Comparative Study of Biometric Models for Individuality Investigation

Oluwatayo Samuel Ogunlana
Adekunle Ajasin University, Akungba Akoko, Nigeria
Information and Communication Technology Application Centre

ABSTRACT
In the entire world, security systems are essential for the protection of life and property. This is a growing technology which has become increasingly used in our daily life. Other areas of application include but not limited to commercial banking sectors, educational institutions, border control via passport verification, voter's registration and verification and so on. In order to provide such needed and adequate security, biometric systems are essential. Biometric is the technique used to identify an individual based on his /her physiological (e.g. fingerprint, face, retina, and so on) and behavioral (gait, signature, voice, and so on) characteristics. Every individual identity relied majorly on these categories of traits. Traditional methods of establishing a person identity include the knowledge (password, username) and possession (card, token)-based. A biometric that uses a single biometric trait for recognition is prone to problems related to non-universality, spoof attacks, limited degree of freedom, large intra-class variability, and noisy data. Some of these problems can be overcome by integrating the use of multiple biometric traits of a user (e.g. face, fingerprint). This paper provides a comparative study of commonly known biometric models for individuality investigation with emphasis on methodologies, strengths and weakness.

General Terms
Pattern Recognition

Keywords
Biometric, fingerprint, individuality investigation, model, security

1. INTRODUCTION
The word 'biometrics' is derived from Greek word 'bios' means life and 'metric' means measurement [1]. Biometric is the most practical means of identifying and authentication individuals in a reliable and fast way through unique physiological and behavioral characteristics. Any characteristic can be used as a biometric identifier to recognize a person as long as it satisfies the following requirements [3-5]:

a. **Universality:** Every individual should possess the biometric characteristic
b. **Uniqueness:** No two persons should be the same in terms of the characteristic.
c. **Permanence:** The biometric characteristic should be invariant over time.
d. **Collectability (Measurability):** Ease of acquisition or measurement of the trait. The acquired data should be in form that allows subsequent processing and extraction of the relevant feature sets
e. **Performance:** The recognition accuracy, speed, and robustness to operational and environmental factors should be accepted.
f. **Acceptability:** Indicate the extent to which people are willing to accept the characteristics such that they are willing to have their biometric traits captured and assessed.
g. **Circumvention:** Refers to how difficult it is for fraudulent techniques to fool a system that is based on the characteristics

Biometric characteristics a person possesses can either physiological characteristics or behavioral characteristics as shown in Figure 1.

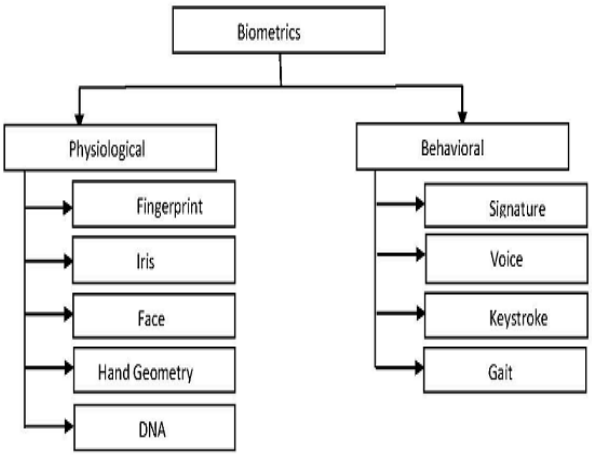

Figure 1: Classification of Biometrics

Physiological characteristics are unique characteristics physically present in human body. This can either be morphological or biological, morphological identifiers mainly consists of face, fingerprint, iris, ear, and biological identifiers are DNA, blood, saliva or urine which may be used by medical teams and police forensics. Behavioral characteristics are related to behavior of a person, which include signature, voice, gait, walking pattern, and so on [2]. Biometrics offers certain advantages such as distinctiveness, cannot be forgotten or lost, and the person to be authenticated needs to be physically present at the point of identification, also, it is difficult to forge or steal biometric identity [3,5]. Human behavioral characteristics can be changed with time, but their physiological characteristics can never be changed and has the benefit of remaining stable throughout the life of an individual. Biometrics is inherently more reliable and more capable than traditional knowledge-based and token-based techniques. In most cases, a typical biometric system consists of the following components as depicted in Figure 2:

