An Investigation towards Effectiveness of Present State of Biometric-Based Authentication System

Gavisiddappa[1], Dr. M Shivakumar[2], Dr. Chandrashekar M Patil[3]

[1]*Associate Professor, Dept. of ECE, CIT, Gubbi, Karnataka, India*
[2]*Professor & Head, Dept. of E&IE GSSSIETW, Mysore, Karnataka, India*
[3]*Professor, Dept. of ECE, VVCE, Mysore, Karnataka, India*

***Abstract*— The adoption of biometric-based authentication mechanism has been already initiated a decade back but still in real-life we get to see usage of only unimodal biometrics. Out of all the different forms of biometrics, we see usage of fingerprint as the dominant attribute in contrast to different other attributes e.g. teeth image, palm, facial geometry, retina network, iris, etc. Multimodal biometrics is believed to offered better security compared to unimodal. Although, there are some of the technical advancement in evolving up with new multimodal methodologies, but still commercial usage of such is yet to be seen. Therefore, this manuscripts aims to explore the level of effectiveness in existing approaches of biometric-based authentication system in order to further investigate the unaddressed solution towards this problem. This paper reviews the approaches used for addressing different problems associated with biometrics and discusses about their technical methodologies as well as their limitations.**

***Keywords*- Biometric, Authentication, Security, Unimodal, Multimodal, Fingerprint, Face, Algorithms**

I. INTRODUCTION

Usage of biometric is one of the increasing mechanisms of performing authentication from small to bigger scale of application environment [1]. According to one recent article of Forbes, it was mentioned that 50% of the smartphone application will adopt using fingerprint sensor by the year 2019 [2]. The major forms of biometrics includes biological signals e.g. fingerprint, retina structure, facial image, teeth image, etc, which is very unique and discrete for one person. These unique data is used as a digital identity of any person utilized for their authentication. Inspite of advantages of biometrics in contrast to conventional password, their implementation is no 100% resilient against attacks [3]. Usage of biometrics allows freedom from memorizing or storing any form of password for accessing. One of the potential challenges of using biometric is to ensure security against integrity and safety of biometric data. There are various forms of unaddressed problems associated with robust and effective usage of biometric-based authentication system. The first concern about usage of biometric is variations of biometric signal within a person. It is highly possible that a biometric signal may differ from the signal that is stored in biometric system over a period of time due to many reasons e.g. stress, growing age, sickness, etc. This results in higher degree of false positive alarms where legitimate person could be denied access of their own accounts. The second problem in biometric usage is associated with the type of sensors used for scanning. The sensitivity, calibration, age, embedded interface may vary with the surrounding environment even if the biometric signals are unchanged. Such system causes false positive while performing authentication. The third problem is associated with type of feature extraction algorithms. It is infeasible to perform matching of queried biometric signal with millions of biometric signals stored, hence, features are extracted which minimizes the search and offer faster results. However, different feature extraction algorithms have different performance which cannot be standardized. If the mechanism for comparison scoring differs from matching algorithm then the performance is seriously affected [4]. The fourth problem is associated with the data integrity which means that it is possible for a legitimate user to corrupt/distort the data due to certain security loopholes. Hence, existing system doesn't offer much data integrity towards biometric template security. The fifth problem is associated with the higher degree of instability associated with biometric signals. None of the biometric attributes offer 100% stability either over shorter or over longer period of time causing greater dependency of updating the template. All the above mentioned challenges adversely affect the decision making operation which completely works on probability. This will mean that all the positive matching biometric signals will represent a probability of precise identification while a negative matching biometric signals represents the same probability an not a concrete inference of conclusion. Therefore, there is greater deal of challenges encountered by the usage of biometric-based authentication system.

This paper reviews the existing approaches used by researches for addressing the challenges associated with biometrics emphasizing its usage in authentication system. Section II discusses about the usage of the biometrics in the form of fundamental discussion followed by existing system .Section III with respect to approaches used and limitation. Section IV discusses about the modern techniques used for authentication by combining different forms of biometric signals. Brief discussion of research gap is carried out in Section V followed by proposed study contribution .In Section VI in the form of conclusion. A brief discussion of future work is also carried out in Section VI at the same time.

II. A SNAPSHOT ON BIOMETRICS USAGE

Biometric systems utilize an individual's human body characteristics, such as the face, iris, fingerprints and hand prints which do not normally change over time and

identification involving the enrollment of these traits in a database for future recognition purposes. The evolution of the usage of the biometrics dates back on 1858 where images from hand and finger were used for identification. Table 1 highlights that since 1858, the usage of fingerprint based authentication system has become quite famous; however it was more used for solving classification problems and less into authentication. The next forms of modalities found to be frequently used are facial image and retina image (i.e. iris). These forms of biometrics are found to offer higher degree of security and hence they were used for designing security-based application that demands resilient authentication mechanism.

Table 1 Evolution of Usage of Biometrics [5]

Year	Modalities	Purposes	Description
1858	Hand and Finger image	Identification	First time the image of the palm was recorded
1870	Anthropometries	Identity individuals	Capable of recording the physical measurements.
1892	Finger print	Categorizations	Used for preliminary identification of users
1894	Finger print	Categorizations	Using fingerprint to solve crime-based investigation
1896	Finger print	Categorizations	Using fingerprint to solve crime-based investigation
1903	Finger print	Identification	For the identification of criminals.
1936	Iris	Identification	Iris patterns as a method to recognize an individual.
1960s	Face	Reorganization	It calculated distances and ratios to a common reference point that was compared to the reference data.
1960	Speech	Speaker Reorganization	It is based on the analysis of x-rays of individuals making specified phonic sounds.
1965	Signature	Recognition	Automated Signature Recognition
1969	Finger print	Automatic Recognition	Challenges: Scanning, Comparing and Matching Finger prints in a minute.
1970s	Face	Automatic Face Recognition	Used 21 specific subjective markers such as hair color and lip thickness to automate face recognition.
1970	Speech	Complex Behavior	Used motion x-ray and included tongue and jaw.
1974	Hand Geometry	Recognition	Physical access, time, attendance and personal identification.
1975	Finger print	Recognition and digital storage	Reduce the cost and digital storage
1976	Voice	Speaker recognition	Speaker recognition
1977	Signature	Personal Identification	Used in US air force for authentication
1980s	Speech	Speaker Recognition	Can assists in recognizing voice of speaker
1985	Two Iris	Similarity measurement	Can perform similarity matching between two different form of iris.
1985	Hand Geometry	Identification	Used for authentication in banking system using hand geometry in US.
1986	Finger Print	Exchange of Finger Print Minutiae data.	Considered as an international standard.
1986	Iris	Identification	Can perform involuntary recognition of iris pattern of human
1988	Face-Video images	Recognition System	Carried out exhaustive database search
1988	Face	Recognition System	Offer magnified version of multiple images of facial recognition
1991	Face	Recognition System	Offers supportability of involuntary recognition of facial image.
1993	Face	Face recognition	Assessment of facial validation from simple to complex mode of facial orientation
1994	Iris	Iris Recognition	First iris recognition system.
1994	Finger print	Identification	Involuntary fingerprint identification
1995	Iris	Recognition system	Commercial Product
1996	Hand geometry	Identification	To manage & safeguard user's entry to specific location
1996	Speech	Recognition System	Targets enhancing speech recognition performance
1998	DNA	To digitally store, search and retrieve	Used for performing DNA sequencing for target suspect identification
1999	Finger print	Identification	Storage of digital image, supports exchanging of data
2000	Finger print, iris	Identification	Recognition using vascular patterns
2002	Standardization of biometrics by ISO/IEC		
2003	Establishment of Forum for European Biometrics		
2008	Initiated coordination of biometric database by US government		
2010	Adoption of biometric antiterrorism activity by US National Security		
2013	Inclusion of biometrics in smartphone		

