International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

Exploring the Use of Biometric Technology in Enhancing Security: A Survey of Current Applications and Future Implications

Prof. M R Desai ,Ms.Poornima B , Ms.Pooja B S ,Ms. Arpitha R , Ms.Bhavya J

UG Scholars, Computer Science and Engineering Department
SJM Institute of Technology, Chitradurga, Karnataka, India

muktadesai0@gmail.com, poornimabpoornima338@gmail.com, bspooja777@gmail.com, arpitharcta@gmail.com ,bhavyakbj600@gmail.com

---

Abstract - Allocating a security to any data of an individual which is predefined is complicated. Biometric is more popularly used technology to recognise an actual user. Biometric practically gives trusted security against data pilfering. Biometrics assist to examine the unique identification of an individual. Commonly used biometric techniques are iris, fingerprint, palmprint and face identification. In some realistic circumstances, biometric techniques fail to achieve requirements in providing security. One of the problem in biometric is spoofing. Malicious user illegally get access to actual data of an user by replicating biometric predefined data. In this survey, we have analysed how biometric plays an vital role in the field of identification and verification of an individual and we have go through various research papers, compared the methods used to provide security to biometric device and biometric data.

***Key Words*:** Biometrics, Fingerprint, Iris, Palmprint, Face.

1.INTRODUCTION *(Size 11, Times New roman)*

Biometric is a safest and new technology recognize and configure an individual based on their biological characteristics like fingerprint, iris, brain, hand geometry, speech etc are popularly used along with growing technology. Biometric is embedded in most of the technologies in order to provide security Biometric used to recognize the authenticate person based on the identity using physical or behavioral features of a person. The captured or stored information of an individual for biometric to check identity also require security. The fingerprint biometric system consists of the stage like fingerprint sensation, analysis of fingerprint and finally matching the respective fingerprint with predefined data of the respective individual.

Fingerprint is unique for each and every individual even the twin person has different fingerprint. Fingerprint contains loop, whorl and arch. This shape of three ridges patterns helps to recognize the individual using unique features. Even though in the presence of so many unique features data which is stored for identification are vulnerable to the various attacks like spoofing attack and acquisition of biometric data. In order to prevent this problem required to take some preventive measures and the methods to avoid the attacks. Fingerprint is taken using online scanner the fingerprint features are extracted and minutia subsets hashes is established. The operation to find minutia and the hashes are transmitted first and then stored in database .While verifying new hashes are produced and it is matched with those which are stored in the database.

2. A Brief Analysis of Existing Methods

A Comparative Review of Biometric Security Systems: In the year 2015 Rayan Ercel O. Paderes Security is most important aspect in protecting the essential data. Advancement on security has been a growing consistently the techniques and methods consist of well- functioning system. Biometric system is one of the safest technique in terms of security. This paper deals with fingerprint and iris recognition. This paper works on 3D method. Here 3D techniques are used for recognition like 3D face, 3D palmprint, 3D fingerprint, and 3D ear. It provides 4 main methods 3D imaging and gives out few case study on 3D biometrics field. But this paper don't explain how to match with authenticated data if matcher is corrupted [1].

Performance and security evaluation of palmprint biometric techniques: In the year 2015 Imen Bouraoui et.al Providing security for templates in biometric system is an big issue because biometric templates cannot issued again. Biometric system is vulnerable to a various type of attacks. So, giving security for biometric template is most important. In this paper, they used biometric cryptosystem that contains biometric together with cryptography is combining with templates of palm print in applications of biometric cryptography. The method involving a series of stages begin with a user choosen transformation of data to encrypt, proceeds with extraction of feature and correction of errors procedure. Encryption of biometric image is done by algorithm hill cipher follows feature extraction method uses algorithm that is Fast-ICA . This proposed work fails to increase this system in order to withstand against attacks [2].

Enhancing security for multimodal biometric using Hyper Image Encryption Algorithm: In the year 2015 K. Nivetha* D.Saraswady 'Multimodal biometrics' uses three sources of biometric like finger print, retina, finger vein is used for

authentication purpose. Uni biometric system is more vulnerable for spoofing attacks by malicious user. In this paper multimodal biometric direct to performance guarantee to provide an greater degree of security by together with finger vein, retina and fingerprint. To biometric template algorithm named hyper image of encryption is applied only to template which is transformed and is stored in the database depending on the secret key. This paper fails to achieve accurate feature extraction technique also maintaining database efficiently [3].