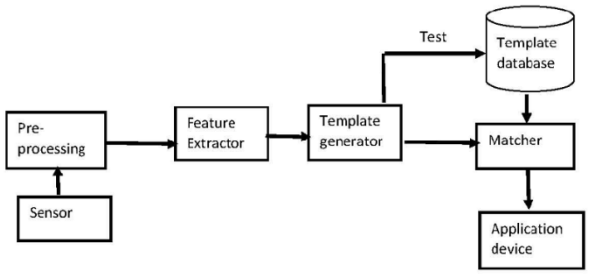

Figure 2: Block Diagram of Biometric System

a. The Sensor module: This module responsible for acquisition of biometric data
b. The feature extraction module: This is where the acquired data is processed to extract feature vectors
c. Matching Modules: The feature vectors in the reference database are compared against those in the template database to ascertain the degree of similarity.
d. Decision module: Where the usher's identity is verified or a claimed identity is accepted or rejected.

A biometric system can either be unimodal or multimodal. A unimodal rely on the evidence of a single source of information for authentication while multimodal rely on more than one source of information for authentication. A unimodal system prone to the following deficiencies [3]: (a) Noisy data from sensors, (b) high intra-class variation, (c) high interclass similarities, (d) non-universality, (e) non-variant representation, (g) spoofing.

A multimodal biometric system based on multiple traits is expected to be more robust to noisy, address the problem of non-universality, improving matching accuracy, and provide reasonable protection against spoof attacks [6-7]. The use of biometric is application dependent and there is no single biometric that can meet all the requirements of every possible application. Generally, a biometric system can operate either in the verification mode or identification mode [7]. In verification (or authentication) mode, a one to many (1:M) comparison against a biometric database in an attempt to establish the identity of an unknown individual is performed. Users template matched with all the templates stored in database to identify with the template that has the highest similarity [8]. Identification mode can be used either for positive recognition (user does not provide any information about the template to be used), or negative recognition where the system establishes a person is truly who he/she claims to be. This can be achieved through biometric since other methods of personal recognition such as password, PIN, or keys are ineffective. Areas of applications of biometrics to ascertain the individuality include but not limited to the following [4]: law enforcement and public security, military, border/travel/immigration control, voter registration and identification, healthcare and subsidiaries, commercial applications, physical and logical access.

Section 2 of this paper presents various biometric models for individuality investigation, while Section 3 presents review of some of research works on biometric models with emphasis on methodologies, strengths and weakness of some biometric models by different authors. The conclusion drawn is also presented in Section 4.

2. BIOMETRIC MODELS FOR INDIVIDUALITY INVESTIGATION

The summaries of various biometric models for individuality investigation are presented below:

2.1 Fingerprint

A fingerprint is an impression left by the ridges and valleys of a human finger. The ridges are the dark and raised portions while the valleys are the white and lower portions [3]. Human fingerprints are detailed, unique, difficult to alter and durable over the life of an individual making them suitable for human identification and classification. The ridges of finger form six major pattern types namely: arch, tented arc, left loops, right loop, twin loop and whorls, as shown in Figure 3 [3-4].

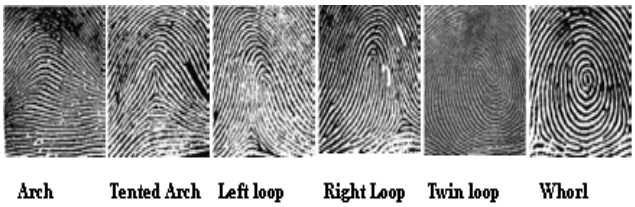

Figure 3: Types of fingerprint patterns

Acquisition of fingerprint image is considered to be the most crucial step in an automated fingerprint identification and authentication system as it has a drastic effect on the overall system performance. The performance of an automated identification system relies heavily on the fingerprint image quality which can be affected by several factors such as, presence of scars, variations of the pressure between the finger acquisition sensor, introduction of spurious, contaminants or artifacts and the environmental conditions during the acquisition stage [4]. The procedure for capturing fingerprint using a sensor (optical, ultrasonic, capacitive, or thermal) consist of rolling or touching the finger on the platen. Fingerprint image enhancement is performed to remove the noticeable noise and other contaminants acquired during enrolment and it requires a number of processes which include segmentation, normalization, filtering, binarization and thinning [3].

