Direct Research Journal of Engineering and Information Technology
Vol. 9 (4), Pp. 224-231, May 2022
ISSN 2354-4155
DOI: https://doi.org/10.26765/DRJEIT13891196
Article Number: DRJEIT13891196
Author(s) retain the copyright of this article
This article is published under the terms of the
Creative Commons Attribution License 4.0.
http://directresearchpublisher.org/drjeit/

Review paper

Application of Biometric Fusion Strategies in Cybersecurity Applications

Sani Suleiman Isah

Department of Computer Studies, Hassan Usman Katsina Polytechnic, Katsina, Katsina State, Nigeria.
*Corresponding author E-mail: ssmaiadua@gmail.com

Received 13 April 2022; Accepted 19 May 2022; Published 29 May 2022

ABSTRACT: Previous studies that used a biometric fusion technique in the creation of cybersecurity applications are presented in this paper. Because it remains unchanging throughout a human's life and the vein pattern is unique to each human, biometric verification utilizing finger vein has been evaluated as very secure and accurate. Finger vein data cannot be intentionally copied or stolen. Furthermore, finger-vein authentication provides secure and dependable capabilities for an authentication system. Individual finger-knuckle prints have strong discriminative power and can tolerate wear. Researchers have employed it in biometric authentication systems to circumvent security issues. It is a new biometric modality at the user's outer finger surface, which surrounds the phalangeal joint. It also demonstrates how a security system based on finger knuckle prints could be successful. This review covers related works on information granulation techniques (a driving factor of granular computing) and datasets utilized in biometric fusion development research.

Keywords: Cybersecurity, biometrics, finger-vein, finger knuckle-print, fusion

INTRODUCTION

Organizations' reliance on cloud services has peaked as a result of the abandonment of legacy systems in favour of cloud and internet of things (IOT) services. Cybersecurity interventions have significant obstacles in countering vulnerabilities in real time before they materialize, necessitating the use of technologies that will aid in the provision of suitable and resilient solutions, particularly in the context of big data (Tang et al., 2017). Researchers are concerned about such vulnerabilities due to attempted solutions in numerous sectors such as artificial intelligence and machine learning. In recent years, digital assets, smart phones, computer operating systems, protected intellectual property, and devices have all relied on biometric verification and authentication technologies to gain access to them in such a way that genuine and imposters can be identified. Pattern recognition, computer vision, and image processing are examples of biometric-based cybersecurity applications. Physical invasions and security evasion could be challenged by the implementation of better biometric-based systems in a modern cybersecurity system (Abomhara and Kien, 2015). All of these systems have advantages and disadvantages, and eliminating these disadvantages has been an exciting area of research. Table 1 summarizes some unimodal and multimodal cybersecurity studies.

Kour et al. (2016) described how biometric technology is used in cybersecurity systems, with a focus on how multimodal biometrics play a major part in system security (Singh et al. 2019; Carr III, Newtson, and Joshi, 2018; Ahmed et al., 2017; Singh et al. 2019; L eghari et al., 2018).

Vulnerabilities in access control systems are exploited by high-level security applications used for cybersecurity (Li and Liao, 2018). Biometrics are utilized for identity verification and authorization in current access control systems. Due to the uncertainty and complexity of biometric data, the current design of multimodal biometrics for high-level security applications suffers from a lack of effective thresholding techniques and reduced performance (Alpar and Krejcar, 2018).

Biometrics is a part of the security agenda for ensuring information security (Onuiri, Idowu, and Komolafe, 2015). Biometric technologies have been used for identification and verification of human physiological features such as fingerprints, voice, face, and iris for decades (Syazana-Itqan, et al., 2016). Access control, forensic analysis, border security, fraud identity, and terrorism detection and prevention are among situations where biometric technologies have a significant advantage (Shaheed et al., 2018).

Several biometric authentication systems based on human physiological and behavioral characteristics are used, including fingerprint recognition (Galbally et al., 2019), face recognition (Chen et al., 2017), voice recognition (Gupta et al., 2018), iris recognition (Zhao et al., 2018), hand geometry (Gupta and Gupta, 2018), and finger vein recognition (Yang et al., 2018).

The biometric recognition process (Figure 1) begins with the gathering of input data in the form of an image, which is then segmented to identify the focus region. Furthermore, pre-processing for data augmentation occurs, with operations such as noise removal and data alignment conducted. The feature extraction stage follows, in which features are extracted from the pre-processed data using various extraction approaches. Finally, classifiers are utilized for recognition. The recognition might be one-to-one, known as identification, or one-to-many, known as verification. This common method is described in detail in (Bhilare et al., 2018).

Related works

Biometric systems are essential in security applications such as surveillance, access control, military operations, and criminal investigations. Human features are the tools utilized to maximize the utility of biometric technologies. In general, physical and behavioral characteristics can be used to identify human attributes. The physical refers to things like fingerprints, faces, irises, veins, and so on. The behavioral characteristics are voice, stride, signature, and handwriting (Jain et al., 2016).

