Journal of Medical Systems (2018) 42: 238
https://doi.org/10.1007/s10916-018-1104-5

SYSTEMS-LEVEL QUALITY IMPROVEMENT

Real-Time Remote Health Monitoring Systems Using Body Sensor Information and Finger Vein Biometric Verification: A Multi-Layer Systematic Review

A. H. Mohsin[1] · A. A. Zaidan[1] · B. B. Zaidan[1] · A. S. Albahri[1] · O. S. Albahri[1] · M. A. Alsalem[1] · K. I. Mohammed[1]

Received: 14 August 2018 / Accepted: 9 October 2018 / Published online: 16 October 2018

Abstract

The development of wireless body area sensor networks is imperative for modern telemedicine. However, attackers and cybercriminals are gradually becoming aware in attacking telemedicine systems, and the black market value of protected health information has the highest price nowadays. Security remains a formidable challenge to be resolved. Intelligent home environments make up one of the major application areas of pervasive computing. Security and privacy are the two most important issues in the remote monitoring and control of intelligent home environments for clients and servers in telemedicine architecture. The personal authentication approach that uses the finger vein pattern is a newly investigated biometric technique. This type of biometric has many advantages over other types (explained in detail later on) and is suitable for different human categories and ages. This study aims to establish a secure verification method for real-time monitoring systems to be used for the authentication of patients and other members who are working in telemedicine systems. The process begins with the sensor based on Tiers 1 and 2 (client side) in the telemedicine architecture and ends with patient verification in Tier 3 (server side) via finger vein biometric technology to ensure patient security on both sides. Multilayer taxonomy is conducted in this research to attain the study's goal. In the first layer, real-time remote monitoring studies based on the sensor technology used in telemedicine applications are reviewed and analysed to provide researchers a clear vision of security and privacy based on sensors in telemedicine. An extensive search is conducted to identify articles that deal with security and privacy issues, related applications are reviewed comprehensively and a coherent taxonomy of these articles is established. ScienceDirect, IEEE Xplore and Web of Science databases are checked for articles on mHealth in telemedicine based on sensors. A total of 3064 papers are collected from 2007 to 2017. The retrieved articles are filtered according to the security and privacy of telemedicine applications based on sensors. Nineteen articles are selected and classified into two categories. The first category, which accounts for 57.89% ($n = 11/19$), includes surveys on telemedicine articles and their applications. The second category, accounting for 42.1% ($n = 8/19$), includes articles on the three-tiered architecture of telemedicine. The collected studies reveal the essential need to construct another taxonomy layer and review studies on finger vein biometric verification systems. This map-matching for both taxonomies is developed for this study to go deeply into the sensor field and determine novel risks and benefits for patient security and privacy on client and server sides in telemedicine applications. In the second layer of our taxonomy, the literature on finger vein biometric verification systems is analysed and reviewed. In this layer, we obtain a final set of 65 articles classified into four categories. In the first

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

✉ A. A. Zaidan
aws.alaa@gmail.com; aws.alaa@fskik.upsi.edu.my

A. H. Mohsin
alihadi.mohsin@gmail.com

B. B. Zaidan
bilalbaha@fskik.upsi.edu.my

A. S. Albahri
ahmed.bahri78@gmail.com

O. S. Albahri
osamsh89@yahoo.com

M. A. Alsalem
mohamed.asum@gtablemail.com

K. I. Mohammed
khalid_b81@yahoo.com

[1] Department of Computing, Universiti Pendidikan Sultan Idris, Tanjong Malim, Perak, Malaysia

category, 80% ($n = 52/65$) of the articles focus on development and design. In the second category, 12.30% ($n = 8/65$) includes evaluation and comparative articles. These articles are not intensively included in our literature analysis. In the third category, 4.61% ($n = 3/65$) includes articles about analytical studies. In the fourth category, 3.07% ($n = 2/65$) comprises reviews and surveys. This study aims to provide researchers with an up-to-date overview of studies that have been conducted on (user/patient) authentication to enhance the security level in telemedicine or any information system. In the current study, taxonomy is presented by explaining previous studies. Moreover, this review highlights the motivations, challenges and recommendations related to finger vein biometric verification systems and determines the gaps in this research direction (protection of finger vein templates in real time), which represent a new research direction in this area.

Keywords Real-time remote monitoring · Healthcare services · Sensor · Biometrics · Finger vein · Vein · Verification · Security

Introduction

Real-time remote health monitoring systems use telecommunication and information technology to provide clinical healthcare from a distance [1–3]. These technologies allow patients and medical staff to communicate with convenience and fidelity and enable the transmission of medical, imaging and health informatics data from one site to another [4, 5]. The telemedicine architecture contains a three-tier pervasive telemedicine system based on a wireless body area network (WBAN) that enables real-time and continuous healthcare monitoring [6–8]. In Tier 1, patients can obtain their vital signals through tiny intelligent wireless sensors. These signals are sent to Tier 2, which is the personal gateway (e.g. handheld devices, personal digital assistants and laptops), through small area network protocols (e.g. Bluetooth and Zigbee) and WBAN. Medical data are then sent from Tier 2 to Tier 3, which is the healthcare provider in medical institutes (MIs), through wide area wireless communication protocols or Internet services. Healthcare providers in Tier 3 apply certain processes and generate services that are sent back to patients as responses. Tiers 1 and 2 represent the client side, and Tier 3 represents the server side. Patients can also use different portable devices, such as cameras, biometric imaging devices and microphones, to transmit or view clinical data or images or to access control systems to perform authorised access at the server side. Figure 1 shows this process of telemedicine [5, 9].

Telemedicine benefits from a large bibliography, but practical challenges remain, especially in improving security engineering and risk management in the context of continuous development of healthcare services in secure channels [10–13]. On the client side, patients' vital signs must be sent to Tier 3 very securely through the Internet in remote monitoring systems [14, 15]. Amongst the major concerns that prevent patients from widely adopting this technology are data privacy and security [16–18]. Wireless medical sensor networks (MSNs) are the building blocks of remote health monitoring systems [16]. The nodes in MSNs are classified into sensors that report measurements about the human body and actuators that receive commands from the medical staff and perform actions. On the server side, authenticating these commands is a critical security issue because any alteration may lead to serious consequences [19, 20]. Patients also need to access telemedicine systems in secure authentication when using health applications to ensure that vital signs/data are transmitted with security and usability [10].

The challenges in the telemedicine environment that are related to security level can be overcome by enhancing patient enrolment operation, which is a standard-based identity-proofing process [21]. Correct patient identification is the key to overcoming challenges in any health system and results in a health system without duplicate records and payment forgery. If a health system can successfully capture and verify a patient's identity, then duplication in patient records can be reduced and patient satisfaction can increase. Moreover, data entry errors and administration costs can be reduced, and patient data and invoice accuracy will increase. In the digital information field, biometrics refers to an authentication system technology that uses human physical characteristics, such as the face, iris, fingerprints, finger veins and hand geometry, or behavioural characteristics (e.g. voice and gait); in recent years, biometrics-based verification systems have been used in many applications that require a reliable verification/identification scheme [22]. Biometrics has become a solution for managing difficulties in security issues through human biological biometrics, which cannot be stolen or copied easily. Thus, traditional authentication systems, which typically identify an individual by using a key or password and other methods, such as magnetic cards, can be improved by adopting this new type of authentication technology because traditional methods may be unsafe considering that the data in these methods can be stolen or forgotten [23, 24]. Finger vein verification is a promising technique that is extensively considered by researchers and developers because of its favourable advantages, such as (1) being contactless, (2) effectiveness in living humans, (3) high security, (4) small equipment size, (5) low cost and (6) minimal defects, unlike other biometric techniques. Table 1 compares the characteristics of various biometric authentications.

Finger vein biometrics plays crucial roles in numerous security applications, such as access control, individual authentication and electronic passport. Biometrics is extensively

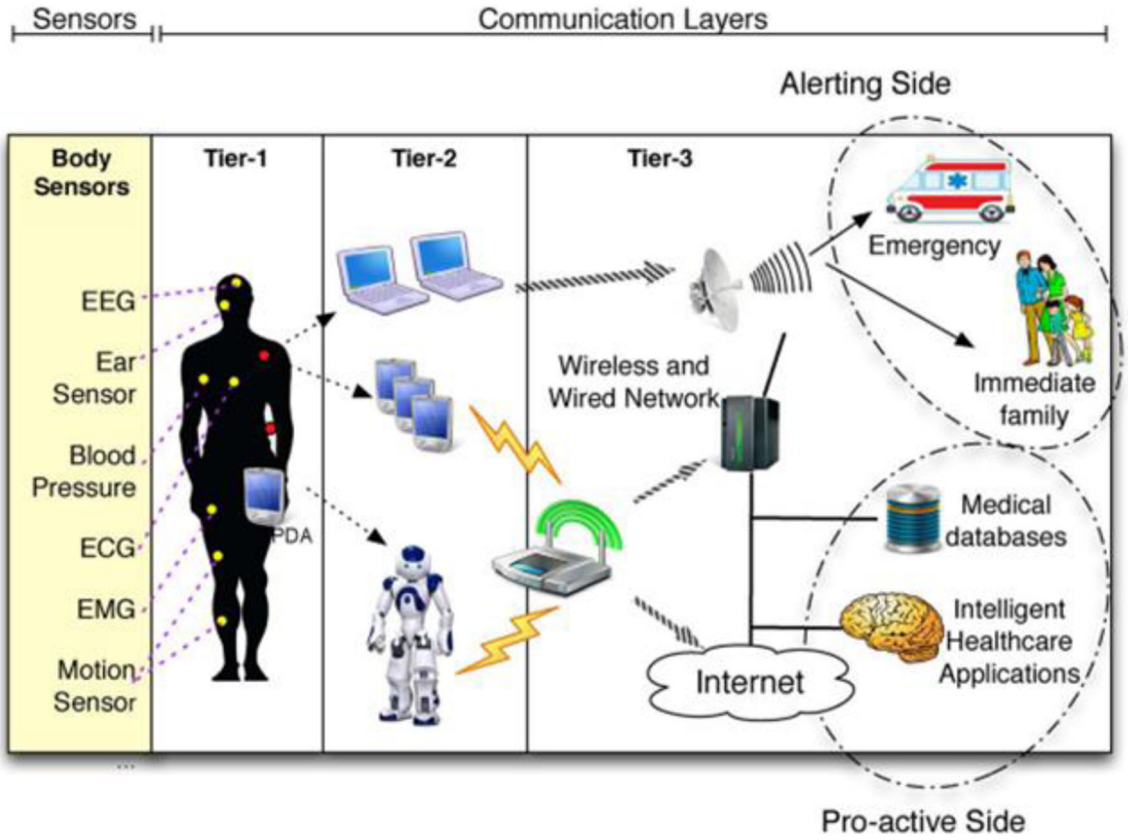

Fig. 1 Three-tiered architecture of a WBAN telemedicine system for healthcare monitoring

applied in door access and controlled border crossing, financial security and attendance systems. A biometric method is imperative for modern telemedicine and mHealth to secure wireless body area sensor networks, but its security remains a formidable challenge to be resolved. Over the past two decades, different types of biometric frameworks have been developed. The finger vein verification system in Reference [25] is more protected and difficult to forge than other biometric verification technologies because veins are located inside the human body. Furthermore, physical contact between the customer and sensor device, which uses a charge-coupled device (CCD) camera with a near-infrared (NIR) filter, is unnecessary during individual enrolment in the finger vein verification system. An infrared light-emitting diode (LED) light (760–1000 nm) can pass through the skin of the finger, but the haemoglobin in the blood can absorb the infrared light and appear as dark lines. The finger vein pattern can be made visible with an infrared-sensitive CCD camera because the reflections of the veins are not equally visible as the surroundings of other areas of the finger [26]. The verification process consists of four main stages, namely, image acquisition, pre-processing, feature extraction and matching. An infrared camera is commonly used to capture finger vein images. Then, pre-processing, such as normalisation and segmentation, is applied to enhance the vein images and extract the region of interest (ROI). Next, processing is conducted through finger vein feature extraction. Matching is then performed to determine the similarity of the extracted features from finger vein patterns and decide whether the individual is genuine or an imposter [27].

Reference [28] indicated that several software developers have become interested in the development of finger vein

Table 1 Comparison of the characteristics of various biometric authentications

Type	Properties	Shortcoming	Security	Sensor device	Cost
Voice	Natural/comfortable	Noise/cold diseases	Normal	No contact required	Low
Face	Remote-controlled/comfortable	Light	Normal	No contact required	Low
Fingerprint	Extensive usage/comfortable	Skin diseases	Good	Contact required	Low
Iris	Highly accurate/uncomfortable	Eyeglasses/side effect	Excellent	No contact required	High
Finger vein	Highly accurate/ comfortable	Few	Excellent	No contact required	Low

verification applications. many technologies, architectures and algorithms are currently used in this area of research, which focuses on using ways, methods and designs, including enhancing finger vein images, extracting these features and conducting the matching process, to achieve highly accurate results and rapid processing. Biometric leakage is one of the most challenging problems, and it causes great risks. For example, repetitive attacks use stolen biometric information, which is difficult to supplant. According to references [29, 30], the environmental impact in image processing is determined by many factors, such as vein patterns, which are captured in addition to vein data, which also contain noise. In addition, different shadowing areas can reduce the accuracy of the verification results

The systematic review in the present study comprises two review layers. The first layer aims to survey the academic literature related to security and privacy of telemedicine application-based sensors, and the second layer aims to survey relevant studies on finger vein biometric verification systems. Figure 2 presents a framework of multi-layer systematic review protocols. The remainder of this paper is organised as follows. Section "First Layer: Systematic Review Method for Security and Privacy Factors of Telemedicine Application-based Sensor" shows the first layer of our systematic review protocol. Section "Second Layer: Systematic Review Method for Finger Vein Biometric Verification Systems" presents the second layer of our systematic review protocol. Section "Discussion" illustrates the challenges, motivations, recommendations and methodological aspects identified from the literature review and collected from diverse studies on finger vein biometric verification systems. Section "Limitations" presents the limitations of the study, and Section "Conclusion" shows the conclusions.

First layer: Systematic review method for security and privacy factors of telemedicine application-based sensor

Methods

The most critical keywords in telemedicine covered by our study are 'telemedicine', 'sensor', 'triage' and 'priority'. All telemedicine-related areas and studies that are related to health domains are considered. However, our scope of literature in the English language is restricted. A general study was adopted to identify every article related to the subject of telemedicine by searching the best and most reliable databases, namely, (1) Science Direct database, which offers access to journals under Elsevier Science publisher (one of the largest electronic group of science, medicine and technology and contains full-text information and references); (2) Institute of Electrical and Electronic Engineers (IEEE) Explorer, which is a database of technical articles in technology and engineering [31–34]; and (3) Web of Science (WoS), which is a database that indexes cross-disciplinary research to discover specialised branches of fields within an academic or scientific discipline in sciences, social sciences, arts and humanities. These selections cover medicinal and technical literature and provide an expansive perspective of the endeavours of developers and designers in a wide but related range of studies. The strategy for selecting pertinent articles involves searching the literature sources in two rounds. In the first round, filtering and screening are performed to exclude duplicates and studies that are unrelated to remote health monitoring systems based on sensor information. The second round performs filtering by accurate full-text reading of the examined articles from the first round based on the security and privacy factors of telemedicine applications. Both rounds apply eligibility criteria in the examining process and are reviewed by authors. Consequently, the final encompassed set is correlated to the security and privacy of telemedicine applications based on sensors through diverse topics (Fig. 3). We began searching in reliable databases, such as Science Direct, IEEE Explorer and WoS, at the end of April 2017 by using search engines and entered different keywords into the search bar of the explorer engine. The combinations of various keywords, including 'medical system', 'telemonitoring', 'e-health', 'telemedicine', 'telehealth', 'healthcare services', 'mHealth', 'remote monitoring', 'mobile doctor', 'triage', 'priority' and 'sensor', in various syntax logical keywords were queried using 'AND' and 'OR' operators, as illustrated in Fig. 3. The search accepted book chapters and different types of reports instead of focusing on journals and scientific conference articles only because the two directions comprise recent and suitable scientific studies related to developing and creating patterns for the security and privacy factors of telemedicine applications. The articles that were selected by following the criteria in Fig. 3 were included in the review. The underlying focus of mapping the scope of research on security and privacy factors of telemedicine applications was set to general and the coarse-grained scientific classification taxonomy of two categories. The categories were obtained from a pre-overview of this study without limitations. The Google Scholar engine was used to obtain a preliminary framework of the scene and directions in this study. Duplicates were eliminated by excluding articles in the two rounds because they do not satisfy the inclusion criteria [35]. The exclusion criteria used in the rounds are listed in Fig. 3. Each included article, with its related beginning categories, was identified from different sources and assembled into a single Excel file to improve the procedures in our investigation and simplify the article classification for readers. Several full-content readings, such as contributions, objectives and comments on the surveyed works, resulted in highlights [36]. The articles were classified according to a previous taxonomy. The entire comments and highlights were included in the body of the texts (depending on our team style, such as print-out or soft-copy versions). The main findings were described and tabulated

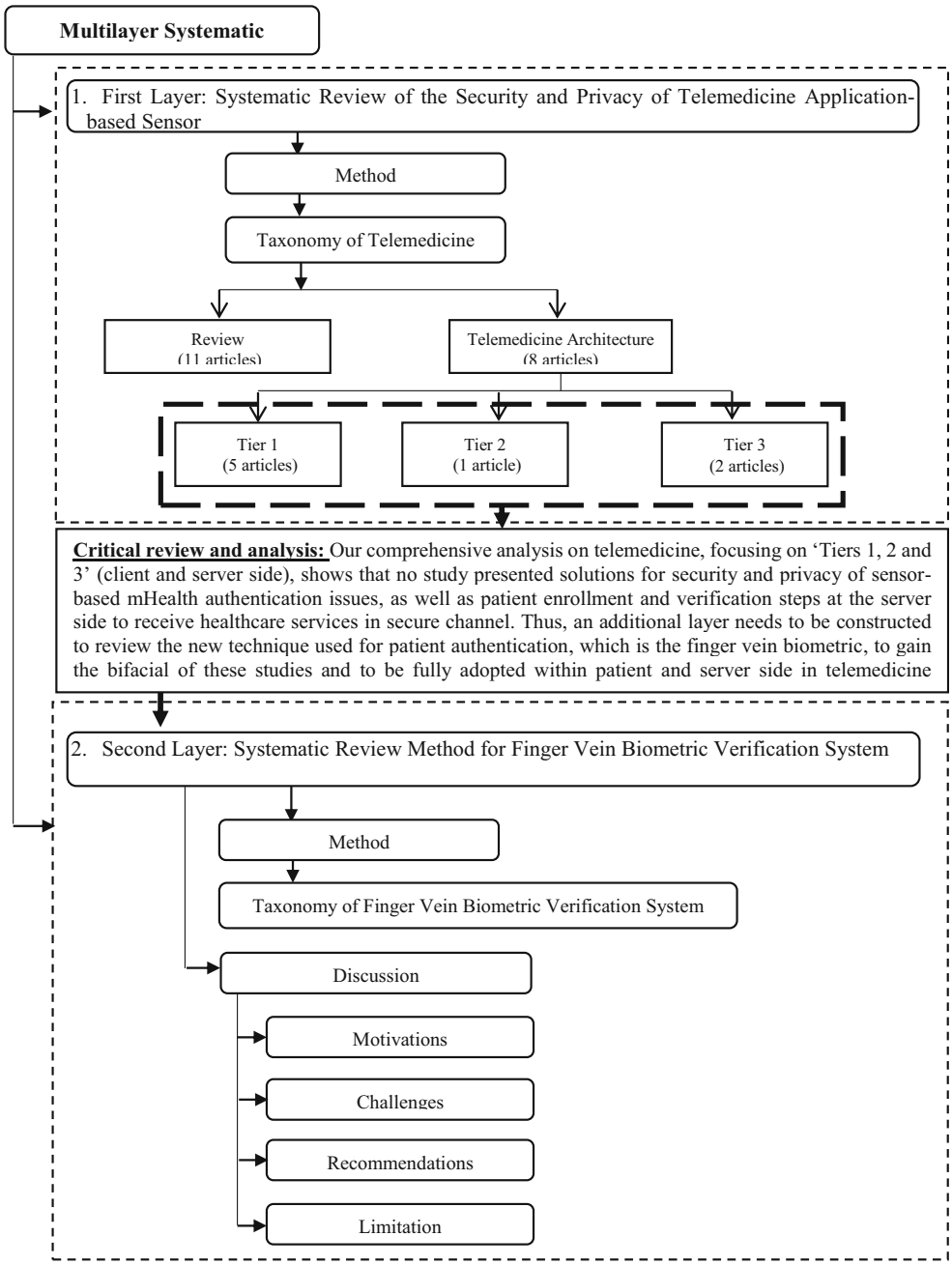

Fig. 2 Framework of multilayer systematic review protocols

after a summary. Word and Excel files were created to save important information, and they consisted of a list of all articles and related databases, tables of summary and details. The tables were classified based on the specialisation of articles in security and privacy factors of telemedicine applications. Valuable information is provided in the supplementary material as a full reference for the findings, as discussed in the next section.