2.2 Iris Recognition

The iris is the elastic, thin, pigmented, circular and connective tissue in the eyes which controls the size and the diameter of the pupil, and limit the amount of light entering the eye [8]. A typical iris is depicted in Figure 4. The iris is developed in early life in a process called morphogenesis [2]. The iris is unique for individual and even the identical twins have different iris patterns. The texture of the iris is very complex and distinctive which is very useful for recognition process. The iris of the eyes has been described as the important part of the body for biometric identification for the following reasons [16]: (a) iris is an internal organ that is well protected against damage and wear, unlike fingerprint which can be difficult to recognize due to bruise or cut. (b) The iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles (sphincter pupillae and dilator pupillae) that control the diameter of the pupil. Challenges confronting iris recognition include growing difficulty from distance larger than few meters and required the cooperation from the individual to be identified. It is also susceptible to low performance for poor quality images [3]. Unlike fingerprint scanner which can be easily acquired, iris scanners are relatively expensive, scanners can be disappointed or fooled by high quality image, and ultimately required the cooperation from the users during iris data acquisition stage [2,12].

Figure 4: Iris Recognition Biometric System [27]

2.3 Face recognition

This is a way of recognizing a human face through technology such as photographic or video. This technology analyses the shape and position of different parts of the faces to determine the match. Facial recognition has received substantial attention due to human activities found in various applications of security purposes like airport, criminal detection, face tracking, forensic, and so on. Automated face recognition involves some processes which include: face detection, face normalization, face feature extraction and matching as depicted in Figure 5.

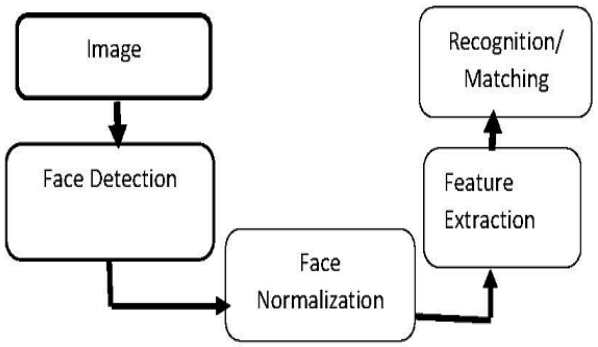

Figure 5: Block Diagram of Face Recognition System

The most common approaches used for facial recognition system are feature-based techniques, template-based techniques, appearance based techniques, model-based technique and hybrid methods [24]. In feature based techniques, facial features like eyes, nose, mouth, eyebrows, shape of the face and their positional relationship between them are extracted and their locations, geometry and appearance are fed into a structural classifier. A major challenge of this technique is the fact that it does not allow for feature restoration, particularly when the system tries to retrieve features that are invisible due to large variations. In template based techniques, features of face like eyes, nose, mouth, and so on are extracted based on template function and appropriate energy function. In appearance based techniques, linear transformations and statistical methods are used to find basic vectors to represent the face. In model-based technique, a new sample is introduced to the model and the parameters of the model are used to recognize the image. This technique usually classifies images as 2D or 3D. Hybrid model uses a combination of both holistic and feature extraction methods. 3D images are generally used in this method. The image of the face is captured in 3D to capture the curves of the eye sockets, or the shapes of the chin or forehead. The 3D system comprises of detection, position, measurement, representation and matching. Each of the feature extraction methods has its shortcomings, for example, template based feature extraction method do not represent global face structure whereas appearance based feature extraction method do represent global face structure with a high computational cost. Detecting faces from image are prone to some limitations which include illumination problem, pose variations occlusions due to accessories. Various face detection techniques that have been developed to address these limitations include Principal Component Analysis, Neural Network, Machine Learning, Geometrical Modelling, Hungh Transform and template matching [24]. Generally, face recognition has a number of significant weaknesses, the technology focuses mainly on the face portion, that is, around the hairline down, as a result, a person has to look straight at the camera to make recognition possible at the enrolment stage. Also, despite the technology is still developing at a rapid pace, the level of security it currently offers does not yet commensurate with that of other biometrics.

