IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⋇ Impact Factor 7.105 ⋇ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.9650

A Review on Various Machine Learning Approaches for Fingerprint Based Health Information Exchange

Vanajakshi S[1], Hemalatha D[2], Chethana C[3], Bharathi R[4] , Kavana M D [5],Manasvi J Maasthi[6]

Student, Department of Computer Science, Vidhyavardhaka College of Engineering, Mysore, India[1-4]

Assistant Professor, Department of Computer Science, Vidhyavardhaka College of Engineering, Mysore, India[5]

Assistant Professor, Department of Computer Science, Vidhyavardhaka College of Engineering, Mysore, India[6]

Abstract: The personal health records (PHR) is created for personal health information and it provides easy access to a wide range patients, consumers, practitioners and healthcare providers. However, improved accessibility of PHR threatening confidentiality, privacy, and personalized health information security. The concept of biometrics is currently used for healthcare provider's technology to prevent unauthorized access to the individual health data. We are implementing a biometric mechanism which will protect your PHR and makes it easier to control access, Safe exchange of health information. In this article, we have looked at different machine learning approaches to exchange patient information and different biometric identification techniques that provide reliable user authentication to ensure that only authorized persons can access patient health data. In addition, biometric systems can also facilitate remote access to healthcare data by using biometric features as an authentication tool. This paper summarizes the studies conducted on fingerprint matching techniques, their recognition methods and performance analysis. 0.1% to 0.01% way FAR(false acceptance rate),FP(finger print) can be classified as spiral, straight ring, arc, tent arch etc. To ensure the performance of finger print recognition, advanced algorithms are required to improve the clarity of the input fingerprint image.

Keywords: Fingerprint (FP), Biometrics, Security and Privacy, Patient health information (PHI), Electronic Health (ehealth).

I.INTRODUCTION

eHealth is the Improvement of patient health information (PHI), free to use, improved efficiency and reduces the cost of providing medical services. Patients rarely spend their time with doctor. Despite its advantages, for example Health still comes before a series of security Problems that need to be addressed. eHealth Data Security and Patient privacy are two of the most pressing health challenges in the organizations implementing eHealth deals with it and need to be addressed. The basic idea of information security is at the heart of eHealth security requirements. Maintaining of the confidentiality of eHealth data, Data integrity, data availability, users Authentication and patient privacy are everything concerns that need to be addressed in some cases about protecting eHealth applications and their communication components. In this context, ensure a trusted user authentication is the basis of Implementation of all other measures.

According to risk of loss, theft or oblivion, inappropriate traditional authentication, username and password access cards are not suitable for eHealth settings. In traditional authentication, the method is not based on a unique person general properties. Biometrics is a basic security technique which assigns a singular ID to an individual Physiological (fingerprint or face) or behavioural characteristics (voice or signature). As a result, bioscience are additional reliable and you'll be able to distinguish one as a licensed person and a cheater ancient authentication method. Reproduction of biometric authentication function is difficult, can't be exchanged or popularized and lost or forgot. In addition, it is the necessary existence of a person to be verified; Difficult to manufacture and unlikely to be manufactured by the user to reject it. Both patients and doctors will benefit from this, providing biometrics and a sense of security and convenient. Health care companies transition from traditional tactics to deployment of biometric technology to maintain against increasing security risks in eHealth security and privacy issues are Public health concerns remain as business, as this article considers. We started checking on emphasize biometrics, an application for addressing parts of eHealth Security and privacy issues. Biometrics User authentication and health application Data encryption is the focus of our research. We are confident that this will create a solid platform for future research in healthcare, data protection and patient privacy protection.

A. *Architecture of Fingerprint Based Health Information Exchange*

The fingerprint based health information exchange allows the patients to control access to electronic medical record and maintains confidentiality and security of medical data. It is ensured by authorized individual biometrics-based validation, medical care is enhanced by centralized real-time sharing of medical data, facilitating physician decisions. The classification steps for biometric authentication indicated in Figure 1a.

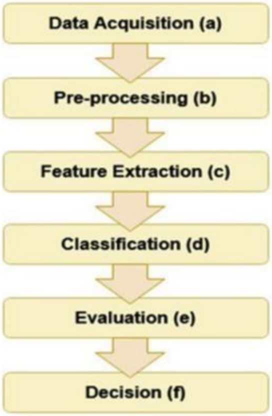

Fig. 1. Classification steps for the biometric authentication

There are four important mechanisms in the biometric system which are divided into five modules.

