IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 19, 2019, accepted January 4, 2020, date of publication January 8, 2020, date of current version January 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2964788

Finger Vein Biometrics: Taxonomy Analysis, Open Challenges, Future Directions, and Recommended Solution for Decentralised Network Architectures

A. H. MOHSIN[1,2], A. A. ZAIDAN[1], B. B. ZAIDAN[1], O. S. ALBAHRI[1], SHAMSUL ARRIEYA BIN ARIFFIN[1], AHMED ALEMRAN[1,3], ODAI ENAIZAN[4], ALI H. SHAREEF[5], ALI NAJM JASIM[6], N. S. JALOOD[7], M. J. BAQER[1], A. H. ALAMOODI[1], E. M. ALMAHDI[1], A. S. ALBAHRI[8], M. A. ALSALEM[9], K. I. MOHAMMED[1], H. A. AMEEN[10], AND SALEM GARFAN[1]

[1]Department of Computing, Faculty of Arts, Computing and Creative Industry, Universiti Pendidikan, Tanjung Malim 35900, Malaysia
[2]Presidency of Ministries, Establishment of Martyrs, Baghdad 10004, Iraq
[3]University of Misan, Amarah 62001, Iraq
[4]Faculty of Economic and Business, Jadara University, Irbid 21110, Jordan
[5]Department of Computer Science, Computer Science and Mathematics College, University of Thi-Qar, Nasiriyah 64001, Iraq
[6]Foundation of Alshuhda, Nasiriyah 64001, Iraq
[7]Ministry of Education, Nasiriyah 64001, Iraq
[8]Iraqi Commission for Computers & Informatics, Informatics Institute for Postgraduate Studies, Baghdad 10069, Iraq
[9]College of Administration and Economic, University of Mosul, Mosul 41002, Iraq
[10]Department of Computer Engineering, Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, Parit Raja 86400, Malaysia

Corresponding author: B. B. Zaidan (bilalbahaa@fskik.upsi.edu.my)

This work was supported by the Universiti Pendidikan Sultan Idris, Malaysia, under UPSI Rising Star Grant 2019, under Grant 2019-0125-109-01.

ABSTRACT A review is conducted to deeply analyse and map the research landscape of current technologies in finger vein (FV) biometric authentication in medical systems into a coherent taxonomy. This research focuses on articles related to the keywords 'biometrics', 'finger veins' and 'verification' and their variations in three major databases, namely, Web of Science, ScienceDirect and IEEE Xplore. The final set of collected articles related to FV biometric authentication systems is divided into software- and hardware-based systems. In the first category, software development attempts are described. The experiment results, frameworks, algorithms and methods that perform satisfactorily are presented. Moreover, the experiences obtained from conducting these studies are discussed. In the second category, hardware development attempts are described. The final articles are discussed from three aspects, namely, (1) number of publications, (2) problem type, proposed solutions, best results and evaluation methods in the included studies and (3) available databases containing different scientific work collected from volunteers, such as staff and students. The basic characteristics of this emerging field are identified from the following aspects: motivations of using FV biometric technology in authentication systems, open challenges that impede the technology's utility, authors' recommendations and future research prospects. A new solution is proposed to address several issues, such as leakage of biometrics that leads to serious risks due to the use of stolen FV templates and various spoofing and brute-force attacks in decentralised network architectures in medical systems, including access points and various database nodes without a central point. This work contributes to literature by providing a detailed review of feasible alternatives and research gaps, thereby enabling researchers and developers to develop FV biometric authentication medical systems further. Insights into the importance of such a technology and its integration into different medical applications and fields are also provided.

INDEX TERMS Biometrics, finger veins, blockchain technology, authentication, verification, decentralised network architecture.

I. INTRODUCTION

Biometrics is defined in the digital information field as an authentication system that performs object identification by exploiting special human physical features, such as iris, fingerprints, face, finger veins (FVs) and hand geometry. Authentication systems also exploit other behavioural features, such as voice and gait, to perform object identification. Biometrics-based authentication systems have recently become useful in applications where reliable identification

The associate editor coordinating the review of this manuscript and approving it for publication was Yassine Maleh.

TABLE 1. Properties of different biometric authentication types.

Type	Characteristics	Weakness	Security	Sensor device	Cost
Voice	Natural/comfortable	Noise/cold diseases	Normal	Without contact, with imaging device	Low
Face	Remote controlled/comfortable	Light	Normal	Without contact, with imaging device	Low
Fingerprint	Extensively used/comfortable	Skin diseases	Good	Contact required	Low
Iris	Highly accurate/uncomfortable	Eyeglasses/side effect	Excellent	Without contact, with imaging device	High
Finger vein	Highly accurate/comfortable	Few	Excellent	Without contact, with imaging device	Low

or verification is required [1], [147]–[149]. Current management of difficult security issues usually depends on the use of human biological biometrics that are extremely specific that they cannot be easily copied or stolen. Traditional authentication systems, which typically identify individuals by using keys or passwords, may be unsafe because these passcodes can be stolen or forgotten; however, this new authentication technology can be used to improve other identification methods, such as those that depend on the use of magnetic cards [2]. The FV biometric authentication system was developed and patented by Hitachi in 2005. This technology is currently used for individual authentication in many applications, such as credit card verification, vehicle security, employee attendance time tracking, end-point security and automated teller machines (ATMs). Researchers consider this biometric method a potential technique due to its numerous advantages, such as effectiveness in living humans, contact-less implementation, high security, low cost, use of small equipment and minimal defects. The characteristics of various biometric authentication methods are compared in Table 1.

Existing applications of biometrics include door access, financial security systems, controlled border crossing and attendance systems. The roles of FV biometrics in numerous security systems have also been enumerated. These roles include access control, electronic passport authentication and individual authentication. Different biometric techniques have been proposed and developed in the past two decades [3]. FV biometrics is more resistant to forgery and replication compared with other types because veins are inside the human body and invisible to human eyes. Furthermore, users cannot be tracked in the future due to the absence of physical contact between customers and sensor devices.

The development of FV biometric systems involves two aspects, namely, software and hardware components. Hardware components pertain to imaging devices, the most common of which are the near-infrared (NIR) LED light source (760–1000 nm) that can pass through the skin of the finger and the CCD camera that is used for the acquisition of vein images. Other basic components are also involved; for example, a database is used to save FV templates, where the finger is placed between the NIR light source and CCD camera [4]. During imaging, haemoglobin in the blood absorbs the infrared light and consequently appears as dark lines, and the vein reflections are more visible than those in other areas of the finger. The software aspect involves four major steps, namely, acquisition of FV images, pre-processing, feature extraction and classification (matching). The processing sequence during user enrolment is shown in Figure 1a.

During image acquisition, FV images are captured using an imaging device. These images are affected by several factors, such as blood pressure, human body temperature and environmental side effects. Pre-processing is performed to improve image quality. Pre-processing consists of region of interest (ROI) extraction, image background removal and filter implementation [5]. Feature extraction is the most important step in the authentication operation. In this step, several features, such as edges and curves, are extracted from FV images by using descriptors, such as the maximum curvature method or local binary patterns (LBPs) [6]. The final step is user verification, where the same sequence of processing is adopted but with an extra step, namely, matching. During this step, the pattern received from enrolment location and the pattern saved in the system database are compared to determine whether the user is genuine or an impostor. The user verification operation is shown in Figure 1b.

Many technologies in hardware architectures are used in this field to obtain high accuracy and rapid processing. These technologies and software are mainly used to enhance FV images, extract image features and conduct matching. One of the most challenging problems is biometric leakage, which poses critical risks; for instance, stolen biometric information can be utilised to launch repetitive attacks, and this circumstance is difficult to detect [7]. Thus, the available studies and challenges in this field must be explored. Several scholars [8]–[10] have reviewed FV biometric technology. However, they analysed the techniques applied in FV identification approaches on the basis of three stages, namely, pre-processing, feature extraction and classification, to identify individual identities. They did not examine the development of FV biometrics on the basis of software components in terms of data protection and data size reduction. Moreover, they did not discuss the development of FV biometrics on the basis of hardware components.