Development of biometric security system using CBIR and EER: In the year 2015 ARAVIND G et.al .In this work focuses on image retrieval systems based on contents to security purpose in the biometric. CBIR is familiar to browse, search and retrieval of images from database of images which are in digital form. Now a days method for biometric security has most important as biometrics technology is advancing and it is more reliable and efficient in the most applications of real world. This paper works on the three image features: color, texture, shape used in biometric for powerful security purpose[4].

Comparison of biometric identification methods: In the year 2016 CSABA OTTI. There are many biometric identification technologies uses knowledge based and possession based identification methods. The main drawback of this paper the new technology is also not secure it maybe stolen or lent and maybe copied to secure and intelligent chip cards are spreading even those have weaknesses [5].

The influence of stress on biometric signature stability: In the year 2016 VALDIMIR SMEJKAL et.al. This paper majorly deals with research on DBS, the features of DBS are security and its resistance to attacks and its stability. Handwritten signature is long term practise but it is not constant always. This paper identifies short signatures with abbreviations or initials show variations of conformations between the individuals signature. It uses own algorithm to evaluate the conformity of signature and requires some points which leads to more variations in comparing with short signatures. It achieves results for short signature not for abbreviated signs [6].

A survey on biometric based authentication in cloud computing: In the year 2016 P. PADMA .This paper deals with various methods of providing biometric security using cloud computing. Cloud computing provides various computing services over internet and store data in cloud servers. It implements physical and behavioural biometric methods. Physical biometric traits reuires additional hardware to provide authentication behavioural method drawback is being mimicked by others easily [7].

Three factor biometric authentication for spiralling of security: In the year 2016 DIANA JUDITH J et.al Biometric authentication provides identification and access control of an individual. In this work visual cryptography scheme is implemented which divides images into shares. This paper deals with three biometric techniques iris, face recognition and fingerprint for data security in the database. Security problems may happen for data stored in database maybe duplicated or altered by middleman. Due to this authenticated person not able to access their own data and privacy is not provided [8].

Integrating biometric cryptosystem with steganography for authentication: In the year 2016 MANJARI BENHAR PREETHALA et.al. Providing security for the information stored in digital format over the internet has got more importance from many years because of flourishing e-commerce. Traditional methods of providing security is based on memory base like passwords or pin are not that much secured. So this paper biometric cryptosystems is introduced to enhance security for authentication purpose followed by steganography method to hide biometric data This paper provides 99% accuracy. RC4 algorithm shows the time complexity as low as 18msec [9].

Biometric layering with fingerprints: Template security and privacy through multi-biometric template fusion: In the year 2016 MUHAMMET YILDIZ et.al. Now a days Biometric is getting more popular to for the purpose of authentication and to prevent biometric data misuse of an individual. Three new methods are implemented in this paper to make it complex to divide the multi-biometric template to constituent biometric sample, in order to avoid the ways of leakages of the actual template, to invent the limitations of biometric layering in three methods .The drawback is that performance is low because of lesser processing power and the memory, data is more vulnerable for attacks if plan matching results for generated card, inappropriate to manage its physical security [10].

A study on biometric and multi modal biometric system modules application technique and challenges: In the year 2017 R.DEVI et.al. This paper uses encryption of templates using cryptographic method, feature transformation is classified into invertible .provides protection for template on the basis of secret key and non-invertible uses one way function on template, biometric cryptosystems is method as same as password key generation, water marking is a method for authentication, hiding data water marking maybe visible or invisible it maybe text, image, audio/video. The main drawback is in decision level fusion decisions incorporates using And-Or rule the results of AND gives match with matchers of biometric for input template OR rule match atleast one biometric of biometric matcher need to match with the input template. Both rule as restriction AND rule applied for FAR multi-biometric system is less and FRR is more and OR rule is greater FAR and small FRR [11].

An analysis of biometric based security systems: In the year 2018 SHEIKH IMROZA MANZOOR et.al. In this paper uses score level fusion based on the SVM along with Z-Score normalization for segmentation finger proceed by finger vein segmentation for a image of finger by using near infrared illuminators . In some realistic condition biometric techniques fail to achieve the safety requirement. Spoofing attack is one of the extensive threats in real time environment [12].

