JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Review of Multimodal and Monomodal Biometric Methods for Individual Identification, Biometric Applications in Security

Brajula W, Dr. Menaka D

Research Scholar, Department of ECE, Associate Professor, Department of EIE

Noorul Islam Centre for Higher Education, Kumaracoil

Abstract

Purpose - multi-model biometrics has performed an important role in recognizing individual for multi-purpose. This research study looking forward to provide a review of various type of bio-metric. This literature review has been takes place to have a great awareness about the literature in egal view to understand the future scopes of research.

Methodology/ Design/ Approach - This research study shows a complete systematic review of theoretical, and qualitative research studies published in existing popular journals and identified research articles that are falls under established search inclusion norm.

Findings – The review of literature point-down numerous norms that connected with multi-model biometric. The review of the research study showed that there is a bigger focus of researches has been done in biometric especially figure prints, face shape and so on. Although multi-model biometric is a one of the most trending emerging topics across the globe in scientific literature, still now there is a deficit of research in developed and developing nation in the globe. Further extension, this finding suggests that literature review is made over the multi-model, fusion and non-fusion techniques along with security system by using of bio-metric. Figure print, eye, face shape has been repeatedly discussed biometric research while other forms of biometric such as lip print, food print, ECG, and so on, have given less attention.

Originality/value - This paper will give a contribution to multi-model biometric and it will be a systematic knowledge base for researchers.

Keywords - Biometrics, multi-modal, fusion techniques, security systems, literature review, fingerprints, facial recognition, research, ECG, biometric modalities.

Article type - Review paper

1.Introduction

Biometric authentication is a conspicuous trend in the modern scientific world and it is a scientific technique that a machine uses to optimize, analysis, and identity of an individual looking to resources of that system [1]. The zone of multi-modal biometrics itself seems interesting and enthusiastic, because it is in some scenario at the frontier of biometrics, and presents tedious design problems and some of important characteristics of biometric are Collectability, Permanence, Accuracy, Universality, Performance, and Uniqueness. Biometrical identification inclusion of palm prints, face, iris, and so on are while behavioral biometrical identifications are keystroke, signature, gait, and so on. Scientific research has verified that mono-modal biometrical templet (single biometric) has tedious avoiding spoof attacks by the bluffer which results in bad performance [3]. Visual clarity of the face image, fingerprint, and iris are applicable in the multimodal biometric device will positively impact the total rate of identification of accuracy and the ought to employe for the secondary man involvement to valuate (Teddy Ko Raytheon in 2005) [2] and the individual bio- prints in the database are analyzed and stored and this database are used to verify the unique identity of an individual by analyzing and comparing the already existing data which has been already stored bio-prints.

The working performance of the authentication mechanism has been enhanced by various modern technologies such as use of valley points and ridges, and heat waves to elicit patters [4] and using numerous distance actions such as Manhattan, city block, Euclidean, and so on [5]. Our main focal point on authentication of multimodal biometric device because it provides an important service in terms of performance and security with an extension of offering ease for the applicator. This review paper explained the present trends in scientific research in multimodal device and determine the degree of positive and negative of this form of authentication device.

2. Major contributions

In this part, we are going to review various article focuses on multimodal biometric method along with various mono-modal that use to identify individual biometric feature and biometric contribution in security and its fusion techniques to enhance performance of biometric of an individual. Figure 1 exhibits the different types of biometric authentications.

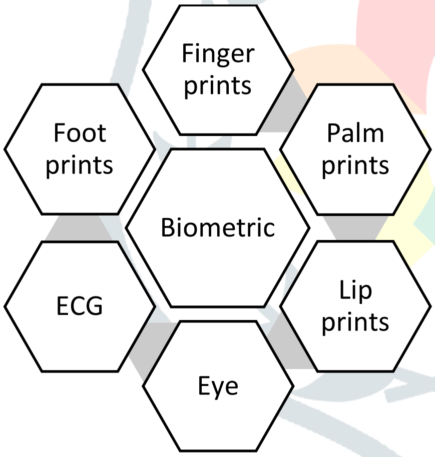


Figure 1: Different biometric authentications

The unique Biometric payment device is applicable for numerous varieties of payment system instead of worry to carrying cad with them and to mug up their tedious passcode, a router and transmission media compulsory contains individuals fingerprint templets to clear up the transaction through an automated clearinghouse [6]. Hourieh Fakourfar and Serge Belongie [7] formulate a method to assess that the performance of minutiae-based FR device degraded by water-induced in the finger and Mihai Hulea *et al* [8] stressed that bring together of FR and universal Positioning System method for both verification and FP identification.

a. Security

The necessity of financial sector is to deliver the good quality of service with the standard of high security of money transaction over the supplies of goods, as well as in the computer internet, and all so offering solutions for Internet based e-commerce such as Flipkart, Amazon and so on [9]. Biometrics can offer good quality of security and convenience than orthodox ways for people analysis, optimize and recognize, even we do not have any requirement to change a traditional method (password or handheld token) through a unique biometric, to ensure, we have great number of applicators in these devices, which new passport modal will even more compulsory unique biometrical identification of an individual [10]. For the security purpose formulating a unique voice pattern identifier by developing of MATLAP (SIMULINK) function blocks and which can verify the algorithm and access control key of an authenticate individual voice pattern and maintain high class of security system [11]. The amount of private individual information in the open platform has the unique biometric enrolment sequence is called as Privacy out flow.