2.4 Gait Recognition

Gait recognition is the study of the way human walk and can also be used for identification purposes. This is a process where the features of human motion are extracted and use these extracted features to authenticate the identity of the person in motion. The major strengths of gait include the following [15]: it does not require user's interaction, it can be easily measured at a distance as long as gait is visible, it is difficult to disguise or occlude. Also, it is robust to low resolution images. Gait recognition system involves capturing human walking image, extract salient gait features, and feature recognition as conceptualized in Figure 6. Typically, there are two approaches to gait recognition systems, Motion based approach and model based approach [23]. In motion based approach, the human gait is considered as a sequence of image and features are extracted from these images while, the model based approach extract the motion of the human body by means of fitting their models to the input images. This approach is scale invariant and reflect in the kinematic characteristics of walking manner. Existing feature extraction techniques include the following [3]: Hidden Markov Model (HMM) and an Exemplar- based HMM, Random Transform with Linear Discriminant Analysis (LDA), Support Vector Machine (SVM), Principal Component Analysis (PCA) and Maximization of Mutual Information [9].

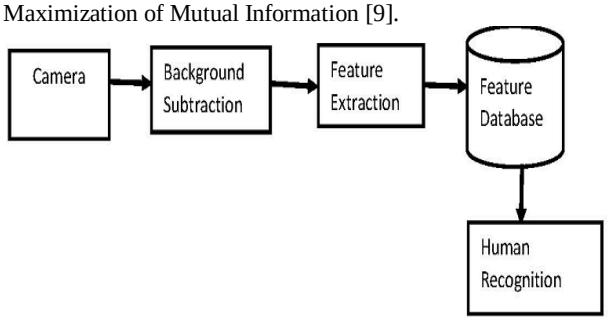

Figure 6: Gait Recognition Process

2.5 Palm Print Recognition

Like fingerprint, the application of palm print is enormous which include criminal, forensic, or commercial. A palm print is an image acquired from the palm region of the hand either through online image (scanner) or offline image (ink and paper). The palm consists of principal lines, wrinkles (secondary lines) and epidemic ridges. Like fingerprint, the uniqueness of palm print is attributed to its formation during birth, no two individuals have exactly the same palm print patterns. Also, palm print is distinctive, easily captured by low resolution device. A palm print recognition system broadly consists of four modules namely: palm print scanning, preprocessing, feature extraction and matching. Scanner is

used to collect palm print images while the acquired palm print image undergo segmentation at preprocessing stage. Most of the preprocessing involves the following steps [16]: (a). Binarizing the palm images (b). Extracting the shape of the hand (c). Detecting the salient points (d). Establishing a coordination systems and (e). Extraction of the central parts. Palm print feature algorithm are categorized into the following: line-based, subspace-based, local statistical-based, global statistical based and coding-based approaches [18]. Palm print classifiers such as neural network, hidden Markov models and correlation filters and various measures which include cosine measure, weight Euclidean distance, and Learning distance have been used for palm print classification [19]. The major weakness of palm print is that it changes with time depending on the type of work the person is doing for an extended duration to time.

2.6 Signature Recognition

This is a behavioral biometric that identifies an individual on the basis of their handwritten text (as conceptualized in Figure 7). Signature recognition requires an individual to supply a sample of text which serves as a basis of measurement of their writing. The purpose of signature recognition process is to identify the writer of a given sample, while signature verification process is to confirm or reject the sample. Basically, there are two techniques for writing signature, the static and dynamic techniques [10]. The static technique (often referred to as off-line mode of recognition) requires the individual to supply their signature on paper, then, digitalized it through an optical scanner or camera and then run it on software algorithm that recognizes the text by a way of analyzing its shape. Dynamic signature recognition, is a biometric modality that uses the anatomic and behavioral characteristics that an individual exhibit when signing his/her name or document. Some of the signature recognition techniques are dynamic time wrapping, hidden Markov model and vector quantization. Dynamic signature recognition characteristics are complex and unique to the handwriting style of the individual, its major weakness is the large intra-class variability, that is an individual's own signature may different from person to person which often making the dynamic signature recognition difficult and cumbersome [11].