The present work aims to contribute to the future development of FV biometric verification system-based software and hardware components via the exploration of the existing techniques and issues in this research field. This work strives

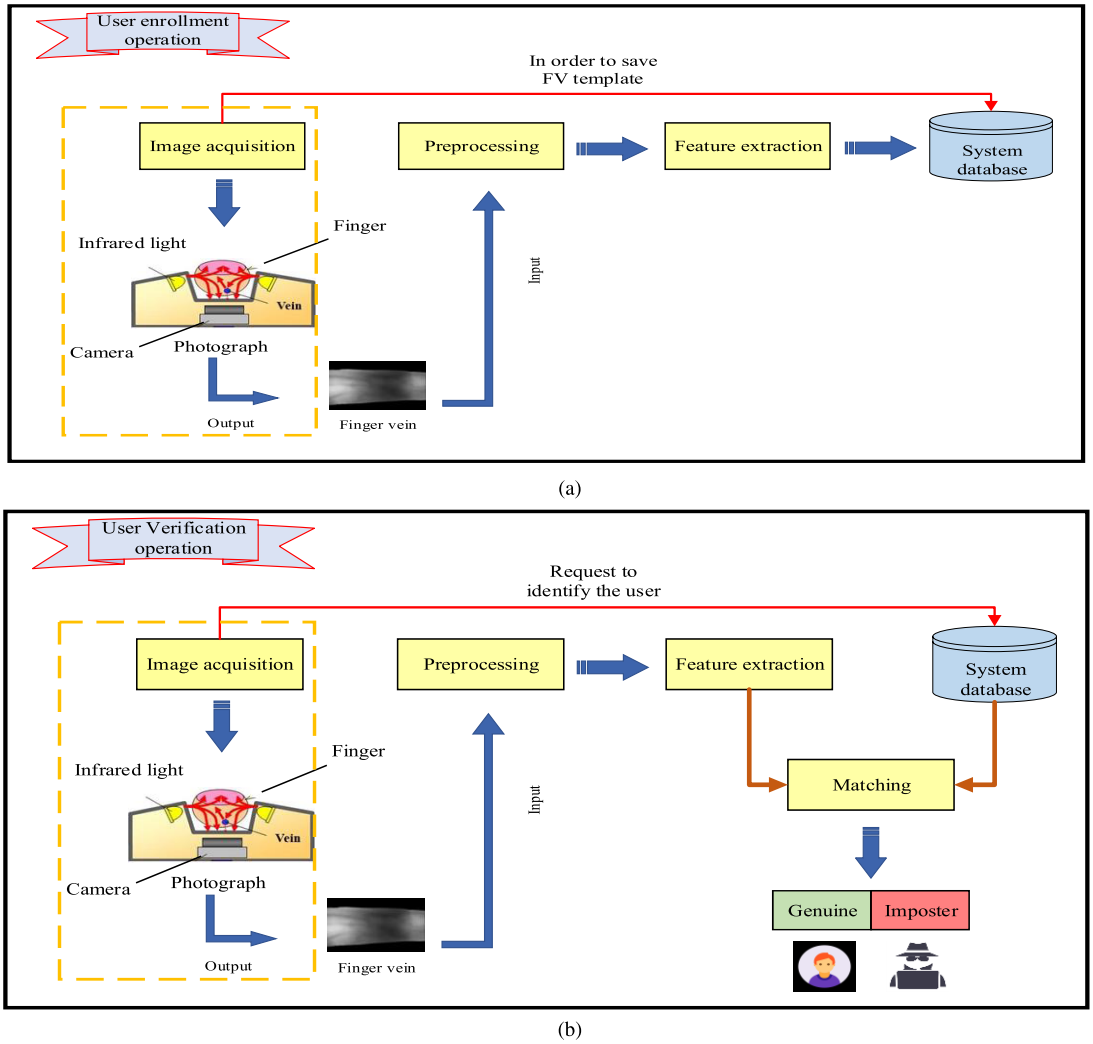

FIGURE 1. a) User enrolment operation. b) User verification operation.

to highlight new disruptive technologies and provide a platform for further studies through a comprehensible classification and identification of the features and characteristics of evolving studies on this topic.

The arrangement of this article is as follows. Section 1 explains basic information on FV biometrics and the main contributions and objectives of this study. Section 2 describes the method used. Section 3 presents the search results and statistical information. Sections 4 and 5 introduce the classification of selected studies and discussions, respectively. Sections 6, 7 and 8 present the proposed solution, the limitations of this study and the conclusions, respectively.

II. METHOD

This study examined articles on FV biometric technology. The articles addressed the implementation of FV biometrics in various domains with regard to development based on software and hardware components. The methodology adopted in the current study is based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol_ [11], [12]. PRISMA is an evidence-based minimum set of items for reporting in systematic reviews and meta-analyses. We proposed a systematic review protocol (Figure 2). This protocol is explained in the following.

This study focused only on the following categories of previous work: those written in English, those that focused on multi- or uni-biometrics and those that reported an investigation of human physical features (e.g. normal fingerprints, the face and palm geometry) or human behavioural biometric features (e.g. voice and gait). However, human FV biometrics was excluded from the search. The search for relevant articles was conducted using the keywords 'biometrics', 'finger veins' and 'verification'. The digital databases used for the article search included IEEE Xplore, Web of Science (WoS) and ScienceDirect [13]–[16]. A sufficient number of studies on FV biometric technology covering a wide scope of disciplines can be obtained from these databases (Figure 2).

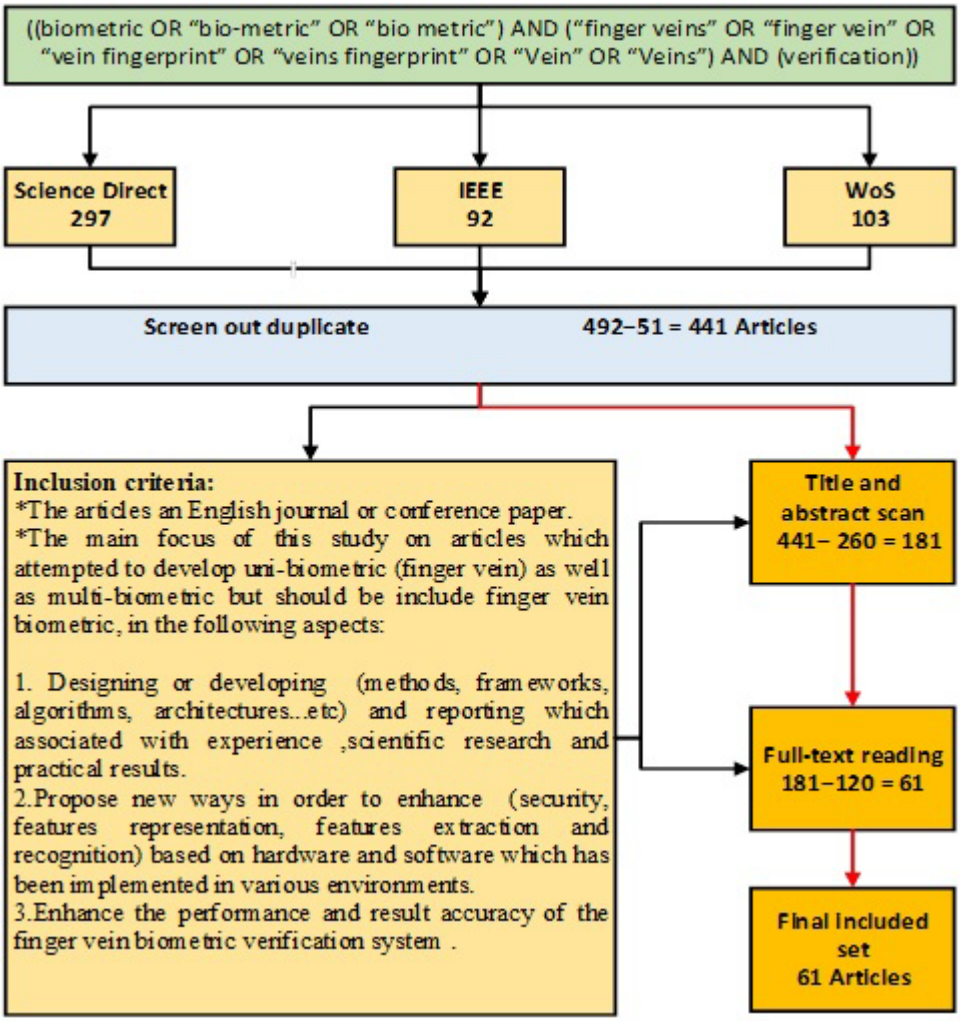

FIGURE 2. Search protocol used in article selection.

