an optic disk [27] or fovea [28]. The features like uniqueness, permanence, highly secure and impossible to forge makes retina based recognition a highly accurate biometric. However, this technique is limited by the intrusiveness of image acquisition, physical contact with the acquisition device, full cooperation demands from the users, requirement of skilled operators, and high cost. These challenges limit the use of retina scanners for civilian purposes.

3.4. Iris Recognition

The complex texture pattern of an iris consists of furrows, crypts, corona and freckles [30]. The iris texture begins to form during the second month of gestation and completes by the eighth month [31]. The factors like clear visibility, uniqueness, lifetime stability, well protectiveness, difficult to forge and easy image acquisition makes iris a highly reliable biometric signature that can be used for verification as well as recognition. The recognition system acquires an iris image by subjecting it to a near-infrared light, extracts the features and finally performs the recognition task based on the iris texture. The works presented in [30][31][32][33] provide an extensive survey of iris recognition technology. Currently, most of the iris recognition systems are based on the pioneering algorithm developed by John Daugman [31]. The highly accurate recognition rate and matching speed motivates the integration of iris recognition systems in large-scale personal identification scenarios such as border crossings [8]. In addition, several efforts have been made to perform the recognition task in visible light [34][35][36] and at a distance [35][37]. However, the illumination changes, non-cooperative subjects, off angled iris images and reflections from ambient light sources including iris itself are some of the challenges to the technology in visible spectrum [38].

3.5. Scelra Vasculature

Sclera is the white and opaque portion of the human eye which contains a unique vein pattern with lifetime stability and hence can be used as a biometric identifier [39]. As evaluated in [40], the sclera vein pattern fulfills all the necessary conditions described in [3] for any physiological or behavioral characteristic to qualify for being a biometric identifier. Nevertheless, a few studies have been conducted to establish the authenticity of sclera vasculature to be used as a biometric characteristic [39][40][41], thereby conformity requires large-scale studies. Nevertheless, all the feature extraction and matching techniques are based on the analysis of the RGB channels of the acquired sclera vein pattern and off-axis iris images [39][40][41][42].

3.6. Palm Print

The palmprint technology identifies an individual based on the unique texture of principal lines and secondary creases present on the human palmar region. . The unique texture of principal lines and secondary creases develop between the third and fifth month of fetal development [44]. An automated palmprint recognition system acquires both the low and high quality palm images through an optical scanner. From the high quality palm images ridges, singular and minutiae points are extracted as features.Whereas, from the low quality images principal lines, wrinkles and palm texture are extracted as feature set using bi-sector based, tangent based and finger based approaches [45][46]. Normally, three different approaches are used for identification purpose such as i) line based approaches in which the principal lines are extracted and are used as feature vectors [47][48], ii) sub-space based approaches: where the Principal Component Analysis (PCA), Local Discriminant Analysis (LDA) and Independent Component Analysis (IDA) are applied directly on the palm images and the coefficients of sub-space are calculated and used as features [49][50], and iii) statistical approachesconsisting of local and global approaches. The local statistical approaches after transforming the image into a different domain, divides the image into small regions thereby the means and variances from these small regions constitute the feature set [51][52]. On the contrary, the global statistical approaches use the global features such as moments, center of gravity and density as their feature set [53][54]. The potential advantage of this technique is the large size of palm since it provides more detailed information as compared to fingerprints. In contrast, more user cooperation, bulky sensors, physical contact with the sensor and lower order of discrimination are some of the challenges associated with the technology.

3.7. Hand Geometry

The shape of human hand is also an important biometric modality having characteristics of variance and stability [55]. A hand geometry system uses a camera or a scanner to acquire the 2D or 3D image of human hand [55]. The feature extraction techniques are categorized as hand geometry based, hand contour based or palmprint based. Usually, the hand geometry based recognition systems use 2D features of hand such as length and width of fingers, aspect ratio of fingers or palm, length, thickness and area of hand [58].Whereas, the 3D hand recognition systems use skin folds and crease patterns of hand as features [59]. In addition, any of the distance measures such as correlation coefficient, absolute distance, Mahalanobis distance and Euclidean distance or their combination can be used as matching measures [57]. The advantages of this technology include higher user convenience, low cost of sensors, small template size and easy integration with existing fingerprint and palmprint systems. In contrast, the accuracy of this technology is limited by therecognition inability, presence of artifacts such as jewelry, and diseases pertaining to human hand such as arthritis, etc.

3.8. Facial Thermograms

A facial thermogram system captures the unique heat radiation patterns of human face with the help of an infrared camerawhich can be used as a biometric signature. Usually, a facial thermogramis obtained from the vasculature structure present beneath the skin of human face;hence, it is almost impossible to forge that pattern [60]. In comparison to other face recognition techniques, facial thermogram not only reveals the detailed anatomical features of the face, but also shows strong invariance to facial expressions and other artifacts such as application of cosmetics and plastic surgery. As a result, face detection, localization and segmentation becomes easier than the facial images acquired in visible wavelength of light [61]. Several studies have proved the efficacy of infrared facial images over visible light facial images [61][62]. The advantages of this technique include non-invasiveness, representation of more detailed features of face, robustness to heterogeneous lighting conditions and pose variations. In contrast, view dependence, skilled operator requirements, ambient physiological or psychological conditions are some of the challenges associated with this technology.

