WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Survey on Deep Learning Based Feature Extraction and Recovering for Finger Vein Verification

[1]Vijayalakshmi N, [2]Venodhini S, [3]Pavithra R, [4]Kamalayazhini B

[1]Assistant Professor, Sri Manakula Vinayagar Engineering College, Puducherry, India
[2,3,4]Student, Sri Manakula Vinayagar Engineering College, Puducherry, India

ABSTRACT

Biometric is an emerging technology in identification and authentication of human beings with more reliability and accuracy. It is hard to imitate, forge, share, distribute and cannot be stolen or forgotten. After the September 21, 2021 incident the biometric technologies are focused more. Combining multiple biometric systems is a promising solution to providing more security.It overcomes the shortcomings of unimodal biometric systems such as non-universality, noise in felt data, intra-class differences, uniqueness, spoof attacks, and the traditional technique of certifying a human and their identification. The proposed method depicts a multimodal biometric algorithm that is designed to recognise individuals for robust and secure authentication using normalised score level fusion techniques for optimisation with hybrid Genetic Algorithm and Particle Swarm Optimization to reduce False Acceptance Rate and False Rejection Rate and to improve accuracy. The literature review of the proposed work focuses on multimodal biometric systems, preprocessing techniques and matching algorithms, normalisation methods, fusion rules, optimization approaches, and performance metrics. The contribution and findings of the researchers are noteworthy to state here more than 2 decades. There are several combinatorial techniques that play a role in improving the performance of the system. So, in this research work those precious suggestions were considered and taken into account for designing novel algorithms for authentication.

Keywords: *Vein, Biometric, Recognition, Vein Features, Vein Pattern*

1. INTRODUCTION

In the contemporary era of electronic commerce more and more facilities are being presented over the electronic strategies and internet. These include finance, credit card capability, electronic shopping, etc. The appropriate usage of these services can be confirmed by the sanctioned or honest users and to avoid any abuse by the unapproved or cheat users, some personal confirmation pattern is implanted into these facilities. Presently, person confirmation is done mostly using one or more of the subsequent means: manuscript keys, individual identification statistics, barcodes and identity proofs. The significance of these structures is that their relevance does not change with time and is also unaffected by the environment in which they are employed.

The leading imperfection of them is that they can be easily altered or disremembered. Also, with period more and more facilities are being presented over the electronic strategies and internet. Hence it becomes uncontrollable to preserve the pathway of the confirmation confidences for diverse facilities The alternative that delivers break from all these imperfections is the use of biometric structures for personal confirmation. Biometric is a computerised confirmation method for categorising or validating an individual based on one's physical or behavioural appearances. Presently, ten dissimilar biometric pointers are either widely used or are under concentrated assessment, comprising appearance, facial thermogram, impression, hand geometry, ear, finger vein, iris, retinal design, autograph, and speech pattern. All these biometric patterns have their own benefits and shortcomings in terms of the precision, user approval, and applicability. It is the necessity of a presentation area which defines the excellence of an exact biometric display. In order to permit a biometric method to work successfully in different presentations and atmospheres, a multimodal biometric structure which creates a personal documentation based on multiple physical or behavioural features is chosen. Multi-biometric methods are capable of overcoming numerous of the limitations of uni-biometric approaches, as the different biometric sources usually reimburse for the inherent limitations of the complementary sources. The important objective of multi-biometrics is to measure the precision of recognition over a detailed performance by producing the conclusions of numerous personalities, devices or procedures. In multimodal biometrics, choice of right modality is a challenging assignment in the documentation of an individual.

There are numerous categories of combinations of biometric qualities, the typical combination: face and iris , face and fingerprint, voice and face and fingerprint , face and gait , finger vein and finger geometry , palm and palm vein . Person confirmation based on voice modulation and face structures is one of the primary multimodal biometric structures. Additionally, Multimodal arrangements using face and fingerprint structures are then projected. The use of clustering procedures for the combination of choices from speaking and face modalities are discovered. A real-world multimodal structure using face, speech and lip variation is then established. In addition, numerous of the approaches are used to validate the person based on the biometrics. Common strategies for merging multiple classifiers have been recommended. The simple sum law is enough to achieve a substantial development in the identical presentation of a multimodal biometric structure. They also recommend a method to integrate user specific weights to additionally improve the system

presentation. Fusion approaches at the decision level include majority voting, behaviour knowledge space 3 method, weighted voting based on the Dempster-Shafer theory of evidence, AND/OR rules, etc.