During the retrieval process, search, selection and categorisation of relevant studies from these databases were carried out in three screening and filtering iteration processes [17]–[20]. In the first iteration process, duplicate articles were eliminated [21]–[24]. The second iteration process involved the identification and elimination of all unrelated articles by scanning the titles and abstracts. The third iteration entailed a full-text review of all the articles that passed the second iteration process. The same eligibility criteria were utilised in all the iteration steps. The final set of articles comprised those that covered different FV biometrics-related topics. The search was conducted near the end of July 2018 in consideration of newly published articles. The search string was modified to allow it to correspond to the formatting requirements of each database. The general strategy used was as follows: (biometric OR 'bio-metric' OR 'bio metric') AND ('finger veins' OR 'finger vein' OR 'vein fingerprint' OR 'veins fingerprint' OR 'vein' OR 'veins') AND (verification). According to the ISO/IEC 2382-37 standard, biometric recognition encompasses biometric verification (one-to-one matching) and biometric identification (one-to-many matching). Thus, this study focused on verification rather than identification.

Book chapters, letters and short correspondences were excluded from the search results by using the advanced search options in the search engines in order to have access to up-to-date scientific studies related to FV biometric verification. All articles that satisfied these criteria were included. Each article was read, analysed and summarised to facilitate the filtration process. With the proposed taxonomy, the selected articles were divided into two categories. The first one describes attempts on software development and presents the experimental results, frameworks, algorithms and methods that perform satisfactorily. It also discusses the experiences obtained from conducting the studies. The second category describes attempts on hardware development.

III. SEARCH RESULTS AND STATISTICAL INFORMATION

The search yielded 492 articles. Amongst these articles, 297 were retrieved from ScienceDirect, and 92 and 103 were

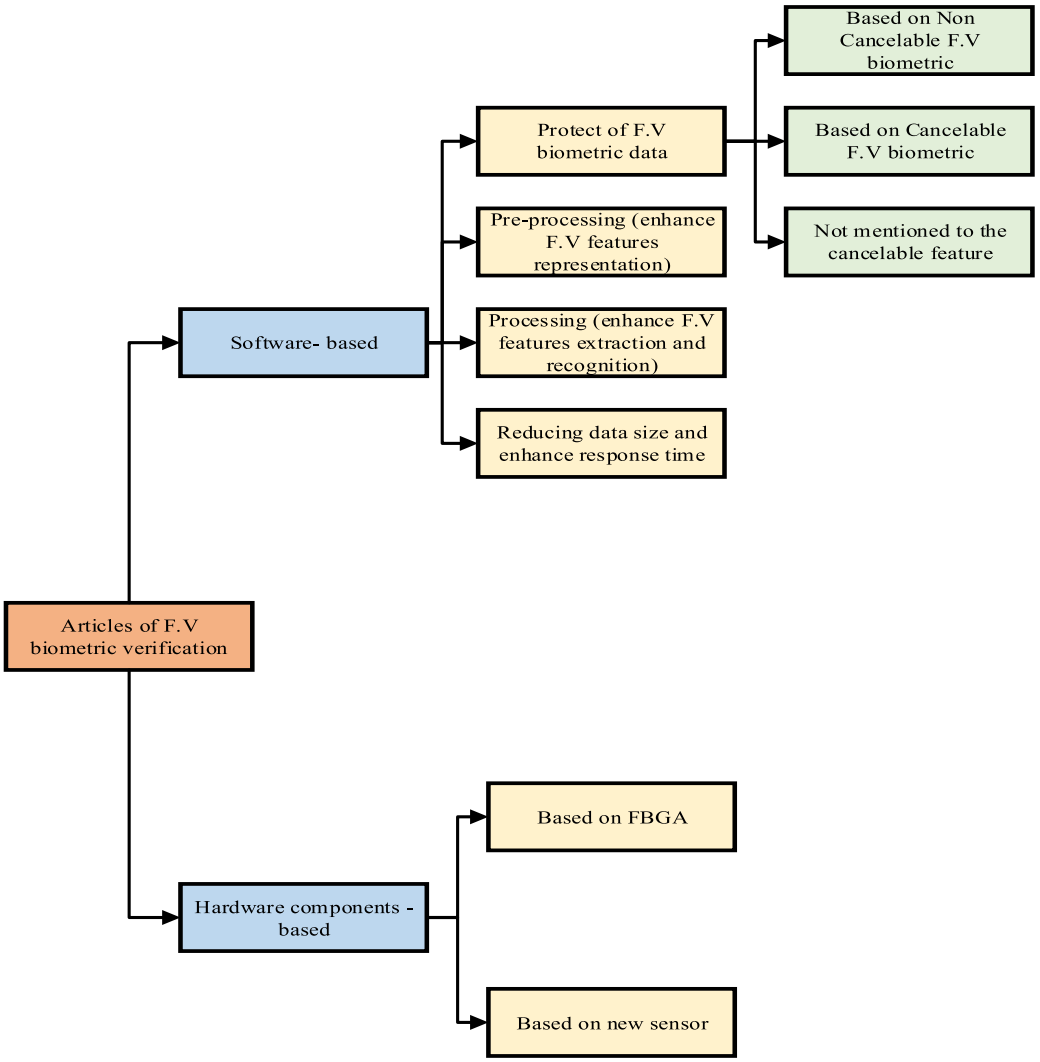

FIGURE 3. Taxonomy of literature on FV biometric authentication.

retrieved from IEEE Xplore and WoS, respectively. The retrieved articled were filtered to identify those published from 2007 to 2018. Fifty-one duplicates were identified from the 492 retrieved articles in the first stage of the three-phase screening iterations, and they were subsequently removed. Another 260 articles were removed in the second iteration process after the titles and abstracts of the retrieved papers were scanned. The full-text screening of the articles in the third iteration phase resulted in the elimination of another 120 articles, leaving only 61 articles in the final set. The remaining 61 articles were classified into different categories and subcategories. The first category (52/61; 85.24%) contained articles on developing various protection means, algorithms, methods, architectures, techniques and other similar contributions. These articles attempted to develop or design FV biometric authentication systems via software development, with the aim of proposing a solution to issues in security, accuracy, quality of FV images, feature extraction and computational time and cost implication of each authentication technique. The second category (9/61; 14.75%) included studies that aimed for development through hardware components. Several patterns were observed from literature, and a taxonomy was created, as shown in Figure 3. Several subcategories with overlapping areas were also noted.

Human biometrics-based authentication systems, especially those that depend on emerging FV authentication technology, have recently been employed in numerous applications where thorough human identification and verification are needed. The distributions of the selected articles' designs and development are listed in Table 2.

A. SOFTWARE-BASED DEVELOPMENT DESIGN

As shown in the article taxonomy described in Figure 3 (development of FV biometrics based on software), 52 of the 61 articles focused on software proposal. This category

TABLE 2. Classification of development and design articles.

Categories	Sub-categories	Reference
Development in FV biometrics based on software	Protection of FV biometric data	[7] and [11–19]
	Pre-processing (enhancement of FV feature representation)	[5] and [20–31]
	Processing (enhancement of FV feature extraction and recognition)	[1–4] and [32–53]
	Reduction of data size	[54–56]
Development in FV biometrics based on hardware	Based on field-programmable gate array (FPGA)	[6] and [57–59]
	Based on new sensors (imaging devices)	[60–64]

comprised methods, algorithms, means of protection and novel techniques that assisted in addressing the issues associated with systems for FV authentication. These issues include improving image acquisition quality, securing FV templates, enhancing the feature extraction process from FV images, ensuring the accuracy of FV pattern matching and improving the general efficiency of FV authentication systems. This category of articles was further sub-classified into the following:

1) PROTECTION OF FV BIOMETRIC DATA

The first sub-group (10 out of the 52 articles) involved the protection of FV biometric data. The studies in this group focused on securing FV pattern information. Biometric data (template) acquisition in this category was carried out after the individual enrolment step. However, in this method, the template information cannot be changed or replaced if it is stolen by an attacker because such information does not change throughout the life of the human owner. Therefore, the development of new technologies that can ensure the protection of biometric templates has received extensive interest. The security of the information in biometric verification systems should be ensured because of their confidential and private nature. Hence, additional studies that extensively focus on protection against spoofing and information leakage should be conducted. We need to answer the question of whether FV biometrics is cancellable or not to explain the various methods that have been proposed for protecting FV biometric pattern data in terms of the nature of FV biometrics that has been created.

a: NON-CANCELLABLE FV BIOMETRIC TEMPLATES

Study [25] used a new algorithm to determine the positions of intersection points in FV and generated an encryption key from these features to extract non-cancellable patterns. The FV pattern cryptosystem is secure against offline brute-force attacks (FAR) that may be conducted to acquire the original image, which can be used for the decryption of encrypted shares by utilising the same secret key in the protection template according to an optimal sequential fusion for multi-biometric cryptosystems [26].