Biometric technologies are used as recognition systems to replace knowledge or possession-based approaches to identification (such as passwords, access cards, PIN). Unimodal systems are biometric systems that use a single authentication modality. These unimodal systems are used for personal identification, but they have several drawbacks, including the inability to handle high security, the inability to resist spoofing attacks, sensitivity to noisy sensors, and reliance on a single, non-universal property (Walia et al., 2019). Unimodal systems are particularly unreliable due to these limits. To address the shortcomings of unimodal systems, multimodal systems have been intensively investigated.

Multimodal biometric systems or biometric fusion are identified based on utilization and combination of different source of information. These multimodal systems are regarded as effective in security applications and more reliable under dynamic conditions. The limitations of unimodal system have been tackled by multimodal approaches due to combination of several participating components from the sensors, instances, algorithms, samples and biometrics. In (Walia et al., 2019), the authors combined fingerprint, iris and finger-vein to provide optimal recognition under dynamic condition.

Even though multimodal systems have been proven to supersede unimodal systems due to strong ability to counter spoofing attacks, and exhibit high reliability and robustness over certain vulnerabilities evident in unimodal systems, they are also facing some limitations, such as user-inconvenience, high cost, high computational demand, high processing time and high storage demand. These makes the choice of modalities of close proximity more preferred as a balance between user-convenience and effective security (Ajay Kumar and Kumar, 2016).

The literature on the use of unimodal biometric systems such as fingerprints, face, and voice has proven its limitations. While multimodal biometric systems are still in the early stages due to intra and intermodal integration, as shown in Table 2, (Wild et al., 2016). This study takes into account two physiological biometric traits: finger vein and finger knuckleprint, which are briefly detailed in the following subsections.

Biometric fusion strategies in cybersecurity applications development

Cybersecurity, also known as control system security (Ye et al., 2015), has evolved over time from a biometric fusion standpoint. In this regard, notable literatures include (Adámek, Matsek, and Neumann, 2015; Condon and Willatt, 2018; Fujita et al., 2018; Gupta et al., 2018; Ogbanufe and Kim, 2018). The adoption of biometric fusion techniques has given rise to optimism regarding the security of cybersecurity applications such as financial, medical, immigration, and smartphone data (Leghari et al., 2018). Table 3 contains a table that describes different biometric fusion strategies.

Sources of biometric fusion

Fusion of biometrics arises from sources that reflect what to combine in order to improve the recognition process. According to the source, the following are the described configurations that fusion can be used as a solo or in combination: I multiple sensor combinations (ii) multiple algorithms combinations (iii) multiple instances combinations (iv) numerous samples combinations and (v) multiple modalities combinations (Singh et al., 2019).

Levels of biometric fusion

Biometric fusion occurs at several stages of the authentication process, including sensor-level, feature-

level, matching score-level, and decision-level. However, as the process progresses, the amount of information decreases, making the fusion strategy less effective at that level. As a result, fusion at the matching score level with proper classifiers is critical in determining the optimal result (Nappi et al.,2018). The aforementioned levels of fusion are explored in the following subsections, along with the benefits and limitations of fusion at such levels.

Sensor level biometric fusion

This is the initial level considered for biometric fusion; it also falls under the category of the authentication process's pre-classification stage. Among those who have considered this stage for fusion are (Bhilare et al., 2018) and (Cvejic et al., 2007). At this point, fusion can occur by joining numerous instances of the same characteristic or by coupling a single instance of a trait to many sensors. The disadvantage of this fusion is that the raw data must be compatible with the sensor.

Finger-vein and finger knuckle-print in biometric fusion strategy

Finger vein as a secured biometric trait

Finger-vein authentication has been ranked as the most secure, with higher accuracy, lower cost, and, most importantly, long-term stability (Shaheed et al., 2018). Both academics and practitioners have found the finger vein characteristic (Miura, Nagasaka, and Miyatake, 2004) to be a particularly appealing biometric pattern identification. Because it remains unchanging throughout a human's life and the vein pattern is unique to each human, biometric verification utilizing finger vein has been evaluated as very secure and accurate. Finger vein data cannot be intentionally copied or stolen. Furthermore, finger-vein authentication provides secure and dependable capabilities for an authentication system (Fang et al., 2018).

Despite its immense promise, finger-vein recognition has difficulties and limits at every level of the recognition process. For example, in the image acquisition stage, the quality of infrared images, which produce optical blurring due to camera proximity, limited texture information, and finger position guidance all have an impact on recognition performance (Hong et al.,2017). Furthermore, associated information from varied widths of the finger muscles, tissues, and bones close to the vein, which is also collected by the near infrared camera, impacts recognition ability (Wenxiong Kang, Yuting Lu, Dejian Li, 2019).
Furthermore, finger vein identification devices are susceptible to spoof attacks (Shaheed et al., 2018). Furthermore, all of the concerns raised are classification problems that occur as a result of the necessity for a robust matching procedure with high recognition performance and accuracy.