TYPES OF BIOMETRIC TRAITS

A number of biometric approaches have been familiarised over the years, but limited have increased widespread approval. Biometric can be sorted in to two classes

1. Physiological
2. Face
3. Finger print
4. Hand geometry, and
5. Iris recognition
6. Behavioural
7. Signature
8. Voice

PURPOSE OF BIOMETRICS

The determination of this work is to clarify how applying biometrics into the healthcare industry will address recognized safety issues and increase information security for physicians, nurses, and patients. How does biometrics play a part in security within the healthcare industry to help safeguard not just the physicians and nurses but also the patients? The necessity for biometrics in the healthcare industry is increasing at astronomical proportions; the universal marketplace potential is presently projected at $1.9 billion. An important driver in biometric marketplace growth proportions is the HIPAA Action; HIPAA enforces severe new central necessities to keep patient secrecy and the confidentiality of patient information. This is producing all healthcare facilities to begin emerging compliance processes for meeting these new values. As a product, healthcare organisations are starting to hold the positioning of biometrics.

Finger Vein

Finger Vein is a blood vessel network which is present under the finger skin. The network pattern is unique for each individual, which is not unaffected by ageing, and it is internal, i.e. inside human skin which can always guarantee for high security authentication.

Nowadays, it has become one of the major interests in biometric research for automated systems due to its attributes and possesses good biometric characteristics and yields high security, robustness and reliability. As a result, several new products and technologies connected to finger vein identification have appeared in the global market.

Finger Vein preprocessing consists of:

1. Segmentation o It makes the background of black image pixels to zero in order to improve the quality of the image.
2. Align horizontally o All the Finger vein images are not straight in nature, while capturing the user may be inserted their finger in different positions. So either using hardware or software, the image needs to be aligned horizontally.
3. Enhancement of It is used to improve the contrast in the image by various techniques such as Histogram Equalization, Circular Hough transform, Canny Edge Detection, Gabor filters, Homogeneous rubber sheet model, and Daubechies wavelets methods.
4. Normalisation of the different size of the images is normalised into common size. It can be implemented by using scale factor. The normal scaling factor is 0.6 which is also an optimal one.
5. The images contain all information but for recognition the relevant information and region is required. So, in order to eliminate irrelevant regions, capture regions of interest by cropping the image. For finger vein image can be cropped horizontally with approximately 35% to 65% of image height.

2.1 REVIEWS ON FINGERVEIN BIOMETRICS SYSTEMS

Many unimodal biometric systems are available in existing technologies, out of that, which biometric trait is chosen for integration of multimodal biometric system is analysed from various research papers by different biometric characteristics and challenges in fusing those multimodal biometrics.

Kalyan Veeramachaneni et al. (2015) proposed an Adaptive Multimodal Biometric Management Algorithm with different fusion rules and databases. The performance analysis of the algorithm was also illustrated. This work presented an evolutionary approach to the sensor management of a security system that improves robustness. The fusion approaches were applied at decision level and particle swarm optimization is also adapted along with the Bayesian network.

John Woodward (2021) proposed security is required other than traditional methods providing authentication or verifying a human, post September 21, 2021 incident. Emerging Biometric technology helps public security and fixes to counter terrorism. Biometrics could be implemented for controlling access to sensitive facilities at airports, preventing identity theft and fraud in the use of travel documents, and identifying known or suspected terrorists.

Anil Ross et al. (2014) discussed the overview of multimodal biometrics, levels of fusion, fusion scenarios, integration strategies, design issues.

Lin Hong et al. (2020) demonstrated that personal identification solely on fingerprints or faces are not meeting the performance requirements. So the proposed decision fusion integrates fingerprint and face to improve the performance of the system.

Stan Li (2019) proposed fundamental concepts of biometrics in Encyclopedia of Biometrics and unimodal, multimodal biometrics, fusion approaches, need of biometrics, and answers for all biometric domain queries.