In the last two decades, the concept of biometrics is associated with huge amount of management systems that increases the open challenges between individual security as well as enterprise security. Biometric techniques are growing popular in public security related applications, such as customs control, building entrance control and terrorist identifications [6]. The procedure of identifying a person using security device is named as authentication device. A biometric system is the pattern recognition system that is used for extracting a feature set from the data, and comparing the feature set in the data base.

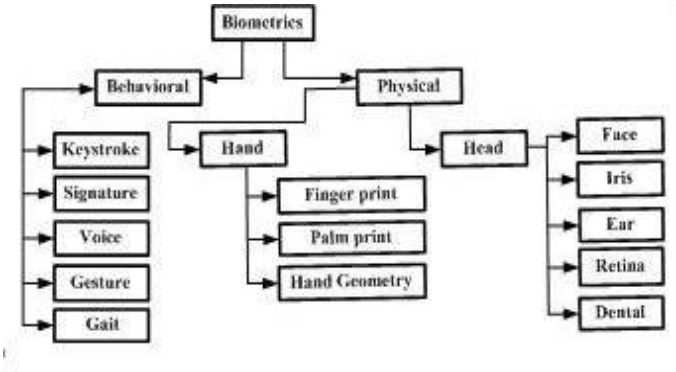

Figure 1 Classification of different Biometrics

Multimodal biometric devices are being progressively more installed in various biometric applications as they overcome limitations of unimodal biometrics. Based on the application scenario, a biometric device may work either in identification mode or a verification mode. Fig.1 shows the classification of different biometrics system. Biometrics is mainly classified into physical and behavioral systems. These are further classified into head, hand, face, iris, fingerprint, hand geometry, palm print, signature, voice etc [7] [8]. The conventional means of using biometric authentication system consists of extracting the feature from the different forms of biometric signals and generate a template. This phase is called as enrollment phase which is followed by template matching phase. In the template matching phase, the queried (or input) of new biometric signal is subjected to feature extraction which is followed by template matching phase called as verification. Fig.2 showcases the process of enrollment and verification in existing system.

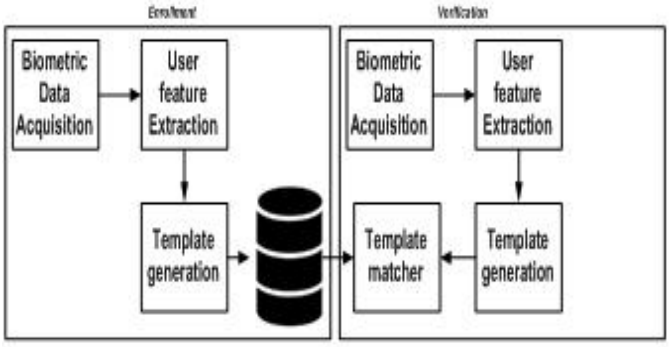

Figure 2 Existing Biometric Authentication

Although biometrics are increasingly used in authentication system in majority of the commercial places, but it suffers from some significant challenges e.g. i) privacy issues, ii) security issues, and iii) irreplaceability issue. The conventional biometric-based authentication system uses central entity in order governs the complete private information of the user. Such central entity is always assumed not to be compromised and that is where it leads to serious privacy issues. The security issues arise when such biometric template has higher level of correlation of user's information with each other. Such information within the template becomes the prime point of attention for the adversaries. Once the biometric template is compromised that collateral attacks begins. The third problem is related to the replication of the biometric details in order to spoof the original one. Table 1(a) showcases the scale of effectiveness of different forms of biometric systems that are used in authentication system till date.

Table 1(a) Existing Factors of biometric system [1]

Factor	**Effectivity Scores of Various Biometric System**									
	Finger Print	**Face**	**Hand Geometry**	**Iris**	**Voice**	**Signature**	**Gait**	**Ear**	**Hand Vein**	**Palm print**
Accuracy	H	L	M	H	M	M	H	H	H	H
Ease of Use	H	M	H	M	H	H	M	M	M	M
Cost	L	M	M	H	H	L	H	H	H	H
Privacy	H	H	M	H	H	H	H	L	L	M
Distinctiveness	H	L	M	H	L	M	M	H	H	H
Universality	M	H	M	H	M	L	M	M	M	M
Performance	H	L	M	H	L	L	L	M	M	H
Collectability	M	H	H	M	M	H	H	M	M	M
Acceptability	M	H	M	L	H	H	H	H	M	M

III. Existing Techniques

This section discusses about the some of the existing techniques implemented during the year 2010-2017 emphasizing on the enhancing the features of biometric system for further trustworthy authentication system. There are various ranges of the studies being presented with different methodology

A study towards usage of biometric for securing the peer-to-peer payment process over the network is introduced most recently by Ghosh et al. [9]. The authors have discussed a prototype model where mobile phone can be used for extracting the finger print information along with account number of device. The transaction of the information uses common GSM network for authentication. However, the technique highly depends on the device ID as well as user ID, which is easier to be faked if the device is stolen. Usage of biometric was also seen to be used in wireless sensor network as seen in the study of Choi et al. [10]. Fuzzy logic was used for strengthening the security features to be used for authentications with an aid of cryptography-based approach. The technique uses a mutual authentication scheme in order to resist guessing & replay attack however the technique doesn't offer enough claims to show its practical usability. Different level of biometric was also found in many studies. The work done by Choi et al. [11] have used electrocardiogram as the biometric attribute used for authentication. Such forms of bio-signals are generated by the sensors residing in wearable devices. The technique uses radial-basis function as well as supervised learning for performing an effective classification used for authentication. Studies towards strengthening biometric-based authentication system was also carried out by Bhuiyan et al. [12] where the retinal-vessel was used as an biometric attribute for performing authentication. The technique extracts the unique vascular network of retinal and performs feature extraction which is further subjected to geometric hashing method. The method finally extracts certain invariant feature, which otherwise is challenging to be extracted by conventional biometrics. The study outcome has proved to offer 96% of precision rate. While working towards biometrics, the user's identity is at a great stake of privacy. Hence, existing literatures have also implemented techniques towards retaining maximum privacy while performing biometric-based authentication.