Biometric, it is a nutshell, that is using of your body as password and it helps to identify individual. Involvement of unique biometric identifier is become huge important in the recent days. The password or passcode can be enriched by using of an individual biometric identification as a password [12] for mobile, lap top, computers, and restricted-access areas and so on. Biometric indicate unique characteristic of an each and every individual in the world so it indicates the requirements of biometric in the security field, which cannot be replicated, for an example characteristic of, finger prints and palm are full fill this needs. There are various kind of bluffer attacks significantly focus on the domestic of the occurrences and internal surfaces of a unique biometric system's module also inclusion of it which can be stressed jammer on the tele-communication media [13] or via snooping tools harm full attack can be reduced by connecting the USB drive devices in the system [14].

b. Multi-Modal Biometric System

Unimodal unique biometric model limitations can be rectified by fusion biometrics model would function well organized manner and three significant levels were preferred for the fusion of any modalities: sensor level, decision level, an feature level and they were explain very detail in the table number 3 [15]. Figure 2 shows an illustration of the multi-modal biometric system.

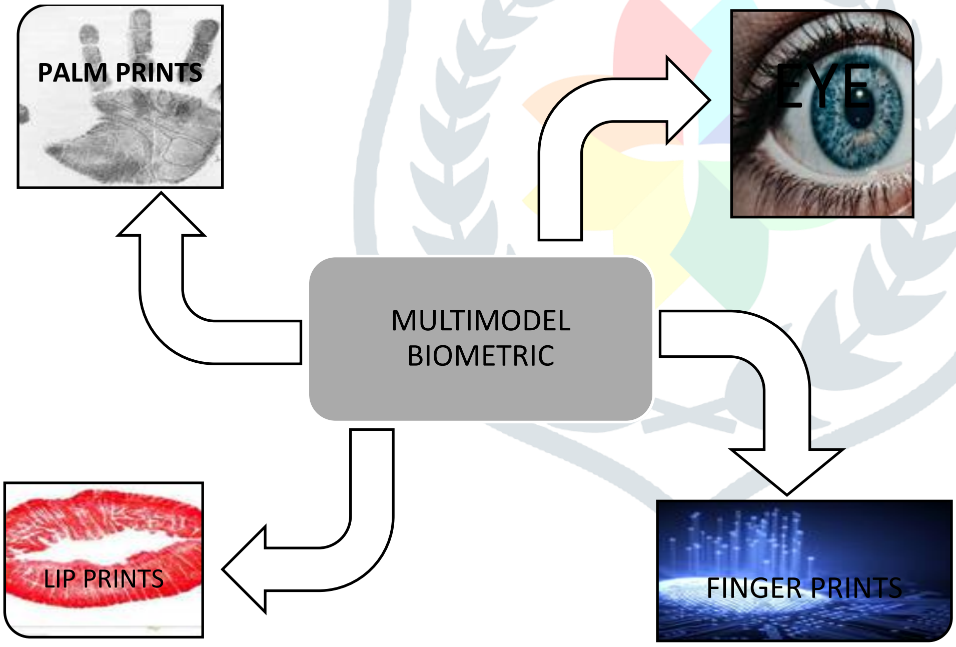


Figure 2: Multi-Modal Biometric System

Biometric device can receive the data from two or more sensing device and which has combined of multiple biometric templets to identify the characteristic of an individual biometric is called as a multi modal biometric device for an example, a system collaborates biometric templets of iris and face physical characteristics for the biometric and it would be optimized by a single image processing machine rather than multiple image processing devices. But do not require the greater number of measures be numerically merged in anyway [16]. The most significant purpose of merging this biometric templet is to enrich the higher level of accuracy. Davit Kocharyan et al [17]. Fingerprints and signature recognition by the multi modal biometric device In that article, researcher was stressed that a framework of the multimodal biometric, taking into an account fingerprints and creates variations and fingerprints difference is the huge famous physiological benchmark followed to authenticate the framework of biometric, due to lastingness, practicality, exactness, unwanted quality, peculiarity and worthiness and Signature difference is stand in a significant place in behavioural benchmark to combine signature as a part of biometric frameworks. In addition to these zones, we accept that the merging of these multi templet techniques will offer a high quality of result.