Results

The search operation resulted in 3064 articles, amongst which 1496 were from IEEE Explorer, 911 were from Science Direct and 657 were from WoS, during the period of 2007–2017. In the first round of filtering, 1612 of the 3064 articles published from 2012 to 2017 were collected.

Only 65 articles from all of the databases were duplicated. Subsequently, the titles and abstracts were read, resulting in the exclusion of 1264 articles that are unrelated to our specific research topic. Thus, the result is 283 articles. Next, full-text reading was performed, leading to the exclusion of 133 additional articles. The 150 remaining articles represented the final result in the filtering of the first round. In the second round of filtering, the articles that resulted from the previous filtering round were filtered again according to the security and privacy

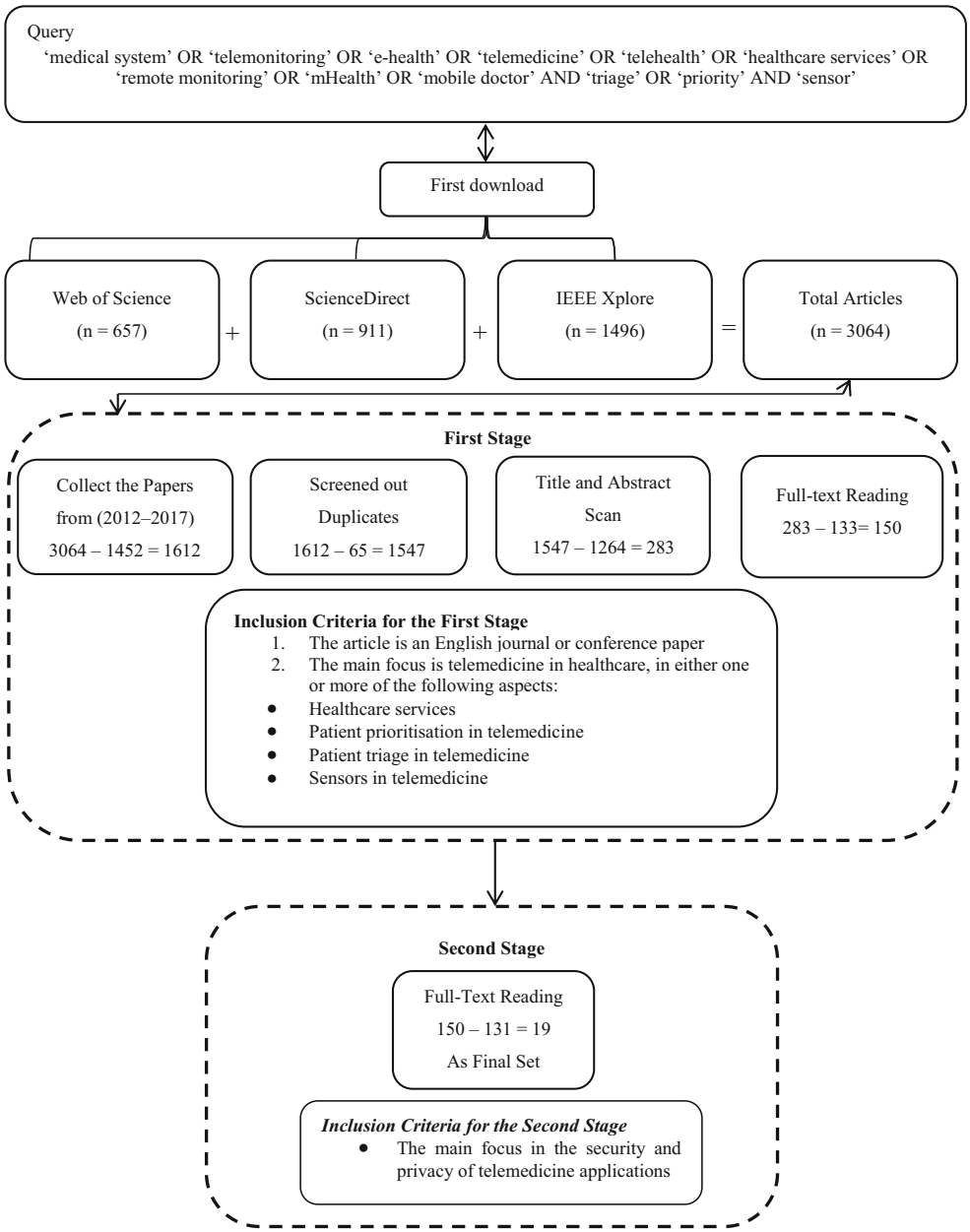

Fig. 3 Explanation of the criteria and search queries adopted in selecting the articles

factors of telemedicine applications, and (n = 131/150) articles were excluded after filtering the full-text. Only 19 articles which were related to the security and privacy of telemedicine applications were obtained. These articles were thoroughly read to develop a general map of the research. Most of the articles (57.89%; 11/19 articles) comprise reviews and surveys that satisfy the current security required by telemedicine and the importance of using security and privacy factors in telemedicine applications in future medical systems.The second group of articles (42.1%; 8/19 articles) consisted of studies that contributed to security and privacy within the telemedicine architecture, which involves three tiers (Tiers 1, 2 and 3). Tiers 1 and 2 represent the client side, which is composed of medical sensors (i.e. ECG, BP and SpO2) connected with mHealth (i.e. laptop, smartphone and taps) to transfer the vital signs of a patient to the medical centre side (Tier 3). The articles in this category are classified into three subsections: (1) Tier 1 (n = 5/8 articles), Tier 2 (n = 1/8 articles) and Tier 3 (n = 2/8 articles). The general categories of the articles that were captured then re-classified into the literature review taxonomy are presented in Fig. 4 and can be distinguished amongst different subcategories in the general categories through the presence of overlaps.

Review

The primary goal of survey and review articles on telemedicine is to understand current thinking and justify the need for

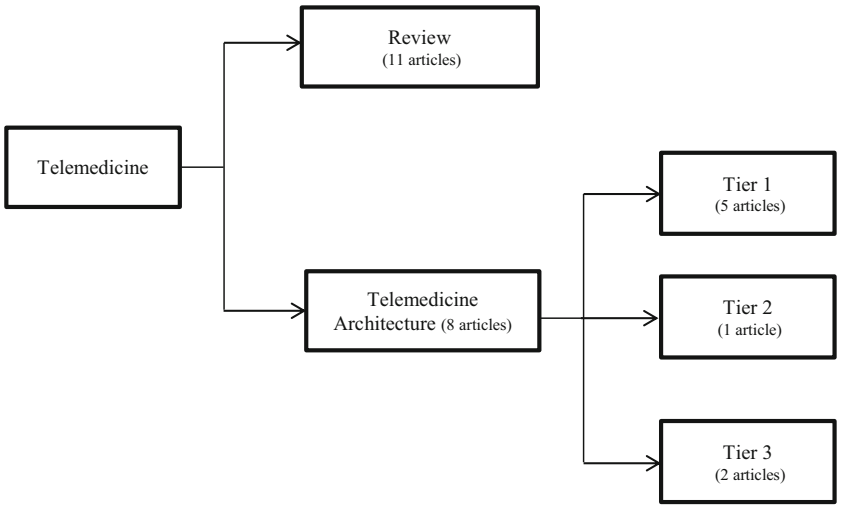

Fig. 4 Taxonomy of research literature on the security and privacy of telemedicine applications

future research on related topics that have been overlooked or understudied. This category contained 11 articles. The review of the penetration of mobile technology into Asia considered the integration with diagnoses and treatment of mental disorders and highlighted the limitations and potential barriers of mHealth for mental health, including data security and privacy, language and literacy and power supply issues [37]. The study conducted by [5] focused on the telemonitoring of a patient's field conducted in European projects to present the common requirements and components of telemonitoring systems in the context of technical issues, services, tools and functionalities and distinguish projects that deal with comfort and security. A comprehensive survey of mHealth research initiatives in Brazil included 42 projects. This analysis considered issues, such as health condition, security features, development and deployment of the main providers involved, types of devices used, target users and the location where each project is tested and/or deployed [38]. Reference [8] presented the review of WBAN applications and highlighted the requirements of QoS. The goal was to provide appropriate wireless technologies for WBAN by studying the various technologies used and attempting to associate WBAN applications with suitable technologies for maximum QoS. Reference [39] explored effective measures and strategies for the promotion of ICT-enabled innovations for people with special needs and the elderly. The study reviewed and evaluated current government initiatives in the field of e-health and accessibility, thereby addressing the challenges encountered by Japan's rapidly ageing society. A review of mHealth technologies for military mental health was presented in [40] to identify high-priority mHealth technology development considerations in two categories, namely, priority considerations for mental healthcare provision and priority considerations broadly applicable to mHealth. This review also included military programmes, such as the Telemedicine and Advanced Technology Research Centre, the Military Operational Medicine Research Programme, United States Army Medical Research and Material Command and the National Centre for Telehealth and Technology. The review in [41] provided an overview of the state of mHealth in a wide array of biomarkers in the context of psychiatric functioning (e.g. anxiety, substance use, autism and psychological stress). This study also identified several specific opportunities for expanding this promising methodology and the advantages and special considerations for incorporating mHealth tools. A comprehensive review of state-of-the-art mHealth applications and services was presented in [42]. It surveyed the most significant studies and presented a thorough analysis of top and novel applications and services proposed by the industry by considering the approaches of the United States and European Union. A study on national domain and quality was conducted, and an overview of US population health, access to care, status of healthcare quality and disparities in care experienced by different socioeconomic, racial and ethnic groups was provided [43]. Reference [44] reviewed different technologies and technological advances applicable to oncology care through websites, books, magazine articles, online product-specific information and peer-reviewed guidelines and studies. Reference [45] systematically reviewed health smart homes and home-based consumer health literature from indexed repositories for healthcare and technology disciplines and categorised the examined articles according to an evidence-based public health typology.

Telemedicine architecture

This category contains eight articles in three subsections (Tier 1, Tier 2 and Tier 3).

Tier 3 A healthcare provider in MIs generally allows medical professionals to monitor and analyse vital signs in real time and provide patients with appropriate healthcare services. It can also manage, organise and support professionals in

telemedicine. Generally, it comprises the medical institution's server, patient history and database and service generation [46]. This subsection contains two articles. Reference [47] proposed an innovative architecture for collecting and accessing large amounts of data generated by MSNs. The architecture overcomes all of the aforementioned challenges and enables easy information sharing amongst healthcare professionals in normal and emergency situations. Furthermore, this study proposed an effective and flexible security mechanism that guarantees confidentiality, integrity and fine-grained access control to outsourced medical data. This mechanism relies on ciphertext policy attribute-based encryption to achieve high flexibility and performance. A machine-to-machine low-cost and secure communication system for e-Healthcare society was proposed in [48]. The system is designed to consider psychological issues, such as stress, anxiety and loneliness, related to all actors in the e-healthcare society. To ensure data privacy, this mechanism involves intelligent authentication based on random distributive key management, electronic certificate distribution and modified realm Kerberos.

Tier 2 Patients can acquire their vital signs in Tier 1 and send them to Tier 2 through small area network protocols (Zigbee and Bluetooth) and WBAN [49]. Tier 2 in the telemedicine architecture is used to bridge sensor-based vital signs to remote stations by using interfaces, such as LAN, 3G, 4G or u-health [50]. This subsection contains only one article. A priority-based health data aggregation (PHDA) scheme with privacy preservation for cloud-assisted WBANs was proposed in [51] to improve the aggregation efficiency amongst various types of health data. The study explored social spots to help forward health data and enable patients to select the optimal relay according to their social ties. The security analysis in this study demonstrated that PHDA can achieve identity and data privacy preservation and resist forgery attacks.

Tier 1 The first tier in the telemedicine architecture is represented by Tier 1, which comprises tiny intelligent wireless sensors that are responsible for gathering a patient's vital signs and transmitting vital information to Tier 2 through WBANs [52]. This subsection contains five articles. Reference [53] implemented TinyECC, which is a public key algorithm with optimisations for resource-constrained hardware platforms, to secure wireless communication between sensor nodes. The feasibility of using TinyECC was examined in a real-time sensor network. A system for the secure logging of events in sensor networks was proposed in [54] by establishing a secure and reliable means to present all information at one central point. The system guarantees the chronological order of logged events sent by different sensors. It also permits an individual to detect the modification, deletion and addition of logged data and design a prototype of the gateway sensor on an FPGA platform. Reference [55] illustrated a security protocol for ultra-wideband impulse radios based on distance bounding. This protocol provides multiple levels of security, including encryption, and a distance bounding test to prevent long-distance attacks used in BANs for medical devices where security is imperative. Reference [56] proposed a priority-based compressed data aggregation scheme with integrity preservation to improve the aggregation efficiency of different types of health data in medical wireless sensor networks. This study used compressed sensing to reduce the communication overhead and minimise power consumption. Then, the compressed data were encrypted, and integrity was protected by a cryptographic hash algorithm to preserve data integrity. A comparative performance analysis between the IEEE 802.15.6-based communication system using UP and the IEEE 802.15.4-based communication system was conducted in [57] to show the effectiveness of IEEE 802.15.6 in the home monitoring of an individual cardiac patient in WBANs.

Critical review and analysis

Nowadays the security matter is considered very challenges for diffrents kind of applications [58–64]. In this study as a conclusion for the first layer and based on literature review analyses, the aforementioned studies within all tiers (client and server side) have not presented solutions for the security and privacy of sensor-based verification systems. Telemedicine applications nowadays require high-level authentication systems to achieve a high level of security and usability and to facilitate patients' convenience [65, 66]. In addition, several challenges related to aging populations and elderly patients with accessibility and usability issues have been encountered [67, 68]. Several techniques can be used, but not all are suitable for the aforementioned categories of people. Traditional methods, such as the use of user names and passwords or RFID cards, are easy to forge, forget (password) or lose (RIFID) [69, 70]. Thus, the most suitable verification techniques are human biometrics. Amongst all human biometrics, the finger vein and iris have a high level of security because these types of biometrics are unique for all people, even for twins. Moreover, they are stable for a long time and have high resistance against forgery and replication. The finger vein biometric has advantages over the iris biometric, such as convenience due to the use of infrared light in every enrolment step and low cost [71, 72]. Consequently, an additional layer needs to be constructed to review finger vein biometric verification systems to gain the bifacial of these studies and fully adopt the telemedicine environment within client and server sides. The new mapping of the sequential multi-layer systematic review allows interring additional knowledge regarding finger vein biometric verification systems within the second layer studies, which make up a wide area of authentication and verification contributions. This

study aims to highlight completed research, such as the abovementioned articles, to address new verification technologies, delineate the research scene from literature to a coherent taxonomy and identify the key aspects that describe this developing research direction (to be proposed and described in detail). After determining the gap in this research direction, our next goal would be to fill this gap and address the problems related to the research gap.

Second layer: Systematic review method for finger vein biometric verification systems

Methods

The most critical keyword in the area covered by this study is 'biometrics'. However, other human body biometrics, such as those found on the face, ear, teeth and fingerprints, are excluded. The focus is on finger vein biometrics. In addition, all multibiometrics and research that are related to the areas of finger vein biometrics are considered. However, our scope of literature in the English language is restricted. We adopted a general study to discover all articles related to the subject of finger vein verification by searching in the best and most reliable databases, namely, (1) Science Direct database, which offers access to journals under Elsevier Science publisher (one of the largest electronic group of science, medicine and technology and contains full-text information and references); (2) IEEE Explorer, which is a database of technical articles in technology and engineering; and (3) WoS, which is a database that indexes cross-disciplinary research to discover specialised branches of fields within an academic or scientific discipline in sciences, social sciences, arts and humanities [46, 50, 73–77]. These selections cover medicinal and technical literature and provide an expansive perspective of the endeavours of developers and designers in a wide but related range of studies. The strategy for selecting pertinent research articles consisted of searching for literature sources in two phases, namely, by examining and performing several filters. The first phase excluded duplicates and unrelated articles determined by reading the titles and abstracts of articles. The second phase filtered articles after an accurate full-text reading of the examined articles. Both phases applied the eligibility criteria used in the examining process and were reviewed by two other authors. We began searching in reliable databases, such as Science Direct, IEEE Explorer and WoS, at the end of May 2017 (with update until the time of writing this paper) by using search engines and entered different keywords into the search bar of the explorer engine. The combinations of various keywords, including 'biometric', 'finger veins', 'vein', 'veins', 'verification' and 'finger vein', in various syntax logical keywords were queried using the 'AND' and 'OR" operators, as illustrated in Fig. 5.

The search accepted book chapters and different types of reports instead of focusing on journals and scientific conference articles because the two directions comprise recent and suitable scientific studies related to developing and creating patterns for finger vein verification. The articles that were selected by following the criteria in Fig. 5 were included in the review. The underlying focus of mapping the scope of research on finger vein verification was set to general and coarse-grained scientific classification taxonomy of four categories (as displayed in the left box in Fig. 6). The categories were obtained from a preoverview of this study without limitations. The Google Scholar engine was used to obtain a preliminary framework of the scene and directions in this study. Moreover, duplicates were eliminated by excluding a few articles in two phases because these articles do not satisfy the inclusion criteria. The exclusion criteria were as follows: (1) the article is non-English; (2) all studies related to investigating physical human characteristics, such as the face, normal fingerprints and palm geometry, or behavioural biometric characteristics (e.g. voice and gait) and whether these studies were multi- or uni-biometrics, which excludes human finger vein biometrics; and (3) the target of the study is unrelated to security verification. Each included article, with its related beginning categories, was assembled from different sources into a single Excel file to improve the procedures in our investigation and simplify the article classification for readers. Several full-content readings resulted in highlights, such as motivations, challenges, limitations and comments, on the surveyed works. Moreover, the articles were classified according to a previous taxonomy. All comments and highlights were included in the body of the texts (depending on our team style, such as printout or soft-copy versions). The main findings were described and tabulated after summary. Word and Excel files were created to save important information, and they consist of a list of all articles and related databases, tables of summary and details. The tables were classified based on the specialisation of the articles in biometric verification, purpose, survey sources, target frameworks and audiences and different figures and diagrams. These datasets are provided in the supplementary material as a full reference for the findings, which are discussed in the next section.