The work carried out by Sedenka et al. [13] has formulated a model for ensuring highest privacy using Principal Component Analysis (PCA). The technique has enhanced protocol for Garbled circuits and applied Advanced Encryption Standard (AES) for further encryption. Kang et al. [14] have presented a study where the resiliency of existing biometrics can be evaluated. The author uses finger print mainly to perform authentication with an aid of a sophisticated mathematical modeling. Liu et al. [15] have presented a discussion of enhancing the system performance during biometric authentication. The technique presents discussion of linear fusion to achieve robustness. The work carried out by Venugopalan et al. [16] have discussed about usage of heart beats to be used as biometric authentication. The authors have also presented an analysis of such biomedical waveforms using impedance factor. Jiping et al. [17] have presented a cryptographic-based authentication scheme in biometrics. Frank et al. [18] have presented a model called as touch altaics that uses pattern analysis of the touch behaviour of the user on the screen as a biometric trait for performing authentication. Klonovs et al. [19] have presented a discussion of authentication system using Electroencephalogram. On the other hand, biometric template plays a critical role in every biometric based authentication that is required to be safeguarded. Studies in such direction have been carried out by Simoens et al. [20] where multiple complex attacks have been studied. The study carried out by Biggio et al. [21] has analyzed the impact of practical adversary associated with spoofing on authentication system in biometrics. Considering the case of facial and fingerprint expression, the authors have presented an analysis for both single and multimodal based authentication. Urtiga and Moreno [22] have explored another novel mechanism of biometrics using keystrokes that analyzes the typing pattern of user. Sui and Du [23] introduced the concept of biometric capsule where it computes the difference between the reference subjects. The technique extracts significant features of user followed by generation of bio-information to further recollect more unique feature. The complete process generates significant feature called as bio-capsules that are stored and used for next step of verification. Safie et al. [24] have presented a technique where the heartbeat is used for biometric signal. The technique introduces a new form of feature that is extracted from active pulse ratio. Kumar and Zhang [25] have presented a technique where different scores of matching is generated from different templates of the user. The technique uses palm print as well as shape of the hand as biometric signal to carry out authentication. Chatterjee et al. [26] have used signal information from the postures for performing biometric-based authentication along with usage of radial-basis function for further strengthening the authentication system. Tao and Veldhuis [27] have presented facial attribute as biometric for authenticating in mobile device. Upmanyu et al. [28] have presented a technique called as blind authentication system that is meant for safeguarding the biometric template. The technique is designed using public key cryptography for offering flexible encryption to the biometric template.

Hence, it can be seen that there are various studies targeting at enhancing the performance of the biometric-based authentication system. The existing studies are much inclined towards evolving up with a new techniques and methodologies to strengthening the biometric-based attributes thereby assisting resiliency against multiple forms of adversaries. Table 2 outlines the existing research contribution.

Table.2 Scaling Effectiveness of Existing techniques of Biometric-based Authentication (B: Biometric, M: Methodology)

Authors	Problem	Technique	Advantage	Limitation
Ghosh [9]	Secure biometrics	B: Fingerprint, Device ID M: Experimental	Easier peer-to-peer transfer	Possibility of device ID to be compromised is not considered
Choi [10].	Securing biometric authentication	B: hypothetical biometric imprints M: Analytical, mutual key exchange	Resist multiple form of attack	Few extensive analyses to prove/benchmark the outcome.
Choi [11]	Adoption of physiological sensor	B: Hear-beat M: Experimental, Support vector Machine, radial basis function	Higher authentication performance	Induces delay due to learning mechanism involved.
Bhuiyan [12]	Biometric authentication	B: Retinal vessel M: analytical, feature extraction using geometric hashing	Higher recall and precision	Success rate depends on threshold value between 20-30.
Sedenka [13]	Privacy preservation	B: hypothetical biometric imprints M: Analytical, PCA, AES	Light-weight protocol	No extensive analyses to prove/benchmark the outcome.
Kang [14]	Resiliency of biometrics	B: fingerprint/ DNA M: Mathematical	Mathematically sound algorithm	No extensive analyses to prove/benchmark the outcome.
Liu [15]	Enhancing performance	B: hypothetical biometric imprints M: Empirical, linear fusion	Highest authentication accuracy	Vagueness in biometric specification, not benchmarked
Venugopalan [16]	Biometric authentication	B: heart bear M: Conceptual, classification	Supports critical authentications	Induces computational complexity.
Jiping [17]	Enhancing performance	B: hypothetical biometric imprints M: Empirical, cryptography, enhancing Das scheme [29]	Supports resisting higher range of attacks	Doesn't discusses the complexity associated with key management
Frank [18]	Biometric authentication	B: Fingerprint M: Analyzing touching behaviour	Performs continuous monitoring	Accumulation and processing of too much feature induces delay for long run. Accuracy cannot be ensured for multiple application usage pattern
Klonovs [19]	Biometric authentication	B: Brain signals M: Experimental, feature-based authentication	A novel mechanism	Not applicable in practical as accessibility depends upon stress signal, which can happen to both regular user & malicious user.
Simoens [20]	Securing biometric template	B: hypothetical biometric imprints M: Conceptual, generic adversary modeling	One framework supporting multiple adversary mitigation	No numerical evidence to support the claim.
Biggio [21]	Impact of spoofing attack	B: Facial, Fingerprint M: Conceptual	Finding suggest higher vulnerability of multimodal compared to single modal, better identification of adversary	No benchmarking
Urtiga [22]	Biometric authentication	B: Keystroke patterns M: conceptual	Performs continuous monitoring	Accumulation and processing of too much feature induces delay for long run. Accuracy cannot be ensured for multiple application usage pattern
Sui and Du [23]	Biometric authentication	B: Iris M: Empirical, feature extraction, experimental	Support multiple level of security	Accuracy depends on static images only
Safie [24]	Biometric authentication	B: Heart beat M: Empirical, feature extraction	Higher accuracy	No extensive analyses to prove/benchmark the outcome.

Kumar [25]	Biometric authentication	B: Palm Print M: Experimental, template matching	Supports two biometric modalities	No benchmark the outcome.
Chatterjee et al. [26]	Biometric authentication	B: posture information M: Experimental, radial-basis function	Offers higher accuracy	No standardization or thresholding for posture that can be mimicked easily.
Veldhuis [27]	Biometric authentication	B: Face M: Experimental,	Offers higher accuracy	Success rate more for dataset and less for real-time facial image.
Upmanyu [28]	Biometric template security	B: hypothetical biometric imprints M: empirical, Blind authentication, public key encryption	Supports security over multiple datasets	Communication overhead increases for more rounds of query.