Finger-knuckle print (FKP) biometric trait

Individual finger-knuckle prints have excellent discriminative power and have been shown to endure wear (Jaswal, Kaul, and Nath, 2016). Researchers have employed it in biometric authentication systems to circumvent security issues (Ozkaya and Kurat, 2014). It is a new biometric modality at the user's outer finger surface, which surrounds the phalangeal joint. It also demonstrates how a security system based on finger knuckle prints could be successful. FKP is close to finger-vein since they are all in close proximity.

Above all, their combination would meet the requirements for a strong biometric fusion in terms of ease of training, ease of deployment, and scalability (Fierrez et al., 2018). Despite the fact that finger knuckle print has been coupled with other biometric features in past research, there is still room for improvement in terms of identification rate and computational complexity by inventing new algorithms (Jaswal et al., 2016). Table 3 lists some of the researchers who used finger knuckle prints.

Fusion levels

Biometric fusion feature extraction level

Fusion at this level, combines diverse sets of feature acquired from multiple sources. Such fusion is also a pre-classification fusion strategy which either uses algorithms on the acquired features from same biometric trait or different features obtained from different traits. Researches that considered such fusion at this level are many including (Kauba, Uhl, Piciucco, Maiorana, and Campisi, 2016; Khellat-Kihel et al., 2016; Wencheng Yang, Wang, Hu, Zheng, and Valli, 2018; Wencheng Yang, Wang, Zheng, and Valli, 2018). In this level, issue of dimensionality is a serious concern due to higher complexity of the features as well as low flexibility that leads to curse of dimensionality.

Matching score level biometric fusion

This is referred to as the post-classification level of biometric authentication, in which the fusion approach is utilized to fuse the scores given by multiple matching algorithms. Related studies on score level fusion have been addressed in (Grover and Hanmandlu, 2015; Ajay Kumar and Kumar, 2016; Saadat and Nasri, 2016; Walia et al., 2019). The capacity to handle missing information that arises as a result of feature extraction done, as well as matching scores, is the main advantage of fusion at this level. However, this level has its own drawbacks, such as requiring more storage space and processing time. This is the initial level, where numerous classifiers can be utilized

Table 1: Some unimodal and multimodal researches applied in cybersecurity.

Authors	Name	Description	Remarks
(Roberts, 2007)	Biometric attack vectors	A defence and counter measures on security threats	An analysis-based research
(Mary Grace Galterio, 2018)	Biometrics for smart devices	A facial recognition system for authentication in smart devices	A combined system of biometrics and password
(Condon and Willatt, 2018)	A proposed electrocardiogram method.	To aid in the protection of services.	Still at its infancy stage
(Wenming Yang, Huang, Zhou, and Liao, 2014)	Personal identification system.	Uses comparative competitive coding for finger-based traits.	A feature level fusion research marred with heterogeneous data source.
(Ajay Kumar and Kumar, 2016)	Adaptive security management	Ant colony optimization is used for selection of key parameters and thresholding.	It is a generalized framework for any classification problem.
(Raghavendra and Busch, 2016)	Anti-presentation attack system	The system is based on finger vein biometric	Algorithms used in preventing presentation attacks in finger vein recognition.
(Leghari et al., 2018)	Fingerprints and online signature verification system	Multimodal biometrics to avoid data theft and misuse.	The evaluation strategy is based on accuracy only.

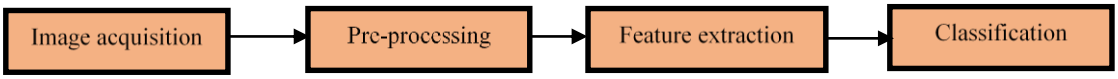

Figure 1: General biometric recognition process

Table 2: Researches that uses finger-vein biometrics in cyber-security settings.

Authors	Name	Description	Remarks
(Miura et al., 2004)	Personal identification based on veins patterns in a finger	Uses line tracking method and achieved 1.45% equal error rate.	Algorithm need improvement due to non-clarity of veins during cold weather
(Sato, 2009)	A finger-vein verification for mobile apparatus	It is directed towards use of enhanced sensors.	A promising authentication method but limited to sensor level
(Ko et al., 2015)	A sensor and matching level application for embedded environments	The method shows the preference of finger-vein method in terms of security and convenience	Even though a simple pattern matching algorithm used has low complexity, the system suffers from acquisition of low quality images.
(He, Li, Chen, and Peng, 2017)	The method uses PCA for image feature extraction	A multiple layer neural network classifier is built.	Feature representation needs simplification and classifier accuracy need to be improved
(Wenxiong Kang, Yuting Lu, Dejian Li, 2019)	It is based on intensity distribution from finger vein tissues	A soft biometric trait recognition based on intensity distribution.	It is based on sensor-level acquisition of images.

to make a final conclusion on the same or separate feature sets (Lumini and Nanni, 2017). For a fusion technique at this level, either a combination approach (which combines normalization scores) or a classification approach (which involves many classifiers) is used. This level of fusion is simpler and offers an advantage over others due to the possibility to use different classification or combining methods for optimal results. Researchers have used a variety of ways for fusion at the score-level of biometric recognition. Sum-rule, SVM, mean score, max score, min score, and likelihood ratio-based score fusions are the most often utilized methodologies.