Operational tradeoffs in the 2018 department of homeland security science and technology directorate biometric technology rally: In 2018 JACOB A. HASSELGREN et.al. This paper uses common algorithm, commercial algorithm and matching algorithm by MdTF to recognize the image against gallery of facial samples of others that captured before by MdTF. While rapidly gathered images under four seconds may results in lesser image quality because of blur, no important relationship evolves among identification and transaction time [13].

An automated garage door and security management system: In the year 2018 R.JENIFER PRARTHANA et.al. In this work uses Raspberry pi 3, fingerprint sensor, DC motor, python idle, virtual network, computing viewer. Interfaced module of sensor for centrally controlled Raspberry Pi 3. Inorder to control the access entry and exit. The Raspberry Pi 3 is connected to module the system to get connected establish a VNC viewer and actual verified data of fingerprint stored in database it don't get improved safeguard the certain information and secrecy [14].

Security and privacy enhancement fo out sourced biometric identification: In the year 2018 KAI ZHOU et.al. In this work KNN algorithm is used to encrypt the x and y templates and the query template that is encrypted z, which template is closer to z is found by cloud to determine which template is closer to z in order to know closest template to z and find elative distance information with templates in database. It expose less information then other system [15].

Investigation the Ateb-Gabar filter in biometric security system: In the year 2018 MARIYA NAZARKEVYCH et.al. This paper is based on aggregate divergence matrix element of filtration theory with the help of genetic algorithm. Two images are taken first image is original one and second is filtered image. To make equal sized image both are filtered. Original image is changed on the basis of habitual gabor filter and filtered second image is replaced with Ateb-Gabor filter. This paper need to conduct the image filtration with more number of filtration [16].

A Lossless model for generation of unique digital code for identification of biometric images: In 2018 Mohan Mishra et.al. This paper uses persons unique ID for verification and identification of authenticated person. Also utilises zero-watermarking which is new method where tempering the biometric image. Uses SVM classification along with PSO, ID algorithm used to create new ID to iris image identification. This model don't discover different fields to resolve biometric image security further application [17].

Biometric authentication system : security concerns and solutions: In the year 2018 Namrata Bhartiya et.al. In this paper involves usage of biometric and encrypted OTP. Weak encryption algorithm data feature collected encrypted using this algorithm to store in database. The owner must have a mobile device that as fingerprint scanner whenever they want to make transaction is time consuming compare to pin authentication based on Electronic data capture machines [18].

Advancement in biometric security system: A case study: In the year 2018 Ramesh kumar. This paper deals with the various techniques to handle biometric data attacks and vulnerable threats on biometric system those techniques are liveness detection used to identify the whether biometric samples are alive or altered also used for to protect data from unauthorised access, cancellable biometric one of the new technology used to protect the template stored in database followed by biometric cryptography which transform original data into encoded data then followed by biometric watermarking and multi biometric approaches [19].

Analysis of security threats and counter measures for various biometric techniques: In the year 2019 k. Muthamil Sudar et.al. Biometric uses two techniques identification/recognition and verification/conformation. Where identification technique used to recognize the person based on the predefined data stored in database. Verification technique used to check the specification based on the physical identity like fingerprint, palmprint, iris. It doesn't achieve liveliness detection in an effective way to avoid spoofing attacks [20].

An authentication model for online transactions using biometric security: In the year 2019 Yoshita Sharma et.al. In this paper uses various speech recognition techniques among them first one is analysis technique in this phase when person speaks that speech contains information is useful for identification purpose this phase is classified into 3 sub phases like segmentation sub segmentation and supra-segmental analysis. Another technique is feature extraction used to extract the features from speech. Then comes modelling technique this method uses extracted feature for representation of speaker. Followed by matching technique is used to match recognized voice with authenticated data.[21].

A Biometric key generation mechanism for authentication based on face image: In the year 2020 Yazhou Wang et.al. In this paper Convolution Neural Networks (CNN) model is introduced has done progress in image recognition field, used

a architecture of deep CNN also L2 normalization used to generate the face vector, embedding of face vector and triple loss method used are extraction of feature and key generation in biometric[22].

Security enhancement in smart home management through multimodal through biometric and passcode: In 2020 Sameer Ibrahim et.al .This paper uses the LBPH algorithm one of the easiest face recognition algorithms, Algorithm is used which is available in the platform of OpenCV. where this paper is carried out in three stages pre-processing, feature-extraction and classification and implemented methods are biometric fusion using the Boolean values and the drawbacks of this paper is a bulk of devices works on the wireless mechanism and broadcast mechanism so it is unprotected in security point of view [23].