Figure 7: Signature Biometric [26]

2.7 Hand Geometry Recognition

This is a biometric that identify persons by the shape of their hands. Hand geometry is very reliable when combined with other forms of identification such as ID card, PIN etc. In large populations, hand geometry is not suitable for one-to-many applications, in which user is identified from his biometric without any other identification. Hand geometry biometric systems utilize features such as finger length, width, thickness, finger area to perform personal authentication [3]. The device measures these features of an individual's hand while guided on a plate. It uses a camera to capture a silhouettes image of the hand. The enrollment process of a hand geometry system typically requires the capture of three segmental images of the hand, which are evaluated and measured to create a template of the user's characteristics. In order to create a verification template, the person places his/her hand on the plate, and the system captures an image, which is compares to the template developed upon enrolment. A similarity score is produced and based on the threshold of the system, the claim is either rejected or accepted. Hand geometry recognition systems have gained immensely popularity and public acceptance as evident from their extensive deployment for applications in access control, time attendance application and several other verification tasks. Major strengths of hand geometry include, simple imaging representations (features can be extracted from low- resolution hand images), the ability to operate under harsh environmental condition (immune to dirt on the hand and other external factors), and verification is extremely fast. One of the weaknesses of the hand geometry characteristics is that it is not highly unique, limiting the applications of the hand geometry system to verification tasks only [11].

2.8 Voice/ Speaker Recognition

The voice recognition relies on how the person speaks. The acoustic pattern traits of the speech are used by voice recognition to differentiate the individuals and these patterns consist of both behavioral pattern (speech style, voice pitch) and physical (shape and size of the throat and mouth) [8]. Speaker recognition is the identification of a person from characteristics of voices. During enrolment, audio devices such as microphones, telephones, and so on are used to capture the voice of the individual and asked to repeat the word or phrase. The electrical signal is then generated for the microphone using Analog to Digital ADC converter as shown in Figure 8. Voice recognition can either be speaker dependent or speaker independent. Speaker dependent system is based on the knowledge of individual voice trait, while speaker independent voice recognition recognizes the speech, words or phrase by the users with the restriction of the context of the speech. There are different techniques for voice recognition, Text-dependent style, where the user is requested to authenticate the word or phrase earlier stored during enrolment for verification purpose. In addition, the use of shared-secrets (passwords and PINs) or knowledge-based information can be employed in order to create a multi-factor authentication scenario, the text during enrolment and verification are usually the same. In case of text-independent system, the text during enrollment and verification is always different, the enrolment may happen without the user's knowledge. Preference template are generated for different phonetic sounds of the human voice rather than samples for certain words [2]. Basically, identification and verification of voice recognition comprises of four stages, voice recording, feature extraction, pattern matching and decision (whether accept/reject). The voice biometric is reliable, inexpensive and easy to use and no special instruction is required. However, some of the limitations include: susceptible to quality of microphone and environmental noise, the voice change if person is sick or old age, high rate of false non match as the technology fail to distinguish recognition when the distance is wide. Also, it depends on emotional condition of individuals [25].

Figure 8: Voice Signal Representation

3. SYNOPSIS OF SOME RESEARCH WORKS ON BIOMETRIC MODELS FOR INDIVIDUALITY INVESTIGATION

The summary of the objectives, methodologies and the limitations of some research works that are based on the models presented in the preceding Section is presented in this Section.

The author in [12] proposed Iris biometric system using a hybrid approach. The algorithm developed comprises of four major steps: (a) image processing using histogram matching, thresholding and Canny edge operator. (b) localization of pupillary and limbic boundary using Circular Hough Transform, (c) Iris normalization using Daugman's rubber sheet model, and, (d) feature extraction using Haar wavelet and binary encoding. The algorithm was validated using B-tree matching with Hamming distance as a matching metrics. The algorithm is not susceptible to pupil dilation due to varying illumination, specular reflections, or erratic and inconsistent limbic or pupillary boundaries.