The first module is the biometric sensor, which collects the user's biometric information. It is the interface between the real world and the biometric system. In second mode, we capture biometric information related to a user's specific region. All necessary pre-processing of the image is done in the next module. The third module is the feature extractor. This is the module where the biometric information received by the sensor is processed to extract feature values. This includes removing arti facts introduced by the sensor, enhancing the input, or even normalizing if needed. The fourth module is where the pairing is done. The subject's values are evaluated against the values contained in the biometric template to calculate the match score. This is an important module where precise area specific Characteristics are optimally extracted. Attribute specific images are used to generate biometric templates. A biometric pattern is a digital pattern that is a binary representation of specific points in a specific region of the finger.The fifth module is where decision making happens. This is where a user's identity is established or a claim is accepted or denied based on information from the previous module.

II. LITERATURE SURVEY

In this section a literature review on various methods of health information exchange is discussed.

A. Ibrahim K et al. proposed vehicle security system is based on driver's license and fingerprint technology. This method protects your vehicle from theft and travel without a valid driver's license. It provides vehicle security by allowing access to the vehicle using biometrics such as a fingerprint scanner. The GSM module needs to send an SMS to the driver's license owner. This system is designed to operate in real time [1].

B. Trupthi Shah et al. proposed the most effective tools for a girl to defend herself is that the planned style for Biometric self-protection device with GSM alerts and GPS tracking. This study presents an formula for developing a women' security app. The projected system saves a user' fingerprint as a model and assigns an id RANGE TO it. Throughout the popularity process, they keep fingerprint and its id number are compared to the user' fingerprint. If it matches, the microcontroller can send a message to the sim 808 module, in conjunction with the position [2].

C. Ambrose A.Azeta et al. proposed a medical institution data control machine that makes use of fingerprint biometrics for authentication. In order to assemble a prototype fitness data machine, they used plenty of technology including machine layout and modelling, the use of the Unified Modelling Language (UML), information control, biometrics, and laptop programming. They've additionally deployed a HIMS on the way to use a password as authentication for any current affected person records. A unified health database with privacy policies has been accessed via biometric identification [3].

D. Lazaurus Kwao et al. proposed a biometric application, which is a real-time application in associate ehealth system that presents a study and economical theme for user verification. Problems appreciate system quality and preparation time related to the usage of those bioscience are considered. They used native trivialities options for user authentication during this study, employing a quick stereo matching technique to check the minutiae features, to compare the fingerprint with minutiae features derived from a gallery of fingerprints so as to verify a person. The proposed approach achieves a machine potency and a balance between computational efficiency and verification method correctness [4].

E. Aman Attrish et al. proposed a contactless fingerprint identification system that uses image sensors to collect finger photographs from a considerable distance. Following that, the collected finger images are processed forward to produce global and local minutiae based characteristics. To extract global properties from a given finger image, a Siamese convolutional neural network (CNN) is created. The suggested approach uses CNN based features and minutiae-based features to calculate the matching score. Finally, the two scores are combined to get a final matching score between the collected fingerprint and the reference fingerprint templates. The Nvidia Jetson Nano development kit was utilized to create this system, which can conduct contactless recognition in real-time with minimal latency and acceptable accuracy [5].

F. Kaoru uchida et al. proposed a fingerprint detection technologies that included a traditional prism-type optical sensor and a solid state sensor. Prism optical sensors are commonly utilized in capture devices. A finger placed on a prism is illuminated by led light, and the reflected picture is collected by a small optical sensing device. this device is based on the frustrated total internal reflection principle (fir).the degree of reflectance at a specific location on a finger varies depending on how far away it is from the prism surface. This is the ridge pattern obtained as a grey-level image. In this fingerprint identification, they applied two methods: picture rectification and structural feature matching. the image correlation method is based on global pattern matching between an enrolled fingerprint and the matching fp.fingerprint identification algorithms like “minutia relation matching” based on ridge counting, correlation, feature-based approaches and fingerprint authentication based on individual fmr (false match rate)[6].

G. Joseph kobina panford et al. proposed a biometric application, which is a real time application in health care system which presents a study and economical theme for user verification exploitation fingerprint biometrics. They used a neighborhood trivialities options for user authentication and used stereo matching algorithmic rule to match the minutiae features of the fingerprint to hold on fingerprints within the gallery to verify a person. This leads to a trade-off between the computation potency and also the accuracy of the verification process [7].