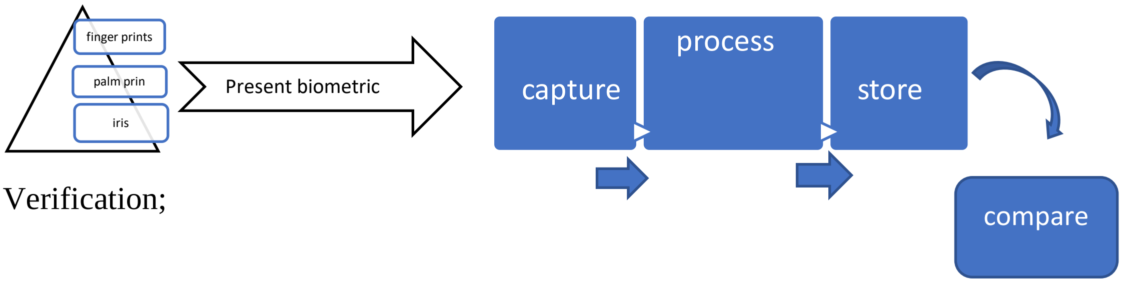
Fusion of biometric modalities has a potential to identify a individual biometrics in multiple ways, Ross[25], et al emphases that unique biometric fusion device can be obtain by merging multiple templet features together, connecting of appropriate nodal together, or a fusion of the biometric made by a person's templets and the significant facility of fusion is the easer technique of feature vectors from a numerous templets were provided as input to the machine, while in the pre-final zone of fusion the element of biometric results from each every templet differentiator in order to take a final decision. Formulating a different path to fusing multiple biometric modalities has underestimated in the different recent biometric authentication studies, Hamami, and Bouzouina [16] emphases a multimodal authentication machine that merge the features in the iris and face modalities at feature level fusion, and this research engaged with multiple models of formulating feature and applicated to support vector machines (SVM) procedure for authenticate the user [18]. A unique biometric device that applicated in the palm prints and ear modalities and merge them at the feature level and they build descriptors and multiple-classification methods [19]. [20] a new feature formulation technique fusing of iris and face traits for a multimodal biometric system, multi-resolution 2 D Long-Gabar filter was extracted from iris feature, but face nomenclature is formulated by using normal inverse Gaussian and singular spectrum analysis, to differentiate, fuzzy k-nearest neighbor (K-NN) was engaged and it is the combination of score fusion and decision fusion.

Gabor facilities are formulated by using a multi-level approach. Then, the user's face model is formulated using Deep Learning techniques and in the recognition phase, the classifier compares and analysis the feature vectors of a normal image with the facial models that are learned during training, and selects the model with the maximum favourite value [23]. [21] stressed that identifying an individual by using of multimodal biometric device, called Iris Conv Net, it connects both the left and right irises using of grade-level fusion and the device initially analysis the iris image in the eye, and then this analysed portion was fall into the CNN model. [22] emphases a DEEP CONTROURLET DERIVATIVE WEIGHTED RANK (DCDWR) framework is used face, fingerprints, and iris modalities to authenticate an individual identities and pre- processing on input picture was performing by Contourlet Transform. Applicator data from mouse, keyboard, and Graphical User Interface (GUI) are applicable to merge a behavioural biometric system then fuse the templet results in a more precious decision depends on a broader view of the applicators system activity, when compare to physical biometric we need less involvement of applicator [24].

3.Performance analyses

Before enter into the performance analyses we can view the detail working structure of multimodal biometric working by using of neat sketch and it is showing in below, and multimodal unique biometric identify systems developed to rectify problem by collecting and combine multiple biometric sample from an individual which gather and combine multiple biometric samples, or characteristics and different research studies stressed that to obtain better performance in the field of biometric authentication we want to considering information from multiple biometric templets [24]. The standard framework of multi-modal biometric authentication system is given in Figure 3.

Enrolment;



Verification;

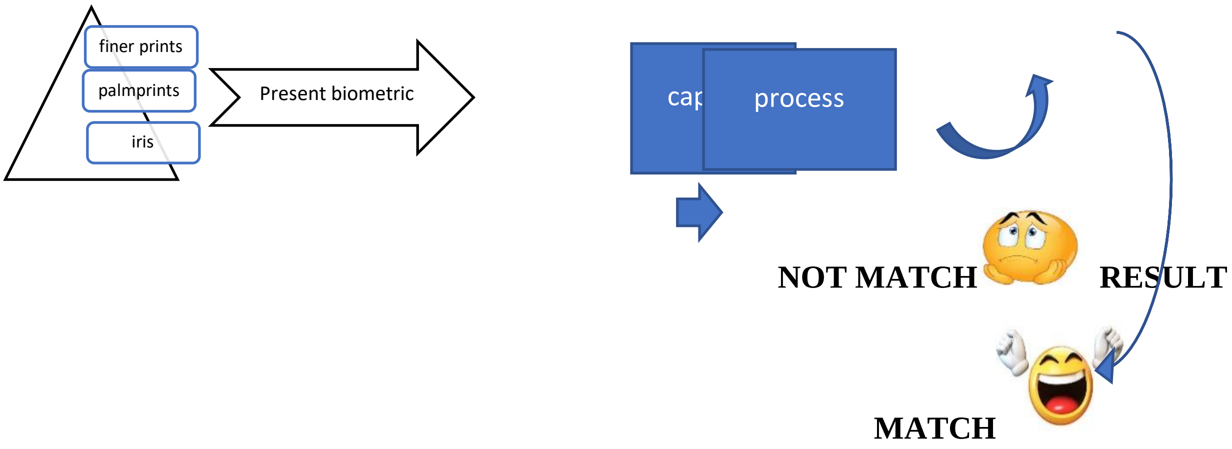


Figure 3: A general architecture of the multi-modal biometric system

There are several factors that can be used to gauge how well any biometric authentication method is working, including [26],

False Accept Rate (FAR) and False Match Rate (MAR): It examines the fraction of poor matches and considers the chance that the system may incorrectly proclaim an exact successful match between an input pattern and a pattern that isn't present in the storage.