3.9. Vein Pattern

The network of blood carrying veins beneath the human skin is unique even in identical twins,and this invariant characteristic helps in declaring it a biometric modality [63]. This recognition system acquires the image of human hand by exposing it to near-infrared light. The deoxidized hemoglobin present in the veins absorbs the infrared light by reducing the reflection and causing the veins to appear black [63]. In terms of features, a typical vein recognition system uses minutiae points such as vein bifurcations and endings [63]. Eventually, adaptive thresholding [64], morphological gradient operator [65], Principal Component Analysis (PCA) [66] or Linear Discriminant Analysis (LDA) [67] are used for feature extraction and matching. Although, the non-intrusiveness, difficult to counterfeit and stability of vein pattern makes thistechnology a strong member of biometric signatures. However, it suffers from a number of challenges including higher user cooperation, physical contact with the imaging sensor, shrinkage of vasculature pattern due to diseases such as diabetes, hypertension, metabolic disorders, tumors and lack of large scale investigations on uniqueness of vein pattern [8][63].

3.10. Deoxyribonucleic Acid (Dna)

DNA is unique to individuals and remains stable throughout the life with the exceptions of identical twins [68][69]. Interestingly, 99.7% of DNA code is shared, while 0.3% of the code is inherited and thus varies from person to person. As a matter of fact, this 0.3% of DNA code obtained from small varying region termed as short tandems is used for recognition purpose [70]. In comparison to the traditional method of acquiring the DNA code from blood samples, several alternatives are also proposed such as human hair, ear wax, dental floss, fingernail clippings etc. Nevertheless, the requirement of physical samples to collect the DNA code makes it different from other biometrics which requires either the impression or image for recognition. Furthermore, the DNA matching cannot be performed in real time and the process is not automated [72]. Although, it is a highly reliable and stable biometric identifier, it also suffers from certain drawbacks such as long processing time, requirement of human expertise, high cost and determination of hereditary diseases from the DNA code.

3.11. Ear Shape

The shape of human ear is unique andremains invariant throughout the life. Hence, it can be used as a biometric signature [73]. An ear recognition system acquires the image of human ear through different techniques such as i) taking the photograph of ear, ii) pushing the ear against a flat surface to get an earmark, iii) taking the thermogram of ear [73][75][76], and iv) measuring the acoustic transfer function of a sound wave projected on ear [77]. Ear recognition techniques can be categorized as i) local feature based approacheswhich use the geometrical features of ear for recognition [78], and ii) holistic approaches which use statistical measures to perform the recognition task [79]. However, 2D ear recognitions techniques are sensitive to illumination conditions, pose variations, imaging conditions and presence of partial and full occlusions due to jewelry and ear muffles [80]. To overcome these challenges, the researchcommunity has proposed the idea of 3D ear recognition thereby getting the image with a range of sensor which provide the range color and range image pair information for recognition.

3.12. Body Odor

Due to the presence of unique combination of organic compounds, human body emits a particular odor which can be used as a biometric signature [82]. This technology acquires the human odor through an array of chemical sensors, where each sensor is sensitive to a particular aromatic compound [3]. However, such type of sensors is not robust enough to perform the task of human recognition. In addition, identification of individuals based on body odor suffers from a number of privacy issues such as the possibility of diagnosing the diseases or the activities carried out during last hours.

3.13. Keystroke Dynamics

It is a behavioral biometric based on the technique used by telegraph operators to identify each other by recognizing the “fist of the sender” [85]. This recognition system identifies an individual based on the typing rhythm, which is unique for every individual based on the combination of duration and interval length between the keystrokes [86]. The system measures the characteristics such as duration of a keystroke, hold time, keystroke latency, typing errors, speed and pressure for recognition. Since the mentioned features are statistical in nature, therefore the recognition methods are the averages and standard deviations [87]. Although, the ability to perform continuous monitoring and user acceptability are some of the advantages associated with this technique, but the information regarding individual’s potential ratability and work effectiveness are considered as challenges to keystroke dynamics [68].

3.14. Signature Recognition

This is a behavioral biometric that identifies an individual based on the measurements of signature dynamics. Such systems are categorized as either static or dynamic [88]. A static verification system requires the users to produce the signatures on a piece of paper, which is then digitized and produced to the system for identification [89][90]. In contrast, a dynamic signature verification system acquires the signatures through digitizing pad and measures the attributes like pen position, pen pressure, direction, acceleration, length of strokes, tangential acceleration, curvature radius and azimuth for authentication [88]. The dynamic signature verification system offers better accuracy as compared to the static system. The merits of this technique include high social acceptance, ease of changing the signatures any time and inclusion of handwriting methods in mobile devices. On the contrary, muscular illness of the subjects, physical and emotional states, and the possibility of signature change over time are some of the challenges associated with this technology.

3.15. Voice Recognition

Human voice is characterized by some physiological and behavioral characteristics such as shape and size of vocal tract, lips, nasal cavities, mouth, and behavioral attributes such as movement of lips, jaws, tongue, velum and larynx, pitch and volume. These characteristics are unique for every individual [91]. A speaker verification system lies in one of the two categories such as i) text-dependent, which performs the identification task based on the utterance of a fixed phrase by the user, and ii) text-independent, which imposes no fixed vocabulary constraints on the user [92]. Although more complex and difficult to develop, the later type of the system provides better accuracy and robustness against the spoof attacks. In terms of feature matching, vector quantization, hidden Markov model and Gaussian mixture model provide better accuracy as compared to other approaches such as dynamic time warping and artificial neural networks [93]. Apart from its advantagesincluding less hardwarerequirements, several factors contribute to the low accuracy rate of these systems such as similarity of voice due to health conditions, aging, emotional states and presence of extraneous noise and poor quality of acquisition devices. Consequently, the technology is limited to verification tasks only.