H. Mozammel chowdary et al. proposed biometric authentication system can be used to control access to an electronic healthcare system in a variety of healthcare settings. They authenticate a person by comparing minute information retrieved from test fingerprints with features of database fingerprints using the matching score matrix (msm) approach. in linear search, the matching score strategy can reduce the number of matching comparisons. The algorithm's primary concept is that the similarity between any two fingerprint templates is calculated in advance, and the matching scores are used to compare them to the input image. This application protects the healthcare system from illegal access while providing privacy and security at the same time [8].

I. Y.n. shin et al.proposed a healthcare system that uses fingerprints as biometric access control for electronic medical records to eliminate token-based access such as passwords, digital signatures, flash drives, and smartphone tokens [9].

J. Vedanthi Suhas Mahulkar et al. proposed fingerprint-based patient system was developed as part of the proposed system for storing, monitoring, and analyzing patient medical records. This employs the AES algorithm, which gives complete specifications and design information, as well as the MDS algorithm, which was created to authenticate signatures. The digital technology uses a fingerprint scanner to retrieve patient information from the system, allowing users to access hospital information at any time. Both researches used fingerprint recognition to search for patient information from central databases [10].

III.COMPARITIVE STUDY

In this section we briefly discuss existing literature review on health Information Exchange and also discuss various methods applied along with the limitations

Sl No	Author	Methodology	Advantages	Disadvantages
1	Ibrahim K Adalgader et al.[1] (2020)	Usage RFID automatic identification technology	Usage RFID automatic identification technology. It provides an additional layer of protection. To provide entry to the car, the system uses biometry within the variety of fingerprint recognition	Some users are unable to enrol in the system.

2	Trupti shah et al.[2] (2019)	Usage of Minutiae-based Using IOT device and HVLC circuit	Every individual has distinct personal characteristics that help to identify them when authentication is required	People' skin issues have a sway on the system' accuracy A
3	Ambrose A.Azeta et al.[3] (2017)	Usage of Unified Modelling Language[UML]	Simpler to spot the patches Passwords, for example, are used to shield laptop systems from unauthorised users while concurrently imparting a fake experience of security	Training time takes longer and it should be trained on High end GPU
4	Lazaurus Kwao et al.[4] (2019)	Usage of minutiae features and Streo matching Algorithm	Low cost	Suffers from security and privacy problems in handling health data
5	Aman Attrish et al.[4] (2021)	Usage of Minutiae based Deep Learning	A contactless fingerprint identification system that uses an image sensor in a suitable setting to capture a finger photo from a distance	The amount of information captured by the image sensor and the quality of the image are both affected by lighting conditions
6	Kaoru Uchida et al.[6] (2005)	Minutiae based Fingerprint User Interface	Fingerprints can be used for user verification as well as system customization based on the preferences of that particular user.	The scope of fingerprint identification technology's possible real-world applications
7	Joseph Kobina Panford et al.[7] (2019)	Stereo matching algorithm	Fingerprints are one-of-akind, and no two people's are alike	Capturing a complete and accurate fingerprint image is challenging due to age.
8	Mozammel Chowdary et al.[8] (2018)	Minutiae based Stereo matching Algorithm	Access manage over healthcare statistics the usage of biometrics can offer the vital protection and privacy	Unauthorized access or hacker assaults can compromise or harm sensitive data in patient health records, potentially exposing personal information

9	Sharmin Jahan et al.[9] (2018)	Matching score matrix[MSM] algorithm	Unauthorized access to the healthcare system is protected by a biometrics authentication technique that protects the system's privacy and security	False positives and inaccuracies, as well as false rejects and accepts, might still happen, prohibiting some users from using the system
10	Vedanthi Suhas Mahulkar et al.[10] (2017)	Advanced encryption standard[AES] MD5 algorithm	Each person's fingerprint is unique, the information gained from it is accurate	Storage space is limited

The above table-1. Provides the comparison of the various methods used in HIE

IV.APPLICATIONS OF FINGERPRINT BASED HEALTH INFRMATION EXCHANGE

Patients are identified based on different traits, ensuring that the right people receive care, leading in a safer and more effective global healthcare environment. Less medical errors, safer prescription procedure and secure patient data transmission among doctors. Decreasing the amount of duplicate health records and the risk of treating the wrong patient, it offers quick access to patients' clinical information.