False Reject Rate (FRR) or False Non-Match Rate (FNMR): The likelihood that the system will erroneously declare that the sample being input and the corresponding template in the file system do not match is being calculated, in addition to the percentage of valid inputs that are being refused.

Equal Error Rate (EER): the quantity of errors that are equal in both acceptable and unaccepted categories. Because both the FAR and the FRR can be precisely changed, ROC or DET charting, which is additionally referred to as relative operating characteristic (ROC) analysis, is utilized. The ERR is frequently utilized when a quick, concise comparison of two systems is necessary. Choose the location on the ROC plot where FAR and FRR have values that are significantly similar. The technique is thought to be considerably more precise the lower the EER.

The importance of biometric authentication methods and some possible future uses in this sector was emphasized by Debnath Bhattacharyya [26]. His study has portrayed the position of biometrics in today's security ecosystem. Additionally, he has determined viewpoints on the applicability of biometric authorization systems, the interaction between special approaches, and the benefits and harms they cause.

Table 1: Evaluation of Biometric Techniques

Biometric	**FRR**	**EER**	**FAR**
Face	10%	Nill	1%
Palm	2%	1%	2%
Finger prints	2%	2%	2%
ECG	4%	7%	5%
DNA	1%	1%	1%
Key strokes	1%	1.8%	2%
voice	10%	6%	7%

Table 2: Comparison of biometric techniques

Author	Data set	Technique	Performance	Acceptability
Rosa R. Heckle, Ant Ozok, and Andrew S. Patrick	Finger prints	A Microsoft Fingerprint Reader was installed on the laptop PC. (Model DG2-00002)	Medium	High
Davide Maltoni, Matteo Ferrara, Raffaele Cappelli, and Annalisa Franco (2007).	Finger prints	FVC is concerned with evaluating verification of fingerprints technology.	Medium	High
A.K. Jain, S. Prabhakar, D. Maltoni, D. Maio, (2009).	Finger prints	Automatic techniques for fingerprint recognition	Medium	High
Mary Lourde R* and Dushyant Khosla (2010).	Finger prints	Two competing algorithms were compared against a common database using MATLAB simulations	Medium	High
Erika Rahmawati, Adam Shidqul Aziz, Fardani Annisa Damastuti, Sritrusta Sukaridhoto, FMochamad Mobed Bachtiar, and Amang Sudarsono (2017)	Finger prints	RSA algorithm.	Medium	High
Ravi Subban and Dattatreya P. Mankame (2013).	Finger prints	FP matching techniques	Medium	High
Adedoyin Adeyinka, Oloyede Muhtahir O, and Adewole Kayode S. (2013).	Finger prints	Building a questionnaire as the data acquiring instrument utilizing multiple biometric technologies is a quantitative method.	Medium	High
Lin Hong and Anil Jain (1998).	Finger prints	Fingerprint classification with tested on the NIST-4 fingerprint database	Medium	High

Karthik Nandakumar, Abhishek Nagar, and Anil K. Jain (2009).	Finger prints	Vault creation with a fuzzy commitment strategy	Medium	High
Moses Okechukwu Onyesolu, Ignatius Majesty Ezeani (2012).	Finger prints	In order to enhance security, fingerprint biometric technology is used with ATMs for user authentication.	Medium	High
D. Ashok Kumar, T. Ummal Sariba Begum (2011).	Finger prints	using fingerprint details to design and analyze the electronic voting system	Medium	High
Nikolaos Kourkoumelis and Margaret Tzaphlidou (2011).	Eye	Near-infrared radiation's biological effects on the human eye with relation to international law	High	Medium
Paul Prasse, Silvia Makowski1, Lena A. J.ager, Sascha Liehr, Maximilian Seidler, and Tobias Scheffer (2020).	Eye	processing the eye-tracking signal using a deep convolutional architecture	High	Medium
Roman Bednarik, Pasi Fränti, Tomi Kinnunen, and Andrei Mihaila (2005).	Eye	biometric eye movement information	High	Medium
Mary Barry, Tracey J. Mehigan, Aidan Kehoe, and Ian Pitt (2011).	Eye	Choose specific user style information based on the FSLSM's Visual/Vocal dimension.	High	Medium
Corey Holland, Oleg V. Komogortsev (2014).	Eye	A promising behavioral biometric method is scanning path-based identification.	High	Medium
Rigas, Ioannis, and Komogortsev, Oleg (2006).	Eye	Fixation Density Map (FDM), a probabilistic representation of spatial and temporal variables associated to eye fixations, is used	High	Medium