3.16. GAIT

A behavioral biometric based on the analogy that the walking pattern of an individual can be used as a biometric identifier. A gait based recognition system obtains the shape and dynamics information for recognition process. The most common recognition techniques include i) temporal aligned basedtechniques, which analyze the time series features such as the full subject silhouette, ii) static parameter based approaches, which analyze the gait dynamic features such as stride, length, cadence and speed, and iii) silhouette shape based approaches,which emphasize on the similarity of silhouette shape instead of the temporal information [95]. Although, the gait offers the advantage of recognition at a distance over other biometrics [96][97], but it does not provide sufficient discriminatory information which limits its ability to perform only the verification task. In addition, the walking speed, walking surface dynamics are some of the other potential challenges lead to high false rejection rates.

3.17. SOFT BIOMETRICS

This term refers to the attributes that are most common amongst the humans such as gender, ethnicity, height, weight, color of skin, color of eye, color of hair and SMT (scars, marks and tattoos), etc. These attributes provide broad information about a person, but are not sufficient to perform the recognition task [99]. However, their combination with hard biometrics (face, iris, fingerprints, etc.) produces better solutions to classification problems by narrowing down the search space and produces better accuracy rates in verification and identification [98][100][101][102].

4. MULTI-MODAL BIOMETRICS

Although, the biometric technology based on the measurements of a single trait is mature enough, but none of the systems guarantee 100% recognition accuracy. This is because several factors affect the recognition accuracy of a mono-modal biometric system, e.g., noisy data, intra-class variations, distinctiveness, non-universality, and spoof attacks[5][103]. In order to overcome these challenges, many researchers have proposed the idea of multi-modal biometric systems. A multi-modal biometric system fuses the information from either single or different biometric modalities to perform a decision. In terms of performance, a multi-modal biometric system offers higher recognition accuracy due to the fusion of multiple independent evidences of biometric information [104].

4.1. MODES OF OPERATION:

Operationally, a multi-modal biometric system functions in one of the following three modes [5][7].

(i) Serial / cascaded mode: Itpertains to the processing of acquired multiple biometric modalities one after another. The output of one biometric trait serves as input to the processing of next biometric trait. The first trait serves as an indexing scheme to narrow down the search space before the next biometric trait is used, which in turn results in the reduction of recognition time. Typical serial arrangement is illustrated in Figure 2.

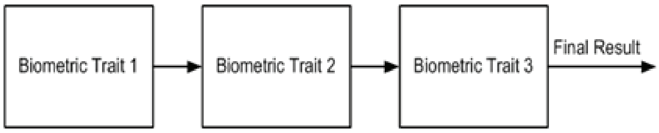

Figure 2: Serial arrangement of multi-modal biometric system

(ii) Parallel mode: In this mode, all the acquired biometric traits are processed simultaneously and the results are combined to get a match score. Although, the architecture provides better results but requires more time to establish an identity. Figure 3 illustrates the parallel architecture.

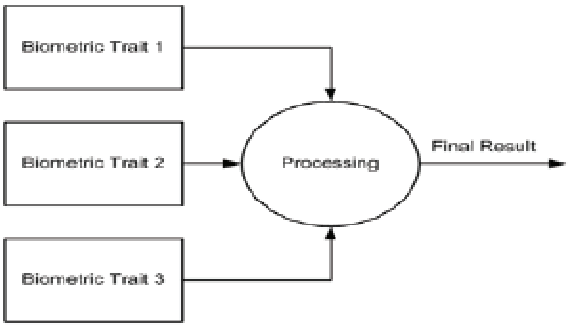

Figure 3: Parallel arrangement of multi-modal biometric system

(iii) Hierarchical mode: In this mode, all the independent classifiers are combined in a tree shape.

4.2. SOURCES OF INFORMATION

Since a multi-modal biometric system performs the recognition based on the presence of multiple biometric samples, these systems can be classified into the following categories according to the source of information [5][7][103][104].

(i) Multi-sensor systems: This pertains to the usage of multiple sensors to acquire a particular biometric trait. The multiple sensors provide detailed and complementary information regarding the measured trait, which helps enhancing the recognition accuracy. Although, the scheme overcomes the problems of poor quality or distorted biometric samples,but may suffer from increased cost of sensors and the constraint of high user cooperation.

(ii) Multi-algorithm systems: Such systems use different feature extraction or matching algorithms on a single biometric trait acquired through a single sensor. Finally, the individual results produced by different algorithms are combined to obtain a decision level, which results in achieving enhanced recognition accuracy.

(iii) Multi-instance systems: These systems capture multiple instances of a single biometric trait to be measured by using a single imaging sensor which produces a complete representation of the trait being used.

(iv) Multi-sample systems: Such systems measure the variations of the same biometric trait, thereby acquiring the underlying biometric trait through a single imaging sensor. However, the attention must be paid to the determination of number of samples in advance given that the acquired samples must show variance and typicality of the particular trait.

(v) Multi-modal systems: These systems perform the recognition task based on the measurements of uncorrelated biometric signatures acquired through different imaging sensors. Although, these systems offer better level of accuracy due to the fusion of increasing number of different biometric traits, but require more effective dimensionality reduction methods. Moreover, the requirements of new sensors and appropriate user interfaces make their deployment costly.

(vi) Hybrid systems: Such systems use different combinations of the above-mentioned scenarios; for example; a system comprising of the multiple imaging sensors and multiple feature extraction or matching algorithms.

4.3. FUSION LEVELS

Exploiting any of the sources of information, the acquired evidences can be combined together at different levels described as follows [5][7][104].

(i) Sensor level: This results in the integration and formation of new data set which is normally used for feature extraction from the raw data acquired through different sensors. As an example, 2D texture information and 3D range (depth) information of human ear acquired through different sensors can be integrated to get the 3D image of human ear.