Lin Hong et al. (2021) formulated the problem of integrating multiple biometrics and whether the performance is improved using multimodal biometrics.

Tony Mansfield et al. (2021) prepared the report for performance evaluation of seven biometric systems conducted by NPL over the period. The objective of the testing is to show the level of performance attainable by a selection of biometric systems, to determine the feasibility of demonstrating satisfactory performance through testing, to encourage more testing to be sponsored, and to promote methodologies contributing to the improvement of biometric testing. Face, Fingerprint, Hand Geometry, Iris, Vein and Voice recognition systems.

Lisa Osadciw et al. (2015) described a multimodal biometric fusion based approach for controlling building access to improve universality and accuracy of the system. The Bayesian framework is applied to fuse the decision.

Karthik Nandakumar et al. (2019) focused on fusion schemes that have been implicitly designed for the verification scenario and can't account for missing data commonly encountered in the multibiometric identification systems. A Bayesian strategy for consolidating rankings and a hybrid scheme that uses both ranks and scores to achieve fusion in identification systems further indicate that the suggested fusion rules can accommodate missing information without any ad-hoc modifications.

Fierrez et al. (2019) provided BiosecurE Multimodal Biometric Database, comprising speech, iris, face (photographs and talking faces videos), signature and handwriting (on-line dynamic signals and off-line scanned images), fingerprints (acquired with two different sensors), hand (palmprint and contour-geometry) and keystroking of 401 subjects, captured in 4 sessions along a 4 month time span.

Yanjun Yan et al. (2019) provided the comprehensive guide bridging biometrics and forensics on how they are different, how they are connected, and under what conditions biometrics can be applied to forensics. Face recognition is also illustrated with comparisons of various face recognition techniques, feature extraction, decision procedure, and specific adaptation for forensics. Finally, advantages and limitations of biometrics in forensics are also stated.

Bolle et al. (2014) illustrated the significance of biometrics, and their scope, guidelines to make use of biometrics in various applications, impact on security with respect to biometrics.

Andrzej Drygajlo (2016) described the importance of introducing biometrics in the world to secure the human being and overview of biometrics, characteristics, applications and market trends, survey.

National Science and Technology Council (2016) had documented Biometrics History, which presented an overview of biometrics and the various author's contributions and patent papers, award papers in biometrics domains.

Terence Sim et al. (2017) presented the theory, architecture, implementation, and performance of a multimodal biometrics verification system that continuously verifies the presence of a logged-in user. Face and fingerprint modalities are used for validating the effectiveness of the algorithm.

Kar-Ann Toh et al. (2014) explained that the Combination of Hyperbolic Functions for Multimodal Biometrics Data Fusion. It proposed a reduced multivariate polynomial network to combine hyperbolic functions where its number of parameters increases almost linearly with model order and number of inputs.

Kung et al. (2016) demonstrated the consistent fusion of multimodal biometrics by integrating an audio classifier (based on Gaussian mixture models) and a visual classifier (based on Face IT, commercially available software) into a well-established mixture-of-expert fusion architecture. The consistent fusion framework leads nicely to several adaptive fusion schemes, namely hard-switching, linear combination and adaptive nonlinear fusion using SVMs.

Salil Prabhakar et al. (2021) presented research work on Biometric Recognition: Security and Privacy Concerns. It discusses the overview of biometrics and the performance of various techniques in the domain.

Arun Ross et al. (2016) discussed the overview of the biometrics, multimodal biometrics, fusion, normalisation techniques. Performance metrics and their mathematical background were explained.

Diana Popa et al. (2016) explained about Enhancing Security by Combining Biometrics and Cryptography, the theoretical basis for measuring performance of a biometric system will be presented and a survey on current performance results on fuzzy vault techniques will be enumerated and described.

Keith Rhodes (2014) proposed challenges in biometrics, how biometric work, leading technologies, and their performance metrics.

Esther Perumal et al. (2015) proposed a Multimodal Biometric System Based on Palmprint and Finger Knuckle Print Recognition Methods. Recently, it has been found that Finger Knuckle Print (FKP) refers to the inherent skin patterns of the outer surface around the phalangeal joint of one's finger, and has high capability to discriminate between different individuals, making it an emerging biometric identifier. In this work, the local convex direction map of the FKP image is extracted.