Study [27] presented multi-biometric finger cryptosystems in various fusion strategies that have been implemented to fuse normal fingerprint, FV, finger knuckle print and finger geometry modalities in each individual enrolment and verification for encrypting and storing finger patterns in the database. This multi-biometric finger cryptosystem focuses on the difficulty of decoding an individual fuzzy commitment scheme as the primary security analysis of cryptosystems in human finger multi-biometrics.

b: CANCELLABLE FV BIOMETRIC TEMPLATES

Most methods used in FV biometric protection generate a bio-key from extracted features. However, they are insufficient with regard to accuracy and security bit length, as mentioned in [28]. In general, bio-key schemes are of three main types: fuzzy vault, fuzzy commitment and dynamic bio-key generation. This study proposed a new bio-key generation method called Fountain Valley High School (FVHS) algorithm to extract a stable and long bio-key (128–256) bit from FV biometrics. This method combines machine learning, biometrics and cryptography technologies because these information are vulnerable to social engineering dictionaries, eavesdropping, spoofing and other network attacks. Another example of using a bio-key was provided in Study [29], which extracted the features of three biometric traits, namely, fingerprint, retina and FV. The features were then fused at the feature level, followed by an encryption operation. The biometric templates were stored in a database for use in verification operations. Study [30] used an FV and signature authentication system that simultaneously utilises the cross number idea and fundamental concept of compound analysis. A visual cryptography scheme was implemented to protect this information. Meanwhile, an FV recognition algorithm was presented in Study [31] to secure biometric data on the basis of deep learning and random project (FVR-DLRP). This work proposed a new framework that uses cancellable FV biometric templates and can keep secret information despite password decryption. However, the confidentiality of FV information needs enhancement. An attacker who successfully breaks the encryption can obtain the FV biometric features. Study [32] proposed a cancellable biometric system based on fingerprints and FVs that combines the minutiae of FV and fingerprint features. However, fingerprint biometrics become unstable over time and are difficult to extract from

the elderly and patients with diabetes. This type of biometric is also traceable via imaging devices because of the device contact required during enrolment.

c: NO MENTION OF THE CANCELLABLE FEATURE

Study [7] 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. A micro-mirror is used to obtain information from FVs as a cipher key for the encryption of this information and storage of raw images in the database. When a user needs database access, information should be verified before the raw image is restored from the database. Study [33] proposed an efficient method of detecting fake FV images (print artefacts). The technique uses total variation (FV) regularisation and LBP descriptors to decrypt structure and noise information in the decomposed components.

2) PRE-PROCESSING (ENHANCING FV FEATURE REPRESENTATION)

The second sub-group (13 out of the 52 articles) focused on FV image pre-processing, which includes various operations, such as ROI localisation, image resizing, normalisation, image cropping and improvement, 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 (i.e. processing). This step should be implemented because input vein images from scanners may contain unwanted data.

Study [5] used the auto-encoder method in learning enhanced features to illustrate FV images. A benefit of using an auto-encoder is enhanced image quality and smoothing, which enables the determination and discrimination of FV features. Another benefit is the learning of these features by using a self-taught learning technique, in which the auto-encoder learns the improved value for 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 redundant parts before enhancement. Study [34] used a Gabor filter to enhance an FV image and applied thinning to obtain the skeleton of FVs in preparation for feature extraction. Study [35] presented a learning model for extracting and retrieving the features of FVs by using limited a priori knowledge. This work presented a segmentation model that has been applied to an FV authentication system; a convolutional neural network (CNN)-based approach was also developed to predict the probability of pixels from the vein image background. This operation is applied by learning deep feature representation. Study [36] focused on creating a new model to improve the peak signal-to-noise ratio (PSNR). Picture components with a high level of quality were compared with a TV model. Study [37] proposed an FV verification system based on a multi-scale filter to enhance the matching results and the quality of FV images captured under non-uniform illumination. Study [38] developed a direction–variance–boundary constraint search model for FV biometrics for four-step restoration to reconstruct damaged FV patterns. Study [39] proposed an FV verification framework with manifold learning based on orthogonal neighbourhood-preserving projections to enhance the quality of FV images. Moreover, Study [40] presented a support vector machine (SVM) technique and an FV pattern authentication system based on principal component analysis (PCA) for image pre-processing and feature extraction by using linear discriminant analysis. However, this work focused on pre-processing rather than processing. Study [41] proposed a new FV recognition method based on a graph and transferred this graph to binary FV patterns. Study [42] focused on enhancing FV features by proposing a new approach to decrease the equal error rate (EER) in biometric verification systems rather than human perception decisions. Study [43] proposed a gradient feature selection algorithm and found that the features extracted from enhanced FV images provide the best discrimination capability in image intensity. The combination of gradient directionality and intensity outperforms the gradient feature alone. Study [44] focused on the matching process in an authentication system, and images were investigated to verify a person and improve the handling of FV segmentation problems. Study [45] proposed a modified unsharp mask (MUM) with a log-Gabor filter to enhance the sharpness and contrast of FV images.

3) PROCESSING (ENHANCING FV FEATURE EXTRACTION AND RECOGNITION)

The third sub-group (26 out of the 52 articles) focused on FV image processing, in which the FV feature operation is implemented for the extraction and preparation of images for the next step (i.e. processing). This operation is performed on vein patterns where networks of blood veins are usually stable. These patterns cannot be modified unless separated by external factors. Thus, the FV network structure was described in these studies by using several methods with reliable results.

Study [1] proposed a new method based on multimodal finger biometrics called band-limited phase-only correlation to measure the similarity of FV patterns. Study [2] developed a new individual verification system by using FV biometrics based on the artificial neural network (ANN) to distinguish FV images. Study [3] proposed a new method based on a personalised best patch map and veins for efficient performance with high accuracy. Study [4] presented a driver verification system based on FV biometrics and ANN to develop training and check modules. Study [46] proposed the use of the local line binary pattern (LLBP) as a feature extraction technique. Robust features can be extracted from patterns with vague veins. In Study [47], PCA was performed in real time to provide end-to-end authentication depending on the FV biometric patterns. Study [48] proposed a new method based on two models, namely, FV and finger shape, by using index and middle fingers. Study [49] developed a new multi-instance method and evaluated it by using multi-FV based on

score-level fusion. Study [50] presented a new method based on a hybrid histogram descriptor to address the weaknesses of line- and point-based FV feature extraction and used binary gradient contour. The histogram of competitive orientations and magnitudes was proposed as a local descriptor for FV feature extraction in Study [51]. Study [52] contributed a new chain code-based feature extraction method combined with fusion techniques of image skeletons. Study [53] applied a new method in which pre-processing and processing are enhanced. However, this method focuses more on processing than pre-processing. A system that uses a bank of Gabor filters was proposed for utilising FV features at various directions and scales. Study [54] developed a method for extracting robust features from FV images in verification systems via FV biometrics and for extracting features with a global layout and local detailed information. This method is based on the bag-of-words concept and learns several robust and discriminative visual words from local base features, such as LBP. Study [55] presented a method based on the geometrical features of the intensity field to simplify the extraction of features from unclear vein patterns.

Study [56] proposed a new individual verification scheme based on FV and neural network techniques and found that using an adaptive neuro-fuzzy inference system shows good performance of the back-propagation network in terms of user verification based on FV biometrics. Study [57] proposed an FV verification method based on deep CNN for achieving improved performance. Study [58] developed an FV authentication system that uses a multi-instance minutiae-based matching method that is implemented in a unified minutia alignment and clipping manner depending on the genetic algorithm and k-modified Hausdorff distance measurement. Study [59] proposed an occurrence probability matrix (OPM) for matching two templates to maintain stability during matching. Study [60] presented a singular-value decomposition-based minutiae matching (SVDMM) method for FV authentication. Study [61] introduced a new design of a novel point set matching algorithm for the non-parametric matching of patch layouts to obtain high efficiency for tree models and high levels of accuracy in problems related to authentication and recognition. Study [62] used an ANN vein methodology to match FV patterns and enhance matching accuracy. Study [63] focused on using multi-modal biometrics, including FVs, to enhance matching accuracy. In this work, a score-level fusion method based on a triangular norm was developed to provide highly accurate matching. Study [64] proposed multi-modal verification systems based on face and FV authentication; multi-level score-level fusion was applied, and the impostor and genuine scores were combined using fuzzy fusion. Study [65] proposed a new method of FV feature description using adaptive vector field estimation. Study [66] presented a new method of FV feature extraction and enhancement and developed the hierarchical hyper-sphere model (HHsM) by using granular computing. Moreover, Study [67] proposed an FV recognition framework that consists of an anatomical structure analysis-based vein extraction algorithm and matching.