Decision level biometric fusion

The decisions made by classifiers at the score level are combined at this level. Despite the disadvantage of losing an excessive quantity of information, this level has been used in several studies (Grover and Hanmandlu, 2015; Dwivedi and Dey, 2018).

Table 3: Researches that uses FKP biometrics in cybersecurity settings.

Authors	Name	Description	Remarks
(Amioy Kumar, Hanmandlu, and Gupta, 2013)	Touch-less biometric system	A bimodal knuckle verification system for high security areas.	Suitable for various security applications
(Condon and Willatt, 2018)	Secured authentication using ECG	A more secured internal modality	It is part of the growing market of access and identity management
(Legahari et al. 2018)	Online signature and fingerprint fusion verification	A multimodal approach to make the biometric data safe from theft and misuse	A biometric authentication by combining modalities.
(Gao, Yang, Qian, and Zhang, 2014)	The use of multiple angle and surface texture information of finger knuckleprint	It uses a local binary pattern and multi-level thresholding scheme to perform orientation coding	A score level fusion for improved verification accuracy
(Ogbanufe and Kim 2018)	Biometric authentication for e-payment	Compares biometric versus credit card authentication	Show the need for implementing biometric authentication for e-payments.
(Khellat-Kihel et al., 2016)	A user characteristics based verification system	A best attribute feature selection method was used to reduce memory space	An optimized fusion of finger-based traits.
(Ozkaya and Kurat, 2014)	Personal authentication system using discriminative common vector	It uses discriminative common vector to verify personal identity.	Performance is highly dependent on feature extraction. And also not scalable to large database.
(Nigam, Tiwari, and Gupta, 2016)	A finger knuckleprint biometric authentication system	The authentication process uses fusion of multiple texture features.	Has high computational complexity.

Table 4: Biometric fusion in cyber-security.

Authors	Idea	Description	Remarks
(Walia et al., 2019)	Classifier optimization for multimodal systems	Adaptively used under dynamic security conditions	It is a score-level fusion based on evolutionary algorithm
(Sharma, Das, and Joshi, 2018)	A belief function-based score level technique on unibiometric scores	An efficient Dezert–Smarandache theory (DSmT) score level fusion	Improves support vector machines and sum rule-based score level fusion
(Leghari et al., 2018)	Fusion of fingerprint and online signature to prevent theft and misuse	An online signature verification system through fusion with fingerprint	Difficulty in fusing data at feature level for fingerprint verification
(Amioy Kumar et al., 2013)	Ant colony optimization based bimodal verification system	It uses fuzzy sets for finger knuckleprint verification	A fuzzy-based classification technique with ACO optimization
(Grover and Hanmandlu, 2015)	Fusion at score and decision levels for finger knuckleprint authentication	A hybridization method to strengthen individual fusion methods	A promising hybrid of a unimodal biometric trait.

Challenges in biometric fusion

The inability to determine the optimal fusion strategy as well as predicting a sustainable sources of biometric information, makes it a challenging process. These challenges arise as a result of the following

Heterogeneous data

Most especially at pre-classification stages of sensor-level and feature extraction level, heterogeneity is a major concern. Therefore, integrating of heterogeneous raw data at sensor level or extracted features at feature extraction

level is very difficult. More so, biometric fusion at score level often encounter heterogeneous data which is challenging (Dwivedi and Dey, 2018).

Fusion complexity

Additional effort, such as building new algorithms to accommodate incompatible sources of information and to deal with noise in the data, might result in the fusion method being more complex. Because of the trade-off between information availability and fusion complexity, many researchers prefer score level fusion (Tran and Liatsis, 2016).

Matcher discrimination ability

When there is a disparity in the power of the matching algorithms, optimal accuracy may not be obtained. As one algorithm is more powerful than another in terms of producing higher accuracy, their combination is likely to effect the achievement of higher accuracy when compared to singular usage (Chowdhury et al.,2018).

Conflicting performance requirements

When requirements such as accuracy and throughput need to be satisfied, then conflict may arise in achieving the trade-off between the two. These four factors, including others such as the impact of correlation between biometric sources, make biometric fusion to still be an active and interesting area of research.

Advantages of biometric fusion

Biometric fusion can be advantageous in the following form:

Since biometric fusion uses combined evidence from different information sources, this will strengthen and improve accuracy.

Combination of different modalities will guarantee flexibility and dynamics of the biometric systems towards identification and verification.