		to translate each eye movement signal into a time-constrained decomposition.		
Along with Aurobinda Routray, Anjith George (2015).	Eye	Biometric identification using the Gaussian Radial Basis Function Network (GRBFN)	High	Medium
Yusuke Morishita, akihiro hayasaka, jianquan liu, hitoshi imaoka, hiroshi hashimoto, koichi takahashi, and kazuyuki sakurai	Face	Deep learning methods	Medium	High
Fatima Syed, Muhammad Jaleed Khan, Khurram Khurshid, and Maheen Zulfiqar (2019).	Face	uses the Viola Jones face detector to find faces in an input picture, and then automatically extracts facial characteristics for recognition using a trained CNN	Medium	High
Michiel van der Veen, Ton H. Akkermans, Geert-Jan Schrijen, Fei Zuo, and Tom Kevenaar.	Face	Integrate this strategy, various templates, the FERET and Caltech databases, and privacy-protected templates.	Medium	High
Bogdan Constantin Neagu, Zoltán Illés, Sandeep Kumar, Shilpa Rani, Arpit Jain, Chaman Verma, Maria Simona Raboaca, and Arpit Jain (2022).	Face	Age, gender, and facial expression are recognized using an advanced artificial neural network architecture-based biometric system that is ace at spoofing.	Medium	High
Sandra Mau, Brian C. Lovell, and	Face	a combination of parallel processing utilizing distributed middleware like ROS, rapid	Medium	High

Abbas Bigdeli (2014).		algorithms, distributed databases, mobile platform integration, and GPU acceleration using CUDA and OpenCL.		
Ranbir Soram, Memeta Khomdram (2010).	DNA	For personal identification in information security systems, use biometric DNA data and the intractability of the Elliptic Curve Discrete Logarithm Problem (ECDLP).	Low	High
Hesham A. Bakarman, Ibrahim Hasan Mohammed Salih AlKharsan, Ali Z. Ghazi Zahid, In 2019.	DNA	Systems of security based on human DNA and its overall impact are also human DNA-based security systems.	Low	High
Sheryl Mathew,G.Saranya (2010).	DNA	DNA cryptography Which is embedded in the door key	Low	High
Ahmad Aizuddin Abdul Aziz, Rozeha A. Rashid, Nur Hija Mahalin, and Mohd Adib Sarijari (2008).	Voice	Security system using speech recognition as the key to access control. A verification method is created utilizing MATLAB (SIMULINK) function blocks that can recognize a person by their voice pattern and verify their identification.	Medium	Low
Anastasis Kounoudes, Vassilis Kekatos, Stephanos	Voice	An Internet application deploying voice biometric authentication	Medium	Low

Mavromoustakos (2006).				
Muhammad Nizam Kamarudin, Hairol Nizam Mohd. Shah*, Mohd. Zamzuri Ab Rashid, Mohd. Fairus Abdollah, Chow Kok Lin, and Zalina Kamis (2019)	Voice	The voice of the administrator may be verified using MATLAB voice recognition software	Medium	Low
Koustav Chakraborty, Asmita Talele , Prof. Savitha Upadhy (2014).	Voice	Mel Frequency Cepstral Coefficients (MFCC) algorithm	Medium	Low
Connie Tee, Michael Goh Kah Ong, and Andrew Teoh Beng Jin (2008).	Hand geometric	In real-time video feeds, the user's palm is tracked and captured using a hand tracking and area of interest (ROI) extraction approach.	Medium	High
Beijing, P. R. China's Wei Shu Zhang David (2000).	Palm prints	We offer a method for verifying palmprints using line feature matching and datum point invariance.	Medium	High
Dr. Vikas T. Humbe and Mr. Shriram D. Raut	Palm prints	utilizing the image processing toolbox in MATLAB software	Medium	High
Maylor K.H. Leung, Cheng Shao Chian, and Fang Li (2009).	Palm print	Method for extracting ROI from palm prints based on RST invariant squares	Medium	High
MI C. Fairhurst (1997).	Signature verification	Automatic signature verification	High	Low
Suraiya Jabin and Farhana Javed Zareen (2015).	Signature verification	System for authenticating mobile biometric signatures and a comparison	High	Low
		The duplicate signature is created using a sigma lognormal		

Miguel A. Ferrer, Andrés Fischer, Réjean Plamondon, and Moises Diaz (2018)	Signature verification	decomposition, and each of the generated signatures is used to train an automated signature validator.	High	Low
Salim Chitroub, Maarouf Korichi, Abdallah Meraoumia, and Aiadi Kamal eddine (2015).	Ear	A Gabor Filter-Based Automated Ear Identification System	Medium	Low

4.Characteristic of multimodal biometric device

Universality: Every single person should have their own distinctive biometric characteristics; however, it is exceedingly difficult to get 100% coverage. Few individuals in our world lack the capacity to talk, and those without fingers, those with broken eyes, and those with disabilities should all be taken care of by worldwide research. Advanced Scientists and Technologists Journal

Uniqueness: The possibility of two distinct individuals having the same iris has been calculated to be very low for twins who are identical, which means that no two or more people were ever born with the same biometric characteristics. At the same time, however, we are unable to be easily distinguished by face recognition and DNA-analysis systems of identical twins.

Permanence: This implies that while the iris can typically remain constant over decades, the characteristics shouldn't remain significantly constant over time. However, we can easily notice major modifications in the face over time in the corresponding period signature, and its dynamics may change as well. The finger is also frequently the site of injuries, and the person's voice can also change when they are ill.

Collectability: It means that the traits must be quantified and that they must be easily obtained. Face recognition systems are non-intrusive, and it is quite easy to acquire a face image. Contrarily, the DNA analysis necessitates the collection of a blood or other body sample, making it challenging, and the retina scan is also somewhat invasive.