4) DATA SIZE AND ENHANCEMENT OF RESPONSE TIME

The fourth sub-group (3 out of the 52 articles) focused on reducing the size of FV databases to minimise the computation complexity and time consumed during processing. Study [68] developed a new smart algorithm based on ASIFT feature matching for FV biometrics to reduce the computation complexity in large FV databases. Study [69] proposed a new matching method for FV patterns to increase accuracy. This study focused on reducing the complexity of the system and the FV database to be used in the authentication system. Study [70] presented a method of obtaining responses from a database in an acceptable time (retrieval solution); the technique was then used in iterative line tracking. This method aligns FV to a fixed location in the patterns in addition to extracting FV features.

B. HARDWARE-BASED DEVELOPMENT AND DESIGN

As shown in the taxonomy presented in Figure 3, development studies based on hardware components (9 out of the 61 articles) focused on the design of full hardware system architectures and the design and/or development of devices for FV authentication systems. This category can be divided into two sub-categories.

1) BASED ON A FPGA

Study [71] proposed a new approach for FPGA implementation that depends on an embedded system by using FV biometric authentication to achieve high biometric recognition rates even with limited resource systems in real time. Studies [6], [72] and [73] attempted to develop an individual authentication system based on FV biometric patterns by implementing the system in FPGA. Recognition was performed in the FPGA instead of a central server because many authentication systems work in unreliable environments.

2) BASED ON A NEW SENSOR (IMAGING DEVICE)

Study [74] proposed a new imaging device for simultaneous FV and fingerprint acquisition and a new FV recognition algorithm. Studies [75], [76] and [77] focused on the development and/or design of an imaging device that can capture either only FV or FV with another biometrics simultaneously; this device presents certain advantages, such as sufficient robustness, low cost and user friendliness. Study [78] proposed a biometric multi-modal authentication system based on a DCNN. Given that the image acquisition positions and light in imaging environments vary from time to time, a CNN NIR light camera sensor was used to address the problem.

IV. CLASSIFICATION OF ARTICLES

This section classifies and discusses the final set of articles from three aspects: (1) number of publications; (2) problem type, proposed solutions, best results and evaluation methods in the included studies; and (3) available databases from

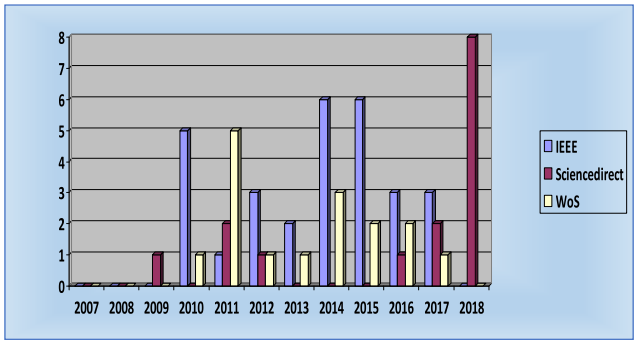

FIGURE 4. Publication trends in the three databases.

different scientific work collected from volunteers, such as staff, students and other individuals.

A. DISTRIBUTION OF ARTICLES DEPENDING ON THE NUMBER OF PUBLICATION

Figure 4 shows the number of publications in the three databases, namely, IEEE Xplore, ScienceDirect and WoS, for each year in the period 2007–2018. A marked increase in publication rate was observed during 2018 with regard to the development of authentication systems based on FV biometric technology.

B. DISTRIBUTION BASED ON PROBLEM TYPE, PROPOSED SOLUTIONS, BEST RESULTS AND EVALUATION METHODS IN INCLUDED STUDIES

This section classifies the articles into groups according to the technical problems, proposed solutions, best experimental performance results and matrix evaluation methods utilised to evaluate the proposed solution. This distribution will help researchers and developers identify and avoid critical challenges. Furthermore, this classification can assist in checking for the best results (state of the art) and appropriate evaluation methods for use.

1) TECHNICAL PROBLEMS IN PREVIOUS STUDIES

Seven types of technical problems were experienced in the previous studies, and they are shown in Figure 5. The first type of technical problems discussed by several studies is the protection of FV biometrics in the verification system by using either uni-biometrics (FV biometrics) or multi-biometrics, which include FV biometrics as a part of the verification system. In Study [7], the technical problem was how to secure FV biometrics during the imaging stage. Studies [6], [25]–[28] and [30]–[32] attempted to solve the problem of leakage of FV pattern information from the authentication system. The last two studies under this type of problem are [29] and [33], which attempted to protect the FV authentication system from several attacks, such as spoofing or use of printed versions of FV biometrics by unauthorised persons to access the system's services.

The second type of technical problems relates to FV feature extraction from FV images. Studies [4], [44], [50]–[52] and [55] focused on enhanced feature extraction performance. Study [46] concentrated on the time consumed during FV feature extraction, and Study [74] focused on the cost imaging device that can be used in capture operation. Studies [38], [48] and [66] tackled the problem of feature extraction accuracy.

The third type of technical problems relates to enhancing the FV pattern recognition rate and matching accuracy that affect the entire system's performance. Studies [1], [3], [40], [53] and [67] focused on improving the FV pattern recognition rate. Studies [57], [59] and [62] concentrated on the accuracy of the FV feature matching problem. Studies [63] and [71]–[73] focused on enhancing the performance of the entire FV verification system.

The fourth type of technical problems relates to the imaging devices used during the user enrolment stage. Study [49] developed a multi-biometric identification system, but the system may need extra imaging devices and has algorithm complexity. Studies [54], [60] and [77] focused on traditional problems facing verification systems, namely, rotation, translation and deformation of FV images. Studies [75] and [76] addressed the problem of the cost of FV capture devices and increased quality of vein images.

The fifth type of technical problems relates to FV image quality and feature representation. Studies [5] and [65] discussed the problem of FV feature representation. Studies [34], [36], [37], [39], [42], [43], [45], [61] and [65] focused on the problem of FV image quality and elimination of the effect of noise and distortion in FV images during the imaging stage.

The sixth type relates to problems in FV input data size that affect system performance; given a large amount of data, system overload occurs, thus decreasing the verification system performance [2], [56]. The seventh and last type of technical problems relates to the time consumption during the verification operation. This type of problem is important in attendance checking systems [41], [70].

2) PROPOSED SOLUTIONS IN PREVIOUS STUDIES

This section highlights the solutions proposed by previous studies according to the types of technical problems.

a: PROPOSED SOLUTIONS FOR FV BIOMETRIC SECURITY PROBLEMS

Several solutions were proposed in previous studies, as shown in Figure 6. Study [6] used an FPGA board for effective and low-cost FV feature extraction and protection. Study [7] secured FV biometrics during the imaging stage by implementing an optical data encryption technique based on compressed sensing. Study [25] used the extracted features to generate an encryption key and applied the data encryption standard algorithm to encrypt and decrypt biometric information. Studies [26] and [27] adopted a fuzzy commitment

FIGURE 5. Classification of technical problems in FV biometric verification systems.

scheme to protect biometric information. This procedure combines an error correcting code and a cryptographic hash function in the enrolment and verification phases. Study [28] focused on secure FV information during online verification by proposing a new bio-key generation algorithm called FVHS, which has the advantages of biometrics and user-key authentications. FVHS instantly generates stable and sufficiently strong bio-key sequences from FV biometrics during the encryption of the corresponding uniform resource locator of different services provided by cloud computing with the shared secret key. Study [30] performed visual cryptography to fuse a template and preserve the security and accuracy of the system; this scheme uses the original biometric data wherein the vein images are divided into small segments called shares, which are then encrypted using a secret key.