An effective fusion scheme can be scalable to large databases.

It is more resistant to spoof attacks as a result of fusing relevant mechanisms to improve the template security.

Disadvantages of biometric fusion

Because of the small training sample size, biometric fusion can become increasingly difficult. It may also be less accurate than non-fused approaches if a proper fusion procedure is not applied. Furthermore, any fusion solution must have an accurate measurement of recognition rate, ease of training, ease of implementation, and scalability (Grover and Hanmandlu, 2015).

Conclusion

This paper discusses relevant research on cybersecurity, biometrics, and biometric methods in cybersecurity. The impetus for this research was the recurrent breach in cybersecurity applications from the standpoint of biometric systems. The literature has reinforced the view that effective biometric fusion approaches will not only improve but also provide robust cybersecurity applications to combat unpredictable and imprecise consistent attacks.

ACKNOWLEDGEMENTS

The author acknowledges the support by Hassan Usman Katsina Polytechnic, Universiti Teknologi Malaysia for providing the enabling ground to undertake this research.

REFERENCES

Abomhara, M., and Kien, G. M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility, 4(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414

Adámek, M., Matýsek, M., and Neumann, P. (2015). Security of biometric systems. Procedia Engineering, 100(January), 169–176. https://doi.org/10.1016/j.proeng.2015.01.355

Ahmed, E., Deluca, B., Hirowski, E., Magee, C., Tang, I., and Coppola, J. F. (2017). Biometrics: Password replacement for elderly? 2017 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2017, 1–6. https://doi.org/10.1109/LISAT.2017.8001958

Alpar, O., and Krejcar, O. (2018). Online signature verification by spectrogram analysis. Applied Intelligence, 48(5), 1189–1199. https://doi.org/10.1007/s10489-017-1009-x

Bhilare, S., Jaswal, G., Kanhangad, V., and Nigam, A. (2018). Single-sensor hand-vein multimodal biometric recognition using multiscale deep pyramidal approach. Machine Vision and Applications, 29(8), 1269–1286. https://doi.org/10.1007/s00138-018-0959-2

Carr III, L., Newtson, A., and Joshi, J. (2018). Towards Modernizing the Future of American Voting. 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), 130–135. https://doi.org/10.1109/CIC.2018.00028

Chen, Z., Huang, W., and Lv, Z. (2017). Towards a face recognition method based on uncorrelated discriminant sparse preserving projection. Multimedia Tools and Applications, 76(17), 17669–17683. https://doi.org/10.1007/s11042-015-2882-0

Chowdhury, A., Atoum, Y., Tran, L., Liu, X., and Ross, A. (2018). MSU-AVIS dataset: Fusing Face and Voice Modalities for Biometric Recognition in Indoor Surveillance Videos. Proceedings - International Conference on Pattern Recognition, 2018-Augus, 3567–3573. https://doi.org/10.1109/ICPR.2018.8545260

Condon, A., and Willatt, G. (2018). ECG biometrics: the heart of data-driven disruption? Biometric Technology Today, 2018(1), 7–9. https://doi.org/10.1016/S0969-4765(18)30011-0

Cvejic, N., Nikolov, S. G., Knowles, H. D., ŁOza, A., Achim, A., Bull, D. R., and Canagarajah, C. N. (2007). The effect of pixel-level fusion on object tracking in multi-sensor surveillance video. Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition. https://doi.org/10.1109/CVPR.2007.383433