Results

A total of 461 articles were gathered in the search operation, amongst which 279 were from Science Direct, 92 were from IEEE Explorer and 92 were from WoS, during 2007–2017. Only 51 articles from all of these databases were duplicated. Subsequently, the titles and abstracts were read, resulting in the exclusion of 252 articles that are unrelated to our specific research topic. Thus, 185 articles remained. Next, full-text reading was performed, leading to the exclusion of 93 additional articles. The 65 remaining articles represent the final filtering result. These articles were thoroughly read to develop

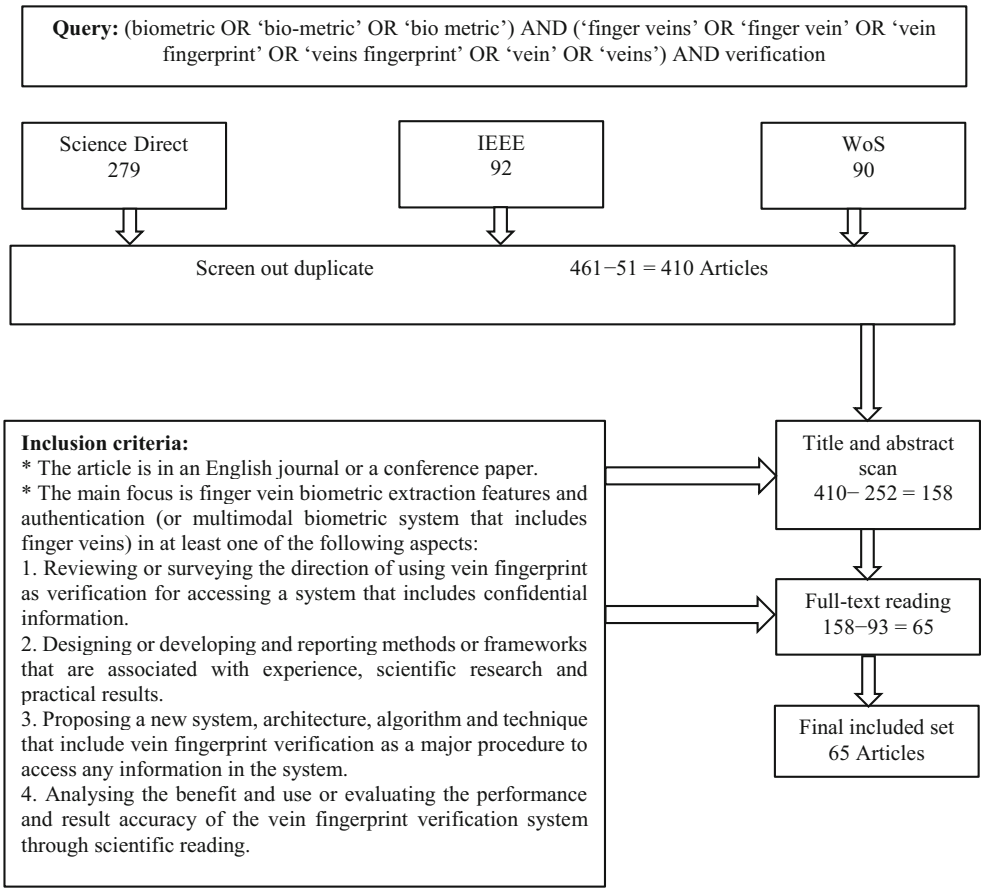

Fig. 5 Explanation of the criteria and search queries that are followed in selecting the articles

a general map of the research. Most of the articles (80%; 52/65) focused on developing various algorithms, methods, architectures, techniques and actual attempts to develop or design a finger vein biometric verification system that aims to introduce a solution for handling security problems, such as accuracy, image quality, feature extraction, time and cost, in individual authentication systems.

The next largest group of articles (12.30%; 8/65) consisted of studies that conducted an evaluative or comparative investigation to evaluate the performance and experiment results of methods that were performed by other researchers to enhance the general implementation of the finger vein verification system. A few researchers (4.61%; 3/65) conducted analytical studies that explored finger vein biometrics and the impact of devices that are used as a system component in the finger vein verification system. The final group with the least number of articles (3.07%; 2/65) comprised reviews and surveys that satisfy the current security requirements and the importance of using this type of biometrics in future authentication systems.

The general categories of the articles that were captured and re-classified into the literature review taxonomy presented in Fig. 6 can be distinguished amongst different subcategories in the general categories through the presence of overlaps. In the subsequent sections, these main and subcategories are listed to simplify the statistics during the discussion.

Development and design studies

In recent years, authentication systems based on human biometrics, especially in finger vein verification, which represents an emerging biometric technology, have been exceedingly used in various applications that require thorough verification or identification of individuals. Most of the articles (52/65) involved the academic community (students as volunteers) in the collection of finger vein pattern databases and used university laboratories or databases to obtain experimental results to understand this verification system technology. Most of the articles described the development and design of a finger vein verification system. Reference [78] applied image segmentation based on ROI to enhance the visibility of images and reduce noise in the patterns by using several image enhancement techniques, such as auto-contrast and smoothing. However, the images must be cropped to remove the redundant areas in the image before applying any enhancement. Table 2 lists the distribution of development and design articles.

Development and design based on a software framework

According to the article classification taxonomy mentioned in Fig. 6 (proposed framework group), 44 of the 52 articles focused on the proposed software framework. This framework

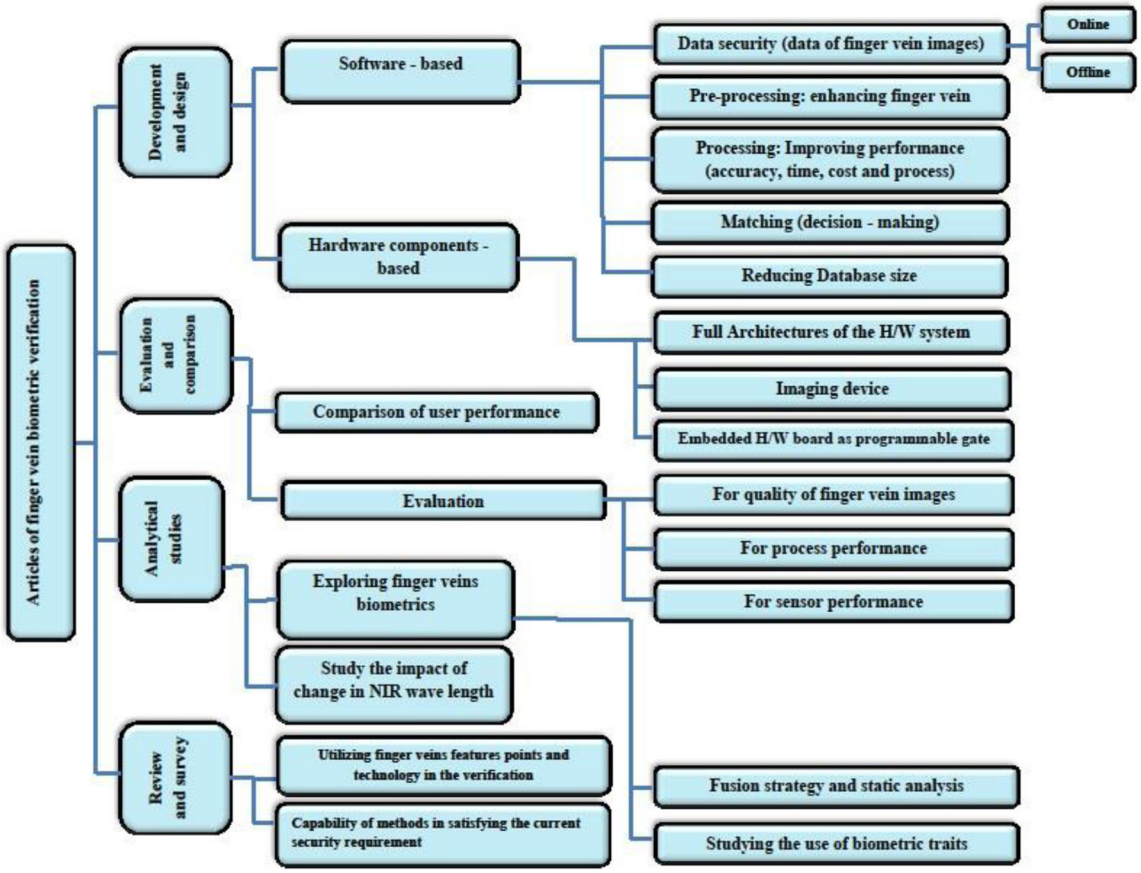

Fig. 6 Taxonomy of research literature on finger vein biometric verification

consists of methods, algorithms and new techniques for overcoming the challenges in finger vein verification systems, such as enhanced image acquisition quality, feature extraction from finger vein images, secure finger vein templates and accuracy of finger vein pattern matching, and enhancing the overall performance of finger vein verification systems. Figure 7 depicts the number of studies that were conducted based on the classification of the software framework in this paragraph.

Table 2 Distribution of development and design articles

Categories	Subcategories	Number of articles
Proposed software framework	Data security	7
	Pre-processing	10
	Processing	16
	Reducing database size	1
	Matching	10
Proposed hardware components (development and/or design of an imaging device)	Full architecture of the hardware system	3
	Development and /or design of an imaging device	4
	Embedded hardware of FVRS	1

This group of articles can be classified into five subgroups. The first subgroup, which pertains to data security, has (7/44) articles that focused on secure finger vein image information. The resulting biometric data called biometric templates are obtained after completing the step in individual enrolment. If this template is stolen by an attacker, then changing or replacing the template information is infeasible because the information remains constant whilst humans live. Therefore, new technologies, such as biometric template protection, have been attracting extensive attention in solving the aforementioned problem. Protecting this information is a critical issue in biometric verification systems because this information is personal and private, and extensive research against spoofing leakage information is required. References [29, 79–83] and [84] secured finger vein information by using different cryptography techniques during individual offline authentication in various applications. Reference [29] proposed a secure biometric verification scheme that secures vein pattern information by implementing an optical data encryption technique based on compressed sensing. Vein images are secured during image capture. Furthermore, a micro-mirror is used to obtain information from the finger veins as a cipher key for

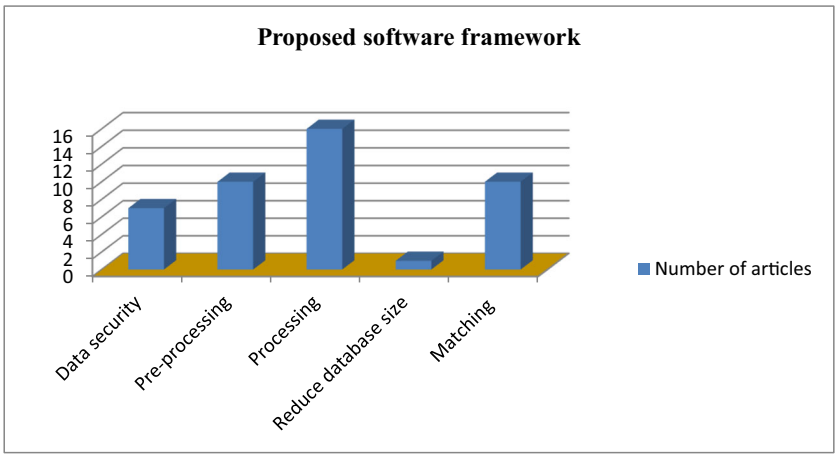

Fig. 7 Number of articles in the proposed software framework

encrypting this information and storing raw images in the database. Information should be verified first before restoring the raw image from the database when a user needs to access the database. Reference [79] generated a secret key from finger veins and then used this key to encrypt and decrypt any images. Reference [80] introduced a visual cryptography scheme to fuse a template and preserve the security and accuracy of the system. This scheme uses the original biometric data, in which the vein images are divided into small segments called shares. Shares are then encrypted using a secret key. Reference [81] secured the vein pattern biometric cryptosystem against offline brute-force attack (FAR) to obtain the original image that performed decryption on these encrypted shares by using the same secret key in protecting templates based on optimal sequential fusion for multibiometrics cryptosystems. Reference [82] focused on secure finger vein information during online verification by proposing a new bio-key generation algorithm called Fountain Valley High School (FVHS), which gathers the advantages of biometrics and user-key authentications. FVHS instantly generates stable and sufficiently strong bio-key sequences from finger vein biometrics during the encryption of the corresponding uniform resource locator of different services provided by cloud computing with shared confidentiality. The key idea of FVHS is to combine machine learning, biometrics and cryptography because these pieces of information are exposed to vulnerability to social engineering dictionaries, eavesdropping, spoofing and other network attacks. Reference [83] focused on the extraction features of three biometrics traits, namely, fingerprint, retina and finger vein. These types of biometrics are fused at the feature level, and the RSA algorithm is used for encryption. Finally, these biometric templates are stored in a database to be used in verification operations. Reference [84] presented a multibiometric finger cryptosystem that adopts various fusion strategies, which has been implemented on fusing normal fingerprint, finger vein, finger knuckle print and finger geometry modalities in each enrolment and verification of individuals to encrypt and store finger patterns in the database. This multibiometric finger cryptosystem focuses on the difficulty of decoding an individual fuzzy commitment scheme as the primary security analysis of cryptosystem in human finger multibiometrics.

The second subgroup (10/44 articles) focused on research on finger vein image pre-processing, including various operations, such as ROI localisation, image resizing, normalisation, cropping and improving images, minimising the noise of vein patterns and increasing the contrast of vein images, to enhance and prepare the quality of these images for the next step, that is, processing. This step should be implemented because the input vein images from the scanner may contain many unwanted data. Reference [30] used the Gabor filter to enhance the finger vein image then applied thinning to obtain the skeleton of finger veins and prepare for feature extraction. References [78, 85] used the auto-encoder method in learning the enhanced features for illustrating finger vein images. Using an auto-encoder enhances image quality and smoothens an image to determine and discriminate finger vein features and learn these features without supervision by using a self-taught learning technique. In this technique, the auto-encoder learns the improved value to allow the weights of the invisible layer to adjust the output that is equivalent to the input layer. However, the images must be cropped to remove the redundant parts before enhancement. Reference [86] presented a learning model for extracting and retrieving the features of finger veins by using limited a priori knowledge. This article presented a segmentation model for a finger vein verification system, in which a convolutional neural network (CNN)-based approach was developed to predict the probability of pixels from the vein image background. This operation was applied by learning deep feature representation. Reference [87] proposed a new method to improve the V denoising model that is implemented on artificial images and actual finger vein images with a favourable segmentation effect and high-speed calculation. Reference [88] performed filtering to reduce noise that is produced through non-uniform illumination, low contrast and hair and skin textile. Reference [89]

proposed a method that can restore more than 10% of finger vein images that lost target points and performed finger vein pattern restoration. Reference [90] proposed a framework that consists of two sections, namely, training and testing. These sections begin by pre-processing the finger vein images to detect the ROI, followed by enhancement and normalisation. This system is adequately robust against noise and distortion. Reference [91] used a support vector machine (SVM) technique to develop a finger vein pattern verification system based on principal component analysis (PCA) for image pre-processing and feature extraction using linear discriminant analysis. However, this article focused on pre-processing rather than processing. Reference [92] presented a novel approach to predict the quality of finger vein patterns by studying the binary inputs of finger veins. Quality definition aims to decrease the equal error rate (EER) in biometric verification systems rather than the human perception decision.

The third subgroup (16/44 articles) focused on studies on finger vein image processing, which consists of the finger vein feature operation that extracts and prepares these images for the next step, which is processing. This operation is performed on vein patterns, where the network of blood veins is usually stable. Thus, these patterns cannot be modified unless they are separated by external effective factors. The finger vein network structure has been described by using several methods with reliable output results. Reference [23] used PCA to extract features from finger vein images, performed classification based on the artificial neural network (ANN) and proved that the large input data dimension causes system overload. Moreover, the identification rate that used the adaptive neuro-fuzzy inference system (ANFIS) shows perfect performance of the back-propagation (BP) network in personal identification. According to Reference [25], the feature extraction process consists of three steps. Firstly, local base features from partitioned pattern patches must be extracted. Secondly, a small codebook that contains visual words called finger vein textures (FVTs), which are patches that are collected through k-means clustering, must be learned. Thirdly, an FVT map (FVTM) must be used as a feature to represent the attributes of a finger vein pattern. Reference [26] developed a finger vein verification system based on Radon transform to extract features and perform classification using ANN. In Reference [28], the local line binary pattern was proposed as a feature extraction technique. Robust features were extracted from patterns with vague veins. The method in Reference [93] determines the intersection point between the index and middle fingers to select the extreme points. The height of pixels in vein images must be intercepted with the abscissa of the point as a benchmark. The image of the abscissa location is constantly relative to the original point, which is the width of pixels. Reference [94] proposed a gradient feature selection algorithm, in which the feature extracted from enhanced finger vein images provides the best discrimination capability in the image intensity. Moreover, the group of gradient directionality and intensity outperforms the gradient feature alone. In Reference [95], enrolment of the user is performed by using three fingers, namely, index, middle, and ring, of the user. The features of these patterns are extracted using a repeated line tracking method. Reference [96] presented a feature extraction method for iterative line tracking. The use of this method in addition to extracting finger vein features aligns the finger vein to a fixed location in the patterns. Reference [97] proposed a method called local histogram of the hybrid texture, where the sign and magnitude extracted from the binary gradient contour are used. In Reference [98], the histogram of competitive orientations and magnitudes was proposed as a local descriptor for finger vein feature extraction. Reference [99] contributed a new chain code-based feature extraction method combined with fusion techniques of image skeletons. Reference [100] proposed a novel discriminative binary code (DBC) learning method for finger vein feature extraction. In Reference [101], a new method, which is enhanced pre-processing and processing, was applied. However, this method focused on processing rather than pre-processing. A system using a bank of Gabor filters was proposed to utilise finger vein features at various directions and scales. Reference [102] developed a new method for extracting robust features from finger vein images in a verification system based on finger vein biometrics and extracted features with a global layout and local detail information. This method is based on bag-of-words by learning several robust and discriminative visual words from local base features, such as local binary pattern (LBP). In Reference [103], a new method based on the geometrical features of the intensity field was used to simplify the extraction of features from unclear vein patterns. Reference [104] adopted PCA to extract features from finger vein images. Moreover, pattern classification was applied through the BP network and adaptive neuro-fuzzy inference system.

The fourth subgroup (10/44 articles) focused on studies on finger vein pattern matching using different methods and techniques, where the matching process contains sufficient information for a system to distinguish whether the individual is genuine or an imposter by matching the input finger vein patterns during the individual enrolment stage with those stored in the system database. In Reference [22], a new approach called band limited phase-only correlation (BLPOC), which is used to measure the similarity of finger vein patterns, was proposed. Reference [105] focused on optimising the matching process, and a new matching method based on deep CNN was proposed. These neural networks can enhance the accuracy of a finger vein verification system. Reference [106] proposed a new finger vein verification system using a multi-instance minutiae-based matching method, which is implemented in a unified minutia alignment and clipping way depending on the genetic algorithm and k-modified Hausdorff distance measurement. Reference [107] applied SIFT features to define finger vein images by calculating the feature associated with enrolment. This study focused on the matching process in the

authentication system, and the images were investigated to verify the person and improve and handle finger vein segmentation problems. In Reference [108], occurrence probability matrix (OPM), which is used in matching two templates, was proposed. In this matrix, each element has a stable value that corresponds to the area of the finger template matrix. In Reference [109], a singular value decomposition-based minutiae matching (SVDMM) method for finger vein verification was used. Reference [110] presented a new design of a novel point set matching algorithm for non-parametric matching of patch layout to obtain high efficiency for the tree model and high level of accuracy in all the problems related to the authentication and recognition processes. Reference [111] used ANN in vein methodology to match finger vein patterns. Reference [112] adopted multimodal biometrics, including finger veins, to enhance the accuracy of matching results. The score-level fusion method based on triangular norm provides highly accurate matching. In Reference [113], proposed multimodal verification systems that are based on face and finger vein verification and multilevel score-level fusion are applied. The imposter and genuine scores are combined using fuzzy fusion.

Belonging to the fifth subgroup (1/44 articles), Reference [114] focused on representing a particular point to reduce the required data space in finger vein verification applications. A method was presented to overcome the shortcomings of large storage data and heavy CPU computation.

Hardware components (architectures and devices) According to the taxonomy presented in Fig. 6, the hardware components (8/52 articles) focused on the design of a full hardware system architecture and the design and/or development of devices in the finger vein verification system. Figure 8 illustrates the number of articles that proposed hardware system components based on the classification in this paragraph.

This group can be divided into three subgroups as follows:

References [115, 116] and [117] indicated that the full architecture of a hardware system can be applied on a field-programmable gate array (FPGA) platform of personal verification that uses infrared finger vein biometrics. References [118–120] and [121] focused on the development and/or design of an imaging device that can capture finger veins only or with another biometrics simultaneously with certain advantages, such as sufficient robustness, low cost and user friendliness. reference [122] suggested the implementation of an embedded hardware of a finger vein recognition system (FVRS) on an FPGA board, which can implement the logic for various algorithms on the basis of the interest of the user

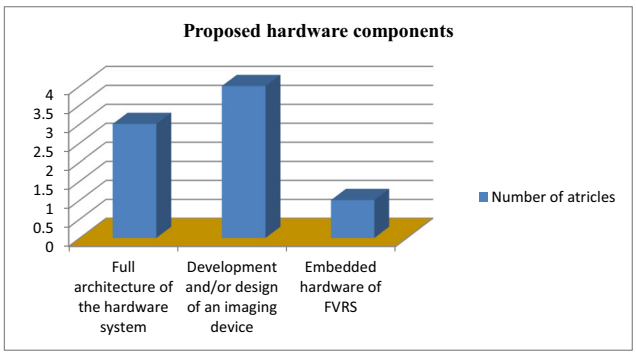

Fig. 8 Number of articles for the components of the proposed hardware system

Evaluation and comparison

The second category (8/65 articles) attempted to present an evaluation and comparison of studies on finger vein verification systems, as depicted in Fig. 9. This category can be divided into two subcategories, namely, evaluation and comparison of user performance. Furthermore, the evaluation subcategory can be divided into three groups as follows:

The first group of evaluation (4/8) focused on evaluating the quality of finger vein images through different methods and techniques. In Reference [123], a modular quality estimation algorithm for a vein verification system based on the analysis of the image and metadata was proposed. In Reference [124], a new approach that depends on a thorough study of feature representation to predict finger vein image quality was introduced. The quality of the vein image is assumed after estimating the quality of a biometric verification system. In Reference [125], the finger vein template evolving method was designed to obtain enhanced templates; it can reduce the impact of templates that change when the matching process is performed. Reference [126] focused on the performance of rules, which are based on fusion and SVMs, by using fusion on multimodal systems and evaluating biometrics, such as normal fingerprint, face, and finger vein modalities.