An algorithm based on deep learning and random projections called FVR-DLRP was utilised in Study [31], and the results showed high accuracy with an acceptable level of security. Study [32] proposed a new multi-biometric system based on a feature-level fusion strategy with three different fusion options and developed it (P-DFT) into enhanced partial discrete Fourier transform-based non-invertible transformation. This system has a high level of security. Study [29] used a technique that adopts the RSA algorithm to protect biometric information and multi-biometric authentication systems. Study [33] utilised a method for detecting presentation attacks based on FV regularisation, block LBP and SVM. The results showed the capability of distinguishing real and fake FV patterns. However, a critical challenge is the leakage of the pattern template, which can be stolen from the database and used in spoofing attacks.

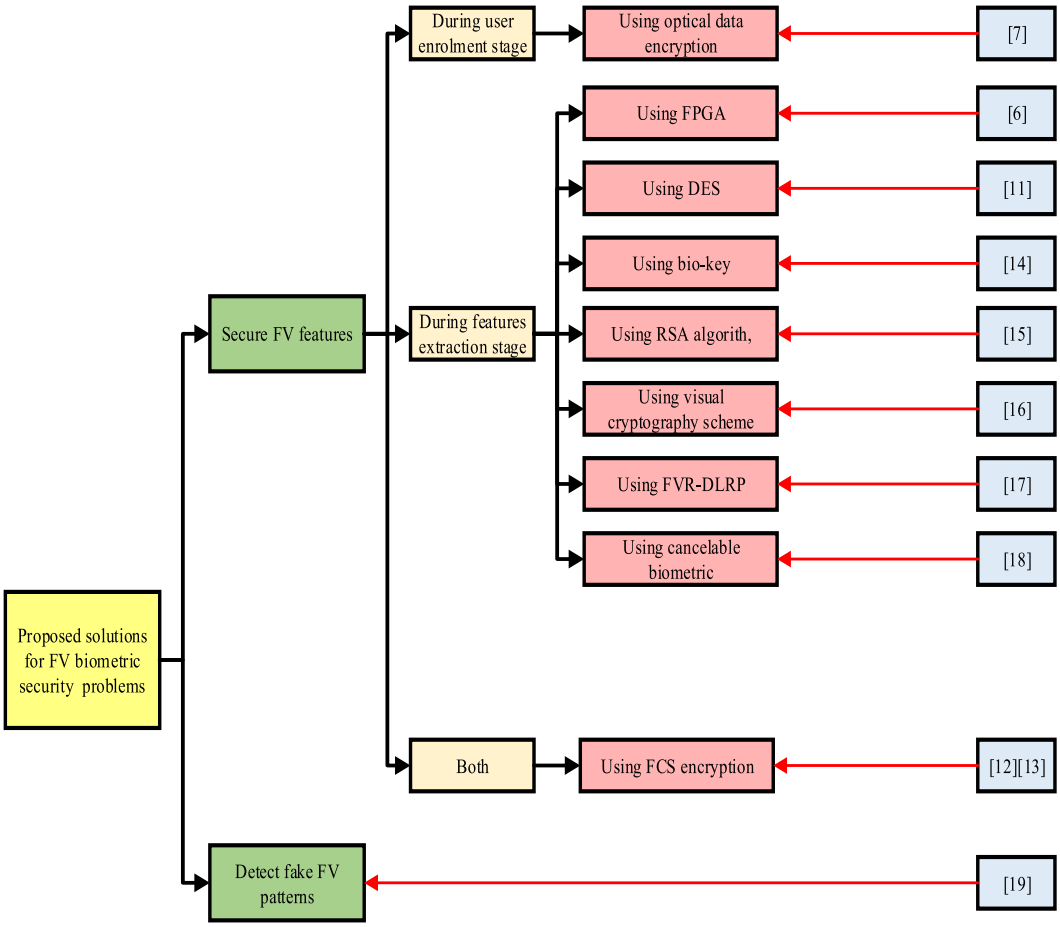

FIGURE 6. Proposed solutions for FV security problems.

b: PROPOSED SOLUTIONS FOR FV FEATURE EXTRACTION PROBLEMS

Study [4] used an approach based on Radon transform for FV feature extraction with ANN for classification. The Radon transform focused on a small amount of data with high-value coefficients, whereas ANN was applied in data analysis and FV pattern recognition. Study [44] utilised Gabor filters with eight orientations for extracting FV features via SIFT to identify the features of FV patterns by calculating the number of matching SIFT and confirm the user. Study [50] enhanced the quality of FV images to eliminate the variation of vein locations, reduced the difference in finger location, enhanced the visualisation of vein lines, and used local histogram to calculate the weight of the sign and magnitude value from the FV descriptor. Study [51] developed a FV biometric user authentication system based on a new descriptor called histogram of competitive orientations and magnitudes. Study [52] proposed a new algorithm that depends on the spatial and orientation features of FV images to potentially eliminate distortion and noise in unstable FV images. To reduce the time of FV feature extraction, Study [46] extracted features from FV images by using a new descriptor called LLBP. In LLBP, the neighbourhood of data is a line, whereas in LBP, the neighbourhood is a square. Study [74] used a low-cost imaging device to enhance the accuracy of feature extraction and the recognition rate. The components of this device are a camera and NIR light sources. Study [38] proposed a method that can restore over 10% of FV images with lost target points and performed FV pattern restoration. Study [48] determined the intersection point between the index and middle fingers to select the extreme points. The height of pixels in vein images must intercept with the abscissa of the point as a benchmark. The image of the abscissa location remains relative to the original point, which is the width of pixels. Study [66] converted an FV image into very small granules, generated a group of hyper-sphere granules and created a new structure to enhance the extracted features.

c: PROPOSED SOLUTIONS FOR FV PATTERN RECOGNITION RATE AND MATCHING ACCURACY PROBLEMS

Several attempts were made to enhance the FV pattern recognition rate. Study [1] enhanced FV pattern recognition by using a new type of features called width–centroid contour distance (WCCD) based on merging the width with the

centroid contour distance (CCD) and performing an integration between FV and finger geometry. Study [3]'s feature extraction method consisted of three steps. Firstly, local base features from partitioned pattern patches are extracted. Secondly, a small codebook that contains visual words called FV textures (FVTs), which are patches collected through the k-means clustering algorithm, is learned. Thirdly, an FVT map is used as a feature for representing the attributes of FV patterns. The output of this method is highly accurate and robust. Study [40] proposed an FV biometric verification method based on PCA, implemented linear discriminant analysis (LDA) during pre-processing to extract FV features and defined the degree of the relationship between training and testing sets for the evaluation of system performance.

Study [53] used normalisation, determined the ROI in FV images, identified the characteristics of FV by using a bank of Gabor filters and classified FV by using the nearest cosine classifier to enhance accuracy. Study [67] extracted vein features by using orientation map-guided curvature depending on the valley- or half-valley-shaped cross-sectional profile. The matching operation used FV network calibration to reduce the displacements. To address the accuracy of FV feature matching problem, Study [57] focused on the optimisation of matching accuracy under various circumstances by proposing a new method called deep CNN and used brute force search to set the hyper parameters due to the very small domain. Study [58] adopted two-step minutiae matching for various FV recognition instances and a sharping approach based on the genetic algorithm and k-modified Hausdorff distance. Study [59] utilised OPM, where each element has a stable value that corresponds to an area in the finger template matrix. OPM defines stability during matching operations and thus allows high-stability regions to enhance the results of matching. Study [63] developed a new approach that uses score-level fusion for multi-biometrics of fingers. Powerful devices are used to provide a simple implementation for complex algorithms and computations. Accordingly, the adoption of this technology in applications requiring low-cost studies is prevented. Studies [71], [72] and [73] developed a new platform that uses FPGA to achieve superior performance through the acceleration of devices and tools during image processing.

d: PROPOSED SOLUTIONS FOR FV IMAGING DEVICE PROBLEMS

To address the need for extra imaging devices to capture additional FV features and high-quality FV images, Study [49] used the index, middle and ring fingers of a hand to enrol a user. The features of these patterns were extracted using three different FVs in a score-level fusion strategy. An FV biometric authentication method based on the bag-of-words concept was proposed in Study [54] to address the problem of rotation, translation and deformation of FV images. The new method was proven to have high accuracy and can reduce the effect of the problem. Study [60] used the SVD method based on minutiae matching for FV recognition to reduce the distortion resulting from the rotation of the user's finger. Study [77] proposed a new image acquisition device to synchronise the capture of FV and finger dorsal images. Study [75] proposed an effective and low-cost imaging device that captures FV images to solve the cost problem of FV capture device and increase the quality of vein images. Study [76] developed a new FV imaging device based on sparse representation to enhance the quality of FV images and increase the recognition rate.