Apart from the above mentioned techniques, we also reviewed other existing literatures as shown in Table 3 for exploring different form of techniques and adopted modalities pertaining to biometric based authentication. There are various approaches that combinely uses different biometric to perform authentication. From Fig. 3, it can be seen that many authors have carried out the work on unimodal as well as multimodal biometric system for strengthening authentication system. These techniques were claimed to offer better security as well as the better recognition rate of the system. However, it is still an open end question to understand the best effectiveness in the existing approaches.

TABLE 3 REVIEW OF MULTIMODAL BIOMETRIC SYSTEM.

Author	**Problem**	**Technique**	**Modalities**
Soltanpour [30]	To Improve face recognition and security.	Local descriptors	2D-3D Face image
Oloyede [31]	To improve the security	Stage in biometric system, architecture, operation.	Uni and Multimodal
Haghighat [32]	Reduce computational complexity.	DCA, feature level fusion.	Uni and Multimodal
Wan [33]	To improve biometric recognition rate.	DOA estimation, OMP, ADMM.	PD Source diagnosis.
Martiri [34]	To person authentication.	Honey template and Bloom filters.	Face image.
Sadhya [35]	To secure database.	Review paper	Multimodal image
Bahrampour [36]	Image classification	Multimodal task-driven dictionary learning algorithm.	Multimodal image
Ding. [37]	Image classification	Comprehensive deep learning, NNs, SAE.	Face
Almaadeed [38]	Authentication, To identify speaker.	Neural network, wavelet transforms., MFCCs.	Voice
Yang [39]	To improve Recognition accuracy and security level.	Mutual dependency	Fingerprint and face.
DeCann[40]	Re-identification	Mathematical Modelling errors in Biometric.	Face and Finger print
Moutafis [41]	To improve recognition rate.	Rank based score normalization	Face.
Meng [42]	To protect user privet information	Biometric identification on Mobile phones	Physiological and behavioral characteristics.
Paul [43]	To improve quality, dimensionality reduction and classifier.	Fisher Linear Discriminant Analysis	Face, ear, signature
Zhang [44]	Dimensionality reduction	Semi supervised Learning Techniques.	Face, finger print
Baig [45]	To improve speed and reduce memory constraints.	Cascaded classifiers, Mahalanbis distance algorithm.	Multimodal biometrics.
Murakami [46]	To improve Wolves and lambs accuracy rate.	Optimal fusion algorithm.	Face, Finger Print.
Shekhar[47]	To improve recognition rate.	Multimodal sparse method and fusion based methods.	Signature, Face.

Simon [48]	To improve recognition rate,	Deep learning convolution neural networks.	Face, Signature.
Roy [49]	identification accuracy	Fuzzy C-means clustering	iris, face
Canuto [50]	To overcome privacy concerns in management.	Feature selection method.	finger print, signature
Kumar [51]	To improve Security	BCH encoding and Hash function.	Unimodal and Multimodal
Neverova [52]	To Identity From Motion Patterns.	Deep learning NN	natural human kinematics
Poignant [53]	To identify unsupervised speakers, to reduce cost.	Speaker diarization module.	Speech, written names.
Mezai [54]	To improve voice and face classification.	PSO algorithm	Face, Voice

From the above studies, it has been seen that facial image and the fingerprint are the most common form of the biometric attributes that has been considered for performing authentication mechanism. Although, there are other attributes e.g. iris, signature, speech, signature, etc are also attempted for evolving up various authentication strategies, they were less in numbers. It is believed that multimodal biometric is the next generation method to strength the authentication potential of unimodal biometrics and is likely to be adopted in faster pace in near future.

IV. Modern Techniques of Multi-Modal Authentication

Usage of multimodal biometric is considered as one of the potential method to ensure highly secured authentication mechanism of biometrics with lesser chances of getting compromised. The prime reason behind this is the usage of more number of sophisticated biometric signals that are used for performing encryption. We reviewed the trend of usage patterns of using multiple forms of biometric signals where the most frequently used signals are face, iris, ear image, fingerprint, and signature.

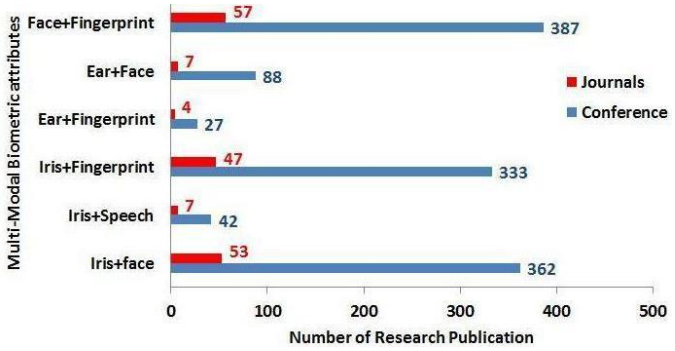

Figure 3 Research Trend of Multimodal Biometrics

Fig.3 highlights the existing research trend where it can be seen that usage of iris and face as well as usage of face and fingerprint are most practiced methods in multimodal biometric authentication. In this section, we give a brief of usage methodology of some of the frequently exercised multimodal biometrical authentication techniques as follows:

- *Iris and Face*: The internal structure of iris as well as facial geometry is the easily available biometrical attribute used for multimodal authentication. Usage of such techniques has been witnessed in the work carried out by Roy et al. [55], Ramachandran et al. [56], Galbally et al. [57], and Tan et al. [58]. Fig.4 shows the common methodology found in the techniques are extraction of features from iris as well as face in order to check their similarity score. The advantage of technique is that iris structure is hard to be replicated or compromised and the disadvantage is the facial geometry features will be required to be consistently updated with the ages of changes of facial structure. Hence, these cannot be used for long run application and calls for constant update.
- *Ear Image and Face*: The combination of ear image and facial structure offers a significant biometric attribute owing to static structure of ear for any human over a longer and longer period of time. The work carried out by Javadtalab et al. [59] is the only standard work that was published during 2010 till date. Such techniques uses feature extraction from both biometric image followed by feature fusion and discriminates analysis (Fig.5). The advantage of this technique is that biometric template pertaining to ear of a specific subject doesn't require any updates in its template; however, it still suffers from frequent updates of facial expression.
- *Face, Fingerprint, and Voice*: Apart from face and voice, duplication of fingerprint is highly challenging and hence this form of multimodal proves to offer secured authentication mechanism. The work carried out by Jain et al. [60] has used such technique. Fig.6 shows the methodology of such technique where a template database is constructed for all three biometric attribute followed by decision-based fusion process to result in acceptance or rejection of query of authentication. The advantage of such techniques is its unique features that are very difficult to be replicated at same time and its disadvantage is a slight variation in pitch of voice can fail the authentication system even for legitimate user.
- *Face, Ear image, and Signature*: Usage of face, ear image, and signature is considered as one of the simplistic form of biometric authentication owing to its charecteristics of non-updation requirement in regular interval. Fig.7 highlights the technique where features of all the attributes are considered for similarity check. Such work was carried out by

Monwar et al. [61] who have perform construction analysis in social network using decision fusion. None of the three attributes is expected to be changed over longer period of time which poses a beneficial factor while the demerit point is the possibility of forged signature. Using three different photographs of face, ear, and signature, even a malicious user can have access to accounts. Hence, this process is not safer.