The authors in [13] presented Face-Iris multimodal biometric identification system. The system used facial feature extraction technique which is singular spectrum analysis (SSA) modeled by normal-inverse Gaussian distribution (NIG) model and statistical features (entropy, energy, and skewness) derived from wavelet transformation. The authors performed the classification process using Fuzzy K-Nearest Neighbor (FK-NN). The fusion of the face-iris features was performed using score fusion and decision fusion. The developed system was performed optimally and efficiently improved the performance of unimodal biometric based on face or iris. However, the system is not effective when using low resolution images.

Silhouette correlation analysis based on human identification approach is proposed in [14]. The author extracted the features which consist of the following three dimensions: horizontal axis (x), vertical axis (y) and temporal axis (t). The correlation result between the original silhouette and the new one are used as raw feature of human gait. The author used discrete Fourier transformation to extract features from the correlation result followed by normalization process of the features to minimize the affection of noise. The dimension of the features was reduced by apply primary component analysis. The implementation was carried out using CASIA database. The algorithm produced efficient and better classification results. However, the system only work with two images correlation but perform poorly for three or more images correlation.

The authors in [15] proposed a model based approached for gait recognition using the mathematical theory of geometry and image processing technique. The images were segmented using Hough transformation and corner detection technique. The authors inputted the segmented images to Canny edge detection algorithms in order to detect the image edges and to reduce the noise by means of Gaussian filtering. The Hough transform algorithm was then implemented to isolate the extracted gait features. The authors then applied Harris Corner Detection technique to detect the corners and then generated the feature points. Digital camera was used by the authors to collect the gait data by placing the camera at an angle 90 degree and 270 degree in an environment with controlled illuminations and store the output in database. The model developed produced a better rate of recognition than other previous methods. Also, it does not require silhouette images. However, the segmentation approach is not robust enough since it produces poor segmented output. The model also failed when gait database is large.

A multimodal biometric system for person identification using palmprint and iris modalities is proposed in [20]. The model was based on Minimum Average Correlation Energy filter (MACE) for matching. The outputs of the subsystem (iris and palmprint) are combined using the concept of data fusion at matching score level. The experimental results proved the superiority of multimodal system over the unimodal system.

A model to establish a measure of discrimination of iris that is statistically inferable is proposed in [21]. The individuality model was validated by transforming the class problem into a dichotomy using a distance measure between two samples of the same class and between those of two different classes. Both features such as distance measure and classifiers were evaluated. Feature extraction was carried out using simple binary and multilevel 2D wavelet approaches. Scalar distance, feature vector distance and histogram distance were used for distance measure while Bayes decision rule, nearest neighbor, artificial neural network and support vector machine served as classifiers.

The authors in [22] proposed a multimodal biometric technique based on palm and fingerprint. IITD palmprint database comprises 230 right and left hand color images and UPEK fingerprint database were used for the experimental evaluation. All the images in the two databases were subjected to image enhancement. The algorithm produced more accurate and fast recognition result when compared to other techniques. The technique is suitable for real-time palmprint verification than other model.

The authors in [23] presented a human gait recognition system. The data were collected by recording a video of the subject from the camera and then converted the video into frames of the still images. Feature extraction technique was applied to get the silhouettes, while noise filtration was applied to the extracted silhouettes a get better quality images and stored in database. The silhouettes were trained with Principal Component Analysis (PCA). The camera produced low quality image. Table 1 shows further, the summary of some of these works.

Table 1: Summary of some of the existing works on biometric models for individuality investigation