Dwivedi, R., and Dey, S. (2018). A novel hybrid score level and decision

level fusion scheme for cancelable multi-biometric verification. Applied Intelligence, 1016–1035. https://doi.org/10.1007/s10489-018-1311-2
Fang, Y., Wu, Q., and Kang, W. (2018). A novel finger vein verification system based on two-stream convolutional network learning. Neurocomputing, 290, 100–107. https://doi.org/10.1016/j.neucom.2018.02.042
Fierrez, J., Morales, A., Vera-Rodriguez, R., and Camacho, D. (2018). Multiple classifiers in biometrics. part 1: Fundamentals and review. Information Fusion, 44(November 2017), 57–64. https://doi.org/10.1016/j.inffus.2017.12.003
Fujita, H., Gaeta, A., Loia, V., and Orciuoli, F. (2018). Resilience Analysis of Critical Infrastructures: A Cognitive Approach Based on Granular Computing. IEEE Transactions on Cybernetics, PP(March), 1–14. https://doi.org/10.1109/TCYB.2018.2815178
Galbally, J., Haraksim, R., and Beslay, L. (2019). A Study of Age and Ageing in Fingerprint Biometrics. IEEE Transactions on Information Forensics and Security, 14(5), 1351–1365. https://doi.org/10.1109/TIFS.2018.2878160
Gao, G., Yang, J., Qian, J., and Zhang, L. (2014). Integration of multiple orientation and texture information for finger-knuckle-print verification. Neurocomputing, 135, 180–191. https://doi.org/10.1016/j.neucom.2013.12.036
Grover, J., and Hanmandlu, M. (2015). Hybrid fusion of score level and adaptive fuzzy decision level fusions for the finger-knuckle-print based authentication. Applied Soft Computing Journal, 31, 1–13. https://doi.org/10.1016/j.asoc.2015.02.001
Gupta, D., Bansal, P., and Choudhary, K. (2018). The State of the Art of Feature Extraction Techniques in Speech Recognition. In S. S. Agrawal, A. Devi, R. Wason, and P. Bansal (Eds.), Speech and Language Processing for Human-Machine Communications (pp. 195–207). Singapore: Springer Singapore.
Gupta, P., and Gupta, P. (2018). Multibiometric authentication system using slap fingerprints, palm dorsal vein, and hand geometry. IEEE Transactions on Industrial Electronics, 65(12), 9777–9784. https://doi.org/10.1109/TIE.2018.2823686
He, C., Li, Z., Chen, L., and Peng, J. (2017). Identification of finger vein using neural network recognition research based on PCA. Proceedings of 2017 IEEE 16th International Conference on Cognitive Informatics and Cognitive Computing, ICCI*CC 2017, 456–460. https://doi.org/10.1109/ICCI-CC.2017.8109788
Hong, H. G., Lee, M. B., and Park, K. R. (2017). Convolutional neural network-based finger-vein recognition using NIR image sensors. Sensors (Switzerland), 17(6). https://doi.org/10.3390/s17061297
Jain, A. K., Nandakumar, K., and Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters, 79, 80–105. https://doi.org/10.1016/j.patrec.2015.12.013
Jaswal, G., Kaul, A., and Nath, R. (2016). Knuckle Print Biometrics and Fusion Schemes -- Overview, Challenges, and Solutions. ACM Computing Surveys, 49(2), 1–46. https://doi.org/10.1145/2938727
Kauba, C., Uhl, A., Piciucco, E., Maiorana, E., and Campisi, P. (2016). Advanced variants of feature level fusion for finger vein recognition. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI), P-260. https://doi.org/10.1109/BIOSIG.2016.7736908
Khellat-Kihel, S., Abrishambaf, R., Monteiro, J. L., and Benyettou, M. (2016). Multimodal fusion of the finger vein, fingerprint and the finger-knuckle-print using Kernel Fisher analysis. Applied Soft Computing Journal, 42, 439–447. https://doi.org/10.1016/j.asoc.2016.02.008
Ko, K. W., Lee, J., Ahmadi, M., and Lee, S. (2015). Development of human identification system based on simple finger-vein pattern-matching method for embedded environments. International Journal of Security and Its Applications, 9(5), 297–306. https://doi.org/10.14257/ijsia.2015.9.5.29
Koteswari, S., Paul, P. J., Dheeraj, A., and Kone, R. (2016). Fusion of Iris and Fingerprint Biometric Identifier for ATM Services: An Investigative Study. International Journal of Communications, Network and System Sciences, 09(11), 506–518. https://doi.org/10.4236/ijcns.2016.911040
Kour, J., Hanmandlu, M., and Ansari, A. Q. (2016). Biometrics in cyber security. Defence Science Journal, 66(6), 600–604. https://doi.org/10.14429/dsj.66.10800.
Kumar, Ajay, and Kumar, A. (2016). Adaptive management of multimodal biometrics fusion using ant colony optimization. Information Fusion, 32, 49–63. https://doi.org/10.1016/j.inffus.2015.09.002.
Kumar, Amioy, Hanmandlu, M., and Gupta, H. M. (2013). Ant colony optimization based fuzzy binary decision tree for bimodal hand knuckle verification system. Expert Systems with Applications, 40(2), 439–449. https://doi.org/10.1016/j.eswa.2012.07.042.
Kumar, Amioy, Hanmandlu, M., Sanghvi, H., and Gupta, H. M. (2010). Decision level biometric fusion using ant colony optimization. Proceedings - International Conference on Image Processing, ICIP, 3105–3108. https://doi.org/10.1109/ICIP.2010.5654019.
Leghari, M., Memon, S., and Chandio, A. A. (2018). Feature-level fusion of fingerprint and online signature for multimodal biometrics. 2018 International Conference on Computing, Mathematics and Engineering Technologies: Invent, Innovate and Integrate for Socioeconomic Development, ICoMET 2018 - Proceedings, 2018-Janua, 1–4. https://doi.org/10.1109/ICOMET.2018.8346358.
Li, Z., and Liao, Q. (2018). Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. Government Information Quarterly, 35(1), 151–160. https://doi.org/10.1016/j.giq.2017.10.006.
Liu, C. (2013). A new finger vein feature extraction algorithm. Proceedings of the 2013 6th International Congress on Image and Signal Processing, CISP 2013, 1(Cisp), 395–399. https://doi.org/10.1109/CISP.2013.6744026.
Lu, Y., Yoon, S., Xie, S. J., Yang, J., Wang, Z., and Park, D. S. (2014). Finger vein recognition using generalized local line binary pattern. KSII Transactions on Internet and Information Systems, 8(5), 1766–1784. https://doi.org/10.3837/tiis.2014.05.015.
Lumini, A., and Nanni, L. (2017). Overview of the combination of biometric matchers. Information Fusion, 33, 71–85. https://doi.org/10.1016/j.inffus.2016.05.003.
Mary Grace Galterio, S. A. S. and T. H. (2018). A Review of Facial Biometrics Security for Smart Devices. Computers. https://doi.org/10.3390/computers7030037
Mezai, L., and Hachouf, F. (2015). Score-Level Fusion of Face and Voice Using Particle Swarm Optimization and Belief Functions. IEEE Transactions on Human-Machine Systems, 45(6), 761–772. https://doi.org/10.1109/THMS.2015.2438005
Miura, N., Nagasaka, A., and Miyatake, T. (2004). Feature extraction of finger vein patterns based on iterative line tracking and its application to personal identification. Systems and Computers in Japan, 35(7), 61–71. https://doi.org/10.1002/scj.10596
Mohamad, N., Ahmad, M. I., Ngadiran, R., Ilyas, M. Z., Isa, M. N. M., and Saad, P. (2014). Investigation of information fusion in face and palmprint multimodal biometrics. 2014 2nd International Conference on Electronic Design, ICED 2014, 347–350. https://doi.org/10.1109/ICED.2014.7015828.
Mohd Asaari, M. S., Suandi, S. A., and Rosdi, B. A. (2014). Fusion of Band Limited Phase only Correlation and Width Centroid Contour Distance for finger based biometrics. Expert Systems with Applications, 41(7), 3367–3382. https://doi.org/10.1016/j.eswa.2013.11.033.
Nappi, M., Ricciardi, S., and Tistarelli, M. (2018). Context awareness in biometric systems and methods: State of the art and future scenarios. Image and Vision Computing, 76, 27–37. https://doi.org/10.1016/j.imavis.2018.05.001.
Nigam, A., Tiwari, K., and Gupta, P. (2016). Multiple texture information fusion for finger-knuckle-print authentication system. Neurocomputing, 188, 190–205. https://doi.org/10.1016/j.neucom.2015.04.126
Ogbanufe, O., and Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. Decision Support Systems, 106, 1–14. https://doi.org/10.1016/j.dss.2017.11.003.
Onuiri, E. E., Idowu, S. A., and Komolafe, O. (2015). Electronic Health Record Systems and Cyber- Security Challenges. International Conference on African Development Issues, 98–105.
Ozkaya, N., and Kurat, N. (2014). Discriminative common vector based finger knuckle recognition. Journal of Visual Communication and Image Representation, 25(7), 1647–1675. https://doi.org/10.1016/j.jvcir.2014.08.003.
Park, K. R. (2011). Finger vein recognition by combining global and local features based on SVM. Computing and Informatics, 30(2), 295–309.