(ii) Feature level: This refers to the fusion of feature sets obtained from different biometric modalities to form a new feature set with higher dimensionality, given that the feature sets are independent and lie within the same measuring scale. Concatenating the feature sets of face and iris is a typical fusion example. Although, the researchers achieved better recognition accuracy at this level, however, it requires the proper solutions to deal with the factors like compatibility, high dimensionality, computational overhead and requirement of complex classifiers. Feature 4 depicts feature level fusion.

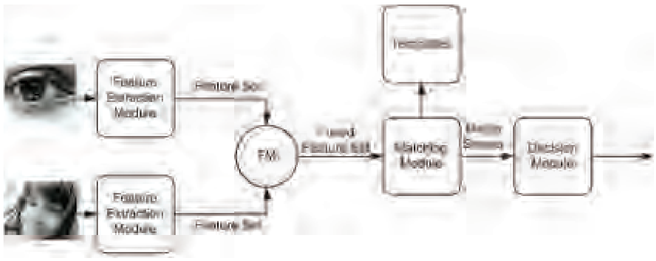

Figure 4: Feature level fusion

(i) Matching score level: This refers to the verification of the claimed identity by matching the obtained feature vectors independently with the pre-stored templates through different classifiers. The outputs are then fused together and finally the decision module makes the decision based onthe composite match score. A match score level fusion is illustrated in Figure 5.

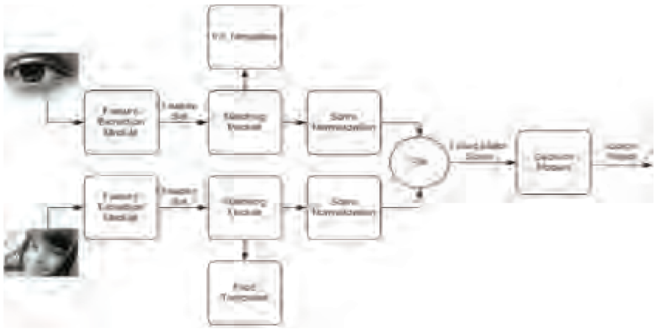

Figure 5: Match Score level fusion

(ii) Decision level fusion: Using this approach, each matcher classifies the observed biometric modality independently.Subsequently, the decisions from different matchers are fused together to make the final decision through the techniques such as majority voting. However, this fusion mode is not considered to be much effective due to the fact that the final classification decision takes longer to arrive. Figure 6 illustrates the decision level fusion.

5. IMPLEMENTATION STAGES OF BIOMETRIC SYSTEMS

The implementation stages of a generic biometric system are shown in Figure 7. The process starts with collecting appropriate samples from different sources. The scenarios considered during the data collection step greatly influence the performance of a biometric system. The collected data is analyzed for missing parts and extraction of appropriate features. It is then split into two parts: one used for learning the inherent patterns, and the other used for evaluation. The pre-processing of the training data follows selection of right features, scaling and rejecting the redundant or unnecessary features from the dataset. The later step finds the inherent relationship between the selected features and builds a classification/prediction model based on the observed patterns. The evaluation of the classification/prediction model is performed with respect to the performance metrics of accuracy, precision and recall. The training data generated during the pre-processing step is used for evaluating the performance of the biometric system.

6. EMERGING BIOMETRIC TECHNOLOGIE

Besides the aforementioned longest serving biometric technologies, several new modalities are striving to find their way to be included in main stream. These include finger knuckle print, periocular skin and heart sound. However, their conformity needs large scale analysis.

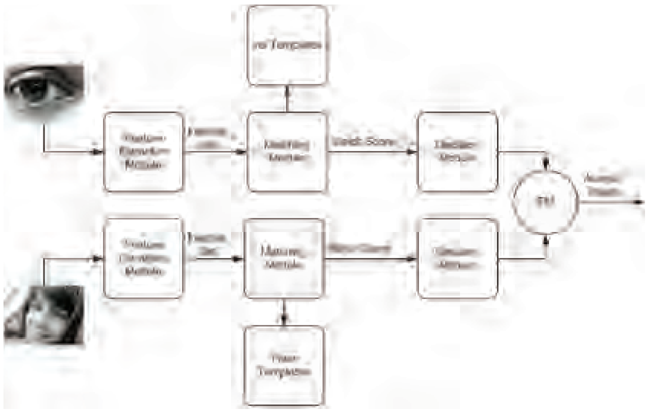

Figure 6: Decision level fusion

7. COMPARATIVE ANALYSIS

We identify a number of features which can be used for the comparative analysis of different biometric modalities. We divide this set of features into two sub-sets, i.e., (i) the set determining the level of universality, uniqueness, permanence, collectability, performance, acceptability, circumvention, and (ii) the set determining imaging procedure, imaging sensor and environmental challenges. Our comparative analysis with respect to these two sets is shown in Table 1 and Table 2.

8. CONCLUSION

Reliable identification is the crucial requirement in a wide variety of systems and different scenarios. Traditional cryptographic methods do not offer reliable identification since they require the users to remember something or to possess something. Besides, several factors affect the efficacyof such systems and their reliability has been challenged from time to time. As an alternative, reliable identification based on the distinctive physiological or behavioral characteristics provides better solutions to high security demands of the present day. Moreover, these distinctive characteristics are sole property of an individual. Hence, the individuals are not required to memorize the large cryptographic words as the passwords. In addition, these features cannot be stolen or forgotten and require the genuine user to be present on the spot for identification.