A score level fuzzy rule based multi biometric framework for enhancing security of cloud access scenario: In the year 2020 Miss Aarohi Vora et.al. This paper uses the Support Vector Machine (SVM) algorithm which generates a decision surface dividing of the two classes also uses fuzzy rule influence algorithm. The drawback of this paper is where the develops rules are more depending on individuals ROC curves. During the designing FRB -MBF the score sets of individual are considered in most application outline [24].

A security enhancement scheme using SVM classifier: In the year 2020 Priya Deshmukh et.al. In this paper the method used is the SVM classifier which finds an optimal hyper plane in between the two classes as a margin which enhances the use of dual class SVM classifier for the authorized and un authorized user classes, the drawback is in which reported many cases of spoofing attacks on the sensors and also merchantile application devices with less cost materials [25].

Image superiority calculation meant calculation meant for biometric fake detection approach of finger print: In the year 2021 Shubham Mahajan et.al. In the this paper the methods used is quality assessment algorithm for proper functioning and recognition of the system and for this study of various weakness of the biometric system because to restrict the profused classification of the hacks and the main drawback in case of increasing the real appearance of features of biometric in the picture as opposed to a fraud there is a common issue in biometric field [26].

On Soft-Biometric Information Stored in Biometric Face Embeddings: In the year 2121 Philipp Terhorst et.al. This paper uses method of investigation which is based on massive attribute classifier(MAC) which trains multiple attributes[27].

Table 1: A study on Features selected and a Method used in providing security to biometric data

SL NO	YEAR	TITLE	FEATURES SELECTED	ALGORITHM / METHODOLOGY
1	2015	A Comparative review of biometric security systems	Finger print and iris recognition	**3D method :** for fingerprint method first the scanner takes the scanner takes the images of fingerprint. Then the unique patterns are read next the unique patterns are analyzed and the patterns then converted to binary format that represent the unique patterns in iris.
2	2015	Performance and security evaluation of palmprint biometric techniques	Palm print	**Hill cipher:** Palmprint images from biometric are encrypted. **Fast-ICA:**This algorithm is used to extract the features and it is done after image encryption.
3	2015	Enhancing security for multimodal biometric using Hyper Image Encryption Algorithm	finger vein, retina and fingerprint	**Hyper Image Encryption Algorithm:** applied only to template which is transformed and is stored in the database depending on the secret key
4	2015	Development of biometric security system using CBIR and EER	Physical and behavioural characteristics	**Histogram based method:** It is used to representation of feature visually because of their usefulness in retrieval of image. **Texture features:** It uses gabor wavelet algorithm using this method wavelets are vastly used in application of image processing it extracts texture feature of image. **Shape features:** This method uses algorithm HU moment invariants

				for feature extraction of image inorder to recognise object.
5	2016	Comparison of biometric identification methods	fingeprint	**Knowledge based identification:** It represents passwords and pins usin in ATMs and it's cost is less **Possession based identification:** In this for person an object is assigned and this technology is widely used. **Biometric identification:** Represents identification of an individual based on his features like face, fingerprint, iris etc.
6	2016	The influence of stress on biometric signature stability	Signature	Identifies short signatures with abbreviations or initials show variations of conformations between the individuals signature. It uses own algorithm to evaluate the conformity of signature and requires some points which leads to more variations in comparing with short signatures. It achieves results for short signature not for abbreviated signs
7	2016	A survey on biometric based authentication in cloud computing	Physical, Behavioural biometric Characteristics	It implements physical and behavioural biometric methods. Physical biometric traits reuires additional hardware to provide authentication behavioural method drawback is being mimicked by others easily
8	2016	Three factor biometric authentication for spiralling	Face, fingerprint, iris	It implements physical and behavioural biometric methods. Physical biometric traits requires
		of security		additional hardware to provide authentication behavioural method drawback is being mimicked by others easily.
9	2016	Integrating biometric cryptosystem with steganography for authentication	fingerprint	**RC4 algorithm:** shows the time complexity as low as 18msec. It works as follows Creates 2 arrays of strings. One array is initialized with number 0 to 255. Fill other array with minutiae feature vectors Randomize first array again depending on second array.
10	2016	Biometric layering with fingerprints: Template security and privacy through multi-biometric template fusion	Fingerprint	For multiple fingerprints it performs **Enrollment and verification:** It collects two different fingers defines the points of minutiae using endings of ridge and bifurcation use it as feature. Next the mass at centre of these minutiae sets is organised and overlapped on other to reduce overlaying minutiae. **Feature extraction:** Extract features from fingerprint. Hidiing angle information Using a subset of the minutiae Layering three finger prints Matching and sorting.