The second group (2/8 articles) evaluated the process performance of the finger vein system. Reference [127] examined the performance of rules, which depend on score level fusion and SVM-based score level fusion. The measure of SVM in the multibiometric fusion performance and experimental results suggests that the performance of SVM can be improved by applying normalisation towards the input score vectors before the training and testing phases. Reference [128] evaluated various methods of dimensionality reduction on a finger vein database to select the most appropriate one for finger vein verification.

The third group (1/8 articles) focused on evaluating sensor device performance. Reference [129] evaluated a new device to capture images from individual fingers and obtained high-quality images.

The second subcategory (1/8 articles) focused on comparing user performance. Reference [130] presented a study on distinguishing certain individuals who perform poorly and cause the majority of errors (FAR and false reject rate or FRR). This subcategory can help in evaluating and improving the performance of biometric systems by analysing animal-like users.

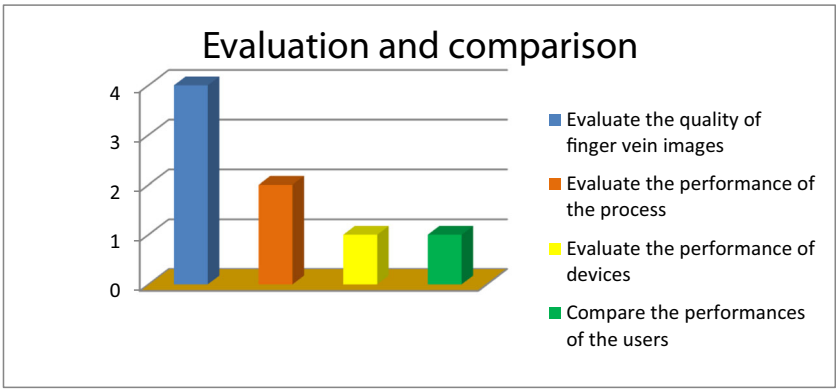

Fig. 9 Evaluation and comparison of the number of articles

Analytical studies

The third category (3/65 articles) attempted to present analytical studies that aimed to explore the traits of finger vein biometrics and investigate the impact of the change in infrared wavelength. Figure 6 shows that this category can be divided into two subcategories as follows:

The first subcategory (2/3 articles) explores finger vein biometrics. In Reference [131], a new fusion strategy at the decision level was proposed to study the personality of a finger vein via statistical analysis. Reference [132] presented the first study on using a soft biometric trait in finger vein recognition based on a comprehensive analysis of the presented criteria and thorough research on a finger vein image.

The second subcategory (1/3 articles) evaluated the impact of the change in NIR wavelength. In Reference [133], the correlation between the wavelengths in NIR spectra and the effectiveness of personal identification in a biometric verification system was examined.

Review and survey

The final and smallest category (2/65 articles) in our taxonomy consists of reviews and surveys of literature in terms of the capability of biometrics and utilises biometric authentication applications. Reference [134] used the geometric representation of finger vein pattern shapes to distinguish amongst people by using minutiae feature points in the verification operation. Reference [135] presented emerging technologies in biometrics to prove that the increase in new modalities provides pieces of evidence about the deficiency, but many problems are retained. Moreover, the capability of a method to satisfy the current security should be investigated.

Figure 10 illustrates the relationship between the number of articles and the years of their publication that were obtained from literature.

This chart explains the number of studies similar to the present study. This differentiation should be considered. Information that is relevant to the objective of this study should be extracted, and the study in this field should be extended. The present study utilised three databases, namely, IEEE Explorer, Science Direct and WoS, for basic research. These engines are the most reliable online databases for research. This study adopted 65 articles from various sources, in which 29 articles were from IEEE Explorer, 18 were from Science Direct, and 18 were from WoS. These databases contain different studies from various international journals, which consist of studies on finger vein biometric verification systems and their various applications. Figure 11 presents the details of the four broad categories of our taxonomy based on the number of articles and databases that were used in this research. This chart consists of all articles that were used in this study. It also displays the relationship amongst the sections of the articles and subgroups within this study, that is, development, design, review and survey, analysis, evaluation and comparison. A total of 65 articles were adopted from various databases. This chart presents various rations among these articles. The development and design category comprises 52 articles, the evaluation and comparison category has eight articles, the analytical studies category has three articles and the review and survey category has two articles.

Figure 12 depicts the distribution of subcategories within the taxonomy based on the database used in the search. The taxonomy consists of four basic sections, namely, development and design, evaluation and comparison, analytical studies, and review and survey. This chart explains various studies used in the current research topic through subcategories in the taxonomy. These subcategories define the directions for several current and future studies in this field.

Moreover, these subcategories may be considered a starting point for many researchers, designers, developers and postgraduate students in their future studies. These subcategories could recommend directions for many future studies in the field of biometric authentication, which will be discussed in detail in the following paragraph.

Discussion

This study aims to provide researchers with an updated overview of research directions related to finger vein biometric

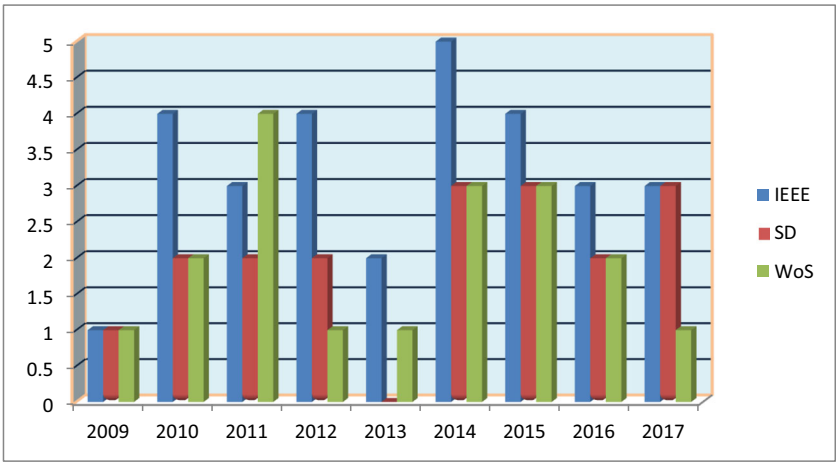

Fig. 10 Categories of articles by year of publication

verification and highlights important data that can help them handle this topic. This literature review investigates previous studies and presents a taxonomy that explains them.

The taxonomy based on this literature review has several advantages. However, a new researcher studying finger vein verification may be confused by the abundant publication on this topic when no classification exists. Moreover, the researcher may be uncomfortable of the actual activities in this topic. Many articles have discussed this topic from a preliminary perspective. Several researchers have investigated a number of current applications and certain articles that consist of developing and/or designing actual applications. This taxonomy assists in classifying different articles collected from reliable online databases for a meaningful, manageable, coherent research. Moreover, this taxonomy supplies researchers with important ideas on this topic in different ways. A researcher can use this taxonomy to determine existing probabilities in a given topic and open a new direction in the research on finger vein biometric verification. This classification also consists of current applications or skills in developing and/or designing these applications. Moreover, this classification simplifies gap detection for researchers about a given topic and the mapping of finger vein verification systems and highlights the weaknesses and strengths in the literature review. The examined articles indicate that several groups have obtained considerable attention in terms of development and design. Experiments were performed, and results were obtained. These works can be in the form of a development paper, a comparative study or an overview by matching their results with those of other studies, sharing future work directions with other researchers and providing recommendations to the audience.

These articles consist of reviews and discussions on finger vein biometric verification systems. They include any proposed system (according to the taxonomy) that consists of new methods, algorithms and techniques and other types of research that have been previously mentioned. Therefore, the following issues are investigated.

1. Available databases that can be used in scientific research to describe the method of collecting data and volunteers who contributed in these databases.
2. Motivations in using this type of technology.
3. Open challenges faced by researchers and users of this technology.

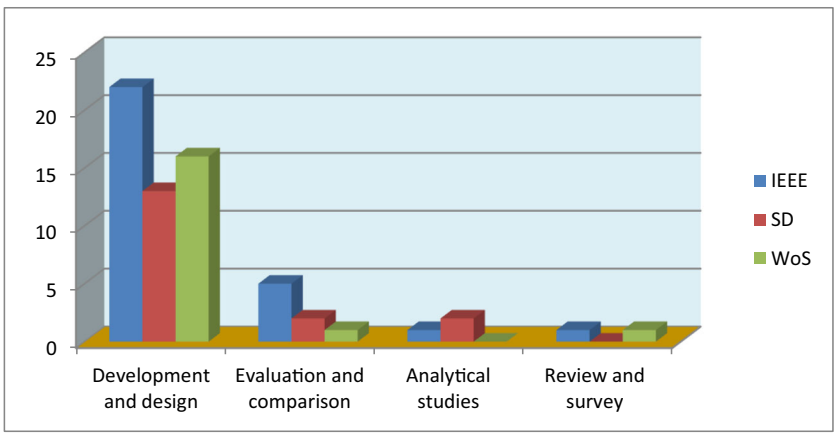

Fig. 11 List of included articles through the main category of article and database source

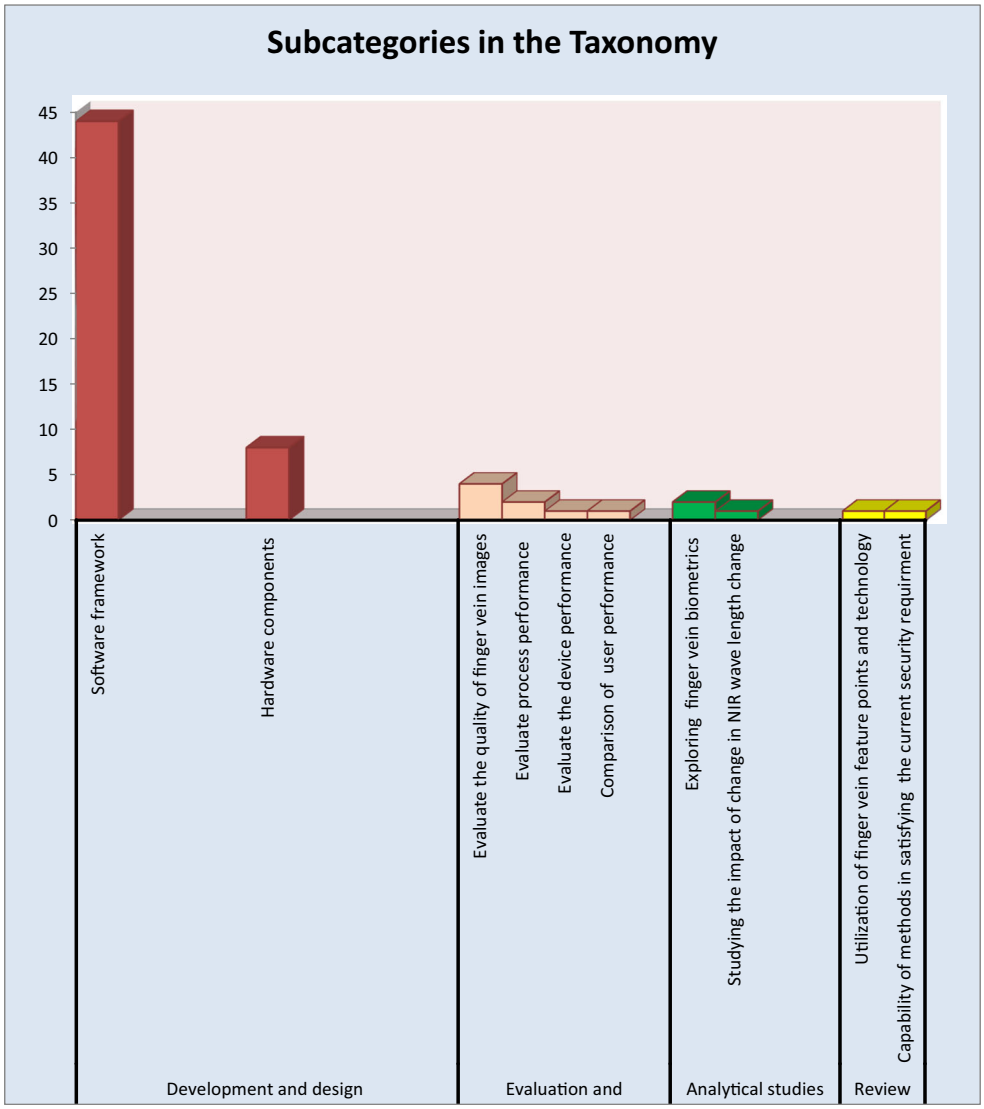

Fig. 12 Study subcategories in the taxonomy

4. Basic recommendations to audiences to avoid problems related to this technology.
5. Limitations of each type of technology used.
6. Description of new directions for research.

Available databases

In this subsection, the available databases for scientific research by companies or universities and databases recommended by researchers on this topic are discussed to enable researchers to select the suitable database and discover several methods that can be adopted to collect these datasets in different environments, as shown in Table 3.

Reference [22] created a database to examine the proposed algorithm. This database contains 2952 finger vein patterns that were collected from 123 volunteers (school staff; 83 males and 40 females). Their average age was 20–52 years. Each volunteer provided four fingers (left index, left middle, right index and right middle), including two features, namely, geometry and vein pattern. The images were captured in two sessions. In reference [23], the database was collected from 10 persons with 10 images from each finger

Reference [25] used an open-access database called polyu database, which was created by the hong kong polytechnic university. The database contains 6264 patterns that were collected from 156 volunteers for 11 months (april 2009–march 2010). In this database, each sample contains one finger vein image and one finger texture image. The total number of images is 6264, of which 1872 are finger vein images. The database in reference [26] was collected from 25 subjects. The vein image (forefinger and middle finger) was captured with 10 images from each finger. Reference [28] collected sample images from 51 volunteers (male and female). These volunteers are staff members and students of universiti sains malaysia aged 21–56 years. Each volunteer provided 10 patterns of

Table 3 Details of databases used in this literature review

References	Name of database	Created by	Time/period of collection	Number of volunteers	Age/gender of volunteers	Number of samples	Type of biometric	Indoor/outdoor	Availability online
[22]	Did not mention	Researchers	2 sessions	123 volunteers	83 males and 40 females (average age is 20–52)	2952 samples	Geometry and vein pattern	Indoor	Open access
[23]	Finger vein database	Researchers	Did not mention	10 volunteers	Did not mention	100 samples obtained from index finger only	Finger vein	Indoor	Did not mention
[25]	The Hong Kong Polytechnic University (PolyU) database	The Hong Kong Polytechnic University	11 months (April 2009–March 2010)	156 volunteers	Did not mention	Total images are 6264; finger vein images are 1872	Each sample contains one finger vein and one finger texture image	Did not mention	Open access
[26]	Did not mention	Researchers	Did not mention	25 volunteers	Did not mention	200 samples	Finger vein	Indoor	Did not mention
[28]	Finger vein database	Researchers	Did not mention	(51 persons, staff and students of Universiti Sains Malaysia)	Male and female (aged 21–56 years)	2040 samples	Finger vein	Indoor	Did not mention
[30]	PolyU database	The Hong Kong Polytechnic University	2 sessions in different times	156 volunteers	Male and female	3132 samples	Finger vein and finger texture image	Did not mention	Open access
	Finger vein database	Taiwan University of Science and Technology	Did not mention	85 volunteers	Male and female	680 samples	Finger vein	Indoor	Open access
[78]	Did not mention	Researchers using virtual instrument commands	Different periods	Did not mention	Did not mention	600 samples	Finger vein	Indoor	Did not mention
[81]	SDUMLA-HMT	Shandong University	Did not mention	505 volunteers	Male and female	33,298 samples	Finger vein	Indoor	Open access
[84, 112]	PolyU Finger database	The Hong Kong Polytechnic University	2 sessions in different times	Selected only 100 volunteers	Male and female	600 samples	Finger vein	Did not mention	Open access
	FVC2002 database	Did not mention	Did not mention	Selected only 100 volunteers	Male and female	600 samples	Fingerprint	Indoor	Did not mention
	PolyU Finger-Knuckle-Print database	Did not mention	Did not mention	Selected only 100 volunteers	Male and female	600 samples	Finger knuckle	Indoor	Did not mention
[85]	SDUMLA-HMT	Shandong University	Did not mention	100 volunteers	Male and female	3816 samples	Finger vein	Did not mention	Open access
[86]	Database A (PolyU database)	The Hong Kong Polytechnic University	Different time period	156 volunteers	Males and females	3132 samples divided into 2 sub-databases (2520 images taken by 156 volunteers and 612 images taken by 51 volunteers)	Finger vein and finger texture image	Did not mention	Open access
	Database B (USM database)	USM	2 separate sessions	123 volunteers	Males 83 and females 40	5904 images	Finger vein	Did not mention	Open access
[88]	PolyU database	The Hong Kong Polytechnic University	2 separate sessions with a gap of	156 volunteers	Did not mention	3132 samples	Finger vein and finger texture image	Did not mention	Open access

Table 3 (continued)

References	Name of database	Created by	Time/period of collection	Number of volunteers	Age/gender of volunteers	Number of samples	Type of biometric	Indoor/outdoor	Availability online
			2 months between these sessions						
[89]	Did not mention	Did not mention	Did not mention	100 fingers	Did not mention	200 samples	Finger vein	Did not mention	Did not mention
[90]	TED-FV	Researchers	Did not mention	Did not mention	19–60 years	164 samples	Finger vein	Indoor	Open access
[91]	Did not mention	Researchers	Did not mention	10 volunteers	Did not mention	100 samples	Finger vein	Indoor	Did not mention
[92]	PolyU database	The Hong Kong Polytechnic University	2 sessions in different times	156 volunteers	Male and female	3132 samples	Finger vein and finger texture image	Did not mention	Open access
	USM database	Universiti Sains Malaysia	2 sessions (2 weeks between these sessions)	123 volunteers	Males and females	5904 samples (index, middle, and ring fingers with 6 images obtained per finger)	Finger vein	Indoor and outdoor	Open access
[93]	Did not mention	Researchers	Did not mention	50 persons (5 fingers from each one)	Did not mention	250 samples	Finger vein	Indoor	Did not mention
[95]	SDUMLA_HNT database	Did not mention	Did not mention	106 volunteers	Did not mention	1272	Finger vein	Did not mention	Open access
[96, 108, 125]	PKU	Researchers	1 year and 6 months	5208 persons	Did not mention	50,700 samples	Finger vein	Did not mention	Open access
[97, 106]	SDUMLA-HMT	Shandong University	Did not mention	106 volunteers	Males and females	3816 grey-scale patterns	Finger vein	Did not mention	Open access
[98]	MMCBNU_6000	Researchers	1 session	100 volunteers	Did not mention	6000 samples	Finger vein	Indoor	Open access
[99]	GUC45	Gjovik University College in Norway	12 sessions	45 volunteers	Males and females	10,800 samples	Finger vein	Did not mention	Did not mention
	UC3M	Gjovik University College in Norway	1 session	29 volunteers	Males and females	348 samples	Wrist vein samples	Did not mention	Did not mention
[93, 102]	PolyU database	The Hong Kong Polytechnic University	11 months (April 2009–March 2010)	156 volunteers	Did not mention	6264 total images, 1872 finger vein images	Each sample contains one finger vein and one finger texture images	Did not mention	Open access
	MLA database	Researchers	20 days	34 volunteers	Did not mention	1020 samples	Finger vein	Indoor	Did not mention
[101]	Did not mention	Researchers	Did not mention	700 persons (30 finger vein images from each person)	Did not mention	2100 total samples (10 images obtained from each finger)	Finger vein	Indoor	Did not mention
[102]	MLA database	MLA Lab	2 separate sessions, 20-day time period between these sessions	34 volunteers	20 males and 14 females between 19 and 48 years old	4080 samples	Finger vein	Indoor	Did not mention
	PolyU database	The Hong Kong Polytechnic University	11 months (April 2009–March 2010)	156 volunteers	Did not mention	6264 patterns	Each sample contains one finger vein and one finger texture images	Did not mention	Open access
	Rotation database	Researchers	Rotating each image in the MLA database	20 males and 14 females aged 19–48 years old	4080 samples	Finger vein	Indoor	Did not mention	
		Researchers			2100 samples	Finger vein	Indoor	Did not mention	