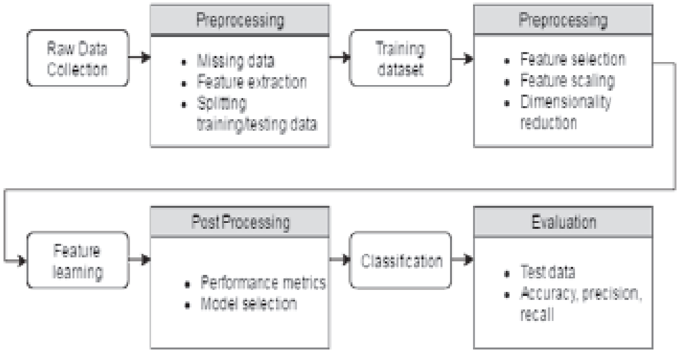

Figure 7: Implementation stages of biometric systems

In this paper, we have provided an overview of the existing biometric technologies along with the composition, classification and performance evaluation indicators. Moreover, we discuss different biometric attributes along with their potential advantages and disadvantages. Besides, we also discuss the necessity of multi-modal biometric systems along with their architecture and different levels of information fusion.

Table 1: Comparative analysis of different biometric modalities

Biometric attribute	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Finger print	Medium	High	High	Medium	High	Medium	High
Face	High	Low	Medium	High	Low	High	Low
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Iris	High	High	High	Medium	High	Low	High
Voice	Medium	Low	Low	Medium	Low	High	Low
Ear shape	Medium	Medium	High	Medium	Medium	High	Medium
Palm print	Medium	High	Medium	High	High	Medium	Low
Finger knuckle print	Medium	Medium	Low	High	Medium	Low	Low
Keystroke dynamics	Low	Low	Low	Medium	Low	Medium	Medium
Signature	Low	Low	Low	High	Low	High	High
Gait	Medium	Low	Low	High	Low	High	Medium

Table 2: Comparison between different biometric modalities

Modality	Imaging procedure	Imaging sensor required	Environment challenges
Finger print	Intrusive	Fingerprint scanner	Dirty / oily surface of sensor, temperature conditions, wet / dry skin
Face	Non-intrusive	Camera	Illumination changes, pose variation, expressions
Hand Geometry	Non-intrusive	Camera	Reflections, health conditions
Palm print	Non-intrusive	Camera	Reflections, health conditions
Finger knuckle print	Non-intrusive	Camera	Reflections, health conditions
Ear shape	Non-intrusive	Camera	Illumination changes, pose variations, presence of jewelry and ear muffles
Iris	Non-intrusive	Camera	Illumination changes, diffuse and specular reflections
Voice	Non-intrusive	Microphone	Background noise, channel distortions, emotional and health condition
Signature	Non-intrusive	Phone screen	Health conditions, emotional states
Gait	Non-intrusive	Accelerometer	Walking surface dynamics, emotional, health and dietary conditions
Keystroke dynamics	Non-intrusive	Keypad	Health conditions, emotional states
Heart sound	Intrusive	Electrodes	Physical contact, needs extra sensors

Although biometric technology does not offer solutions to all the applications and security scenarios, yet the recent interest and inclusion of biometric solutions to a number of identity management systems in government as well as private sectors promise a bright future to the science of biometrics.

REFERENCES

[1] Oxford Online Dictionary., "Definition of Biometrics 2012, visited on 12-09-2016, available at: http://oxforddictionaries.com/definition/biometry?q=biometrics," 2014.

[2] R. de Luis-Garcıa, C. Alberola-López, O. Aghzout, and J. Ruiz-Alzola, "Biometric identification systems,"Signal Processing, vol. 83, pp. 2539-2557, 2003.

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

[4] N. Clarke and S. Furnell, "Biometrics – The promise versus the practice,"Computer Fraud &amp; Security, vol. 2005, pp. 12-16, 2005.

[5] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security,"IEEE Transactions on Information Forensics and Security, vol. 1, pp. 125-143, 2006.

[6] A. K. Jain, S. Pankanti, S. Prabhakar, H. Lin, and A. Ross, "Biometrics: a grand challenge,"Proceedings of the 17th International Conference on Pattern Recognition, pp. 935-942 Vol.2, 2004.

[7] M. Deriche, "Trends and Challenges in Mono and Multi Biometrics,"First Workshops on Image Processing Theory, Tools and Application, pp. 1-9, 2008.

[8] A. K. Jain and A. Kumar, "Biometrics of Next Generation: An Overview," ed: Springer, 2010.

[9] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: security and privacy concerns,"IEEE transactions on Security & Privacy, vol. 1, pp. 33-42, 2003.

[10] History of Fingerprinting. Available: http://www.fingerprinting.com/hisotry-of-fingerprinting.php. Accessed on 12-09-2016.

[11] M. Liu, "Fingerprint classification based on Adaboost learning from singularity features,"Pattern Recognition, vol. 43, pp. 1062-1070, 2010.

[12] S. Prabhakar and A. K. Jain, "Decision-level fusion in fingerprint verification,"Pattern Recognition, vol. 35, pp. 861-874, 2002.

[13] A. K. Jain and F. Jianjiang, "Latent Fingerprint Matching,"IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, pp. 88-100, 2011.

[14] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems,"IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, pp. 3-18, 2006.

[15] A. S. Code. List of fingerprint databses available on web.Available:http://www.advancedsourcecode.com/fingerprintdatabase.asp. Accessed on 12-12-2014.

[16] A. F. Abate, M. Nappi, D. Riccio, and G. Sabatino, "2D and 3D face recognition: A survey,"Pattern Recognition Letters, vol. 28, pp. 1885-1906, 2007.

[17] X. Zhang and Y. Gao, "Face recognition across pose: A review,"Pattern Recognition, vol. 42, pp. 2876-2896, 2009.

[18] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey,"Acm Computing Surveys (CSUR), vol. 35, pp. 399-458, 2003.