11	2017	A study on biometric and multi modal biometric system modules applicatio n technique and challenges .	Physiological and behavioural characteristics	Decision level fusion decisions incorporates using And-Or rule the results of AND gives match with matchers of biometric for input template OR rule match atleast one biometric of biometric matcher need to match with the input template. Both rule as restriction AND rule applied for FAR multi-biometric system is less and FRR is more and OR rule is greater FAR and small FRR.
12	2018	An analysis of biometric based security systems	Fingerprint	Methods involve correlation-based, minutiae-based, local versus global matching of minutiae and matching of non-minutiae feature based.
13	2018	Operation al tradeoffs in the 2018 departmen t of homeland security science and technolog y directorate biometric technolog y rally	Face	common algorithm, commercial algorithm and matching algorithm by MdTF to recognize the image against gallery of facial samples of others that captured before by MdTF. While rapidly gathered images under four seconds may results in lesser image quality because of blur, no important relationship evolves among identification and transaction time
14	2018	An automated garage door and security manageme nt system	fingerprint	In this work uses **Raspberry pi 3, fingerprint sensor, DC motor, python idle, virtual network computing viewer**. The Raspberry Pi 3 is connected to module the system to get connected establish a VNC viewer and actual verified data of fingerprint stored in database it don't get improved safeguard the certain information and secrecy
15	2018	Security and privacy enhancem ent fo out sourced biometric identificati on	Template	**KNN algorithm** is used to encrypt the x and y templates and the query template that is encrypted z, which template is closer to z is found by cloud to determine which template is closer to z in order to know closest template to z and find elative distance information with templates in database. It expose less information then other system
16	2018	Investigati on the Ateb-Gabar filter in biometric security system	fingerprint	**Ateb-Gabor filter** :Two images are taken first image is original one and second is filtered image . To make equal sized image both are filtered. Original image is changed on the basis of habitual gabor filter and filtered second image is replaced with Ateb-Gabor filter. This paper need to conduct the image filtration with moe number of filtration
17	2018	A Lossless model for generation of unique digital code for identificati on of biometric images	Iris	uses persons unique ID for verification and identification of authenticated person. Also utilises zero-watermarking which is new method where tempering the biometric image. Uses SVM classification along with PSO, ID algorithm used to create new ID to iris image identification. This model don't discover different fields to resolve biometric image security further application.
18	2018	Biometric authentica	fingerprint	**Weak encryption algorithm** data

		tion system : security concerns and solutions		feature collected encrypted using this algorithm to store in database. The owner must have a mobile device that as fingerprint scanner whenever they want to make transaction is time consuming compare to pin authentication based on Electronic data capture machines
19	2018	Advancement in biometric security system: A case study	face	This paper deals with the various techniques to handle biometric data attacks and vulnerable threats on biometric system those techniques are liveness detection used to identify the whether biometric samples are alive or altered also used for to protect data from unauthorised access, cancellable biometric one of the new technology used to protect the template stored in database followed by biometric cryptography which transform original data into encoded data then followed by biometric watermarking and multi biometric approaches.
20	2019	Analysis of security threats and counter measures for various biometric techniques	Fingerprint, Signature, Face	Biometric uses two techniques identification/ recognition and verification/conformation. Where identification technique used to recognize the person based on the predefined data stored in database. Verification technique used to check the specification based on the physical identity like fingerprint, palmprint, iris.
21	2019	An authentication model for online transactions using biometric security	speech	• **Analysis technique** in this phase when person speaks that speech contains information is useful for identification purpose this phase is classified into 3 sub phases like segmentation sub segmentation and supra-segmental analysis. • **Feature extraction** used to extract the features from speech. • **Modelling technique** this method uses extracted feature for representation of speaker. **Matching technique** is used to match recognized voice with authenticated data.
22	2020	A Biometric key generation mechanism for authentication based on face image.	Face	**Convolution Neural Networks** model is introduced has done progress in image recognition field, used a architecture of deep CNN also L2 normalization used to generate the face vector, embedding of face vector and triple loss method used are extraction of feature and key generation in biometric.
23	2020	Security enhancem	Face	**LBPH algorithm** one of the easiest