Table 3 (continued)

References	Name of database	Created by	Time/period of collection	Number of volunteers	Age/gender of volunteers	Number of samples	Type of biometric	Indoor/outdoor	Availability online
	Illumination database		Selecting 70 fingers influenced by illumination from the MLA database	20 males and 14 females aged 19–48 years old					
[103]	Finger vein database	Researchers	Did not mention	125 fingers	Did not mention	1125 samples	Finger vein	Indoor	Did not mention
[104]	Finger vein database	Researchers	Did not mention	10 volunteers	Did not mention	100 samples obtained from index finger only	Finger vein	Indoor	Did not mention
[105]	Did not mention	Researchers	Did not mention	More than 300,000 fingers	Did not mention	More than 700,000 samples	Finger vein	Indoor	Did not mention
[107]	Did not mention	Researchers	Did not mention	10 volunteers	Did not mention	100 samples	Finger vein	Indoor	Did not mention
[110]	Did not mention	Researchers	3 months	116 volunteers	Male and female	10 vein images obtained from 232 fingers	Finger vein	Indoor	Did not mention
[113]	Multimodal biometric database	Researchers	Did not mention	35 University of Cairo staff and students	Male and female	6 images per user	Finger vein and face	Indoor	Did not mention
[115]	Did not mention	Researchers	Did not mention	20 hands	Did not mention	100 samples	Finger vein	Indoor	Did not mention
[116]	Did not mention	Researchers	Did not mention	20 fingers	Did not mention	100 samples	Finger vein	Indoor	Did not mention
[117]	Did not mention	Researchers	Did not mention	50 fingers	Did not mention	500 samples	Finger vein	Indoor	Did not mention
[118]	Multimodal database	Researchers	3 months	41 volunteers	10 females and 31 males (90% aged 20–35 years, while 10% are older than this age range)	1500 samples	Fingerprint and finger vein	Indoor	Did not mention
[119]	Did not mention	Researchers	2 months	32 volunteers	10 females and 22 males (90% aged 21–35 years and the rest are older than this age range)	1780 samples	Finger vein	Indoor and outdoor	Did not mention
[120]	Finger vein database	Researchers	Did not mention	100 volunteers	55% male and 45% female (aged 21–51 years)	6000 samples	Finger vein	Indoor	Did not mention
[121]	THU-FVFDT database	Researchers	2 sessions	220 volunteers	male and female	4 finger vein images and 4 finger dorsal images per session	Finger vein and finger dorsal	Indoor	Open access
[122]	SDUMLA-FV	Joint Lab for Intelligent Computing and Intelligent Systems of Wuhan University	Did not mention	106 volunteers	Did not mention	500 samples	Finger vein	Indoor	Open access
[123]	GUC45	Gjovik University College in Norway	12 sessions	10 fingers	Males and females	10,800 samples	Finger vein	Indoor	Did not mention
	UC3M	Gjovik University College in Norway	1 session	2 wrists	Males and females	348 samples	Wrist vein samples	Indoor	Did not mention
	SNIR	Gjovik University College in Norway	1 session	2 dorsal	Males and females	732 samples	Dorsal hands	Indoor	Did not mention

Table 3 (continued)

References	Name of database	Created by	Time/period of collection	Number of volunteers	Age/gender of volunteers	Number of samples	Type of biometric	Indoor/outdoor	Availability online
	SFIR	Gjovik University College in Norway	1 session	2 dorsal	Males and females	173 samples	Dorsal hands	Indoor	Did not mention
[124]	Universiti Sains Malaysia (USM) database	Universiti Sains Malaysia	2 sessions (two weeks between these sessions)	123 volunteers	Males and females	5904 samples (index, middle, and ring fingers with 6 images per finger)	Finger vein	Indoor and outdoor	Open access
	PolyU database	The Hong Kong Polytechnic University	2 sessions	156 volunteers	Did not mention	3132 samples	Finger vein and finger texture image	Did not mention	Open access
	MM- CBNU_6000	Researchers	1 session	100 volunteers	Did not mention	6000 samples	Finger vein	Indoor	Open access
	SDUMLA-HMT finger vein database	Shandong University	Did not mention	106 volunteers	Males and females	3816 samples	Finger vein	Indoor	Open access
[126, 127]	NIST-multimodal	National Institute of Standards and Technology NIST	Did not mention	517 volunteers	Did not mention	2 face and 2 fingerprint images for each person (517 total images and 266,772 total imposter patterns)	Fingerprint and face samples	Did not mention	Did not mention
	NIST-face	National Institute of Standards and Technology NIST	Did not mention	3000 users	Did not mention	2 face images from each user, (2999 total images)	Face samples	Did not mention	Did not mention
	NIST-fingerprint	National Institute of Standards and Technology NIST	Did not mention	6000 users	Did not mention	6000 genuine samples	Fingerprint	Did not mention	Did not mention
	Merged databases of fingerprint, face and finger veins	Researchers	Did not mention	Fingerprint from 510 virtual users and finger vein images from 85 users	Did not mention	510 fingerprint samples	Fingerprint and finger vein	Did not mention	Did not mention
[128]	Did not mention	Researchers	Did not mention	204 persons (10 samples per person)	Did not mention	2040 samples	Finger vein	Indoor	Did not mention
[129]	Did not mention	Researchers	2 months	32 volunteers	21–35 years old	1780 samples	Finger vein	Indoor and outdoor	Did not mention
[131]	Did not mention	Researchers	Did not mention	320,100 school staff volunteers	152,549 male and 167,511 female	718,399 samples	Finger vein	Indoor	Did not mention
[132]	PolyU database	The Hong Kong Polytechnic University	2 sessions in different times	156 volunteers	Male and female	3132 samples	Finger vein and finger texture images	Did not mention	Open access
	Did not mention	Researchers	2 sessions in different times	34 volunteers	20 males and 14 females	2720 samples	Finger vein	Indoor	Did not mention
[133]	Did not mention	Researchers	Different period time	107 volunteers	Male and female	11,556 samples	Finger vein	Indoor	Did not mention

four fingers. Reference [30] used two databases, namely, hong kong polytechnic university and taiwan university databases. The dataset in reference [78] included 600 finger vein patterns collected at different time intervals and tested through labview using virtual instrument commands; online availability was not mentioned. Reference [81] used the sdumla-hmt finger vein database, which was created by shandong university. The total number of patterns during enrolment and authentication phases was 33,298. These patterns were collected from 505 users, and each user provided index, middle and ring fingers from each hand. References [84, 112] used a multimodal biometric database built from three unimodal databases. Thus, the resulting database contains finger vein, fingerprint and finger knuckle images. The finger vein database is the hong kong polytechnic university finger database, which only has 100 fingers, and the fingerprint database is the fvc2002 database, which also contains 100 fingers. The finger knuckle print dataset is a subset of the polyu finger–knuckle–print database that contains 100 fingers. Each database used six images per user, that is, three images during enrolment and three images for matching during the test step. Sdumla-hmt database, which is only available online for research and non-commercial purposes, was used in reference [85]. This database was created by shandong university and is the first free-access finger vein biometric database. A total of (100) volunteers contributed in creating this database. The volunteers provided finger vein images of their index, middle and ring fingers on both hands, and the collection for each of the six fingers was repeated six times. Reference [86] used two databases where images were collected during different periods. Database (a), namely, polyu database, contains 3132 images collected from 156 subjects. This database is divided into two sub-databases. The first sub-database contains 2520 finger vein images captured from 156 volunteers in different periods with an average of 66.8 days. Each volunteer provided six images. The second sub-database was collected from 51 volunteers who provided 612 images in one session. Database (b) is called usm database, which was collected from 123 volunteers, of which 83 were males and 40 were females. A total of 492 classes were provided in two separate sessions. A total of 5904 images were obtained in both sessions. Reference [88] used a database that contains 3132 finger vein images from 156 subjects. Reference [89] used a database collected from 100 fingers. Two images from each finger were captured, and two imaging devices were used. Reference [90] created the database called ted-fv, which contains 164 finger vein images. The age of the volunteers, who are university staff members, ranged between 19 and 60 years. The database in reference [91] was collected from 10 volunteers, and 10 patterns were collected from each finger. Moreover, these researchers used a ccd camera to capture these patterns. Each pattern was captured at (640 × 480) pixels. Reference [92] used two databases, which were obtained from hong kong polytechnic university and universiti sains malaysia finger vein databases. Reference [93] used the database created by the contribution of 50 volunteers. Images of five fingers from each volunteer were captured. Thus, the total number of finger vein images was 250; online availability was not mentioned. Reference [95] used the sdumla_hnt database, which was created by collected finger vein images from 106 users. These users provided three finger vein images from each hand. Thus, the total number of samples is 1272. References [96, 108] and [125] used the pku finger vein database that contains 50,7000 patterns collected from 5208 volunteers who provided 10,140 fingers. References [97, 106] used the sdumla-hmt finger vein database, which was created by shandong university and collected from 106 volunteers. Each sample was captured from index, middle and ring fingers for both hands of the volunteer. Thus, the total number of samples is 3816 grey-scale patterns. Reference [98] adopted the mmcbnu_6000 database that contains 6000 grey-scale images collected from 100 volunteers. Reference [99] utilised two finger vein databases created by gjovik university college in norway using a ccd camera at an extended period. The first database is guc45, which was collected from 45 subjects and has 10,800 finger vein images in 12 separate sessions. The second database is uc3m, which contains wrist vein patterns collected from 29 volunteers captured from six images from each wrist in one session. Thus, the total number of images is 348. References [100, 109] used two databases. The first database is the polyu database, where images were collected from 156 volunteers for 11 months. Each volunteer provided six images. The second database is the mla database, which was created by the researchers in the laboratory. This database used samples collected from 34 volunteers for 20 days through an imaging device created by the joint lab for intelligent computing and intelligent system of wuhan university, china. Each volunteer provided 30 images for each hand (left and right) and three fingers (index, middle and ring). The database in reference [101] consisted of 2100 finger vein patterns collected from 700 volunteers. Each volunteer contributed 30 finger vein images of their fore-, middle and ring fingers, and 10 images per finger on the right hand. Reference [102] used four databases in the experiments. The first database was the mla database created by the mla lab. The samples in this database were collected from 34 volunteers (20 males and 14 females) and captured from each volunteer within two separate sessions (20 days was the period between these sessions. The age of these volunteers was between 19 and 48 years. The volunteers included students, lecturers and workers of the school. Each volunteer provided four images from their left index, left middle, right index and right middle fingers. Thus, each volunteer provided 30 images. Therefore, the total number of samples was 4080. The second database is the polyu finger vein database, which contains 6264 patterns collected from 156 volunteers for 11 months (april 2009–march 2010) in two separate sessions. The third database is

the rotation database, which was created by rotating each image in the mla database with random degree angles. This database contains 4080 patterns. The fourth and final database is the illumination from the database, which was created by selecting 70 fingers that were influenced by the illumination from the mla database. In this database, pre-processing was applied to the images. This database contains 2100 finger vein patterns. Reference [103] used a database that was collected from 125 fingers obtained by a prototype device. Reference [104] created a finger vein database that contains 100 finger vein images collected from 10 volunteers and captured 10 images of the index finger only thus, this database contains 100 finger vein images. Reference [105] utilised a database that was collected from a laboratory (indoor environment) and contained more than 300,000 fingers and 700,000 images. Reference [107] used 10 images for each index finger in the right hand collected from 10 volunteers. Thus, the total number of samples was 100. Reference [110] used 10 vein images obtained from 232 fingers of 116 subjects. The images were collected by using a 280 × 400 ccd image sensor. Reference [113] collected a dataset from 35 staff and students of the university of cairo. The database in reference [115] contained 100 finger vein images from 20 hands; online availability was not mentioned. The database in reference [116] contained 100 finger vein images that were collected from 20 fingers, and each finger had five patterns. Online availability was not mentioned. Reference [117] used a database that consisted of 500 finger vein patterns collected from 50 fingers, with 10 images for each finger; online availability was not mentioned. In reference [118], the researchers created a database in the lab for three months from 41 subjects (10 females and 31 males); 90% of these subjects were aged 20–35, and 10% were older. Each subject presented three fingers from each hand (index, middle and ring fingers) with 10 images per finger. Thus, this database contains 1500 patterns, including fingerprint and finger vein patterns. Reference [119] created a database indoors (inside a lab) by using artificial light and outdoors (outside the lab) under sunlight. Data collection was conducted for two months. The total number of samples, which were collected from 32 volunteers (10 females and 22 males), was 1780. A total of 90% of the subjects were 21–35 years old, and the remaining portion was older. Each subject provided three fingers (index, middle and ring fingers) from each hand. In reference [120], the researcher created a finger vein database that was collected from 100 volunteers (55% males and 45% females) aged 21–51 years. The images were captured from the index, middle and ring fingers of each hand of the volunteers with 10 images per finger. Therefore, the total number of images is 6000. Reference [121] focused on the vein and dorsal side of the fingers. A database that includes both biometrics is unavailable. Thus, the researchers created their own database by collecting these biometric data from 220 volunteers and labelled the database thu-fvfdt. Currently, thu-fvfdt is an open-access database for other researchers. In this database, four finger vein and four finger dorsal images are collected in each of the two sessions

The SDUMLA-FV database was used in Reference [122]. This database is available online for scientific research and contains a collection of finger vein patterns. This database was designed by the Joint Laboratory for Intelligent Computing and Intelligent System of Wuhan University. Reference [123] adopted four databases. The first database is GUC45 (20), which contains 10 finger samples and 45 subjects in 12 sessions. The total number of samples is 10, 800. The second database is UC3M (21), which contains two wrist samples and 29 subjects in one session. The total number of samples is 348. The third database is SNIR, which has 22 samples from two dorsal hands and 122 subjects in one session. The total number of samples is 732. The fourth database is SFIR, which contains two dorsal hands and 33 subjects in one session. The total number of samples is 173. The database in Reference [124] utilised four public databases. Database (A), which was created by Universiti Sains Malaysia, contains 5904 finger vein images that were collected from 123 volunteers in two separate sessions (two weeks between these sessions) using both hands (index and middle fingers) with six images per finger. Database (B) is a public database, which was created by the Hong Kong Polytechnic University. This database contains 3132 images that were collected from 156 volunteers in two separate sessions. Database (C), namely, MM-CBNU_6000, contains 6000 images that were collected from 100 volunteers in one session. Database (D), namely, SDUMLA-HMT finger vein database, was created by Shandong University. The samples in this database were collected from both hands (index, middle and ring fingers) in one session. Thus, the total number of samples is 3816. The experiments in References [126, 127] adopted four databases. The first database, namely, NIST-multimodal, contains two face scores and two fingerprint scores. These scores were collected from 517 subjects. The number of genuine and imposter scores was 517 and 266,772, respectively. The second database is NIST-face, which contains 3000 two-face images from each volunteer. Thus, the total number of images was 2999. The third database is NIST-fingerprint, which was collected from 6000 volunteers. This database can provide 6000 genuine scores and (6000 × 5999 = 35,994,000) imposter scores. The fourth database was produced from the merged database of fingerprint, face and finger vein and consisted of 510 virtual users. The images were captured from the right index fingerprint, and a finger vein image was collected from 85 volunteers; online availability was not mentioned. The database in Reference [128] contains 2040 finger vein patterns collected from 204 subjects, with 10 samples per person. Reference [129] used a new sensor device for collecting finger vein data in two ways, namely, indoor using artificial light and outdoor using normal sunlight. All data were collected within two

months from 32 volunteers with an average age of 21–35 years. The total number of samples is 1780). These samples were captured from three fingers of each hand. Reference [131] used a database that consists of 718,399 finger vein images from 363,703 fingers. The dataset in Reference [132] used two databases, namely, an open-access database and a database created by the researchers. The first database was created by the Hong Kong Polytechnic University and contains 3132 finger vein and texture images collected from 156 volunteers by capturing vein and texture images of the index, middle and ring fingers of each hand in two separate sessions. However, this study used only finger vein images. The second database was created by the researchers themselves and contains 2720 finger vein images collected from 34 volunteers (20 males and 14 females) in two separate sessions for 20 days. Twenty images were captured from the index and middle fingers of each hand of every volunteer between sessions. In Reference [133], the finger vein database consisted of 11,556 unique patterns collected from 107 volunteers and captured at nine wavelengths of NIR light.

Motivations

The finger vein biometric verification system is a product of the development of the modern society to satisfy the requirements in many applications of human biometric verification. We can observe increasing requirements for accurate and efficient personal verification. In this section, we discuss several characteristics of the present study. These characteristics are identified and grouped into categories to aid in further discussion. Figure 13 displays the number of articles that served as motivations for the present study. The repetitions in this chart highlight the biological attributes related to security motivation, which is the main motivation of this research owing to the repetition of the same motivations in more than one article.

Figure 14 presents the benefits of using the finger vein biometric verification system according to the classifications to provide readers a clear picture and identify the benefits of using this type of verification system.