[19] X. Tan, S. Chen, Z.-H. Zhou, and F. Zhang, "Face recognition from a single image per person: A survey,"Pattern Recognition, vol. 39, pp. 1725-1745, 2006.

[20] T. Theoharis, G. Passalis, G. Toderici, and I. A. Kakadiaris, "Unified 3D face and ear recognition using wavelets on geometry images,"Pattern Recognition, vol. 41, pp. 796-804, 2008.

[21] Face Recognition Organization. Face Recognition Databases.Available:http://www.face-rec.org/databases/. Accessed on 12-09-2016.

[22] Á. Serrano, I. M. de Diego, C. Conde, and E. Cabello, "Recent advances in face biometrics with Gabor wavelets: A review,"Pattern Recognition Letters, vol. 31, pp. 372-381, 2010.

[23] H. Oinonen, H. Forsvik, P. Ruusuvuori, O. Yli-Harja, V. Voipio, and H. Huttunen, "Identity verification based on vessel matching from fundus images,"17th IEEE International Conference on Image Processing, pp. 4089-4092, 2010.

[24] R. Hill, "Retina Identification,"Biometrics: Personal Identification in Networked Society (The International Series in Engineering and Computer Science), Kluwer Academic Publishers, Dordrecht, vol. 256, pp. 67-72, 1999.

[25] B. Miller, "Vital signs of identity [biometrics],"IEEE Spectrum, vol. 31, pp. 22-30, 1994.

[26] M. Sofka and C. V. Stewart, "Retinal Vessel Centerline Extraction Using Multiscale Matched Filters, Confidence and Edge Measures,"IEEE Transactions on Medical Imaging, vol. 25, pp. 1531-1546, 2006.

[27] J. Xu, O. Chutatape, E. Sung, C. Zheng, and P. Chew Tec Kuan, "Optic disk feature extraction via modified deformable model technique for glaucoma analysis,"Pattern Recognition, vol. 40, pp. 2063-2076, 2007.

[28] L. Huiqi and O. Chutatape, "Automated feature extraction in color retinal images by a model based approach,"IEEE Transactions on Biomedical Engineering, vol. 51, pp. 246-254, 2004.

[29] VARIA. Varpa retinal images for authentication. Available: http://www.varpa.es/varia.html, accessed on 12-09-2016.

[30] R. P. Wildes, "Iris recognition: an emerging biometric technology,"Proceedings of the IEEE, vol. 85, pp. 1348-1363, 1997.

[31] J. Daugman, "How iris recognition works,"IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 21-30, 2004.

[32] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "Image understanding for iris biometrics: A survey,"Computer Vision and Image Understanding, vol. 110, pp. 281-307, 2008.

[33] M. Li, T. Tieniu, W. Yunhong, and Z. Dexin, "Efficient iris recognition by characterizing key local variations,"IEEE Transactions on Image Processing, vol. 13, pp. 739-750, 2004.

[34] H. Proença and L. A. Alexandre, "Introduction to the Special Issue on the Segmentation of Visible Wavelength Iris Images Captured At-a-distance and On-the-move,"Image and Vision Computing, vol. 28, pp. 213-214, 2010.

[35] H. Proença and L. A. Alexandre, "Introduction to the Special Issue on the Recognition of Visible Wavelength Iris Images Captured At-a-distance and On-the-move,"Pattern Recognition Letters, vol. 33, pp. 963-964, 2012.

[36] T. Tan, Z. He, and Z. Sun, "Efficient and robust segmentation of noisy iris images for non-cooperative iris recognition,"Image and Vision Computing, vol. 28, pp. 223-230, 2010.

[37] J. Matey, D. Ackerman, J. Bergen, and M. Tinker, "Iris recognition in less constrained environments,"Advances in Biometrics, pp. 107-131, 2008.

[38] H. Proenca and L. A. Alexandre, "The NICE.I: Noisy Iris Challenge Evaluation - Part I,"First IEEE International Conference onBiometrics: Theory, Applications, and Systems, 2007, pp. 1-4, 2007.

[39] Z. Zhi, E. Y. Du, and N. L. Thomas, "A comprehensive sciera image quality measure,"11th International Conference onControl Automation Robotics & Vision, pp. 638-643, 2010.

[40] R. Derakhshani and A. Ross, "A texture-based neural network classifier for biometric identification using ocular surface vasculature," 2007, pp. 2982-2987.

[41] S. Crihalmeanu and A. Ross, "On the use of multispectral conjunctival vasculature as a soft biometric,"IEEE Workshop onApplications of Computer Vision (WACV), pp. 204-211, 2011.

[42] S. Crihalmeanu and A. Ross, "Multispectral Scleral Patterns for Ocular Biometric Recognition,"Pattern Recognition Letters, vol. 33, No. 14, pp. 1860-1869, 2012.

[43] A. W. K. Kong, D. Zhang, and G. Lu, "A study of identical twins' palmprints for personal verification,"Pattern Recognition, vol. 39, pp. 2149-2156, 2006.

[44] A. Kong, D. Zhang, and M. Kamel, "A survey of palmprint recognition,"Pattern Recognition, vol. 42, pp. 1408-1418, 2009.

[45] D. Zhang, W. K. Kong, J. You, and M. Wong, "Online

palmprint identification,"IEEE Transactions onPattern Analysis and Machine Intelligence, vol. 25, pp. 1041-1050, 2003.

[46] X. Wu, K. Wang, and D. Zhang, "HMMs based palmprint identification,"Biometric Authentication, pp. 1-11, 2004.

[47] M. K. H. Leung, A. Fong, and S. C. Hui, "Palmprint verification for controlling access to shared computing resources,"IEEE Pervasive Computing, pp. 40-47, 2007.