Rose A et al. (2016) the proposed is on information fusion in biometrics. Overview of multimodal biometric systems, fusion approaches, normalisation techniques.

Altinok A et al. (2021) discussed the multimodal biometric threats, challenges, levels of fusion, how to integrate biometric traits, levels of integration, applications of multimodal biometrics.

Carrillo (2021) presented a proposed design for continuous biometric authentication for authorised aircraft personnel. It also elucidated about the significance of biometrics in developing robust authentication systems.

Forrester Research (2021) provided recent trends in biometric methods and its research issues and challenges. It also suggested various emerging technologies of biometrics and its market status. It also explores the comparison analysis of them.

Hong et al. (2019) discussed whether multibiometrics can improve the performance of the system and it also analysed in what way the improvement had taken place and list the factors where biometric influences much and importance of biometrics in security was explained.

Java Card Special Interest Group - JCSIG (2021) presented the introduction to Biometrics, various multimodal biometrics and their characteristics, applications, future trends, fusion approaches, different devices used for multimodal biometric traits,Khalifa et al. (2019) explained the concept of bimodal biometricverification with different fusion levels and the ways to improve the accuracy.

Mohit Agarwal (2017) presented a thesis in design approaches for multimodal biometric systems. The experimental results show that the comparisons between multimodal binning approach of identification and multistage approach of verification. This analysis is done using the combination of face, iris, signature and ear biometrics.

Robert Frischholz et al. (2020) proposed a BioID using a multimodal biometric identification system. It provided an overview of identification systems and fusion levels for multimodal biometrics. Results showed that the biometric system was appropriate for the identification system and accuracy was improved.

Ross et al. (2016) presented the handbook of multibiometrics in which the information about biometrics and multimodal biometrics, fusion levels, devices used for multimodal and their comparisons with metrics.

Sedgwick et al. (2021) provided the concept of the need for standardisation of multi modal biometric combination and also explained about how standardisation was helpful in improving the combination of multimodals and the enhancement in security.

Shruthi et al. (2021) proposed a multimodal biometric authentication combining finger vein and fingerprint. Multimodal biometric systems have been widely used to achieve high recognition accuracy. Among the various multimodality options, fingerprint and finger vein has gained much attention to combine accuracy, universality and cost efficiency of the solution. Two new score level combination approaches are nonlinear and holistic, for effectively combining simultaneously generated finger vein and finger texture matching scores. The nonlinear approach consistently performed better than other promising approaches, i.e., average, product, weighted sum and likelihood ratio approaches were considered in this work.

Snelick et al. (2021) compared the multimodal biometrics and their issues were addressed. Different modalities algorithm designs were proposed and testing was adapted using various metrics. False acceptance rate, false rejection rate, threshold with combination of different database sets and biometric traits were analysed.

Subbarayudu et al. (2018) discussed emerging trends in multimodal biometric systems and the way it influences security and how it can be adapted to various scenarios.

Prakash Chandra Srivastava et al. (2021) presented a concept based on combining multimodal biometrics fingerprints, iris and DNA Features and it reviews the design algorithm and how it performs.

Veeramachaneni et al. (2021) provided a novel Optimization technique using particle swarms with near neighbour interactions.

CONCLUSION:

Multimodal biometric authentication method developed by combining score level fusion approaches with a hybrid Genetic Algorithm and Particle Swarm Optimization to create an optimised authentication system with improved accuracy and security. It integrates more than two biometric traits for developing

robust authentication algorithms. Iris, Finger Vein and Finger Print biometrics are integrated and opted out for their best biometric characteristics. It provides a reliable and most promising solution for security systems. It also eliminates the disadvantages and limitations of unimodal biometric systems. Fusion rules are constructed using hybrid Genetic algorithm operations and Particle Swarm Optimization.