Biological attributes related to security motivations

References [22, 91] and [112] found that biometric technology authentication systems are extensively popular because they provide a high level of security and reliability for individual authentication; biometric systems are more reliable than traditional security systems, which have been used to secure critical information or personal authentication, such as passwords and access cards. These types of authentication technologies are easy to copy and replicate and prone to counterfeiting. Thus, criminals can easily use the stolen information. in addition, the incidence of forgetting passwords or cards is high. By contrast, finger vein biometrics demonstrates numerous attributes in terms of security purposes, such as the uniqueness of each person and long-term stability during human life. finger veins are invisible to the human eye because veins are located underneath the skin; thus, finger veins are not prone to external distortion or modification. moreover, references [26, 106] indicated that biometric verification is unique to every person. thus, biometric identification systems are more reliable in verifying identity than other techniques, such knowledge- or token-based identification systems. references [78, 107, 109] and [134] indicated that finger vein biometrics exhibits various characteristics; biometrics information is invisible, difficult to invade, difficult to copy, provides high levels of accuracy and security and is matchless even between twins. Furthermore, each finger vein pattern verification differs from other finger identification, even in the same person. biometric information is also incomparable between the same fingers of each hand in the same person. references [79, 89, 115] and [116] showed that finger vein biometrics is inherent and highly reliable, cannot be lost nor forgotten and is resistant to counterfeiting. this technology is extremely difficult to duplicate or copy by an attacker because the information is within the individual, and authentication requires the presence of the person involved. references [85, 99, 100] and [119] indicated that the motivation for using finger vein biometrics is attributed to its natural state, uniqueness, and universality. finger vein biometrics has high spoofing resistance and provides a wide range of advantages, such as (1) suitability and ease of

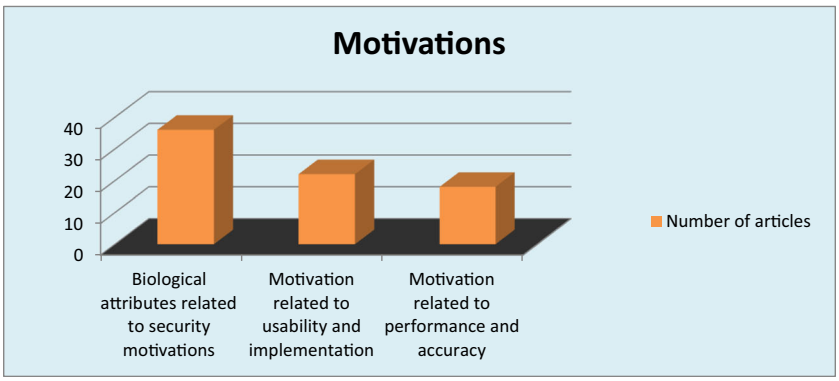

Fig. 13 Major motivations for the present study

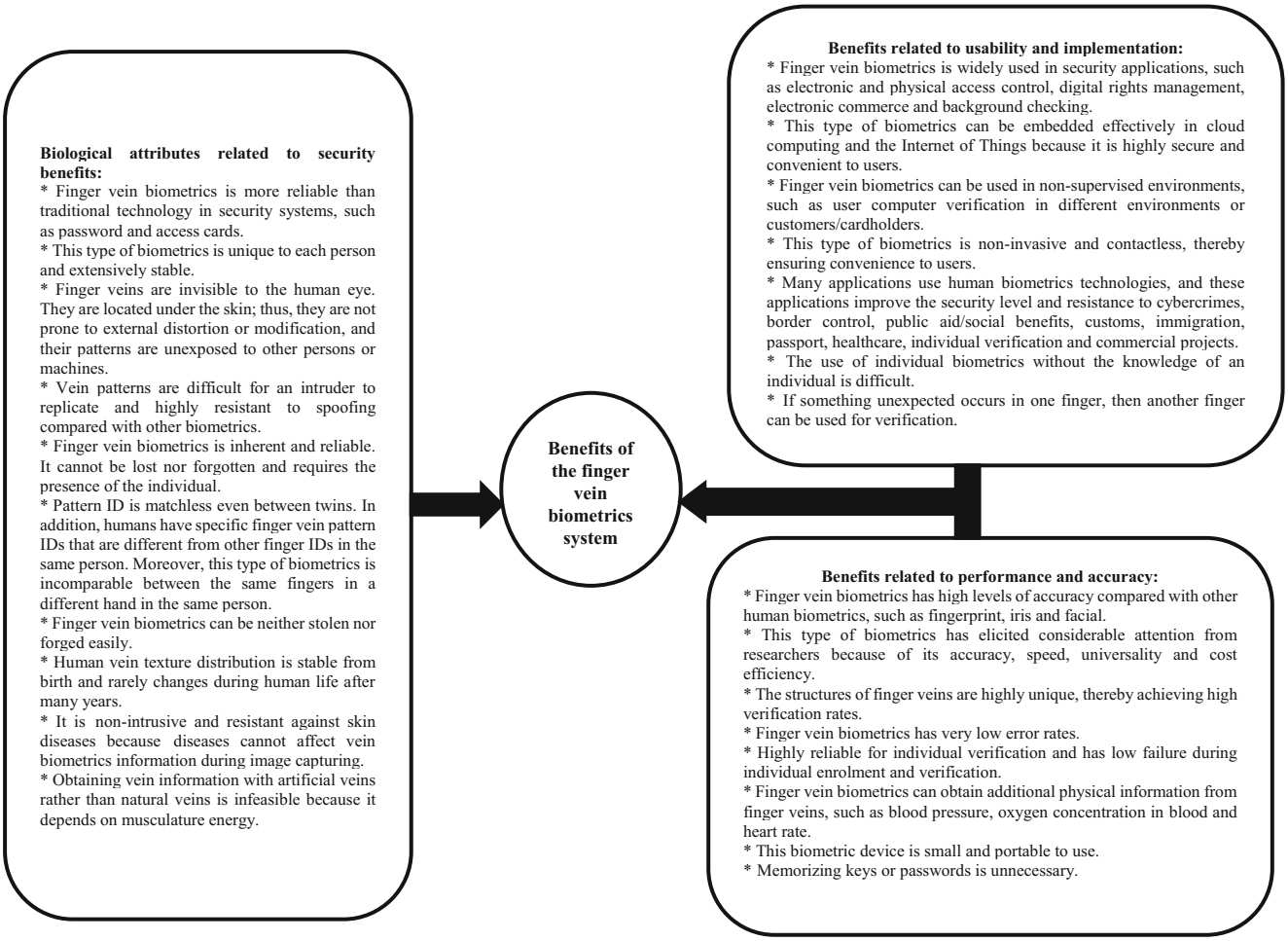

Fig. 14 Benefits of using the finger vein verification system

capture, (2) unique personal information and high verification accuracy and (3) only for live body verification. reference [95] showed that in a finger vein biometrics verification system, contact with the sensor device during the enrolment step is unnecessary; thus, leaving traces in the sensor, which can be used as a threat in the future, is infeasible. Therefore, stealing and forging biometrics information are very difficult. References [97, 110] indicated that in the verification phase of using finger vein biometrics, the skin condition is not a hindrance to obtaining a clear image; thus, finger vein biometrics is robust against finger surface conditions. reference [98] showed that finger vein patterns have rich piecewise line attributes and are stable to use, and these patterns clearly describe finger vein patterns for individual verification. Another feature is that obtaining vein information using artificial veins rather than natural veins is infeasible because this system depends on musculature energy [101]. according to references [103, 119], this feature of invisibility provides additional security because patterns are concealed from other individuals or machines compared with other verification technologies, and the replication of vein patterns is difficult for an intruder, resulting in the finger vein biometrics verification system having high resistance to spoofing compared with other biometrics systems. This technology is thus excluded from the abovementioned problems. References [105, 120] revealed that finger vein patterns are captured inside the finger and thus cannot be stolen or forged easily. Spoofing of this type of system technology is extremely difficult, and finger vein verification is much safer than the widely used fingerprint system. reference [108] indicated that finger vein biometrics has its inherent superiority in terms of accuracy, speed and security. According to references [110, 132], the favourable features of finger vein biometrics are its non-intrusive nature and resistance to skin diseases because these diseases cannot affect vein biometric information during image capture. reference [114] indicated that these types of biometric identification systems are distinctive to differentiating among individuals, and biological information from finger veins, such as blood pressure, oxygen concentration in the blood and heart rate, can be obtained. Moreover, human vein texture distribution is permanent from birth and rarely changes during the human lifetime; thus, this security technology is robust and stable. references [115, 124] reported that biometric information is extensively stable (from birth to death), rarely changes under any

circumstance, is located underneath the skin and is therefore invisible and not prone to external distortion, except in cases of deep wounds or intense burns. reference [116] showed that in the authentication phase, an individual should be present at the location of the sensor device when he/she must enrol his/her pattern to gain access to a system

Motivation related to usability and implementation

References [23, 82] showed that biometrics technology can be embedded effectively into cloud computing and the internet of things because it is highly secure and convenient to users because remembering a password is unnecessary. This technology can also be crucial in various security task applications, such as e-passports. references [26, 28, 99] and [131] showed that finger vein biometrics is used in the financial sector, such as bank transactions and end-user verification. In the digital world, various applications and users have high demands for accuracy and reliability. thus, finger vein verification systems can be a reliable solution for verification in public devices, such as entrance control systems and door access control. References [30, 79] reported that the use of finger vein biometrics technology is growing rapidly in terms of handling security issues, such as electronic and physical access control, digital rights management, electronic commerce and background checking. In addition, reference [78] indicated that this type of biometrics is simpler and more efficient than fingerprint techniques. reference [83] showed that technologies that use human biometrics in authentication are highly appropriate for enhancing security level and cybercrime prevention. Border control, public aid/social benefits and commercial projects can benefit from these technologies. Reference [86] showed that finger vein biometrics has an ideal feature, that is, using the biometric information of an individual without his/her knowledge is very difficult. Moreover, this type of biometrics is widely applied to identify and verify criminals and is used to prevent access to sensitive systems and authorize access to digital devices. References [88, 105] and [120] indicated that capturing images during individual enrolment to obtain finger vein patterns is non-invasive and contactless, thereby enhancing hygiene, preventing skin infections and ensuring user convenience. references [90, 120] showed that each person normally has 10 fingers; if something unexpected occurs to one finger, another finger can be used for verification. references [97, 99] and [124] indicated that currently, technologies that use finger vein patterns are used in various fields, such as medical, financial, law enforcement, airports and other applications that require high levels of security and privacy. reference [101] showed that for user familiarity, finger vein patterns can be captured conveniently and prevent any contamination from other people because touch/contact with the sensor during enrolment is unnecessary. Reference [123] indicated that the system is also false-resistant; this feature strengthens the application of this technology in non-supervised environments, such as computer user verification in different environments, customer/card user verification during authentication when using atms or working in non-supervised environments. For example, finger vein products in poland are highly successful in the financial sector, where most organizations (top commercial and cooperative banks) use this technology [133]

Motivation related to performance and accuracy

During individual enrolment, touching/contact with the sensor is unnecessary because the veins are detected by a CCD camera through a NIR filter. The haemoglobin in the blood absorbs this light; thus, the veins that appear as dark lines are easily detected, as shown in References [23, 111] and [132]. Information embedded inside the veins can be easily retrieved at any time using certain devices [28]. Devices can be small and portable [103]. Finger vein biometrics has high levels of accuracy compared with other human biometrics, such as fingerprint, iris and facial biometric systems [80]. Finger vein biometrics also has an inherent and natural connection with user verification and does not require remembering any key [82]. This type of biometrics has been widely used in studies. Finger vein biometrics has low levels of failure during individual enrolment. In addition, it has high reliability for individual verification and low failure during enrolment and verification [88]. Finger vein patterns are highly reliable because of low error rates, high levels of immunity against spoofing and user convenience compared with other biometric systems used for identification, as shown in References [89, 98, 118] and [119]. Accordingly, finger vein biometrics has elicited considerable attention from researchers because of its combined accuracy, speed, universality and cost-efficiency [94, 131]. Biometrics information is highly available and easier to acquire using cost-efficient sensor devices compared with other types of verification systems [97]. Finger vein biometrics has several advantages over other biometric systems (for example, face, voice, fingerprint and iris), such as low forgery rate, non-invasiveness and noncontact live-body detection, as shown in References [101, 102] and [122]. The following additional advantages represent perfect motivations for using this technology.

1. High levels of security
2. Small and portable devices
3. Crucial roles in various tasks related to critical applications, such as access control, individual verification and electronic passport.

Finger vein biometrics has gained popularity over other types of biometric systems because of its resistance to forgery, live body detection, non-invasive data acquisition, and stability over extended periods [117]. Moreover, this technology is convenient to apply in many applications [124]. Compared

with other recognition technologies, finger vein technology is newly developed, has high levels of security, high-speed performance, and highly authentic verification results and similarity of patterns of different fingers [125]. Comparison between finger vein biometrics technology and facial recognition for individual verification reveals certain differences between these technologies. Finger vein biometrics is superior because facial recognition is affected by appearance factors, such as cosmetics, medical glasses or sunglasses and headwear; therefore, finger vein biometrics retains a high level of accuracy in verification [128]. Finally, the structures of finger veins are highly unique, thereby contributing to a high verification rate [129].

Challenges

The protection of information systems is important in preventing an attacker from accessing these systems and obtaining sensitive information. Thus, access to these systems should be controlled, and only authorized persons should be able to access this information. The finger vein biometrics verification system is an important technology to handle this task. Many developers and researchers have attempted to find easy and active solutions by creating a security system using finger vein biometrics, proposing various software frameworks and presenting an entire architecture to assist companies and organizations in securing their information. These studies focused on challenges related to finger vein biometrics applications. These challenges are discussed along with their references to enable readers to trace these resources and further the discussion on these challenges. These challenges are categorized into groups according to their nature, as presented in Fig. 15.

Challenges related to user performance

This type of challenge is a combination of factors that affect system performance and the result accuracy of matching. These factors are as follows:

User errors The shift and rotation of fingers in a sensor device are still major challenges in finger vein verification, as shown in References [25, 107] and [109]. This problem can reduce verification performance because the fingers move during enrolment; that is, shifting and rotation significantly affect matching results. Furthermore, during finger vein imaging, any movement or rotation of the fingers generates noise, which cannot be recovered later and therefore causes irregular luminance; as a result, different segments of the finger gain different amounts of light absorption, and irregular luminance can produce a processing error [103]. In biometric verification systems, several users perform poorly during enrolment, and this performance causes high FAR and FRR. These users affect the entire performance of the biometric systems [130].

Biometric finger features As regards another factor related to biometric finger features [88], in addition to varying thickness, certain attributes related to finger skin affect image captures, such as pigmentation, thickness and hair. Moreover, capturing images obtains information, such as the difference in thicknesses of finger muscles, bones and texture of networks surrounding the finger veins, which produce a shadow area, as indicated in References [90, 132]. References [119, 129] showed the varying thickness of finger skin, which yields unequal light distribution that passes through the fingers. Thus, vein patterns are difficult to capture in high quality because veins are underneath the skin, thereby requiring sufficient light density to be penetrated or reflected from the finger to obtain a clear structure of the vein. Capturing high-quality finger vein images remains challenging.

User gender Reference [93] reported that the quality of vein lines during image capture is insufficient because certain females do not have sufficient features that can be used during feature extraction and matching steps.

User's unpleasant habits Reference [125] showed that image quality changes slightly because unpleasant habits and accidents, such as deep wounds and burns that deform the veins, influence the structure of the fingers.

Challenges related to environmental influences

References [28, 103] showed that after image acquisition, images contain noise and unequal shadow areas in addition to vein patterns. this noise can reduce the accuracy of the verification result. References [78, 85] indicated that image acquisition is affected by venous pressure and body temperature changes, but the centreline of the vein remains stable. According to reference [79], the work environment affects authentication. thus, we must remove environmental noise. The verification process is also sensitive to these environments, thereby representing an important trade-off between accuracy and usability

References [86, 124] reported that finger vein image acquisition is naturally affected by factors, such as the environment, surrounding temperature, light propagation in imaging the finger vein, physiological changes and user performance. in this section, we discuss the influence of the environment on image acquisition. References [88, 125] showed that repeated image acquisition for an extended duration changes the templates slightly because environmental conditions, such as temperature, visible light confusion and noise, occur due to non-uniform lighting, low local contrast and hair and skin conditions

Challenges related to device performance

Reference [95] indicated that using multibiometrics in authentication systems may require extra acquisition sensors.

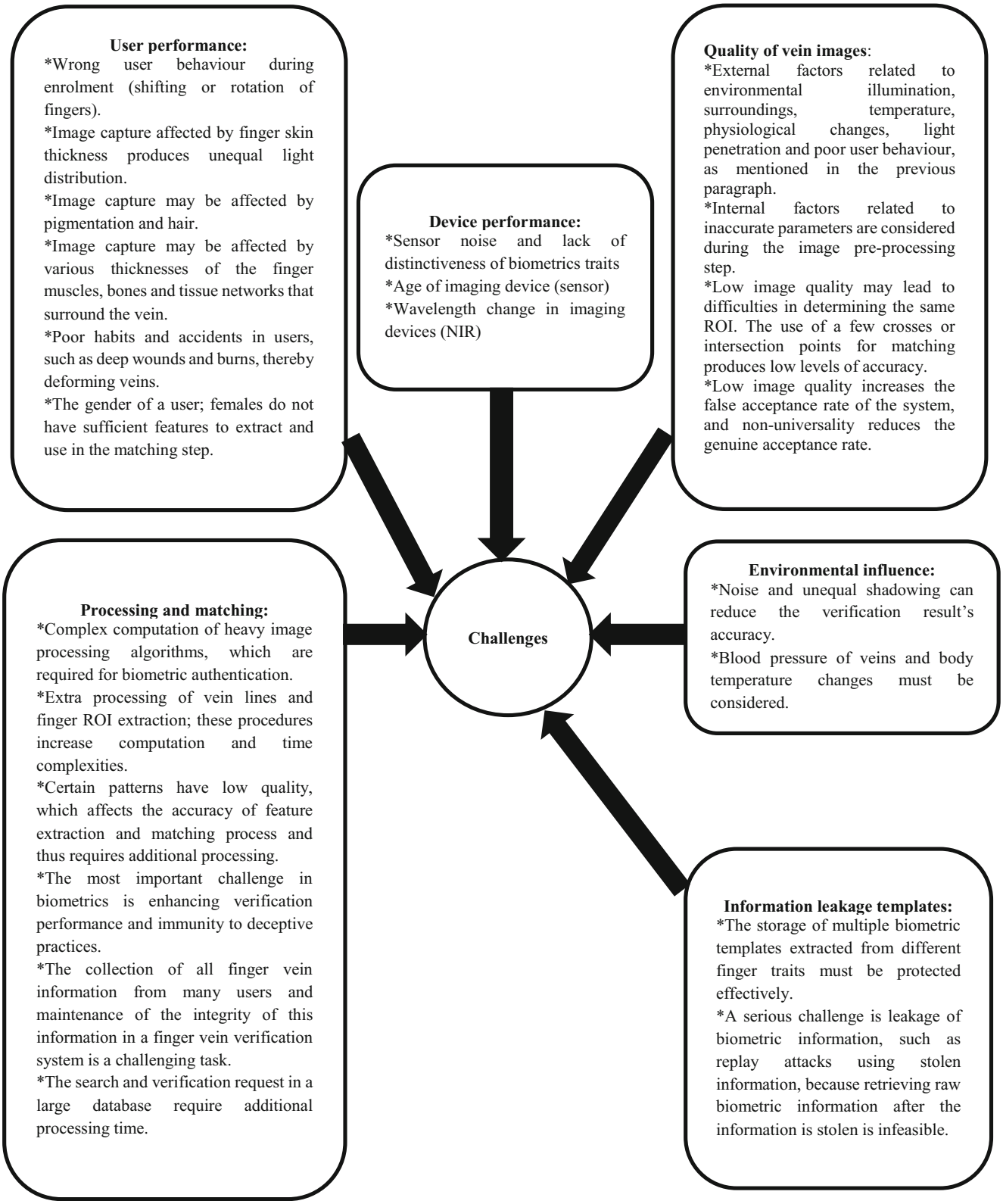

Fig. 15 Categories of challenges according to their nature

References [99, 101] showed that the extracted dark lines from finger vein images, which represent the veins, are unstable because the first images obtained during enrolment have low contrast and include certain noise and non-uniform brightness. Reference [114] reported that typically, finger vein verification techniques involve heavy and accurate computation and

analysis. Therefore, hardware devices and equipment are required to perform the process on finger vein data. Matching accuracy is mostly poor when finger vein data contain large amounts of irrelevant data. Reference [125] indicated that vein image templates captured many times for long durations are changed slightly because of the age of the device. The noise in sensors that lacks distinctiveness of the biometric trait produces unacceptable error rates [127]. Vein imaging requires nir light for complex vein structures in the fingers to be visible to the human eye [133]. These structures are hidden under the skin and do not leave traces on the imaging device because any traces could be used against users in the future. Therefore, several wavelengths (NIR) in the range of the spectrum can raise the finger vein structures as dark lines under the skin.

Challenges related to image quality

References [25, 85, 115] and [123] showed that the elimination of noise and other image enhancement indicates an increase in computational costs, and this task leads to an unacceptable processing rate. We have mentioned that low-quality vein images affect system performance and produce low processing speed, thereby leading to poor system performance because determining the same ROI is difficult using minimal cross or intersection points. the accuracy of matching results will become low. Thus, low quality may lead to far of the system, and non-universality reduces the genuine acceptance rate [83]. References [87, 92] indicated that the most important factor in finger vein verification is image quality because low-quality images produce fake or missing features simultaneously, thereby providing inaccurate results and decreasing verification accuracy. pattern quality is inherently affected by several factors, which can be divided into the following two categories.

1) External factors related to environmental illumination, surrounding temperature, physiological changes, light penetration and user unpleasant behaviour.
2) Internal factors during the image pre-processing phase that are related to inaccurate parameters, such as segmentation and enhancement processes, applied on finger vein images; thus, the quality of these images represent a huge challenge in the accuracy of matching results, security, scalability and privacy.

According to Reference [94], vein image acquisition using infrared light results in different shading areas produced from the difference in skin thicknesses, finger bones and finger muscles. A significant challenge to vein biometrics is improving the verification performance and obtaining maximum immunity to false practices. Reference [97] showed that optical blurring, irregular shading and noise in low-quality vein images produce false extraction features or lose several vein features, thereby leading to inaccurate verification results. Reference [108] reported that the conflicts amongst various finger vein patterns in the same finger affect verification accuracy more seriously than the similarity of patterns of different fingers. In these patterns, certain areas are stable, whereas other areas are unstable. Furthermore, performance accuracy diminishes, and methods for improving the performance of these regular verification systems are required.