Performance: In order to attain the desired level of accuracy, the resources and their operational or surroundings must meet the feasible identification/verification precision.

Acceptability: This emphasizes the areas where people are ready to accept the biometric system. Although I don't find face recognition systems to be invasive, there are some nations where it is illegal to photograph people, and only a small number of users approve the usage of retina scanners, which need an infrared laser beam to be directed through the cornea of the eye**.**

Circumvention: This shows how hard it is to trick the system using bluffer methods. It is less secure to use an automated access control system that can be tricked using a fingerprint model or a photo of the applicant's face.

Table 3: Various interpretations of quality in multi-biometrics from literature

YEAR	Author name	Modality Fused	Level of Fusion	Interpretation
2007	W. Wheeler Tong Frederick	Face and Fingerprint	Score-level	develop cutting-edge biometric fusion technology
2022	Yang Wang, Weibin Zhou, and Dekai Shi	Face and Finger Vein	Feature- level	Convolutional neural network (CNN), where the feature layer is where the fusion takes place.
2018	Krishna Shinde, Sumegh Tharewal	Face and Signature	Score- level	behavioral model for signature recognition and physiological model for face recognition
2007	Javier Ortega-Garcia, Daniel Ramos-Castro, Julian Fierrez-Aguilar, and Joaquin Gonzalez-Rodriguez	Fingerprint, Face and Signature	Feature- level	For the estimate of the between and within-source variabilities of the test pattern, reliable estimation approaches with acceptable generalization capabilities are needed.
2020	Heyam H. Al-Baity Nada Alay	Iris, Face, and Finger Vein	Score- level	based on a deep learning method for biometrically identifying people
2019	Regouid, Meryem Nicholas Costen, Mohamed Benouis, and Mohamed Touahria	ECG, ear and iris	Feature-level	Pre-processing techniques including normalization and segmentation
2017	Nabil Hezil, Abdelhani Boukrouche	ear and palmprint	Feature-level	thorough experimental investigation based on the reference IIT Delhi-2 ear and IIT Delhi palmprint databases
2020	Toufik Bouden, Basma Ammour, Larbi Boubchir, and Messaoud Ramdani	Face and iris	Feature-level	2D Log-Gabor filter with several resolutions to collect textural data at various sizes and orientation
2012	Dr Shubhangi D, Manohar Bali	Face and Fingerprint	Feature- level	Using an information theory method, the facial picture is coded and decoded.

2007	A.Rattani, D.R.Kishu, M.Bicego	Multiple Fingerprints	Decision- level	Decision level fusion is a technique used in multibiometric cryptosystems to combine several fingerprints.
2009	R.K.Subramanian , Nazmeen bibi boodoo.	Face and Ear	Decision -level	The Karhunen-Loeve (KL) expansion
1998	Anil Jain, Lin Hong.	Face and Fingerprint	Decision -level	The feature extraction stag's Eigen face approach for face and minutiae extraction
2013	Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari	Iris and Fingerprint	Decision -level	In order to combine each sort of biometric result, fuzzy logic is employed.
2007	Plamen Prodanov, Jonas Richard, Krzyszof, and Andrzejn Drygajlo	Face and Speech	Decision -level	a multimodal biometric authentication system's reliability estimate process
2015	Hunny Mehrotra, Richa Singh, Mayank Vatsa, and Banshidhar Majhi,	Iris and Cornea	Score -level	Zernike polynomials are employed for the cornea and Log-Gabor feature representation is used for the iris texture.
2011	Feifei cui, Gongping yang	Fingerprint and Finger Vein	Score -level	Minimum-maximum normalization used for normalization
2009	Nageshkumar, Mahesh.PK, Shanmuka swami M. N	Palmprint and Face	Score -level	Palmprint and facial feature extraction using PCA
2010	Marzuki Khalid, Rubiyah Yuosf, and Muhammad Imran Razzak	Face. finger Vein	Score -level	Weighted Fuzzy
2012	Krishneswari K, Arumugam S,	Palmprint and Fingerprint	Feature- level	Utilizing Information Gain (IG) and the Discrete Cosine Transform (DCT), features may be extracted and certain properties can be chosen.
2007	Rattani, Kishu, and Bicego	Face, Fingerprint	Feature - level	Face picture feature extraction using the SIFT (Scale Invariant Feature Transform) technique and finger print detail matching.

5.Design problems in Multibiometric devices

- Higher level of fusion.
- Quantities and option of biometric indicators.
- Identification, optimization and analyzation of system and templet
- Matching scores (preferred; normalize matching scores but more than normalize matching gives high accuracy).
- Too rigid in decision making'.
- Learning weightages of a person's unique biometric for each and every applicator.

6.Applications of Multimodal unique Biometrics identification

Multimodal unique biometric identification is applicable in numerous sectors and the main purpose of using biometric identification is security in both micro and macro level of security and multimodal biometric enhance the efficiency of anti-bluffing and popular fusion in biometric and their application fields.