- *Face, Teeth Image, and Voice*: Usage of facial image, teeth image, and voice is another innovative technique evolved up in recent times. The logic behind such approach is to extract features using different techniques on different biometric attributes followed by score fusion techniques. The work carried out by Kim et al. [62] is one such example shown in Fig.8. The advantage of this technique is its simpler usage and its disadvantage is related to its sensitivity associated with the pitch of the voice.
- *Fingerprint, Iris, and Face*: This is one of the most frequently used practices in multimodal biometric-based authentication system. The work done by Ravi et al.[63] and, Ko [64] has used similar approach. The advantage of this mechanism is its speedy and precise authentication mechanism and the disadvantage of this mechanism is its consistent update of the biometric dataset as it cannot identify forged fingerprints and facial structure. A malicious user can carry a photograph of a person and rubber print of fingerprint to have an easy access to legitimate person resource.

All the above mentioned techniques are quite a new beginning of research attempts towards using multimodal biometric-based authentication system. It is still in nascent stage of development.

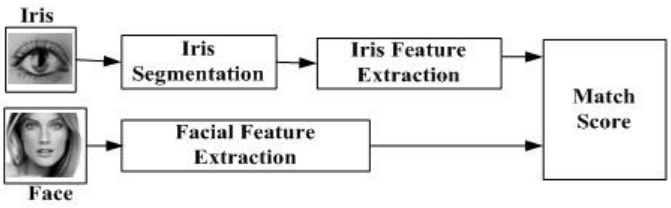

Figure 4 Usage of Iris & Facial Feature [55,56,57,58]

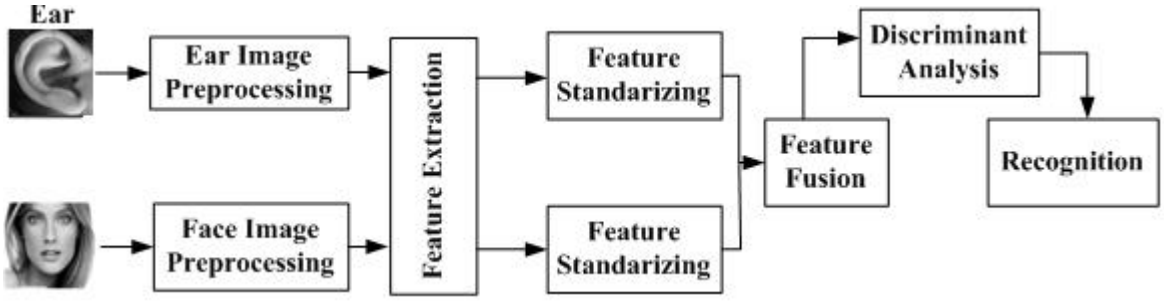

Figure 5 Usage of ear Image & Facial Feature [59]

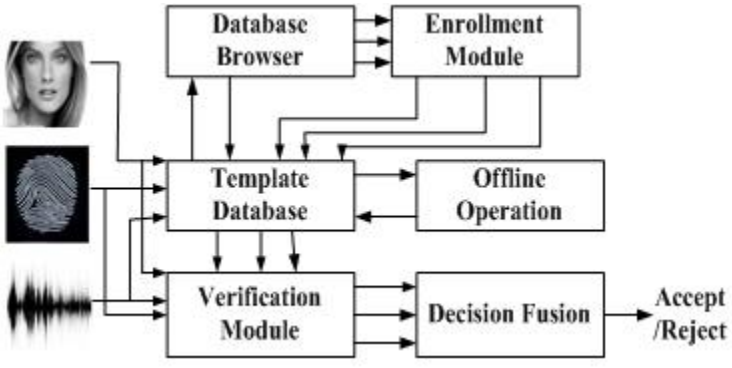

Figure 6 Usage of Face, Fingerprint, and Voice [60]

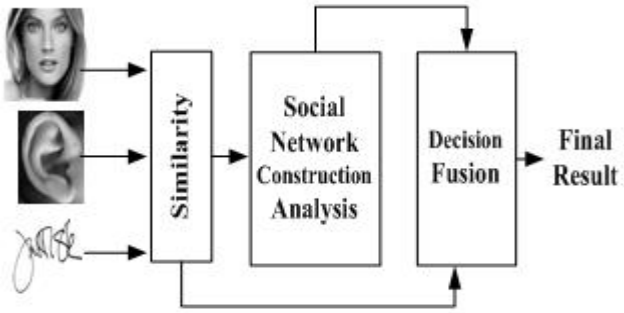

Figure 7 Usage of Face, ear image, and Signature [61]

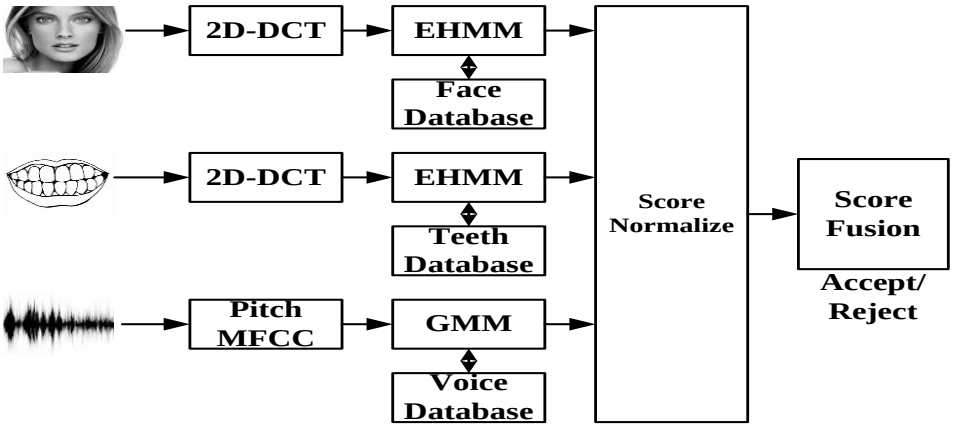

Figure 8 Usage of Face, teeth image, and voice [62]

Existing implementation of the all the above mentioned methodologies towards multimodal biometric-based authentication have been performed in standard datasets e.g. FERET dataset [65], CASIA image dataset [66], CVRL dataset [67], Biometric Recognition Group [68], Poly U Palm print database, etc. These datasets have images pertaining to face, fingerprint, palm, signature, iris, gait, etc. Out of all the technique used in multi-modal forms, fingerprint is definitely one of the dominant attribute being used in experiments. There have been highest number studies towards the direction of using fingerprints alone owing to the potential advantages associated with it. Therefore, it can be said that fingerprint is one of the essential biometric frequently considered in many existing techniques of multimodal authentication system. Combining fingerprint with other biometrics offered highest level of security and faster authentication at same time.