e: PROPOSED SOLUTIONS FOR FV IMAGE QUALITY AND FEATURE REPRESENTATION PROBLEMS

To solve the problem of FV feature representation, Study [5] used a self-taught feature learning system that enhances FV feature representation to learn a set of representative features via auto-encoders. The proposed solution adopts an unsupervised feature learning method without heavy processing. Study [65] proposed a method of estimating the curve length field (CLF) and a Gaussian weighting scheme with CLF constraint by using vein vector fields (VVFs) for FV features. To solve the problem in the quality of FV images and eliminate the effect of noise and distortion in FV images, Study [34] presented a new FV extraction method that discovers valley structures by using curvature in random space. Study [36] introduced a new model to improve the quality of FV images and eliminate noise according to fourth- and second-order partial differential equations, thus increasing PSNR by 2 db. Study [37] performed filtering at various scales to reduce noise, which is produced through non-uniform illumination, low contrast and hair and skin textile. Study [39] proposed a new framework that consists of training and testing sections. These sections begin by preprocessing FV images to detect ROI, followed by enhancement and normalisation. This system is adequately robust against noise and distortion. Study [42] presented a new method for FV quality assessment based on deep neural network to predict the quality of FV patterns by studying the binary inputs of FV. Study [43] developed a new method to extract FV features from distortion by using the gradient algorithm and a matching operation adopting the Euclidean distance algorithm. Study [45] used modified repeated line tracking to extract high-quality FV features and eliminate FV image sharpness. The study addressed image quality based on un-shaping mask and the MUM algorithm. Study [61] proposed a new method involving a joint discriminative and generative vocabulary tree-based model for FV authentication. Study [65] presented a method of estimating CLF, in which a spatial curve transform is used to extract FV features. VVFs are used to enhance recognition accuracy.

f: PROPOSED SOLUTIONS FOR FV DATABASE AND INPUT DATA SIZE PROBLEMS

Input data size affects system performance. Large amounts of data cause overload and decrease system performance. Several studies focused on addressing this problem. Study [2] used PCA to extract features from FV images and performed

classification via ANN; the authors showed that a large input data dimension causes system overload. Meanwhile, the identification rate obtained with the use of an adaptive neuro-fuzzy inference system (ANFIS) exhibits perfect performance of a back-propagation (BP) network in personal identification. Study [56] adopted PCA to extract features from FV images and applied pattern classification through a BP network and ANFIS to eliminate the overload produced by a large input data size. Study [68] used a method based on the efficient recognition and detection of the defects of FV patterns and reduced the size of the database by implementing a fuzzy scheme. This study presented a new procedure to achieve best matching and high resistance against defect issues in FV data. Study [69] focused on representing a particular point to reduce the required data space in FV authentication applications. A method was presented to overcome the shortcomings posed by large storage data and heavy CPU computation requirements.

g: PROPOSED SOLUTIONS FOR TIME CONSUMPTION PROBLEMS DURING VERIFICATION

The discriminative binary code (DBC) learning method was proposed in Study [41] for FV recognition systems. To make the FV pattern discriminative and representative, this method formulates the specific problem into an optimisation problem. The efficiency of the DBC method leads to enhanced recognition rate and retrieval time. Study [70] developed a new verification system using FV patterns for checking attendance and discovered a means for fast searching in image databases to obtain a response within an acceptable amount of time.

3) PERFORMANCE RESULTS AND EVALUATION METRICS APPLIED BASED ON EXISTING TECHNIQUES

The best results of the proposed solutions that have been evaluated using various metrics, such as false acceptance rate (FAR) and false rejection rate (FRR), are explained in this section. Biometric identification systems evaluate matching accuracy and determine whether a user is genuine or not when the user attempts to access the system. A suitable threshold is determined. If the threshold is too low, then genuine users will be rejected. If the threshold is too high, then impostors will enter the system. The value of the threshold depends on the level of security required in the system. FAR and FRR metrics can be defined as shown at the bottom of this page.

The best results for the proposed solutions achieved by previous studies are shown in Figure 7. Various proposed methods were compared through analysis under translation, rotation and noise. In terms of rotation performance, all methods, except those in [54] and [60], are affected by rotation.

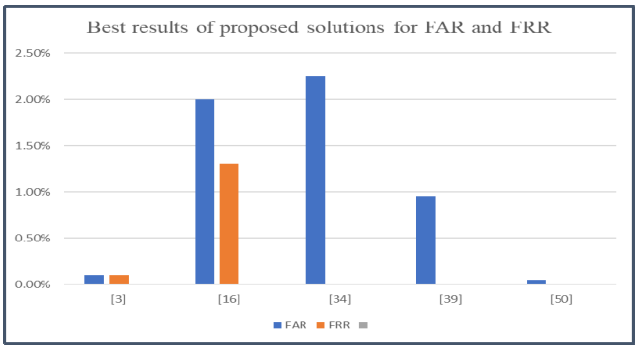

FIGURE 7. Best FAR and FRR values.

The first study removed all false pairs using local extensive binary pattern during feature extraction to enhance reliability. In the second study, each FV image was mapped into a matrix, and spatial pyramid matching was implemented to retain the spatial layout information. By observing the possible translation in ROI, various matches were conducted by translating one set of feature maps in the horizontal and vertical directions of three pixels. The maximum of the resulting distances was considered the final distance.

Several methods are robust against noise, as mentioned in Section (4.2.2.2). Figure 7 shows that Study [64] has good results in terms of FAR, but the value of FRR is not mentioned. In Study [3], FAR and EER are equal. The values of the two metrics depend on the threshold value. When the threshold is increased, FAR decreases and FRR increases and vice versa. When FAR equals FRR, their value at this point is called the equal error rate (EER). This value can be used to compare various biometric systems. The best results of EER in the proposed solutions by previous studies are shown in Figure 8. The values of EER were obtained from the articles reported by the authors. Comparing the results of various proposed methods in a direct way is not logical because these methods use different datasets in their experiments. The type of dataset affects the results and the entire biometric verification performance. Thus, a direct comparison of different methods is difficult and sometimes impossible. An investigation of the previous studies showed that several methods have a very small value of EER, such as in Study [47] where the value of ERR is 0.0009%. Figure 8 shows the value of EER for several studies.

In biometric verification systems, accuracy measures the number of impostor users that are accepted and the number of genuine users that are rejected. Accuracy is affected by the quality of features extracted during user enrolment, which depends on the quality and angle of the camera, light and

$$FAR = \frac{Number\ of\ successful\ attempts\ by\ impostors}{Number\ of\ attemps\ at\ authentication\ by\ unauthorized\ users}$$

$$RR = \frac{Number\ of\ failed\ attemps\ at\ authentication\ by\ authorized\ user}{Number\ of\ attemps\ at\ authenticationby\ genuine\ users}$$

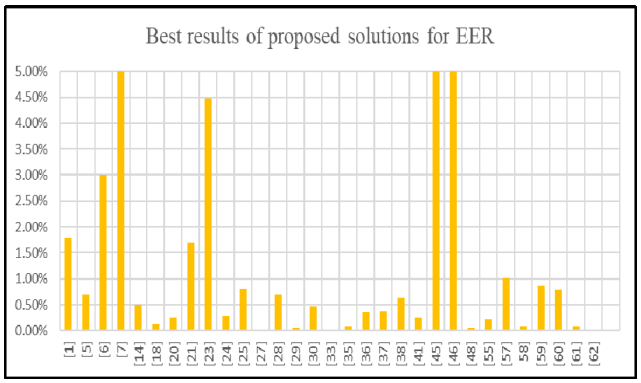

FIGURE 8. Best results of EER.

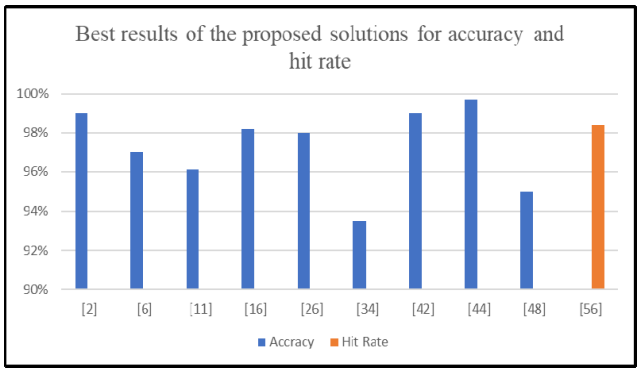

FIGURE 9. Best accuracy value and hit rate.

other circumstances in the enrolment environment. Several studies referred to this measure as biometric system accuracy, as shown in Figure 9 The best accuracy of 99.7% was reported in Study [58].