Challenges related to processing and matching

One of the most important challenges in finger vein verification system is processing a large number of articles; thus, a framework (algorithm, methods and techniques) for enhancing system performance is proposed. We discuss the challenges extracted from all articles that are included in the present study. References [22, 101] and [110] indicated that in vein image segmentation, the results are unsatisfactory and largely sensitive to noise because these images have low quality. Moreover, segmenting a well-networked finger vein image is typically impractical when the image has low contrast. References [23, 25, 96] and [104] showed that if the input data are large, then the system will overload. Searching and verification requests in a huge database require additional processing time. Thus, if the database is large, then processing will be complex, and the number of patterns in the database should not affect the processing rate. The verification of an individual should not detect other individuals to achieve privacy. According to References [79, 105] and [134], the verification process can lead to low accuracy when vein images have minimal vein intersection points; the most important problem remains the accuracy of matching personal verification. References [89, 100] indicated that several patterns have low quality, thereby affecting the extraction and matching accuracy. During feature extraction of finger vein images, computation procedures are highly complex and may take an extended time in obtaining results, as reported by Reference [97]. The segmentation process is affected when the quality of vein images is low; the extracted features based on an inaccurate network lead to a decrease in the performance of the verification system [102]. The collection of all finger vein data from many users and maintaining the integrity of these data within the finger vein verification systems are challenging tasks according to Reference [114]. Biometrics verification systems perform complex and heavy image processing algorithms, and powerful computers are required to achieve suitable processing times [116]. Biometric systems cannot constantly achieve the high processing speed required by real-time applications, such as in the military, which requires nearly pressing verification [117]. Two of the most important challenges in biometrics depend on enhancing verification performance to obtain resistance against any attack; the main challenges include extracting robust vein features

from vein images even when these images have irregular shading and noise and improving system efficiency [120].

Challenges related to template information leakage

References [29, 121] examined the threat of the leakage of biometric information, such as repetitive attacks using stolen information, because exchanging raw biometric information to forge biometric data after these data are stolen is infeasible. References [82, 122] showed that the security of authentication systems based on biometrics technology has been challenged because of information leakage of biometric templates. Therefore, these systems require the security of multibiometric templates [84]. All biometric patterns stored in the database, which are extracted as biological biometrics by the authentication process, should be secured and protected effectively from any types of attacks. In the real world, billions of devices are connected through networks. The issue lies in protecting personal information and keeping this information secure. This challenge is becoming a popular topic in all types of systems, especially authentication systems [98]

Recommendations

We briefly provide readers with certain recommendations that have been extracted from our survey. This section aims to mitigate the challenges encountered by developers and designers and help them present a robust and highly accurate finger vein biometric verification system that meets the needs of companies and organizations in terms of security. These recommendations are categorized into groups according to their audience to inform readers of each type (Fig. 16).

Recommendations to researchers

Researchers working on biometric authentication systems should follow various recommendations. In this section, we divided these recommendations into subcategories as follows:

Recommendations related to enhancing vein images According to Reference [79], studies on vein intersection points of patterns to solve image quality problems may obtain false-positive verification results. Reference [85] mentioned that to achieve high performance of verification systems, additional processing can be implemented to enhance the sharpness of finger vein images. Therefore, improving low-quality finger vein features in the future is required [114].

Recommendations related to protecting the authentication system The most important aim of any authentication system is security. Therefore, researchers must focus on protecting the system from any attacker and the leakage of biometric information. Reference [82] further indicated that this process should improve the efficiency and security of the verification system, especially in cloud computing. Moreover, the security analysis can be improved by accurate modelling of biometric feature distributions in finger vein databases [84]. Highly secure matching algorithms must be used.

Recommendations related to optimizing authentication problems The search for a method of selecting an optimal subset from extracted features is beneficial for personal verification [22]. Thus, researchers must follow optimization problem approaches to solve these problems [113]. According to Reference [130], we select the maximal imposter and minimal genuine scores of users when measuring performance. The influence of different measurements on the results requires a strict mathematical analysis. Researchers should focus on optimizing problem verification and addressing physical threats that may appear in the future [123]. An intruder may affect environmental factors artificially for their gain.

Recommendations related to processing enhancement According to Reference [28], researchers are recommended to use various fusion methods to combine vein features with the shape of the finger. The entire verification system should achieve a high level of performance and high matching accuracy via improvement. References [83, 86] indicated that for future extended use of modelling feature extraction methods, databases should be managed effectively, and matching methods and the entire verification system performance using various levels of fusion should be evaluated to enhance the result accuracy of the matching process. Furthermore, obtaining thorough information from binary finger vein patterns produces a high level of performance compared with recent methods of predicting high and low finger vein patterns and reducing EER accordingly [92]. In line with Reference [93], the present study found various finger vein network feature extractions that have been developed; however, research on the corresponding verification algorithm has not been conducted sufficiently. In addition, performing other types of score-level fusion strategies other than the maximum fusion should be investigated [95]. Using another biometrics for the fusion of finger veins compared with other multimodal trait verification systems has also been proposed. The reduction of the required computing time by exchange pixel-based chain code extraction with a convolution-based approach, reduction of selected reference points for dark lines in the patterns in enrolment and comparison to reduce the size of the feature vector are important [99]. Reference [100] overcame the dislocation problem. According to Reference [108], certain research should be conducted to determine whether OPM can evolve to improve performance when the system has run extensively and, following reference [111], to study the capability to use neural network methodology with other types of biometrics. Reference [115] presented a grey-scale intermediate filter. The process of ROI detection and

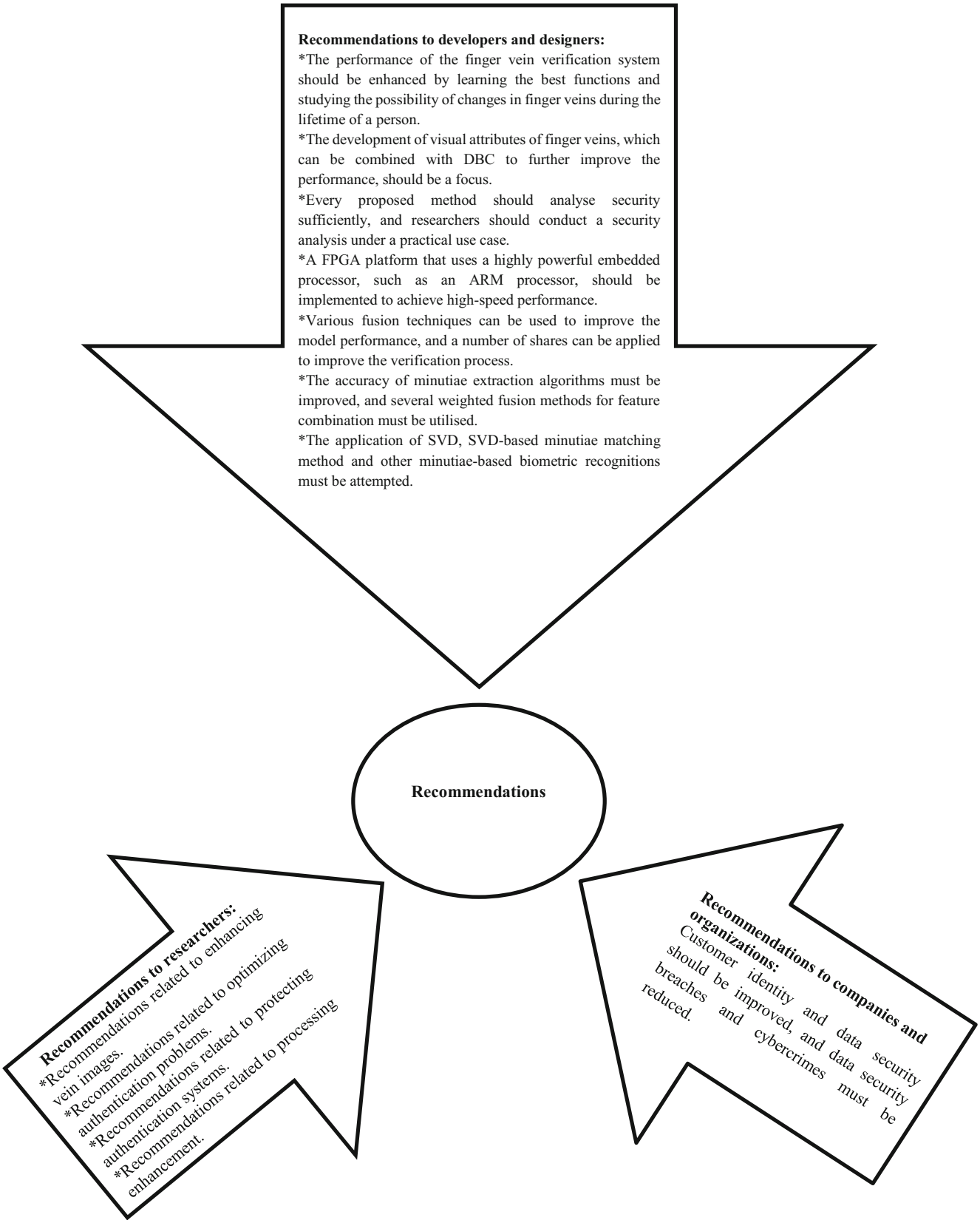

Fig. 16 Categories of recommendations according to audience

thinning consumes most of the processing time of system hardware components. Reference [132] focused on the design of highly effective soft biometrics traits. The LBP operator was used to extract finger vein features when focusing on the soft biometrics traits. The combination of soft biometrics traits and other finger vein features is another future research direction.

Recommendations to companies and organisations

This category is related to companies and organisations, such as banks, commercial companies and military organisations, which use various types of authentication systems, such as finger vein biometric verification.

References [78, 134] indicated that these recommendations can be applied when a high level of security is required, such as in military zone entry, confidential zones and atms. Thus, researchers should focus on enhancing user identity and data security to reduce data system threats from any intruder and defend against cybercrimes

Recommendations to developers and designers

This category is related to developers and designers who aim to develop biometrics authentication systems. As shown in reference [29], every proposed method should analyse security sufficiently. Moreover, applying various fusion techniques is possible to improve model performance, and the number of shares can be expanded to improve the verification level [80]. Therefore, researchers should conduct a security analysis under a practical use case. These developers and designers should focus on reducing time cost through proposed methods [89]. Reference [90] indicated that developers and designers should learn improved functions and study whether a finger vein will change or not during the lifetime of an individual to enhance the performance of the finger vein verification system; this topic should gain sufficient focus in future studies. Developers and designers should likewise focus on developing the visual attributes of finger veins, which can be combined with DBC to further improve performance [100]. The accuracy of minutiae extraction algorithms and using several weighted fusion methods for feature combination should be improved [109]. In addition, SVDMM and SVD-based minutiae matching methods should be applied to other minutiae-based biometric verification, such as fingerprint and palm vein identification. The system should be implemented on an FPGA platform using a highly powerful embedded processor, such as an ARM processor, to achieve high-speed performance [117].

Limitations

A limitation of this study is associated with the number of databases used in our search. Several criteria, such as reliability and wide representativeness of a collection of references, were followed in selecting these databases. Moreover, the growing progress in this field limits the timeliness of this study. Furthermore, the overview of research on these authentication systems based on human biometrics does not necessarily reflect the actual use or effects of the system. We found that the results of this study reflect the response of the research community to current trends.

Conclusion

The study highlights a few key issues for future investigation, including finger vein biometric verification system for telemedicine environments. This study aims to provide an up-to-date substructure of verification techniques for sensor-based telemedicine architectures. The research focused on the directions that deal with this subject. The first layer of our taxonomy, namely, security and privacy of telemedicine applications based on sensors, was presented, and the studies related to the security issues were analysed and discussed in three tiers. In the second layer of our taxonomy, the comprehensive survey focused on previous articles on documentation techniques without applications. We also reviewed new directions in exploiting finger vein biometric verification systems as innovative side channels to conclude taps on verification systems in telemedicine applications. This development resulted from the increasing popularity and wide deployment of sensor applications as well as patient privacy risks and low level of security awareness in telemedicine applications. All up-to-date and published works on finger vein biometric verification systems were surveyed. Their findings and important contributions were highlighted. Studies that attempted to develop finger vein verification applications and software frameworks were investigated. Moreover, datasets of finger veins used in previous studies were highlighted. We found that several domains have received more attention than other domains from researchers. These domains and functions reflect the type of studies on finger vein biometric verification and provide a clear indication of the gaps in terms of development and evaluation. Researchers have described the challenges they faced, and many have provided recommendations for resolving current and expected challenges, which encourage other researchers to determine opportunities and obtain solutions by further research in this field. Other researchers have focused on designing full hardware system architectures and/or developing devices for finger vein verification systems, whereas certain researchers have focused on evaluating the quality of vein images, process and device performance and studying the effects of changes in the NIR wavelength. Furthermore, a few researchers have studied the use of finger vein feature points and technology in the verification and the capability of methods to satisfy current security requirements.

To the best of our knowledge, our study is the first to provide a multi-layer comprehensive overview of the sensors and security in the telemedicine architecture as well as finger vein biometric verification systems in literature to match benefits to patient security and privacy in the telemedicine architecture. We hope that other researchers will benefit from this study and use it as a starting point to further expand the research based on the challenges we have discussed. The present study has determined the gap in this research area. Thus, future research should enhance the security level in finger vein verification systems and protect finger vein features (on client and server sides at real time through the communication channel), which represent critical challenges at present.

Compliance with Ethical Standards

Conflict of Interest The authors declare no conflict of interest.

Ethical Approval All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki Declaration and its subsequent amendments or comparable ethical standards.

Informed Consent Informed consent was obtained from all individual participants included in the study.

References

1. Doumbouya, M. B., Kamsu-Foguem, B., Kenfack, H., and Foguem, C., A framework for decision making on teleexpertise with traceability of the reasoning. *IRBM* 36(1):40–51, 2015.
2. Kalid, N. et al., Based on real time remote health monitoring systems: A new approach for prioritization 'large scales data' patients with chronic heart diseases using body sensors and communication technology. *J. Med. Syst.* 42(4):69, 2018.
3. Iqbal, S. et al., Real-time-based E-health systems: Design and implementation of a lightweight key management protocol for securing sensitive information of patients. Health Technol. (Berl)., 2018.
4. Kalid, N. et al., Based real time remote health monitoring systems: A review on patients prioritization and related 'big data' using body sensors information and communication technology. *J. Med. Syst.* 42(2):30, 2017.
5. Hamdi, O., Chalouf, M. A., Ouattara, D., and Krief, F., eHealth: Survey on research projects, comparative study of telemonitoring architectures and main issues. *J. Netw. Comput. Appl.* 46:100–112, 2014.
6. Abdulnabi, M. et al., A distributed framework for health information exchange using smartphone technologies. *J. Biomed. Inform.* 69:230–250, 2017.
7. Rajan, S. P., Review and investigations on future research directions of mobile based telecare system for cardiac surveillance. *Rev. Mex. Trastor. Aliment.* 13(4):454–460, 2015.
8. Negra, R., Jemili, I., and Belghith, A., Wireless body area networks : Applications and technologies. *Procedia - Procedia Comput. Sci.* 83:1274–1281, 2016.
9. Salman, O. H. et al., Novel methodology for triage and prioritizing using 'big data' patients with chronic heart diseases through telemedicine environmental. *Int. J. Inf. Technol. Decis. Mak.* 16(05):1211–1245, Sep. 2017.
10. Xiao, Y. and Chen, H., Mobile telemedicine: A computing and networking perspective. Auerbach Publications, 2008.
11. Sene, A., Kamsu-Foguem, B., and Rumeau, P., Telemedicine framework using case-based reasoning with evidences. *Comput. Methods Programs Biomed.* 121(1):21–35, 2015.
12. Zaidan, A. A. et al., Multi-criteria analysis for OS-EMR software selection problem: A comparative study. *Decis. Support Syst.* 78: 15–27, 2015.
13. Kiah, M. L. M. et al., Open source EMR software: Profiling, insights and hands-on analysis. *Comput. Methods Programs Biomed.* 117(2):360–382, 2014.
14. Zaidan, A. A. et al., Challenges, alternatives, and paths to sustainability: Better public health promotion using social networking pages as key tools. *J. Med. Syst.* 39(2):7, 2015.
15. Zaidan, B. B. et al., A security framework for Nationwide health information exchange based on telehealth strategy. *J. Med. Syst.* 39(5):1–19, 2015.
16. Hayajneh, T., Mohd, B. J., Imran, M., Almashaqbeh, G., and Vasilakos, A. V., Secure authentication for remote patient monitoring with wireless medical sensor networks. *Sensors (Basel).* 16(4):424, 2016.
17. Hussain, M. et al., Conceptual framework for the security of mobile health applications on android platform. *Telemat. Inform.* 35(5):1335–1354, 2018.
18. Hussain, M. et al., A security framework for mHealth apps on android platform. *Comput. Secur.* 75:191–217, 2018.
19. Alanazi, H. O. et al., Meeting the security requirements of electronic medical records in the ERA of high-speed computing. *J. Med. Syst.* 39(1):165, 2015.
20. Kiah, M. L. M., Nabi, M. S., Zaidan, B. B., and Zaidan, A. A., An enhanced security solution for electronic medical records based on AES hybrid technique with SOAP/XML and SHA-1. *J. Med. Syst.* 37(5):9971, 2013.
21. Hamdan, O. A. et al., Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance. *J. Med. Plants Res.* 4(19):2059–2074, 2010.
22. Mohd Asaari, M. S., Suandi, S. A., and Rosdi, B. A., Fusion of band limited phase only correlation and width centroid contour distance for finger based biometrics. *Expert Syst. Appl.* 41(7): 3367–3382, 2014.
23. Da Wu, J., and Liu, C. T., Finger-vein pattern identification using principal component analysis and the neural network technique. *Expert Syst. Appl.* 38(5):5423–5427, 2011.
24. M. Hussain et al., "The rise of keyloggers on smartphones: A survey and insight into motion-based tap inference attacks," Pervasive and Mobile Computing, vol. 25. Elsevier, pp. 1–25, 01-Jan-2016.
25. L. Dong, G. Yang, Y. Yin, F. Liu, and X. Xi, "Finger vein verification based on a personalized best patches map Lumei," 2012.
26. Da Wu, J., and Ye, S. H., Driver identification using finger-vein patterns with Radon transform and neural network. *Expert Syst. Appl.* 36(3 PART 2):5793–5799, 2009.
27. Masys, D., Baker, D., and Butros, A., Giving patients access to their medical records via the internet. *Am. Med.* 9(2):181–191, 2002.
28. Rosdi, B. A., Shing, C. W., and Suandi, S. A., Finger vein recognition using local line binary pattern. *Sensors* 11(12):11357–11371, 2011.
29. Suzuki, H., Suzuki, M., Urabe, T., and Obi, T., Secure biometric image sensor and authentication scheme based on compressed sensing. *Appl. Opt.* 52(33):8161–8168, 2013.
30. Qin, H., He, X., Yao, X., and Li, H., Finger-vein verification based on the curvature in radon space. *Expert Syst. Appl.* 82:151–161, 2017.