[48] D. S. Huang, W. Jia, and D. Zhang, "Palmprint verification based on principal lines,"Pattern Recognition, vol. 41, pp. 1316-1328, 2008.

[49] X. Wu, D. Zhang, and K. Wang, "Fisherpalms based palmprint recognition,"Pattern Recognition Letters, vol. 24, pp. 2829-2838, 2003.

[50] L. Shang, D. S. Huang, J. X. Du, and C. H. Zheng, "Palmprint recognition using FastICA algorithm and radial basis probabilistic neural network," Neurocomputing, vol. 69, pp. 1782-1786, 2006.

[51] J. You, W. K. Kong, D. Zhang, and K. H. Cheung, "On hierarchical palmprint coding with multiple features for personal identification in large databases,"IEEE Transactions onCircuits and Systems for Video Technology, vol. 14, pp. 234-243, 2004.

[52] A. Kumar and H. C. Shen, "Palmprint identification using palmcodes," 2004, pp. 258-261.

[53] L. Zhang and D. Zhang, "Characterization of palmprints by wavelet signatures via directional context modeling,"IEEE Transactions onSystems, Man, and Cybernetics, Part B: Cybernetics, vol. 34, pp. 1335-1347, 2004.

[54] Y. Li, K. Wang, and D. Zhang, "Palmprint recognition based on translation invariant Zernike moments and modular neural network,"Advances in Neural Networks–ISNN 2005, pp. 822-822, 2005.

[55] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzalez-Marcos, "Biometric identification through hand geometry measurements,"IEEE Transactions onPattern Analysis and Machine Intelligence, vol. 22, pp. 1168-1171, 2000.

[56] J. Renaghan, "Etched in stone,"Zoogoer, August, 1997.

[57] D. Nicolae, "A survey of biometric technology based on hand shape,"Pattern Recognition, vol. 42, pp. 2797-2806, 2009.

[58] M. Adán, A. Adán, A. S. Vázquez, and R. Torres, "Biometric verification/identification based on hands natural layout,"Image and Vision Computing, vol. 26, pp. 451-465, 2008.

[59] D. L. Woodard and P. J. Flynn, "Finger surface as a biometric identifier,"Computer Vision and Image Understanding, vol. 100, pp. 357-384, 2005.

[60] F. J. Prokoski, R. Riedel, and J. Coffin, "Identification of individuals by means of facial thermography," 1992, pp. 120-125.

[61] S. G. Kong, J. Heo, B. R. Abidi, J. Paik, and M. A. Abidi, "Recent advances in visual and infrared face recognition—a review,"Computer Vision and Image Understanding, vol. 97, pp. 103-135, 2005.

[62] P. Buddharaju, I. T. Pavlidis, P. Tsiamyrtzis, and M. Bazakos, "Physiology-based face recognition in the thermal infrared spectrum,"IEEE Transactions onPattern Analysis and Machine Intelligence, vol. 29, pp. 613-626, 2007.

[63] A. Kumar and K. V. Prathyusha, "Personal Authentication Using Hand Vein Triangulation and Knuckle Shape,"IEEE Transactions on Image Processing, vol. 18, pp. 2127-2136, 2009.

[64] Y. Ding, D. Zhuang, and K. Wang, "A study of hand vein recognition method,"IEEE International Conference Mechatronics and Automation, 2005, pp. 2106-2110 Vol. 4.

[65] K. A. Toh, H. L. Eng, Y. S. Choo, Y. L. Cha, W. Y. Yau, and K. S. Low, "Identity verification through palm vein and crease texture,"Advances in Biometrics, pp. 546-553, 2005.

[66] M. Heenaye-Mamode Khan, R. K. Subramanian, and N. Ali Mamode Khan, "Representation of Hand Dorsal Vein Features Using a Low Dimensional Representation Integrating Cholesky Decomposition," 2nd International Congress onImage and Signal Processing,pp. 1-6, 2009.

[67] L. Wenjing, Q. Xinjun, and L. Chenghang, "Fusion of Palm Dorsal Vein and Hand Geometry for Personal Identification Based on Linear Discriminant Analysis,"Fifth International Conference onFrontier

of Computer Science and Technology (FCST), pp. 532-536, 2010.

[68] K. Delac and M. Grgic, "A survey of biometric recognition methods," in Electronics in Marine, 2004. Proceedings of 46th International Symposium Elmar, pp. 184-193, 2004.

[69] FINGERPRINTING. (2012). DNA Fingerprint Identification.Available:http://www.fingerprinting.com/dna-fingerprint-identification.php. Accessed on 12-09-2016.

[70] Shannon Soltysiak. and Hamed Valizadegan. DNA as a Biometric Identifier. Available: http://www.cse.msu.edu/~cse891/Sect601/CaseStudy/DNABiometricIdentifier.pdf. Accessed on 12-09-2016.

[71] A. C. Weaver, "Biometric authentication,"Computer, vol. 39, pp. 96-97, 2006.

[72] IBG. Is DNA a Biometric? Available: http://www.ibgweb.com/products/reports/free/dna-biometric. Accessed on 12-09-2016.

[73] A. V. Iannarelli, Ear identification: Paramont Publishing Company, 1989.

[74] K. Pun and Y. Moon, "Recent advances in ear biometrics," 2004, pp. 164-169.

[75] A. Hoogstrate, H. Van den Heuvel, and E. Huyben, "Ear identification based on surveillance camera images,"Science & Justice, vol. 41, pp. 167-172, 2001.

[76] R. Purkait and P. Singh, "A test of individuality of human external ear pattern: Its application in the field of personal identification,"Forensic science international, vol. 178, pp. 112-118, 2008.