Peng, J., Li, Y., Li, R., Jia, G., and Yang, J. (2014). Multimodal Finger Feature Fusion and Recognition Based on Delaunay Triangular Granulation. In S. Li, C. Liu, and Y. Wang (Eds.), Pattern Recognition (pp. 303–310). Berlin, Heidelberg: Springer Berlin Heidelberg.

Pisani, P. H., Poh, N., de Carvalho, A. C. P. L. F., and Lorena, A. C. (2017). Score normalization applied to adaptive biometric systems. Computers and Security, 70, 565–580. https://doi.org/10.1016/j.cose.2017.07.014.

Raghavendra, R., and Busch, C. (2016). Presentation Attack Detection Algorithms for Finger Vein Biometrics: A Comprehensive Study. Proceedings - 11th International Conference on Signal-Image Technology and Internet-Based Systems, SITIS 2015, 628–632. https://doi.org/10.1109/SITIS.2015.74.

Raghavendra, R., Dorizzi, B., Rao, A., and Hemantha Kumar, G. (2011). Designing efficient fusion schemes for multimodal biometric systems using face and palmprint. Pattern Recognition, 44(5), 1076–1088. https://doi.org/10.1016/j.patcog.2010.11.008.

Roberts, C. (2007). Biometric attack vectors and defences. Computers and Security, 26(1), 14–25. https://doi.org/10.1016/j.cose.2006.12.008

Saadat, F., and Nasri, M. (2016). A multibiometric finger vein verification system based on score level fusion strategy. 2nd International Congress on Technology, Communication and Knowledge, ICTCK 2015, (Ictck), 501–507. https://doi.org/10.1109/ICTCK.2015.7582719

Sato, H. (2009). Finger Vein Verification Technology for Mobile Apparatus. Secrypt, 37–41. Retrieved from http://dblp.uni-trier.de/db/conf/secrypt/secrypt2009.html#Sato09.