		ent in smart home management through multimodal through biometric and passcode.		face recognition algorithms, Algorithm is used which is available in the platform of OpenCV. where this paper is carried out in three stages pre-processing, feature-extraction and classification and implemented methods are biometric fusion using the Boolean values
24	2020	A score level fuzzy rule based multi biometric framework for enhancing security of cloud access scenario	Fingerprint, Face	**Support Vector Machine (SVM) algorithm** which generates a decision surface dividing of the two classes also uses fuzzy rule influence algorithm.
25	2020	A security enhancement scheme using SVM classifier	Fingerprint, Palmprint	**SVM classifier** which finds an optimal hyper plane in between the two classes as a margin which enhances the use of dual class SVM classifier for the authorized and un authorized user classes
26	2021	Image superiority calculation meant calculation meant for biometric fake detection approach of finger print	Fingerprint	Quality assessment algorithm for proper functioning and recognition of the system and for this study of various weakness of the biometric system because to restrict the profused classification of the hacks
27	2021	On Soft-Biometric Information Stored in Biometric Face Embeddings	Face	This paper uses method of investigation which is based on massive attribute classifier(MAC) which trains multiple attributes.

3. A comparative Analysis of Methods Used:

Year	Title	Most widely used features	Algorithm
2015	1) A Comparative review of biometric security systems 2) Performance and security evaluation of palmprint biometric techniques 3) Enhancing security for multimodal biometric using Hyper Image Encryption Algorithm 4) Development of biometric security system using CBIR and EERComparison of biometric identification methods	Fingerprint, palmprint, iris	**3D method** for fingerprint and **Fast-ICA** for palmprint
2016	1) Comparison of biometric identification methods 2) The influence of stress on biometric signature stability 3) A survey on biometric based authentication in cloud computing 4) Three factor biometric authentication for spiralling of security 5) Integrating biometric cryptosystem with steganography for authentication 6) Biometric layering with fingerprints: Template security and privacy through multi-biometric template fusion	fingerprint	RC4 algorithm
2017	A study on biometric and multi modal biometric system modules application	Physical and behavioural	And-Or rule

	technique and challenges.	characters	
2018	1) An analysis of biometric based security systems 2) Operational tradeoffs in the 2018 department of homeland security science and technology directorate biometric technology rally 3) An automated garage door and security management system 4) Security and privacy enhancement fo out sourced biometric identification 5) Investigation the Ateb-Gabar filter in biometric security system 6) A Lossless model for generation of unique digital code for identification of biometric images 7) Biometric authentication system : security concerns and solutions 8) Advancement in biometric security system: A case study	Fingerprint, face	KNN algorithm
2019	1) An authentication model for online transactions using biometric security 2) Analysis of security threats and counter measures for various biometric techniques	voice, Fingerprint	Identification and verification
2020	1) A Biometric key generation mechanism for authentication based on face image. cement in smart home hrough multimodal through passcode. 3) A score level fuzzy rule based multi biometric framework for enhancing security of cloud access	Fingerprint, Palm, face	SVM Classifier
2021	1) Image superiority calculation meant calculation meant for biometric fake detection approach of finger print 2) On Soft-Biometric Information Stored in	Fingerprint, face	Quality assessment algorithm
	Biometric Face Embeddings		

4. Graphical representation on usage of features

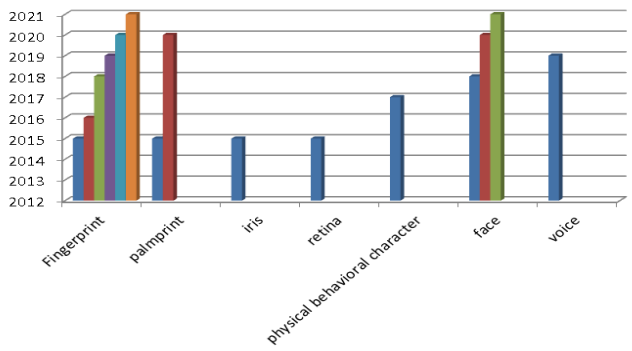

Fig 1: A graphical representation of methods used in a particular Year: X-Axis: Features selected and Y-Axis: Years

Above Fig 1 represents the graph drawn by comparing with year features of human including fingerprint, palmprint, iris, retina, face, voice and some more physical and behavioral characteristics. Fingerprint is highly used in 2021, in 2020 palmprint is high, 2015 iris and retina are highly used, face is most used in 2021, voice in 2019.