V.CONCLUSION & FUTURE ENHANCEMENTS

Biometrics may be carried out in one of the kind of fitness-care contexts. The aim of healthcare government to supply higher healthcare offerings at a discounted value has brought about using digital healthcare. When it involves fitness information, there are nevertheless safety and privateness issues. Every day the maximum eHealth safety troubles encompass person authentication, information integrity, information confidentiality, and affected person privatives. Biometrics era addresses the aforementioned safety issues via way of means of permitting customers to authenticate themselves in a stable and truthful manner.

Further research will includes the application of healthcare biometrics reflects a growing global need for healthcare fraud security as well as a requirement to protect patient privacy and healthcare. Identity confirmation and protection will be provided through biometric-based identification systems, which will reduce healthcare fraud while simultaneously boosting privacy and security. By eliminating medical errors, biometric technologies can help in improvement of the healthcare system's operational efficiency, saving expenses, reducing waste, and enhancing patient loyalty. As a result, healthcare institutions and insurers are using biometrics as an identifying tool in the form of electronic health reports (EHRs).

REFERENCES

[1] Sharmin Jahan, Mohammed Chowdhury, Rafiqul Islam. "Robust fingerprint verification for enhancing security in healthcare system", 2017 International Conference on Image and Vision Computing New Zealand (IVCNZ), 2017.

[2] Arwa M. Ali, Heisum M. Awad, Ibrahim K. Abdalgader. "Authenticated Access Control for Vehicle Ignition System by Driver’s License and Fingerprint Technology", 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), 2021.

[3] "Biometrics Applications in e-Health Security: A Preliminary Survey", Lecture Notes in Computer Science, 2015.

[4] Varsha Suri, Bhavna Arora. "A Review on Sentiment Analysis in Different Language", 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), 2021.

[5] S. Khanam and T. Shah, "Self Defence Device with GSM alert and GPS tracking with fingerprint verification for women safety," 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), 2019, pp. 804- 808,doi:10.1109/ICECA.2019.8822114.

[6] Sharmin jahan,mozammel Chowdhury and Rafiqul Islam,” Robust user authentication model for securing electronic healthcare system using fingerprint biometrics”, International Journal of Computers And Application,2018.

DOI: 10.17148/IARJSET.2022.9650

[7] B. M. Nelligani, N. V. U. Reddy and N. Awasti, "Smart ATM security system using FPR, GSM, GPS," 2016 International Conference on Inventive Computation Technologies (ICICT), 2016, pp. 1-5, doi: 10.1109 /INVENTIVE. 2016.7830093.

[8] Vedanthi Suhas madhukar, Priyanka Babu Kachare and Divya Jain, ”Fingerprint Based Patient Information System”, International Journal of Innovative Science and Research Technology, 2017.

[9] J. Park, Y. Yoon, J. Kim and W. Yoo, "Design and implementation of fingerprinting-based broadcasting content identification system," 16th International Conference on Advanced Communication Technology, 2014, pp. 626629,doi:10.1109/ICACT.2014.6779037. [10] D. Shawl. “Biometrics – Implementing into the Healthcare Industry Increases the Security For The Doctors, Nurses, and Patients”. Thesis for Master’s Degree Information Assurance, 2013.

[11] H. Jhaveri, and D. Sanghavi, “Biometric security system and its applications in healthcare”. International Journal of Technical Research and Applications 2014.

[12] A. Aditya Shankar, P.R.K.Sastry, A.L.Vishnu, Ram, A.Vamsidhar “Finger Print Based Door Locking System” International Journal of Engineering and Computer Science ISSN: 2319-7242.

[13] Sharmin Jahan, Mozammel Chowdhury, Rafiqul Islam. "Robust user authentication model for securing electronic system using fingerprint biometrics", International Journal of Computers and Applications, 2018.

[14] Arwa M. Ali, Heisum M. Awad, Ibrahim K. Abdalgader. "Authenticated Access Control for Vehicle Ignition System by Driver’s License and Fingerprint Technology", 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), 2021.

[15] Rinku Datta Rakshit, Dakshina Ranjan Kisku. "Chapter 1 Biometric Technologies in Healthcare Biometrics", IGI Global, 2019.

[16] Sharmin Jahan, Mozammel Chowdhury, Rafiqul Islam. "Robust fingerprint verification for enhancing security in healthcare system", International Journal of Computers and Applications, 2018.

[17] Exclude quotes Off Exclude bibliography On Exclude matches Off 2017 International Conference on Image and Vision Computing New Zealand (IVCNZ), 2017.