Shaheed, K., Liu, H., Yang, G., Qureshi, I., Gou, J., and Yin, Y. (2018). A Systematic Review of Finger Vein Recognition Techniques. Information, 9(9), 213. https://doi.org/10.3390/info9090213

Sharma, R., Das, S., and Joshi, P. (2018). Score-level fusion using generalized extreme value distribution and DSmT, for multi-biometric systems. IET Biometrics, 7(5), 474–481. https://doi.org/10.1049/iet-bmt.2017.0076.

Sim, H. M., Asmuni, H., Hassan, R., and Othman, R. M. (2014). Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images. Expert Systems with Applications, 41(11), 5390–5404. https://doi.org/10.1016/j.eswa.2014.02.051.

Singh, M., Singh, R., and Ross, A. (2019). A Comprehensive Overview of Biometric Fusion. Information Fusion. https://doi.org/10.1016/j.inffus.2018.12.003.

Syazana-Itqan, K., Syafeeza, A. R., Saad, N. M., Hamid, N. A., and Bin Mohd Saad, W. H. (2016). A Review of Finger-Vein Biometrics Identification Approaches. Indian Journal of Science and Technology, 9(32). https://doi.org/10.17485/ijst/2016/v9i32/99276

Tan, D., Yang, J., Shi, Y., and Xu, C. (2013). A hierarchal framework for finger-vein image classification. Proceedings - 2nd IAPR Asian Conference on Pattern Recognition, ACPR 2013, 833–837. https://doi.org/10.1109/ACPR.2013.151.

Tang, M., Alazab, M., and Luo, Y. (2017). Big Data for Cybersecurity: Vulnerability Disclosure Trends and Dependencies. IEEE Transactions on Big Data, X(X), 1–1. https://doi.org/10.1109/tbdata.2017.2723570

Tran, Q. D., and Liatsis, P. (2016). RABOC: An approach to handle class imbalance in multimodal biometric authentication. Neurocomputing, 188, 167–177. https://doi.org/10.1016/j.neucom.2014.12.126

Walia, G. S., Singh, T., Singh, K., and Verma, N. (2019). Robust multimodal biometric system based on optimal score level fusion model. Expert Systems with Applications, 116, 364–376. https://doi.org/10.1016/j.eswa.2018.08.036.

Wenxiong Kang, Yuting Lu, Dejian Li, and W. J. (2019). From Noise to Feature: Exploiting Intensity Distribution as a Novel Soft Biometric Trait for Finger Vein Recognition. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 14(13), 858–869. https://doi.org/10.1109/TIFS.2018.2866330.

Wild, P., Radu, P., Chen, L., and Ferryman, J. (2016). Robust multimodal face and fingerprint fusion in the presence of spoofing attacks. Pattern Recognition, 50, 17–25. https://doi.org/10.1016/j.patcog.2015.08.007

Yang, J., Wei, J., and Shi, Y. (2018). Accurate ROI Localization and Hierarchical Hyper-sphere Model for Finger-vein Recognition. Neurocomputing, 0, 1–11. https://doi.org/10.1016/j.neucom.2018.02.098.

Yang, Wencheng, Wang, S., Hu, J., Zheng, G., and Valli, C. (2018). A fingerprint and finger-vein based cancelable multi-biometric system. Pattern Recognition, 78, 242–251. https://doi.org/10.1016/j.patcog.2018.01.026.

Yang, Wencheng, Wang, S., Zheng, G., and Valli, C. (2018). Impact of feature proportion on matching performance of multi-biometric systems. ICT Express, 1–4. https://doi.org/10.1016/j.icte.2018.03.001

Yang, Wenming, Huang, X., Zhou, F., and Liao, Q. (2014). Comparative competitive coding for personal identification by using finger vein and finger dorsal texture fusion. Information Sciences, 268, 20–32. https://doi.org/10.1016/j.ins.2013.10.010.

Yang, Wenming, Yu, X., and Liao, Q. (2009). Personal authentication using finger vein pattern and finger-dorsa texture fusion. Proceedings of the Seventeen ACM International Conference on Multimedia - MM '09, 905. https://doi.org/10.1145/1631272.1631444.

Ye, X., Zhao, J., Zhang, Y., and Wen, F. (2015). Quantitative vulnerability assessment of cyber security for distribution automation systems. Energies, 8(6), 5266–5286. https://doi.org/10.3390/en8065266.

Yu, C., Qing, H., and Zhang, L. (2008). A research on extracting low quality human finger vein pattern characteristics. 2nd International Conference on Bioinformatics and Biomedical Engineering, ICBBE 2008, 1876–1879. https://doi.org/10.1109/ICBBE.2008.798.

Zhao, D., Luo, W., Liu, R., and Yue, L. (2018). Negative Iris Recognition. IEEE Transactions on Dependable and Secure Computing, 15(1), 112–125. https://doi.org/10.1109/TDSC.2015.2507133.