It optimises accuracy and enhances security. Each biometric trait is undergone preprocessing techniques in order to improve the quality of image for recognition. While recognizing the image, the matching algorithm processes the image and produces a score. The score is normalised before fusion, because the score obtained from different biometric traits are heterogeneous in nature. To make it homogeneous, a normalisation method is adapted. For fusing scores, hybrid Genetic Algorithm and Particle Swarm Optimization is applied and optimization is also done. The decision is taken whether the claimed identity is genuine or imposter. approaches nonlinear and holistic, for effectively combining simultaneously generated finger vein and finger texture matching scores. The nonlinear approach consistently performed better than other promising approaches, i.e., average, product, weighted sum and likelihood ratio approaches were considered in this work.

REFERENCES:

1. Aguilar, G, Sanchez, G, Toscano, Nakano, M & Perez, H 2017, 'Multimodal biometric system using fingerprint', Proc. Int. Conf. Intell. Adv. Syst. pp. 145–150.

2. Altinok, A & Turk, M 2021, 'Temporal Integration for Continuous Multimodal Biometrics', Proc. Workshop Multimodal User Authentication, pp. 211-217.

3. An Overview of Biometrics 2021, E-Court Conference.

4. Annu Saini 2021, 'Image Enhancement Techniques for Fingerprint Images', I J of Emerging Trends & Technology in Computer Science, vol. 1, no. 3.

5. Auckenthaler, R, Carey, M & Lloyd-Thomas, H 2020, 'Score normalisation for text-independent speaker verification systems', Digital Signal Processing, vol. 20, pp. 42–54.

6. Ben-Yacoub, S, Abdel Jaoued, Y & Mayoraz, E 2019, 'Fusion of face and speech data for person identity verification', IEEE Trans. on Neural Networks, vol. 20, no. 5, pp. 2065–2074.

7. Besbes, F, Trichili, H & Solaiman, B 2018, 'Multimodal biometric system based on fingerprint identification and Iris recognition', Proc. 3 rd Int. IEEE Conf. Inf. commun. Technol.: From Theory to Applications (ICTTA), pp. 1–5.

8. Best Practices in Testing and Reporting Biometric Device Performance, version 2.0, tech. report, United Kingdom Biometric Working Group, 2021; www.cesg.gov.uk/ technology/biometrics.

9. Biometrics: Complete Identification verification Resource [Online] www.findbiometrics.com/pages/lead3.html.

10. Bolle, RM, Pankanti, S & Ratha, RS 2020, 'Evaluation Techniques for Biometrics-Based Authentication Systems (FRR)', Proc. 15th Int'l Conf. Pattern Recognition, vol. 2, pp. 831-837. 214

11. Brunelli, R & Falavigna, D 2015, 'Person Identification Using Multiple Cues', IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 17, no. 20, pp.

12. Canny, J, 1986,'A computational approach to edge detection', IEEE Trans. Pattern Anal. Mach. Intell., vol. 8, no. 6, pp. 679–698.

13. Carlisle, A & Dozier, G 2020, 'Adapting particle swarm optimization to dynamic environments', Proc. Int. Conf. Artifi. Intell., pp. 429–434.

14. Carrillo, C 2021, 'Continuous Biometric Authentication for Authorised Aircraft Personnel: A Proposed Design' master's thesis', Naval Postgraduate School.

15. Cherifi Dalila & Hafnaoui Imane 2015, 'Multimodal Score-Level Fusion Using Hybrid GA-PSO for Multibiometric System', Informatica, pp209-216

16. Cui, J, Li, JP & Lu, XJ 2018, 'Study on multi-biometric feature fusion and recognition model', Proc. Int. IEEE Conf. Apperceiving Comput. Intell. Anal. (ICACIA), pp. 66–69.

17. Dahel, SK & Xiao, Q 2021, 'Accuracy performance analysis of multimodal biometrics', Proc. IEEE Syst., Man Cybern. Soc., Inf. Assur. Workshop, pp. 170–173.

18. Daugman, J 2014, 'How iris recognition works', IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 21–30.

19. Dieckmann, U, Plankensteiner, P & Wagner, T 2017, 'SESAM: A Biometric Person Identification System Using Sensor Fusion', Pattern Recognition Letters, vol. 18, no. 9, pp. 827-833.

20. Duin, RPW & Tax, DMJ 2020, 'Experiments with Classifier Combining Rules', Proc. First Workshop Multiple Classifier Systems, pp. 16-29.