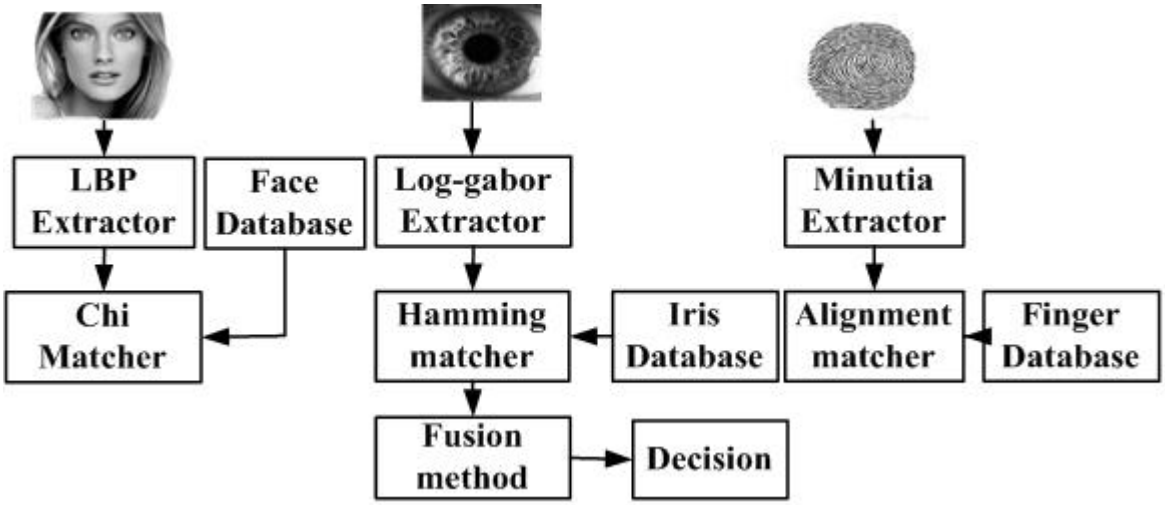

Figure 9 Usage of Face, iris, and Fingerprint [63, 64]

V. Open Research Challenges

Till prior section, various research-based techniques have been discussed to show that there has been evolution of different techniques and algorithm towards strengthening the biometric-based authentication. This section discusses about the open research challenges that were identified not to be addressed by any existing system. Some of the existing challenges that are unaddressed are as following:

- *More Studies Towards Unimodal and Less Towards Multimodal*: Majority of the existing techniques of biometrics have used single biometric attributes for performing authentication. Although, some researchers have also explored better feasibility of using multi-modal approaches, but there are less amount of research work in proportion for this. The security complications used in unimodal is very different than considered for multimodal that is also found missing to be addressed in existing approaches of multi-modal authentication.
- *Lesser focus on Computational Complexity*: Some of the biometrics consumes enough data for both storing and performing authentication. Hence, there is always a complexity associated with processing algorithm in order to perform similarity match. Although, many system uses feature extracted for performing similarity check, but the amount of feature (especially in multi-modal authentication) is quite higher as compared to unimodal authentication system. However, almost none of the existing approaches have ever considered computational complexity into consideration while assessing the effectiveness of the research outcomes.
- *Less Emphasis to Iris*: The potential usage of iris as well as the internal networks of veins inside retina is the best non-duplicable biometric attribute. However, the adoption of iris is found in less proportion in contrast to fingerprint, teeth image, ear image, voice, etc. Moreover, usage of iris image has been always considered from dataset and less work towards real-time iris has been reported till date.
- *More usage of Iterative Methods*: Existing approaches are mainly found to follow highly iterative mechanism for performing algorithm implementation. Usage of iterative has good effect on accuracy but adverse effect on system performance e.g. response time, energy consumption, resource dependencies, memory. Hence, iterative methods are not much found to be enhanced in order to solve such system performance problems in any of the existing literatures.

VI. Conclusion

The proposed paper mainly aims to study the effectiveness of the existing approaches towards enhancing the biometric-based authentication system. The study contributions of the presented paper are as follows: i) Existing review-based studies toward effectiveness of existing biometric-based authentication mechanism is very less to find. Available review works towards biometric doesn't discuss about limitations and was not found to emphasize on multimodal approaches. Therefore, the first contribution of proposed study is that this paper offers a wide visualization of the study effectiveness of complete biometric based authentication system be it unimodal or multimodal system. ii) The second study contribution is the essential findings of proposed investigation e.g. open issues in biometric design principle, usage of symptomatic approaches, multimodal approaches still being underrated, less extent of studies towards multimodal as compared to unimodal based authentication, etc. Therefore, our future work will be to address some of the significant issues. We will initiate our investigations towards developing a novel framework that offers highly resilient authentication using iris as there has been no significant enhancement in adopting iris in existing system. An attempt will be to evolve with a novel combinatorial-based optimization approach where the data integrity will be emphasized along with biometric template security.

References

[1]. Virginio Cantoni, Dimo Dimov, Massimo Tistarelli, "Biometric Authentication: First International Workshop, BIOMET 2014, Sofia, Bulgaria, June 23-24, 2014. Revised Selected Papers", Springer, pp. 265, 2014

[2]. Forbes Technology Council, "The Promise And Challenges Of Biometrics", Forbes Community Voice, 2016

[3]. Aumi, Md Tanvir Islam, and Sven Kratz. "AirAuth: towards attack-resilient biometric authentication using in-air gestures." In Proceedings of the extended abstracts of the 32nd annual ACM conference on Human factors in computing systems, pp. 1585-1590. ACM, 2014.

[4]. Pflug, Anika, and Christoph Busch. "Ear biometrics: a survey of detection, feature extraction and recognition methods." IET biometrics 1, no. 2 (2012): 114-129.

[5]. Arun A. Ross, Karthik Nandakumar and Anil K. Jain, "Handbook of Multibiometrics (international Series On Biometrics)", Springer science and Business Media, YES edition, 2011.

[6]. B. Arslan, E. Yorulmaz, B. Akca and S. Sagiroglu, "Security Perspective of Biometric Recognition and Machine Learning Techniques," *2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Anaheim, CA, 2016, pp. 492-497.