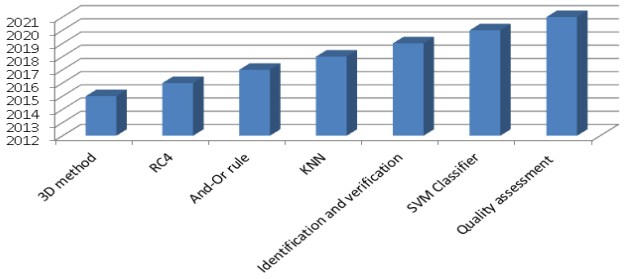

Fig 2: Year V/S Algorithms that are widely used for biometrics

Above Fig 2 graph plotted with algorithm and year 3D method widely used in 2014, RC4 is used in 2015, And or rule used in 2016, KNN algorithm used in 2017, SVM Classifier in 2019, Quality assessment in 2020.

5. Conclusion

Biometrics is one of the widely used and safest method of verifying authentication and authorization of an actual user it works on the biological and behavioral features of an individual like fingerprint, palm print, face, iris and so on. Biometric system uses sensors to capture these characters of an user. As it offers high level security it is associated with risk like spoofing, data duplication, real time hacking and so on. The survey results show that while biometric technology is generally perceived as convenient and secure, there are still concerns about privacy and data protection. Respondents expressed willingness to use biometric authentication for personal devices and services. It is our hope that this survey

will contribute to a better understanding of the complex issues surrounding biometric authentication and inform the development of effective strategies for implementing this technology in a responsible and ethical manner.

References

[1] R. E. O. Paderes, "A Comparative Review of Biometric Security Systems," 2015 8th International Conference on Bio-Science and Bio-Technology (BSBT), Jeju, Korea (South),2015, pp. 8-11, doi: 10.1109/BSBT.2015.12.

[2] A. Aglio-Caballero, B. Ríos-Sánchez, C. Sánchez-Ávila and M. J. M. de Giles, "Analysisof local binary patterns and uniform local binary patterns for palm vein biometric recognition," 2017 International Carnahan Conference on Security Technology (ICCST),Madrid, Spain, 2017, pp. 1-6, doi: 10.1109/CCST.2017.8167808.

[3] K. Nivetha and D. Saraswady, "Enhancing security for multimodal biometric using Hyper Image Encryption Algorithm," 2015 2nd International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India, 2015, pp. 943-947, doi: 10.1109/ECS.2015.7125053.

[4] Aravind G, Andan H M, T. Singh and G. Joseph, "Development of biometric security system using CBIR and EER," 2015 International Conference on Communications and SignalProcessing (ICCSP), Melmaruvathur, India, 2015, pp. 0884-0888, doi: 10.1109/ICCSP.2015.7322622.

[5] C. Otti, "Comparison of biometric identification methods," 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 2016, pp. 339-344, doi: 10.1109/SACI.2016.7507397.

[6] V. Smejkal, L. Sieger and J. Kodl, "The influence of stress on biometric signature stability," 2016 IEEE International Carnahan Conference on Security Technology (ICCST), Orlando, FL, USA, 2016, pp. 1-5, doi: 10.1109/CCST.2016.7815680.

[7] P. Padma and S. Srinivasan, "A survey on biometric based authentication in cloud computing," 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2016, pp. 1-5, doi: 10.1109/INVENTIVE.2016.7823273.

[8] I. Diana Judith, G. J. J. Mary and M. M. Susanna, "Three factor biometric authentication for spiraling of security," 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), Pudukkottai, India, 2016, pp. 1-3, doi: 10.1109/ICETETS.2016.7603017.

[9] M. B. Peethala and S. Kulkarni, "Integrating Biometric Cryptosystem with steganography for authentication," 2016 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE), Pune, India, 2016, pp. 28-31, doi: 10.1109/WIECON-ECE.2016.8009080.

[10] M. Yildiz, B. Yanikoğlu, A. Kholmatov, A. Kanak, U. Uludağ and H. Erdoğan, "Biometric Layering with Fingerprints: Template Security and Privacy Through Multi-Biometric Template Fusion," in The Computer Journal, vol. 60, no. 4, pp. 573-587, March 2017, doi: 10.1093/comjnl/bxw081.

[11] R. Devi and P. Sujatha, "A study on biometric and multi-modal biometric system modules, applications, techniques and challenges," 2017 Conference on Emerging Devices and Smart Systems (ICEDSS), Mallasamudram, India, 2017, pp. 267-271, doi: 10.1109/ICEDSS.2017.8073691.