[77] A. Akkermans, T. Kevenaar, and D. Schobben, "Acoustic ear recognition for person identification," 2005, pp. 219-223.

[78] M. Choras, "Ear biometrics based on geometrical feature extraction,"ELCVIA, vol. 5, pp. 84-95, 2005.

[79] A. Sanaa, P. Guptaa, and R. Purkaitb, "Ear biometrics: A new approach,"Biometrics, vol. 1, p. 1ntroduction, 2007.

[80] K. P. Ramesh and K. N. Rao, "Pattern extraction methods for ear biometrics - A survey," in Nature & Biologically Inspired Computing, 2009. NaBIC 2009. World Congress on, 2009, pp. 1657-1660.

[81] L. Yuan and Z. c. Mu, "Ear recognition based on local information fusion,"Pattern Recognition Letters, vol. 33, pp. 182-190, 2012.

[82] M. D. Gibbs, "Biometrics: Body Odor Authentication Perception and Acceptance,"SIGCAS Computers and Society, vol. 40, p. 16, 2010.

[83] A. P. Pons and P. Polak, "Understanding user perspectives on biometric technology,"Communications of the ACM, vol. 51, pp. 115-118, 2008.

[84] Z. Korotkaya, "Biometric person authentication: Odor,"Inner report in Department of Information Technology, Laboratory of Applied Mathematics, Lappeenranta University of Technology. in “Advanced Topics in Information Processing: Biometric Person Authentication, 2003.

[85] A. Peacock, K. Xian, and M. Wilkerson, "Typing patterns: a key to user identification,"IEEEtransactions on Security & Privacy, vol. 2, pp. 40-47, 2004.

[86] M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review,"Applied Soft Computing, vol. 11, pp. 1565-1573, 2011.

[87] M. Villani, C. Tappert, G. Ngo, J. Simone, H. S. Fort, and S. H. Cha, "Keystroke biometric recognition studies on long-text input under ideal and application-oriented conditions," 2006, pp. 39-39.

[88] J. D. Woodward Jr, "Biometrics: A look at facial recognition," DTIC Document2003.

[89] F.-Z. Marcos, "On-line signature recognition based on VQ-DTW,"Pattern Recognition, vol. 40, pp. 981-992, 2007.

[90] C. Vivaracho-Pascual, M. Faundez-Zanuy, and J. M. Pascual, "An efficient low cost approach for on-line signature recognition based on length normalization and fractional distances,"Pattern Recognition, vol. 42, pp. 183-193, 2009.

[91] A. Fazel and S. Chakrabartty, "An Overview of Statistical Pattern Recognition Techniques for Speaker Verification,"IEEEtransactions on Circuits and Systems Magazine, vol. 11, pp. 62-81, 2011.

[92] S. Nemati and M. E. Basiri, "Text-independent

speaker verification using ant colony optimization-based selected features,"Expert Systems with Applications, vol. 38, pp. 620-630, 2011.

[93] S. Sadıç and M. Bilginer Gülmezoğlu, "Common vector approach and its combination with GMM for text-independent speaker recognition,"Expert Systems with Applications, vol. 38, pp. 11394-11400, 2011.

[94] S. A. Niyogi and E. H. Adelson, "Analyzing gait with spatiotemporal surfaces,"Proceedings of IEEE Workshop onMotion of Non-Rigid and Articulated Objects, pp. 64-69, 1994.

[95] L. Zongyi and S. Sarkar, "Improved gait recognition by gait dynamics normalization,"IEEE Transactions onPattern Analysis and Machine Intelligence, vol. 28, pp. 863-876, 2006.

[96] L. Wang, W. Hu, and T. Tan, "Recent developments in human motion analysis,"Pattern Recognition, vol. 36, pp. 585-601, 2003.

[97] A. Kale, A. Sundaresan, A. N. Rajagopalan, N. P. Cuntoor, A. K. Roy-Chowdhury, V. Kruger, and R. Chellappa, "Identification of humans using gait,"IEEE Transactions on Image Processing, vol. 13, pp. 1163-1173, 2004.

[98] P. Unsang and A. K. Jain, "Face Matching and Retrieval Using Soft Biometrics,"IEEE Transactions onInformation Forensics and Security, vol. 5, pp. 406-415, 2010.

[99] J. R. Lyle, P. E. Miller, S. J. Pundlik, and D. L. Woodard, "Soft biometric classification using periocular region features,"Fourth IEEE International Conference onBiometrics: Theory Applications and Systems (BTAS), pp. 1-7, 2010.

[100] K. Niinuma, P. Unsang, and A. K. Jain, "Soft Biometric Traits for Continuous User Authentication,"IEEE Transactions onInformation Forensics and Security, vol. 5, pp. 771-780, 2010.

[101] D. L. Woodard, S. Pundlik, P. Miller, R. Jillela, and A. Ross, "On the Fusion of Periocular and Iris Biometrics in Non-ideal Imagery,"International Conference onPattern Recognition (ICPR, pp. 201-204, 2010.

[102] S. Bharadwaj, H. S. Bhatt, M. Vatsa, and R. Singh, "Periocular biometrics: When iris recognition fails,"Fourth IEEE International Conference onBiometrics: Theory Applications and Systems (BTAS), pp. 1-6, 2010.

[103] L. P. Rodriguez, A. G. Crespo, M. Lara, and B. R. Mezcua, "Study of Different Fusion Techniques for Multimodal Biometric Authentication,"IEEE International Conference on Wireless and Mobile Computing, Networking and Communications,pp. 666-671, 2008.

[104] M. Gudavalli, S. V. Raju, A. V. Babu, and D. S. Kumar, "Multimodal Biometrics--Sources, Architecture and Fusion Techniques: An Overview," pp. 27-34, 2012.

-