Research	Methodology	Strength	Weakness
Sarin [12]	Circular Hough transformation and Haar wavelets algorithm	Developed competent iris biometric system	Performance diminish with noisy and blurred images
Ammon et al [13]	Iris features extraction using 2D Log-Gabor filter. Face features extracted using SSA-NN method	Faster in identification process	2D contains limited information for human recognition. Also, the system will not work when using a mask or other face covering vein.
Chen [14]	Discrete Fourier transformation method	Efficient and better classification result	Perform poorly on three or more images correlation.
Rafi et al [15]	Hough transformation and Corner Detection technique	Produced improved rate of recognition and does not require silhouette images	Segmentation approach not robust and model fail when the gait database is large
Abdullah et al [20]	Minimum average correlation energy filter	Performance superior to the unimodal system	The system failed when large size database is used
Sungsoo et al [21]	Combination of multilevel 2D wavelet features, histogram distance and a support vector machine.	Effective iris individuality model was developed	Only effective using small size iris database. The accuracy of the system is greatly affected as more reflection in pupil and iris region
Mohd et al (2020) [22]	Feature extraction approach, IITD palmprint and UPEK fingerprint database used	Faster than other model and suitable for real-time palm print verification	Unable to handle fusion image. Performance diminishes with images with substantial amount of noise.
Jawed et al [23]	Feature extraction approach using PCA for training the database	Efficient and better classification result	Low quality image, Interlacing in the video
Naidu and Reddy [28]	Score level fusion and Gaussian Mixture approach	Improves recognition performance. Less response time and improves accuracy	Manually extraction of individual voice is time consuming and cumbersome
Dutta and Singh [29]	Using skin color localization and Morphological operation techniques	Develop more secure and robust email security model. The algorithm able to detect dark skin-tone and bright skin-tone using YUC color space model.	The algorithm performs poorly with HSV and ycbc color spaces.
Nakhdoomi et al [30]	Average Silhouettes's algorithm, similarity score and matching process	A stronger, faster and more precise gait recognition algorithm developed.	Model greatly affected by the effect of terrain and slopes, bad weather poor visibility and effect of shoe type.

4. CONCLUSION

Biometric recognition has been an essential tool for increasing security in all facet of human endeavor due to its increasing public acceptance, massive accuracy gains, and today, many applications make use of biometric technology. This paper has presented some of the existing biometric models for individuality investigation. The motivations, methodologies, strengths and weaknesses of the physiological and behavioral forms of biometric have also been presented. These techniques of identifying individuality offer advantages over traditional methods involving ID cards or PIN numbers. Hence, these systems are proven highly confidential computer-based security system. The usefulness and selection of a particular biometric systems depend on the application areas and this allows its usefulness and applications in all biometric authentication systems.

5. REFERENCES

[1] Kaur, G. and Verma, C. K. 2014 Comparative Analysis of Biometric Modalities. International Journal of Advanced Research in Computer Science and Software Engineering, 4(4), Available at: www.ijarcsse.com.

[2] Mane, V.M, and Judhav, D. V. 2009 Review of Multimodal Biometrics: Applications, Challenges and Research Areas. International Journal of Biometric and Bioinformatics, 3(5), pp 90-95.

[3] Iwasokun G. B., Udoh, S.S. and Akinyokun O. C. 2015 Multi- Biometrics: Applications, Strategies and Operations. Global Journal of Computer Science and Technology, 15(2), pp 1-15.

[4] Ogunlana, S.O. 2021 Pattern Analysis Model for the Investigation of Fingerprint Individuality. Ph.D Thesis, Department of Computer Science, Federal University of Technology, Akure, Nigeria.

[5] Yadav, A.K. and Grewal, S. K. 2014 A Comparative Study of different Biometric Technologies. IJCSC, 5(1), pp 37-42.

[6] Delac, K. and Grgic M. 2004. A Survey of Biometric Recognition Methods. 46th International Symposium Electronic in Marine, pp184-193.

[7] Ross, A, and Jain, A.K: Multi Modal Biometrics: An Overview Proceedings of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp 1221-1224).

[8] Jain, A. Nandakumar, K Ross A. 2005. Score Normalization in Multimodal Biometric Systems. The Journal of the Pattern Recognition Society, pp 2270-2285. Available online at www.sciencedirect.com.

[9] Sasidhav, K Kakulapati, VL, Ramakrishna, K. Rao, K K. 2010. Multimodal Biometric Systems-study to Improve Accuracy and Performance. International Journal of Computer Science & Engineering survey (IJCSES), 1(2).

[10] Chahal, R: A Comparative Study of Various Biometric Approaches. International Journal of Engineering Applied Sciences and Technology, 2(4), 2017, pp30-35, Available at http://www.ijeast.com.