[7]. Pandey, Shubham, Ruchi Varshney, Shivani Gupta, Neha Chaudhary, and Sangeeta Singh. "Study of a Secure Communication System." Imperial Journal of Interdisciplinary Research 2, no. 11 (2016).

[8]. Mellado, Daniel, ed. IT Security Governance Innovations: Theory and Research: Theory and Research. IGI Global, 2012.

[9]. S. Ghosh, A. Majumder, J. Goswami, A. Kumar, S. P. Mohanty and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs: A Digital Card Module using NFC and Biometric Authentication for Peer-to-Peer Payment," in *IEEE Consumer Electronics Magazine*, vol. 6, no. 1, pp. 82-93, Jan. 2017.

[10]. Y. Choi, Y. Lee, and D. Won, "Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction", International Journal of Distributed Sensor Networks, 2016

[11]. H. S. Choi, B. Lee and S. Yoon, "Biometric Authentication Using Noisy Electrocardiograms Acquired by Mobile Sensors," in *IEEE Access*, vol. 4, no. , pp. 1266-1273, 2016.

[12]. Bhuiyan, A. Hussain, A. Mian, T. Y. Wong, K. Ramamohanarao and Y. Kanagasingam, "Biometric authentication system using retinal vessel pattern and geometric hashing," in *IET Biometrics*, vol. 6, no. 2, pp. 79-88, 3 2017.

[13]. J. Šeděnka, S. Govindarajan, P. Gasti and K. S. Balagani, "Secure Outsourced Biometric Authentication With Performance Evaluation on Smartphones," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 384-396, Feb. 2015.

[14]. W. Kang, D. Cao and N. Liu, "Deception With Side Information in Biometric Authentication Systems," in *IEEE Transactions on Information Theory*, vol. 61, no. 3, pp. 1344-1350, March 2015.

[15]. Y. Liu, Z. Yang, C. Y. Suen and L. Yang, "A Study on Performance Improvement Due to Linear Fusion in Biometric Authentication Tasks," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 9, pp. 1252-1264, Sept. 2016.

[16]. S. Venugopalan, M. Savvides, M. O. Griofa and K. Cohen, "Analysis of Low-Dimensional Radio-Frequency Impedance-Based Cardio-Synchronous Waveforms for Biometric Authentication," in *IEEE Transactions on Biomedical Engineering*, vol. 61, no. 8, pp. 2324-2335, Aug. 2014.

[17]. L. Jiping, D. Yaoming, X. Zenggang, and L. Shouyin, "An improved biometric-based user authentication scheme for C/S system", International Journal of Distributed Sensor Networks, 2014

[18]. M. Frank, R. Biedert, E. Ma, I. Martinovic and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 136-148, Jan. 2013.

[19]. J. Klonovs, C. K. Petersen, H. Olesen and A. Hammershoj, "ID Proof on the Go: Development of a Mobile EEG-Based Biometric Authentication System," in *IEEE Vehicular Technology Magazine*, vol. 8, no. 1, pp. 81-89, March 2013.

[20]. K. Simoens, J. Bringer, H. Chabanne and S. Seys, "A Framework for Analyzing Template Security and Privacy in Biometric Authentication Systems," in *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 833-841, April 2012.

[21]. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis and F. Roli, "Security evaluation of biometric authentication systems under real spoofing attacks," in *IET Biometrics*, vol. 1, no. 1, pp. 11-24, March 2012.

[22]. E. V. Cunha Urtiga and E. D. Moreno, "Keystroke-based biometric authentication in mobile devices," in *IEEE Latin America Transactions*, vol. 9, no. 3, pp. 368-375, June 2011.

[23]. Y. Sui, X. Zou and E. Y. Du, "Biometrics-Based Authentication: A New Approach," *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, Maui, HI, 2011, pp. 1-6.

[24]. S. I. Safie, J. J. Soraghan and L. Petropoulakis, "Electrocardiogram (ECG) Biometric Authentication Using Pulse Active Ratio (PAR)," in *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 4, pp. 1315-1322, Dec. 2011.

[25]. Kumar and D. Zhang, "Improving Biometric Authentication Performance From the User Quality," in *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 3, pp. 730-735, March 2010.

[26]. Chatterjee, R. Fournier, A. Nait-Ali and P. Siarry, "A Postural Information-Based Biometric Authentication System Employing S-Transform, Radial Basis Function Network, and Extended Kalman Filtering," in *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 12, pp. 3131-3138, Dec. 2010.

[27]. Q. Tao and R. Veldhuis, "Biometric Authentication System on Mobile Personal Devices," in *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 4, pp. 763-773, April 2010.

[28]. M. Upmanyu, A. M. Namboodiri, K. Srinathan and C. V. Jawahar, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol," in *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 255-268, June 2010.

[29]. Ross and A. Abaza, "Human Ear Recognition," in Computer, vol. 44, no. 11, pp. 79-81, Nov. 2011.

[30]. S. Soltanpour and Q. J. Wu, "Multimodal 2D–3D face recognition using local descriptors: pyramidal shape map and structural context," in IET Biometrics, vol. 6, no. 1, pp. 27-35, 1 2017.

[31]. M. O. Oloyede and G. P. Hancke, "Unimodal and Multimodal Biometric Sensing Systems: A Review," in IEEE Access, vol. 4, no. , pp. 7532-7555, 2016

[32]. M. Haghighat, M. Abdel-Mottaleb and W. Alhalabi, "Discriminant Correlation Analysis: Real-Time Feature Level Fusion for Multimodal Biometric Recognition," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1984-1996, Sept. 2016.

[33]. L. Wan, G. Han, L. Shu, S. Chan and N. Feng, "PD Source Diagnosis and Localization in Industrial High-Voltage Insulation System via Multimodal Joint Sparse Representation," in IEEE Transactions on Industrial Electronics, vol. 63, no. 4, pp. 2506-2516, April 2016.

[34]. E. Martiri, M. Gomez-Barrero, B. Yang and C. Busch, "Biometric template protection based on Bloom filters and honey templates," in IET Biometrics, vol. 6, no. 1, pp. 19-26, 1 2017.

[35]. Sadhya, S. K. Singh and B. Chakraborty, "Review of key-binding-based biometric data protection schemes," in IET Biometrics, vol. 5, no. 4, pp. 263-275, 12 2016.

[36]. S. Bahrampour, N. M. Nasrabadi, A. Ray and W. K. Jenkins, "Multimodal Task-Driven Dictionary Learning for Image Classification," in IEEE Transactions on Image Processing, vol. 25, no. 1, pp. 24-38, Jan. 2016.

[37]. Ding and D. Tao, "Robust Face Recognition via Multimodal Deep Face Representation," in IEEE Transactions on Multimedia, vol. 17, no. 11, pp. 2049-2058, Nov. 2015.