[12] S. I. Manzoor and A. Selwal, "An Analysis of Biometric Based Security Systems," 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, India, 2018, pp. 306-311, doi: 10.1109/PDGC.2018.8745722.

[13] J. A. Hasselgren, J. J. Howard, Y. B. Sirotin, A. J. Blanchard and A. Vemury, "Operational Tradeoffs in the 2018 Department of Homeland Security Science andTechnology Directorate Biometric Technology Rally," 2018 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 2018, pp. 1-4, doi: 10.1109/THS.2018.8574183.

[14] R. J. Prarthana, A. M. Dhanzil, N. I. Mahesh and S. Raghul, "An Automated Garage Door and Security Management System (A dual control system with VPN IoT & Biometric Database)," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018, pp. 1468-1472, doi: 10.1109/ICECA.2018.8474630.

[15] K. Zhou, J. Ren and T. Li, "Security and Privacy Enhancement for Outsourced Biometric Identification," 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-5, doi: 10.1109/GLOCOM.2018.8647899.

[16] M. Nazarkevych, I. Klyujnyk and H. Nazarkevych, "Investigation the Ateb-Gabor Filter in Biometric Security Systems," 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), Lviv, Ukraine, 2018, pp. 580-583, doi: 10.1109/DSMP.2018.8478535.

[17] M. Mishra, A. Bhattacharya, A. Singh and M. K. Dutta, "A Lossless Model for Generation of Unique Digital Code for Identification of Biometric Images," 2018 4th International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, India, 2018, pp. 1-5, doi: 10.1109/CIACT.2018.8480297.

[18] N. Bhartiya, N. Jangid and S. Jannu, "Biometric Authentication Systems: Security Concerns and Solutions," 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, India, 2018, pp. 1-6, doi: 10.1109/I2CT.2018.8529435.

[19] K. M. Sudar, P. Deepalakshmi, K. Ponmozhi and P. Nagaraj, "Analysis of Security Threats and Countermeasures for various Biometric Techniques," 2019 IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES),

Krishnankoil, India, 2019, pp. 1-6, doi: 10.1109/INCCES47820.2019.9167745.

[20] Y. Sharma, H. Gupta and S. K. Khatri, "An Authentication Model for Online Transactions Using Biometric Security," 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2019, pp. 7-11, doi: 10.1109/ISCON47742.2019.9036284.

[21] Y. Wang, B. Li, Y. Zhang, J. Wu, P. Yuan and G. Liu, "A Biometric Key Generation Mechanism for Authentication Based on Face Image," 2020 IEEE 5th International Conference on Signal and Image Processing (ICSIP), Nanjing, China, 2020, pp. 231-235, doi: 10.1109/ICSIP49896.2020.9339252.

[22] S. Ibrahim, V. K. Shukla and R. Bathla, "Security Enhancement in Smart Home Management Through Multimodal Biometric and Passcode," 2020 International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 2020, pp. 420-424, doi: 10.1109/ICIEM48762.2020.9160331.

[23] A. Vora, C. Paunwala and M. Paunwala, "A Score Level Fuzzy Rule based Multi-Biometric Framework for enhancing security of cloud access scenario," 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Goa, India, 2019, pp. 1-5, doi: 10.1109/ANTS47819.2019.9118019.

[24] A. Vora, C. Paunwala and M. Paunwala, "A Score Level Fuzzy Rule based Multi-Biometric Framework for enhancing security of cloud access scenario," 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Goa, India, 2019, pp. 1-5, doi: 10.1109/ANTS47819.2019.9118019.

[25] P. Deshmukh and S. Mohod, "Biometric Jammer: A Security Enhancement Scheme using SVM Classifier," 2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India, 2020, pp. 1-6, doi: 10.1109/ICRAIE51050.2020.9358289.

[26] S. Mahajan, S. Gupta and A. K. Pandit, "Image Superiority Calculation Meant for Biometric Fake Detection Approach of Fingerprint," 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, 2020, pp. 368-374, doi: 10.1109/CICN49253.2020.9242602.

[27] P. Terhörst, D. Fährmann, N. Damer, F. Kirchbuchner and A. Kuijper, "On Soft-Biometric Information Stored in Biometric Face Embeddings," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 3, no. 4, pp. 519-534, Oct. 2021, doi: 10.1109/TBIOM.2021.3093920.