- National security (entrance core room, finger prints, eye, voice, palm prints, ear, and so on)
- Domestic security (entrance in core room, palm prints, eye, finger prints, and so on)
- Unique identification ID card (finger prints, eye)
- Office (finger prints, signature)
- Passport-office (finger prints, retina, iris, and signature)
- Banking sector (signature, finger prints)
- Airport (passport, eye, finger prints, and so on)
- Educational industries (fingerprints, eye and so on)

7.Research gap and challenges

Most of the existing techniques do not satisfy the appropriate template protection requirements in the real life. From my observation the major research gap in the biometric area is bad network connectivity issue because of it sometime a correct templet also under went "NOT MATCH" biometric and another major research gap in bluffer in both cyber (such as Data diddling, virus attack, cyberattack, web hijacking and so on) and offline (such as silica finger, palm, lip, foot). To avoid such a hypocrite action, we can store the templets by using of block chain technology and also, I found there was a lack of research in multimodal biometric data base, then very few researches were conducted in lip prints as a biometric. From my observation proportion of researcher's focal point in the biometric research field is showed below bar chart. Figure 4 shows the Contribution of the collected articles, a special attention towards the multi-modla biometric systems.

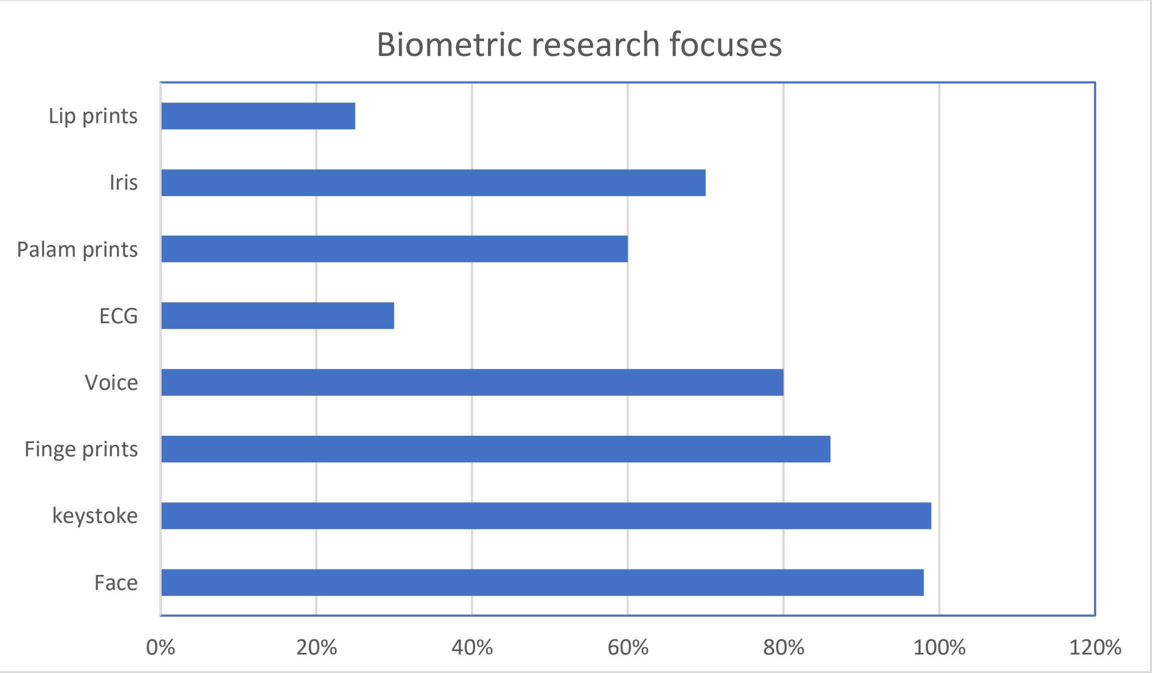


Figure 4: Contribution of the collected articles: A focus on Biometric research

8.Conclusion

There are many multimodal unique biometric systems in use today for the authentication and verification of an individual. However, choosing the right templet, choosing the best level of fusion, and redundancy in the extracted features are still some design flaws that need to be fixed. In multidimensional biometric systems, there are a vast array of possible techniques. With the right level of fusion, the integration strategies that can be selected to obtain holistic information were discussed here, and the combination of multiple biometrics can be used to increase security. Multimodal biometric systems have become one of these industries' most noticeable trends due to performance and advancements in security technology. By using several feature selection strategies to lower the dimensionality, such as hybrid optimization algorithms and deep learning approaches, it is possible to attain high precision.

REFERENCES

[1] Schneier, B., Walker, J., and Jorasch, J.: „Remote-auditing of computer-generated outcomes and authenticated biling and access control system using cryptographic and other protocols‟, in Editor (Ed.) (Eds.): „Book Remote-auditing of computer-generated outcomes and authenticated biling and access control system using cryptographic and other protocols‟ (Google Patents, 1998, edn.).

[2] Teddy Ko Raytheon in 2005, 'Multimodal Biometric Identification for Large User Population Using Fingerprint, Face and Iris Recognition'. Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop (AIPR05) 0-7695-2479-6/05 $20.00 © 2005 IEEE.

[3] Feature Level Fusion of Face and Signature using a Modified Feature Selection Technique (Suryanti Awang, Rubiyah Yusof, Mohamad Fairol Zamzuri, Reza Arfa) 2013 International Conference on Signal-Image Technology & Internet-Based Systems.