[11] Sabhanayagam, T., Venkatesan, V. P, and Senthamaraikannan, K. 2018 A Comprehensive Survey on Various Biometric System, International Journal of Applied Engineering Research 13(3), pp 2276-2292. Available on http://www.ripublication.com

[12] Sarin, A. 2014 Iris Biometric System using a Hybrid Approach. Computer Science & Information Technology, pp149-159.

[13] Ammour, B., Boubchir, L., Bouden, T. and Ramdani, M. 2020 Face-Iris Multimodal Biometric Identification System. vailable on: www.mdpi.com/journal/electronic, 9(35).

[14] Chen, J. 2014 Gait Correlation Analysis based on Human Identification. The Scientific World journal.

[15] Rafi, M., Khammari, H., Nahidabanu R.S.D. and Taj, Y. 2013 A Model Based Approach for Gait Recognition System. International Journal of Soft Computing and Engineering (IJSCE), 2(6), pp 223-228.

[16] Satpute, B.S. and Jodhav, B.D. 2015 Automated Iris Recognition System. An overview. International Journal of Computer Application, 115(17), pp 50-54.

[17] Kayani, C.H. 2017 Various Biometric Authentication Techniques: A Review. Journal of Biometrics and Biostatistics, 8(5), pp 1-5.

[18] Rani, M. P. and Arumugan, G. 2010 An Efficient Gait Recognition System for Human Identification using Modified ICA. International Journal of Computer Science & Information Technology (IJCSIT), 2(1), pp 55-67.

[19] Sharma, V. and Vasudeva, N. 2017 Review on Palm Print Recognition Technologies. International Journal of Advanced Research in Computer Science and Software Engineering, 7(3), Available online at www.ijarcsse.com

[20] Abdullah, M., Salim, C. and Ahmed, B. 2012 Multimodal Biometric Person Recognition System based on Iris and Palmprint using Correlation Filter Classifier. ICCIT, pp 782-787.

[21] Sungsoo, Y., Seung-Seok, C., Sung-Hyuk, C., Yillbyung, L. and Charles, C.T. 2005 On the Individuality of the Iris Biometric. ICGST-GVIP Journal, 5(5), pp 63-70.

[22] Mohd, S.W., Gaurav, K.S., Neeraj, B., Akanksha, S. and Pooja, V. 2020 Palm and Fingerprint based Multimodal Biometric Technique. International Journal of Recent Technology and Engineering (IJRTE). ISSN:2277-3874, 8(6), pp 789-792.

[23] Jawed, B., Khalifa, O.O. and Bhuiyan, S.S.N. 2018 Human Gait Recognition System. 7th International Conference on Computer and Communication Engineering (ICCCE), pp 89-92.

[24] Pandey, S. and Sharma, S. 2014 Face Detection and Recognition Techniques. International Journal of Computer Science and Information Technologies, 5(3), pp. 4111-4117.

[25] Vincenzo, C., Militello, C. and Vitabile, S. 2017 Biometric Authentication Overview. A Fingerprint Recognition Sensor Decription. *Int J Biosen Bioelectron.*

[26] Choudjary, J. 2012 Survey of Different Biometric Technology. International Journal of Modern Engineering Research (IJMER). 2(5), pp. 3150-3155, ISSN:2249-6645.

[27] Elfes, J., Vos, P. and Knegt, E. 2021 Five Common Biometric Techniques Compared. Available: https://

www.recgtech.com/en/knowledge-base. Accessed: 16/04/2021.

[28] Naidu, B.R. Reddy, P. 2019 Fusion of Face and Voice for a Multimodal Biometric Recognition System. International Journal of Engineering and Advanced Technology (IJEAT). 8(3), ISSN:2249-8958.

[29] Dutta, C. Singh, R. 2015 Automatic Face Detection using RGB Color Model for Authentication. International Journal of Soft Computing and Engineering (IJSCE). 5(5), ISSN: 2231-2307.

[30] Nakhdoomi, N.A. Gunawan, T.S. Habaebi, M.H. 2013 Human Gait Recognition and Classification using Similarity Index for various conditions. IOP Conference Series: Materials, Science and Engineering. pp 1-6.