31. Zaidan, A. A. et al., A survey on communication components for IoT-based technologies in smart homes. *Telecommun. Syst.* 69(1): 1–25, 2018.
32. Z. T. Al-qaysi et al., "A review of disability EEG based wheelchair control system: Coherent taxonomy, open challenges and recommendations," *Comput. Methods Programs Biomed.*, vol. 164, Elsevier, pp. 221–237, 2018.
33. Albahri, A. S. et al., Real-time fault-tolerant mhealth system: comprehensive review of healthcare services, opens issues, challenges and methodological aspects. *J. Med. Syst.* 42(8):137, 2018.
34. Zaidan, A. A. and Zaidan, B. B., A review on intelligent process for smart home applications based on IoT: Coherent taxonomy, motivation, open challenges, and recommendations, *Artif. Intell. Rev.*, 1–25, 2018.
35. Hamada, M. et al., A systematic review for human EEG brain signals based emotion classification, feature extraction, brain condition, Group Comparison. *J. Med. Syst.* 42(9):162, 2018.
36. M. A. Alsalem et al., "A review of the automated detection and classification of acute leukaemia: Coherent taxonomy, datasets, validation and performance measurements, motivation, open challenges and recommendations," *Comput. Methods Programs Biomed.*, vol. 158. Elsevier, pp. 93–112, 2018.
37. Brian, R. M., and Ben-Zeev, D., Mobile health (mHealth) for mental health in Asia: Objectives, strategies, and limitations. *Asian J. Psychiatr.* 10(2014):96–100, 2014.
38. Iwaya, L. H. et al., Mobile health in emerging countries: A survey of research initiatives in Brazil. *Int. J. Med. Inform.* 82(5):283–298, 2013.
39. Obi, T., Ishmatova, D., and Iwasaki, N., Promoting ICT innovations for the ageing population in Japan. *Int. J. Med. Inform.* 82(4): e47–e62, 2013.
40. Review of Mobile Health Technology for Military Mental Health. *Mil. Med.* 179, no. 8, 865–878, 2014.
41. Adams, Z. W., McClure, E. A., Gray, K. M., Danielson, C. K., Treiber, F. A., and Ruggiero, K. J., Mobile devices for the remote acquisition of physiological and behavioral biomarkers in psychiatric clinical research. *J. Psychiatr. Res.* 85:1–14, 2017.
42. Silva, B. M. C., Rodrigues, J. J. P. C., de la Torre Díez, I., López-Coronado, M., and Saleem, K., Mobile-health: A review of current state in 2015. *J. Biomed. Inform.* 56:265–272, 2015.
43. Point, C., Accreditation, E., and Benton, D., Health care delivery. *J. Nurs. Regul.* 7(4):S12–S16, 2017.
44. Schulmeister, L., Technology and the transformation of oncology care. *Semin. Oncol. Nurs.* 32(2):99–109, 2016.
45. Reeder, B., Meyer, E., Lazar, A., Chaudhuri, S., Thompson, H. J., and Demiris, G., Framing the evidence for health smart homes and home-based consumer health technologies as a public health intervention for independent aging: A systematic review. *Int. J. Med. Inform.* 82(7):565–579, 2013.
46. Albahri, O. S. et al., Systematic review of real-time remote health monitoring system in triage and priority-based sensor technology: Taxonomy, open challenges, motivation and recommendations. *J. Med. Syst.* 42(5):80, 2018.
47. A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. *Future Gen. Comp. Syst.* 55: 266–277 (2016)
48. Saleem, K., Derhab, A., Al-Muhtadi, J., and Shahzad, B., Human-oriented design of secure machine-to-machine communication system for e-healthcare society. *Comput. Human Behav.* 51(Part B):977–985, 2015.
49. A. S. Albahri et al., "Real-time fault-tolerant mhealth system: comprehensive review of healthcare services, opens issues, challenges and methodological aspects," Journal of Medical Systems, vol. 42, no. 8. Springer, p. 137, 2018.
50. Albahri, O. S. et al., Real-time remote health-monitoring Systems in a Medical Centre: A review of the provision of healthcare services-based body sensor information, open challenges and methodological aspects. *J. Med. Syst.* 42(9):164, 2018.
51. Zhang, K., Liang, X., Baura, M., Lu, R., and Sherman Shen, X., PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs. *Inf. Sci. (Ny).* 284:130–141, 2014.
52. Moreno, S., Quintero, A., Ochoa, C., Bonfante, M., Villareal, R., and Pestana, J., Remote monitoring system of vital signs for triage and detection of anomalous patient states in the emergency room. 2016 XXI symposium on signal processing, images and artificial vision (STSIVA), 2016, no. 1–5, 2015.
53. Baehr, D., McKinney, S., Quirk, A., and Harfoush, K., On the practicality of elliptic curve cryptography for medical sensor networks. 2014 11th annual high capacity optical networks and emerging/enabling technologies (photonics for energy). 41–45, 2014.
54. de la Piedra, A., Braeken, A., Touhafi, A., and Wouters, K., Secure event logging in sensor networks. *Comput. Math. with Appl.* 65(5):762–773, 2013.
55. Hedin, D. S., Kollmann, D. T., Gibson, P. L., Riehle, T. H., and Seifert, G. J., Distance bounded energy detecting ultra-wideband impulse radio secure protocol. 2014 36th annual international conference of the IEEE engineering in medicine and biology society, 2014. 6619–6622, 2014.
56. Soufiene, B. O., Bahattab, A. A., Trad, A., and Youssef, H., Lightweight and confidential data aggregation in healthcare wireless sensor networks. *Trans. Emerg. Telecommun. Technol.* 27(4): 576–588, 2016.
57. Benmansour, T., Ahmed, T., and Moussaoui, S., Performance evaluation of IEEE 802.15.6 MAC in monitoring of a cardiac patient. 2016 IEEE 41st conference on local computer networks workshops (LCN workshops). 241–247, 2016.
58. Hmood, A. K. et al., On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates. *Int. J. Phys. Sci.* 5(7):1054–1062, 2010.
59. Naji, A. W. et al., Novel approach for cover file of hidden data in the unused area two within EXE file using distortion techniques and advance encryption standard. *Proc. World Acad. Sci. Eng. Technol.* 56(5):498–502, 2010.
60. Naji, A. W. et al., Novel framework for hidden data in the image page within executable file using computation between advanced encryption standard and distortion techniques. *Int. J. Comput. Sci. Inf. Secur.* 3(1):1–6, 2009.
61. Zaidan, A. A. et al., Novel approach for high (secure and rate) data hidden within triplex space for executable file. *Sci. Res. Essays* 5(15), 1965.
62. Zaidan, A. A. et al., Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem. *Int. J. Phys. Sci.* 5:1776–1786, 2010.
63. Salem, Y. et al., A review on multimedia communications cryptography. *Res. J. Inform. Technol* 3:146–152, 2011.
64. Abomhara, M. et al., Suitability of using symmetric key to secure multimedia data: An overview. *J. Appl. Sci.* 10(15):1656–1661, 2010.
65. Lin, Y. H., Jan, I. C., Ko, P. C. I., Chen, Y. Y., Wong, J. M., and Jan, G. J., A wireless PDA-based physiological monitoring system for patient transport. *IEEE Trans. Inf. Technol. Biomed.* 8(4):439–447, 2004.
66. Farahani, B. et al., Towards fog-driven IoT eHealth : Promises and challenges of IoT in medicine and healthcare. *Futur. Gener. Comput. Syst.* 78:659–676, 2017.
67. Czaja, S. J., and Lee, C. C., The impact of aging on access to technology. Univers. Access Inf. Soc. 5(4):341–349, 2007.
68. F. J. S. Thilo, S. Hahn, R. J. G. Halfens, and J. M. G. A. Schols, "Usability of a wearable fall detection prototype from the

perspective of older people - a real field testing approach," *J. Clin. Nurs.*, 2018.
69. Medani, A. et al., Review of mobile short message service security issues and techniques towards the solution. *Sci. Res. Essays* 6(6): 1147–1165, 2011.
70. Al-bakri, S. H. et al., Securing peer-to-peer mobile communications using public key cryptography : New security strategy. *Int. J. Phys. Sci.* 6(4):930–938, 2011.
71. Bolle, R. M., Connell, J., Pankanti, S., Ratha, N. K., and Senior, A. W., Guide to biometrics. Springer Science & Business Media, 2013.
72. Shea, J. J., Handbook of fingerprint recognition [book review], vol. 20, no. 5. Springer Science & Business Media, 2004.
73. Q. M. Yas et al., A systematic review on smartphone skin Cancer apps: Coherent taxonomy, motivations, open challenges and recommendations, and new research direction. *J. Circuits, Syst. Comput.*, vol. 27, no. 05, p. 1830003, 2018.
74. Hussain, M. et al., The landscape of research on smartphone medical apps: Coherent taxonomy, motivations, open challenges and recommendations. *Comput. Methods Programs Biomed.* 122(3): 393–408, 2015.
75. Alsalem, M. A. et al., Systematic review of an automated multiclass detection and classification system for acute Leukaemia in terms of evaluation and benchmarking, open challenges, issues and methodological aspects. *J. Med. Syst.* 42(11): 204, 2018.
76. Zaidan, A. A. et al., A review on smartphone skin cancer diagnosis apps in evaluation and benchmarking: Coherent taxonomy, open issues and recommendation pathway solution. *Health Technol. (Berl).* 8(4):223–238, 2018.
77. Alaa, M. et al., A review of smart home applications based on internet of things. *J. Netw. Comput. Appl.* 97(1):48–65, 2017.
78. V. P. N. Sugandhi, M. Mathankumar, "Real time authentication system using advanced finger vein recognition technique," *Int. Conf. Commun. Signal Process.* April 3–5, 2014, India, pp. 1183–1187, 2014.
79. J. Chavez-Galaviz, J. Ruiz-Rojas, and A. Garcia-Gonzalez, "embedded biometric cryptosystem based on finger vein patterns," 2015 12th *Int. Conf. Electr. Eng. Comput. Sci. Autom. Control. CCE* 2015, pp. 1–6, 2015.
80. Nandhinipreetha, A., and Radha, N., Multimodal biometric template authentication of finger vein and signature using visual cryptography. *2016 Int. Conf. Comput. Commun. Inform. ICCCI* 2016: 7–10, 2016.
81. Murakami, T., Ohki, T., and Takahashi, K., Optimal sequential fusion for multibiometric cryptosystems. *Inf. Fusion* 32:93–108, 2016.
82. Wu, Z., Tian, L., Li, P., Wu, T., Jiang, M., and Wu, C., Generating stable biometric keys for flexible cloud computing authentication using finger vein. *Inf. Sci. (Ny).* 0:1–17, 2016.
83. D. Jagadiswary and D. Saraswady, "Biometric authentication using fused multimodal biometric," *Procedia - Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 109–116, 2016.
84. Jialiang Peng, X. N., Li, Q., and Abd El-Latif, A. A., Finger multibiometric cryptosystems: Fusion strategy and template security. *J. Biomed. Opt.* 19(2):020901, 2014.
85. Fayyaz, M., Hajizadeh-Saffar, M., Sabokrou, M., Hoseini, M., and Fathy, M., A novel approach for finger vein verification based on self-taught learning. *Iran. Conf. Mach. Vis. Image Process. MVIP* 2016:88–91, 2016.
86. Qin, H., and El-Yacoubi, M. A., Deep representation-based feature extraction and recovering for finger-vein verification. *IEEE Trans. Inf. Forensics Secur.* 12(8):1816–1829, 2017.
87. Zhang, F., Guo, S., and Qian, X., Segmentation for finger vein image based on PDEs denoising. *Proc. - 2010 3rd Int. Conf. Biomed. Eng. Informatics, BMEI 2010* 2(Bmei):531–535, 2010.
88. Gupta, P., and Gupta, P., An accurate finger vein based verification system. *Digit. Signal Process. A Rev. J.* 38:43–52, 2015.
89. Liu, T., Xie, J., Yan, W., Li, P., and Lu, H., Finger-vein pattern restoration with direction-variance-boundary constraint search. *Eng. Appl. Artif. Intell.* 46:131–139, 2015.
90. Liu, Z., Yin, Y., Wang, H., Song, S., and Li, Q., Finger vein recognition with manifold learning. *J. Netw. Comput. Appl.* 33(3):275–282, 2010.
91. Da Wu, J., and Liu, C. T., Finger-vein pattern identification using SVM and neural network technique. *Expert Syst. Appl.* 38(5): 5423–5427, 2011.
92. Qin, H., and El-Yacoubi, M. A., Finger-vein quality assessment by representation learning from binary images. *Lect. Notes Comput. Sci. (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9489:421–431, 2015.
93. Li, Z., Sun, D., Di, L., and Hao, L., Two modality-based bi-finger vein verification system. *Int. Conf. Signal Process. Proceedings, ICSP*, 1690–1693, 2010.
94. Parthiban, K., Wahi, A., Sundaramurthy, S., and Palanisamy, C., Finger vein extraction and authentication based on gradient feature selection algorithm. *5th Int. Conf. Appl. Digit. Inf. Web Technol. ICADIWT* 2014:143–147, 2014.
95. Fateme Saadat, M. N., A Multibiometric Finger Vein Verification System Based On Score Level Fusion Strategy. *Second Int. Congr. Technol. Commun. Knowl. (ICTCK 2015)*, 11–12, 2015 - Mashhad Branch, Islam. Azad Univ. Mashhad, Iran, no. Ictck, pp. 11–12, 2015.
96. Tang, D., Huang, B., Li, R., and Li, W., A person retrieval solution using finger vein patterns. Proc - Int Conf Pattern Recogn. 1306–1309, 2010.
97. William, A., Ong, T. S., Lau, S. H., and Goh, M. K. O., Finger vein verification using local histogram of hybrid texture descriptors. *IEEE 2015 Int. Conf. Signal Image Process. Appl. ICSIPA 2015 - Proc.*, 304–308, 2016.
98. Lu, Y., Wu, S., Fang, Z., Xiong, N., Yoon, S., and Park, D. S., Exploring finger vein based personal authentication for secure IoT. *Futur. Gener. Comput. Syst.* 77:149–160, 2017.
99. Pflug, A., Hartung, D., and Busch, C., Feature extraction from vein images using spatial information and chain codes. *Inf. Secur. Tech. Rep.* 17(1–2):26–35, 2012.
100. Xi, X., Yang, L., and Yin, Y., Learning discriminative binary codes for finger vein recognition. Pattern Recognit. 66:26–33, 2017.
101. Yang, J., Shi, Y., and Yang, J., Personal identification based on finger-vein features. *Comput. Human Behav.* 27(5):1565–1570, 2011.
102. Dong, L., Yang, G., Yin, Y., Xi, X., Yang, L., and Liu, F., Finger vein verification with vein Textons. *Int. J. Pattern Recognit. Artif. Intell.* 29(04):1556003, 2015.
103. Song, W., Kim, T., Kim, H. C., Choi, J. H., Kong, H. J., and Lee, S. R., A finger-vein verification system using mean curvature. *Pattern Recognit. Lett.* 32(11):1541–1547, 2011.
104. Wu, J.-D., Liu, C.-T., Tsai, Y.-J., Liu, J.-C., and Chang, Y.-W., Development of neural network techniques for finger-vein pattern classification. *Second Int. Conf. Digit. IMAGE Process.* 7546: 75460F, 2010.
105. Huang, H., Liu, S., Zheng, H., Ni, L., Zhang, Y., and Li, W., DeepVein: Novel finger vein verification methods based on deep convolutional neural networks. *2017 IEEE Int. Conf. Identity, Secur. Behav. Anal. ISBA* 2017(5), 2017.
106. Ong, T. S., Teng, J. H., Muthu, K. S., and Teoh, A. B. J., Multi-instance finger vein recognition using minutiae matching. *Proc. 2013 6th Int. Congr. Image Signal Process. CISP 2013* 3(Cisp): 1730–1735, 2013.
107. J. Peng, N. Wang, A. a. A. El-Latif, Q. Li, and X. Niu, "Finger-vein verification using Gabor filter and SIFT feature matching.

2012 Eighth Int. Conf. Intell. Inf. Hiding Multimed. Signal Process., pp. 45–48, 2012.
108. Tang, D., Huang, B., Li, R., Li, W., and Li, X., Finger vein verification using occurrence probability matrix (OPM), *Proc. Int. Jt. Conf. Neural Netw.* 21–26, 2012.
109. Liu, F., Yang, G., Yin, Y., and Wang, S., Singular value decomposition based minutiae matching method for finger vein recognition. *Neurocomputing* 145:75–89, 2014.
110. Wang, J., Xiao, J., Lin, W., and Luo, C., Discriminative and generative vocabulary tree: With application to vein image authentication and recognition. *Image Vis. Comput.* 34:51–62, 2015.
111. Noori Hoshyar, A., and Sulaiman, R., Vein matching using artificial neural network in vein authentication systems. Conf. Graph. Image Process. (ICGIP 2011) 8285(Icgip):82850Z, 2011.
112. Peng, J., El-Latif, A. A. A., Li, Q., and Niu, X., Multimodal biometric authentication based on score level fusion of finger biometrics. *Optik (Stuttg).* 125(23):6891–6897, 2014.
113. Razzak, M. I., and Yusof, R., Multimodal face and finger veins biometric authentication. *Sci. Res. Essays* 5(17):2529–2534, 2010.
114. Cheng, Y., Chen, H., and Cheng, B., Special point representations for reducing data space requirements of finger-vein recognition applications. *Multimed. Tools Appl.* 76(278), 2016.
115. P. C. M. Khalil-Hani Eng, FPGA-based embedded system implementation of finger vein Biometrics. 2010 IEEE Symp. Ind. Electron. Appl. (ISIEA 2010), Oct. 3–5, 2010, Penang, Malaysia FPGA-Based, no. Isiea, pp. 700–705, 2010.
116. Khalil-Hani, M. and Eng, P. C., Personal verification using finger vein biometrics in FPGA-based system-on-Chip. 2011 7th Int. Conf. Electr. Electron. Eng., p. II-171-II-176, 2011.
117. Khalil-Hani, M. and Lee, Y. H., FPGA embedded hardware system for finger vein biometric recognition. *IECON Proc. (Industrial Electron. Conf.*, 2273–2278, 2013.
118. Raghavendra, R., Raja, K. B., Surbiryala, J., and Busch, C., A low-cost multimodal biometric sensor to capture finger vein and fingerprint. *IJCB 2014 - 2014 IEEE/IAPR Int. Jt. Conf. Biometrics*, 2014.
119. Raghavendra, R., Surbiryala, J., Raja, K. B., and Busch, C., Novel finger vascular pattern imaging device for robust biometric verification. *IST 2014–2014 IEEE Int. Conf. Imaging Syst. Tech. Proc.*, 148–152, 2014.
120. Xin, Y., Liu, Z., Zhang, H., and Zhang, H., Finger vein verification system based on sparse representation. *Appl. Opt.* 51(25):6252–6258, 2012.
121. Yang, W., Huang, X., Zhou, F., and Liao, Q., Comparative competitive coding for personal identification by using finger vein and finger dorsal texture fusion q. *Inf. Sci. (Ny).* 268:20–32, 2014.
122. Jadhav, M., and Nerkar, P. M., Implementation of an embedded hardware of FVRS on FPGA. *Proc. - IEEE Int. Conf. Inf. Process. ICIP* 2015:48–53, 2016.
123. Hartung, D., Martin, S., and Busch, C., Quality estimation for vascular pattern recognition. *2011 Int. Conf. Hand-based biometrics, ICHB 2011 - Proc.* 258–263, 2011.
124. Qin, H., and El Yacoubi, M. A., Deep representation for finger-vein image quality assessment. *IEEE Trans. Circuits Syst. Video Technol.* 8215(c):1, 2017.
125. Tang, D., Huang, B., Li, W., and Li, X., A method of evolving finger vein template. *Proc. - 2012 Int. Symp. Biometrics Secur. Technol. ISBAST* 2012:96–101, 2012.
126. He, M. et al., Performance evaluation of score level fusion in multimodal biometric systems. *Pattern Recogn.* 43(5):1789–1800, 2010.
127. Horng, S. J., Chen, Y. H., Run, R. S., Chen, R. J., Lai, J. L., and Sentosal, K. O., An improved score level fusion in multimodal biometric systems. *Parallel Distrib. Comput. Appl. Technol. PDCAT Proc.* 239–246, 2009.
128. Damavandinejadmonfared, S., Mobarakeh, A. K., Suandi, S. A., and Rosdi, B. A., Evaluate and determine the most appropriate method to identify finger vein. *Procedia Eng.* 41(Iris):516–521, 2012.
129. Raghavendra, R., Raja, K. B., Surbiryala, J., and Busch, C., Finger vascular pattern imaging - a comprehensive evaluation. *2014 Asia-Pacific signal Inf. Process. Assoc. Annu. Summit Conf. APSIPA 2014*, 2014.
130. Zheng, H., Ni, L., Xian, R., Liu, S., and Li, W., BMDT: An optimized method for biometric menagerie detection. *2015 IEEE 7th Int. Conf. Biometrics Theory, Appl. Syst. BTAS 2015*, 2015.
131. Ye, Y., Zheng, H., Ni, L., Liu, S., and Li, W., A study on the individuality of finger vein based on statistical analysis. *2016 Int. Conf. Biometrics ICB* 2016:1–5, 2016.
132. Yang, L., Yang, G., Yin, Y., and Xi, X., Exploring soft biometric trait with finger vein recognition. *Neurocomputing* 135:218–228, 2014.
133. Waluś, M., Bernacki, K., and Konopacki, J., Impact of NIR wavelength lighting in image acquisition on finger vein biometric system effectiveness. *Opto-Electronics Rev.* 25(4):263–268, 2017.
134. Ibrahim, M. M. S., Al-namiy, F. S., Beno, M., and Rajaji, L., Biometric authentication for secured transaction using finger vein technology. *Seiscon*. 760–763, 2011.
135. Goudelis, G., Tefas, A., and Pitas, I., Emerging biometric modalities: A survey. *J. Multimodal User Interfaces* 2(3):217–235, 2009.