[38]. N. Almaadeed, A. Aggoun and A. Amira, "Speaker identification using multimodal neural networks and wavelet analysis," in IET Biometrics, vol. 4, no. 1, pp. 18-28, 3 2015.

[39]. W. Yang, J. Hu, S. Wang and C. Chen, "Mutual dependency of features in multimodal biometric systems," in Electronics Letters, vol. 51, no. 3, pp. 234-235, 2 5 2015.

[40]. DeCann and A. Ross, "Modelling errors in a biometric re-identification system," in IET Biometrics, vol. 4, no. 4, pp. 209-219, 12 2015.

[41]. P. Moutafis and I. A. Kakadiaris, "Can We Do Better in Unimodal Biometric Systems? A Rank-Based Score Normalization Framework," in IEEE Transactions on Cybernetics, vol. 45, no. 12, pp. 2654-2667, Dec. 2015.

[42]. W. Meng, D. S. Wong, S. Furnell and J. Zhou, "Surveying the Development of Biometric User Authentication on Mobile Phones," in IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1268-1293, thirdquarter 2015.

[43]. P. P. Paul, M. L. Gavrilova and R. Alhajj, "Decision Fusion for Multimodal Biometrics Using Social Network Analysis," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 11, pp. 1522-1533, Nov. 2014.

[44]. Q. Zhang, Y. Yin, D. C. Zhan and J. Peng, "A Novel Serial Multimodal Biometrics Framework Based on Semisupervised Learning Techniques," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1681-1694, Oct. 2014.

[45]. Baig, A. Bouridane, F. Kurugollu and B. Albesher, "Cascaded multimodal biometric recognition framework," in IET Biometrics, vol. 3, no. 1, pp. 16-28, March 2014.

[46]. T. Murakami, K. Takahashi and K. Matsuura, "Toward Optimal Fusion Algorithms With Security Against Wolves and Lambs in Biometrics," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 2, pp. 259-271, Feb. 2014.

[47]. S. Shekhar, V. M. Patel, N. M. Nasrabadi and R. Chellappa, "Joint Sparse Representation for Robust Multimodal Biometrics

Recognition," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 36, no. 1, pp. 113-126, Jan. 2014.

[48]. M. O. Simón et al., "Improved RGB-D-T based face recognition," in IET Biometrics, vol. 5, no. 4, pp. 297-303, 12 2016.

[49]. K. Roy, J. Shelton, B. O'Connor and M. S. Kamel, "Multibiometric system using fuzzy level set, and genetic and evolutionary feature extraction," in IET Biometrics, vol. 4, no. 3, pp. 151-161, 9 2015.

[50]. M. de Paula Canuto, M. C. Fairhurst and F. Pintro, "Ensemble systems and cancellable transformations for multibiometric-based identification," in IET Biometrics, vol. 3, no. 1, pp. 29-40, March 2014.

[51]. Kumar and A. Kumar, "A Cell-Array-Based Multibiometric Cryptosystem," in IEEE Access, vol. 4, no. , pp. 15-25, 2016.

[52]. N. Neverova et al., "Learning Human Identity From Motion Patterns," in IEEE Access, vol. 4, no. , pp. 1810-1820, 2016.

[53]. J. Poignant, L. Besacier and G. Quénot, "Unsupervised Speaker Identification in TV Broadcast Based on Written Names," in IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 23, no. 1, pp. 57-68, Jan. 2015.

[54]. L. Mezai and F. Hachouf, "Score-Level Fusion of Face and Voice Using Particle Swarm Optimization and Belief Functions," in IEEE Transactions on Human-Machine Systems, vol. 45, no. 6, pp. 761-772, Dec. 2015.

[55]. K. Roy, J. Shelton, B. O'Connor and M. S. Kamel, "Multibiometric system using fuzzy level set, and genetic and evolutionary feature extraction," in IET Biometrics, vol. 4, no. 3, pp. 151-161, 9 2015.

[56]. R. P. Ramachandran et al., "Vertical Integration of Biometrics Across the Curriculum: Case Study of Speaker, Face and Iris Recognition," in IEEE Circuits and Systems Magazine, vol. 14, no. 3, pp. 55-69, thirdquarter 2014.

[57]. J. Galbally, S. Marcel and J. Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition," in IEEE Transactions on Image Processing, vol. 23, no. 2, pp. 710-724, Feb. 2014.

[58]. W. Tan and A. Kumar, "Efficient and Accurate At-a-Distance Iris Recognition Using Geometric Key-Based Iris Encoding," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 9, pp. 1518-1526, Sept. 2014.

[59]. S. Tiwari, S. Jain, S. S. Chandel, S. Kumar and S. Kumar, "Comparison of adult and newborn ear images for biometric recognition," *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Waknaghat, India, 2016, pp. 421-426.

[60]. K. Jain, "Biometrics: Proving Ground for Image and Pattern Recognition," *Fourth International Conference on Image and Graphics (ICIG 2007)*, Sichuan, 2007, pp. 3-3.

[61]. M. M. Monwar and M. L. Gavrilova, "Multimodal Biometric System Using Rank-Level Fusion Approach," in IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 39, no. 4, pp. 867-878, Aug. 2009.

[62]. J. Kim, K. W. Chung and K. S. Hong, "Person authentication using face, teeth and voice modalities for mobile device security," in *IEEE Transactions on Consumer Electronics*, vol. 56, no. 4, pp. 2678-2685, November 2010.

[63]. S. Ravi and D. P. Mankame, "Multimodal biometric approach using fingerprint, face and enhanced iris features recognition," *2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, Nagercoil, 2013, pp. 1143-1150.

[64]. Ko, Teddy. "Multimodal biometric identification for large user population using fingerprint, face and iris recognition." In Applied Imagery and Pattern Recognition Workshop, 2005. Proceedings. 34th, pp. 6-pp. IEEE, 2005.

[65]. Phillips PJ, Moon H, Rizvi SA, Rauss PJ. The FERET evaluation methodology for face-recognition algorithms. IEEE Transactions on pattern analysis and machine intelligence. 2000 Oct;22(10):1090-104.

[66]. Proenca, H., Filipe, S., Santos, R., Oliveira, J. and Alexandre, L.A., 2010. The ubiris. v2: A database of visible wavelength iris images captured on-the-move and at-a-distance. IEEE Transactions on Pattern Analysis and Machine Intelligence, 32(8), p.1529.

[67]. G. Santos, P. T. Fiadeiro and H. Proença, "BioHDD: a dataset for studying biometric identification on heavily degraded data," in *IET Biometrics*, vol. 4, no. 1, pp. 1-9, 3 2015.

[68]. Phillips, P. Jonathon, Patrick J. Flynn, and Kevin W. Bowyer. "Lessons from collecting a million biometric samples." Image and Vision Computing 58 (2017): 96-107.