[4] Adhami, R.: „Peter Meenen and Reza Adhami‟, 1997.

[5] Han, J., Pei, J., and Kamber, M.: „Data mining: concepts and techniques‟ (Elsevier, 2011. 2011)

[6] International Journal of Advanced Science and Technology Vol. 4, March, 2009 25 "A Brief Introduction of Biometrics and Fingerprint Payment Technology" Dileep Kumar, Yeonseung Ryu Department of Computer Software Myongji University, Yongin-Si, Kyonggi Do, South Korea 449-728

[7] H. Fakourfar and S. Belongie, ―Fingerprint recognition system performance in the maritime environment,‖ in *Proc. Applications of Computer Vision*, IEEE, 2009, pp. 1-5.

[8] M. Hulea, A. Aştilean, T. Leţia, R. Miron, and S. Folea, ―Fingerprint recognition distributed system,‖ in *Proc. Automation, Quality and Testing, Robotics*, IEEE, 2008, pp. 423-428.

[9] International Congress on Interdisciplinary Business and Social Science 2012 (ICIBSoS 2012) "Biometrics Technologies Implementation in Internet Banking Reduce Security Issue"

Normalini, M.K.a*, T. Ramayah b *abSchool of Management, Universiti Sains Malaysia, 11700 Minden, Penang, Malaysia.*

[10]" **Biometric security technology1"** Marcos Faundez-Zanuy Escola Universitaria Politècnica de Mataró Avda. Puig i Cadafalch 101-111 08303 MATARO (BARCELONA) SPAIN, and This work has been supported by FEDER and MEC, TIC-2003-08382-C05-02.

[11] Rozeha A. Rashid, Nur Hija Mahalin, Mohd Adib Sarijari, Ahmad Aizuddin Abdul Aziz *Department of Telecommunication and Optics, Faculty of Electrical Engineering Universiti Teknologi Malaysia, 81310 UTM Skudai, Johor, MALAYSIA (2008).*

[12] F. Mathis, H. I. Fawaz, and M. Khamis, "Knowledge-driven biometric authentication in virtual reality," Conf. Human Factors in Computer System Proc., 2020, doi: 10.1145/3334480.3382799.

[13] A. K. Jain, K. Nandakumar and A. Nagar, Biometric template security, *EURASIP Journal on Advances in Signal Processing*, 2008.

[14] L. Thalheim, J. Krissler and P.-M. Ziegler, Body check: Biometric access protection devices and their programs put to the test, *c't Magazine*, 2002.

[15] Bimodal biometric system: feature level fusion of iris and fingerprint; Ujwalla Gawande, Mukesh Zaveri, Avichal Kapur 2013.

[16] Teddy Ko Raytheon 1300 North 17th Street – 8th Floor Arlington, VA 22209; in 2005.

[17] S.Nanavati, M. Thieme and R. N a 2002, Biometrics: Identity in a networked world, Ed.John Wiley 20M.,

[18] Bouzouina, Y.; Hamami, L. Multimodal biometric: Iris and face recognition based on feature selection of iris with GA and scores level fusion with SVM. In Proceedings of the 2017 2nd International Conference on Bio-Engineering for Smart Technologies, Paris, France, 30 August–1 September 2017; pp. 1–7.

[19] Hezil, N.; Boukrouche, A. Multimodal biometric recognition using human ear and palmprint. *IET Biom.* **2017**, *6*, 351–359. [CrossRef].

[20] Ammour, B.; Boubchir, L.; Bouden, T.; Ramdani, M. Face–iris multimodal biometric identification system. Electronics **2020**, 9, 85. [CrossRef].

[21] Al-Waisy, A.S.; Qahwaji, R.; Ipson, S.; Al-Fahdawi, S.; Nagem, T.A.M. A multi-biometric iris recognition system based on a deep learning approach. Pattern Anal. Appl. **2018**, 21, 783–802. [CrossRef]

[22] Gunasekaran, K.; Raja, J.; Pitchai, R. Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images. *Automatika* **2019**, *60*, 253–265.

[23] Catalin-Mircea DUMITRESCU*, Ioan DUMITRACHE

University POLITEHNICA of Bucharest, 313 Splaiul Independenței, Bucharest, Romania dumitrescu.catalin.m@gmail.com (**Corresponding author*), ioan.dumitrache@acse.pub.ro; 2013.

[24] Kyle O. Bailey, James S. Okolica, Gilbert L. Peterson Air Force Institute of Technology Graduate School of Engineering and Management 2950 Hobson Way, WPAFB, Ohio 45433 fkyle.bailey, james.okolica, gilbert.petersong@afit.edu Corresponding Author: Gilbert Peterson (937)-785-6565 x4281 ;2014.

[25] K. Sentosa, " Performance Evaluation of Score Level Fusion in Multimodal Biometric Systems", Department Of Computer Science And Information Engineering National Taiwan University Of Science And Technology, M.Sc. Thesis, 2007.

[26] Sakshi Kalra , Anil Lamba *CSE Department, KUK University Haryana, India* ,2014., Debnath bhattacharya " Biometric Authentiction :A Review " Vol. 2 , Issue 3 , Sep 7 2009 , pp 13-26