Study [70] focused on running time performance and obtaining a response within an acceptable amount of time. The experimental results showed that a response can be obtained in about 10 seconds when the database consists of 50,700 samples, as shown in Figure 9. Time consumption, which depends on the processing speed of the equipment used in the system, was determined to be the major factor that affects the performance of biometric verification systems.

C. AVAILABLE DATABASES

Available databases for scientific research that are recommended by companies, universities and researchers are presented in this section to enable researchers to select suitable databases and identify several methods that can be used in different environments, as shown in Appendix (A). Most of the datasets were collected from different volunteers, such as students or staff with different genders and ages. Several datasets are available online (open access) for research purposes. This classification helps researchers select appropriate databases according to the number of samples, images captured depending on the environment (indoor/outdoor or under artificial light or sunlight), image size, image quality, imaging device type and other parameters.

V. DISCUSSION

The basic characteristics of this emerging field are provided from the following aspects: motivations of using FV biometric technology in authentication systems, open challenges that impede the technology's utility, recommendations of authors and future study prospects.

A. MOTIVATION

FV biometric authentication systems are products of modern society's effort of fulfilling requirements in many applications of human biometric authentication. Increasing requirements for accurate and efficient personal verification are observed, and several of the motivations and benefits of using FV biometric technology in authentication systems are discussed. These motivations are identified and grouped into categories to aid further discussions. Figure 10 displays these motivation groups.

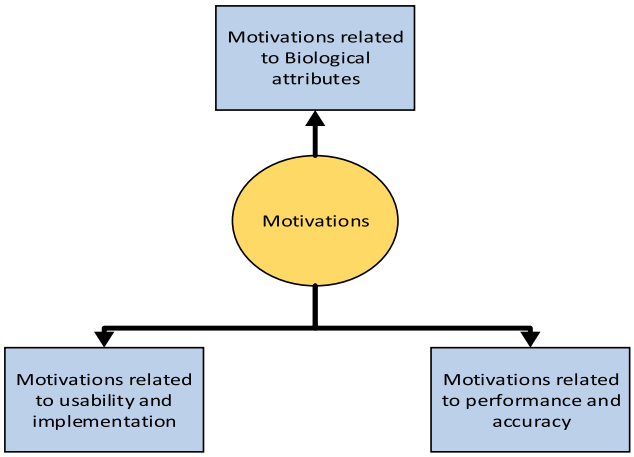

FIGURE 10. Types of motivations.

1) MOTIVATION RELATED TO BIOLOGICAL ATTRIBUTES

Studies [1], [40] and [63] found that biometric technology authentication systems are extensively popular because they provide high levels of security and reliability for individual authentication systems. Biometric systems are more reliable than traditional technology in security systems, which are used for securing 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 stolen information.

In addition, passwords and cards are usually forgotten. By contrast, FV biometrics demonstrates numerous attributes with regard to security purposes, such as the uniqueness of each person and long-term stability of information during human life. FVs are located underneath the skin and are thus invisible to the naked eye and not prone to external distortion or modification. Moreover, biometric verification is unique to every person [58]. Hence, biometric identification systems are more reliable in verifying identities than other

techniques, such as knowledge- or token-based identification systems.

FV biometrics has the following characteristics: (1) biometric information is invisible and difficult to invade and copy; (2) provides high levels of accuracy and security; (3) remains matchless even between twins and (4) each FV pattern authentication differs from another even in the same person [47], [44], [60]. Moreover, biometric information is incomparable even between the same fingers of each hand in the same person. Studies [25], [38], [71] and [72] found that FV biometrics is inherent and highly reliable, can neither 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. The motivation for using FV biometrics is attributed to its natural state, uniqueness and universality [5], [52], [41], [75]. Moreover, FV biometrics has high spoofing resistance and provides numerous advantages, such as (1) suitability and ease of capture, (2) uniqueness of personal information, high verification accuracy and (3) appropriateness for live body verification only. Contact with the sensor device during enrolment is unnecessary in an FV biometric authentication system; thus, traces cannot be left on the sensor (these traces can be used as a threat in the future) [49]. Therefore, stealing and forging biometric information are difficult. In the verification phase of using FV biometrics, the skin condition is not a hindrance to obtaining a clear image; hence, FV biometrics is robust against finger surface conditions [50], [61].

FV patterns have rich piecewise line attributes and are stable for use, thereby clearly describing FV patterns for individual verification [51]. Another feature is that obtaining vein information using artificial veins rather than natural veins is infeasible because this system depends on musculature energy [53]. This invisibility feature provides additional security because patterns are concealed from other individuals or machines, unlike in other verification technologies [55]. Replication of vein patterns is difficult for intruders. Thus, FV biometric authentication systems have higher resistance to spoofing compared with other biometric systems. This technology is free of the abovementioned problems. Studies [57] and [76] revealed that FV patterns are captured inside the finger and hence cannot be stolen or forged easily. Spoofing this type of system technology is extremely difficult, thereby rendering FV verification much safer than the widely used fingerprint system. FV biometrics is inherently superior in terms of accuracy, speed and security [59]. The other favourable features of FV biometrics are its non-intrusive nature and resistance to skin diseases (skin diseases cannot affect vein biometric information during image capture) [61]. These types of biometric identification systems are distinctive among individuals, and biological information from FVs, such as blood pressure, oxygen concentration in the blood and heart rate, can be obtained [69]. Moreover, human vein texture distribution is permanent from birth and rarely changes during the human lifetime. Thus, this security technology is robust and stable. Study [71] reported that biometric information is highly stable (from birth to death), rarely changes under any circumstance, is concealed underneath the skin, invisible and not prone to external distortion, except in cases of deep wounds or intense burns. In the authentication phase, an individual should be present at the location of the sensor device when he/she enrols his/her pattern to gain access to a system [72].

2) MOTIVATION RELATED TO USABILITY AND IMPLEMENTATION

Biometric technology can be embedded effectively in cloud computing and the Internet of Things (IoT) because it is highly secure and convenient for users, given that the memorisation of passwords is unnecessary; this technology can also play a crucial role in various security task applications, such as e-passports [2], [28]. FV biometrics is used in the financial sector, such as in bank transactions and end-user verification [4], [46], [52]. In the digital world, various applications and users have high demands for accuracy and reliability. FV authentication systems can be a reliable solution for verification in public devices, such as entrance control systems and door access. Studies [25] and [34] reported that the application of FV biometric technology is growing rapidly with regard to handling security issues, such as electronic and physical access control, digital rights management, electronic commerce and background checking. To enhance security and cybercrime prevention, technologies using human biometrics in authentication are highly appropriate [29]. Moreover, border control, public aid/social benefits and commercial projects can benefit from these technologies. FV biometrics has an excellent feature, that is, using the biometric information of an individual without his/her knowledge is difficult [35].

In addition, this type of biometrics is widely applied to identify and verify criminals. This technology is also used to prevent access to sensitive systems and authorise access to digital devices. Capturing images during individual enrolment to obtain FV patterns is non-invasive and contactless, thereby enhancing hygiene, preventing skin infections and ensuring user convenience [37], [57], [76]. Each person normally has 10 fingers; therefore, if something unexpected occurs to one finger, another finger can be used for verification [39]. This type of biometrics is simpler and more efficient than fingerprint techniques [47]. Currently, technologies using FV patterns are used in various fields, such as medical, financial, law enforcement facilities, airports and other applications that require very high levels of security and privacy [50], [52]. For user familiarity, FV patterns can be captured conveniently without any contamination from other people because touch/contact with the sensor during enrolment is unnecessary [53].

3) MOTIVATION RELATED TO PERFORMANCE AND ACCURACY

During individual enrolment, touch/contact with the sensor is unnecessary because the veins are detected by a CCD camera through an NIR filter; as the haemoglobin in the blood absorbs this light, the veins appear as dark lines and are thus easily detected [2], [62]. The information embedded inside the veins can be easily retrieved at any time by using certain devices [46]. Such instruments can be small and portable [34]. FV biometrics has higher levels of accuracy than other human biometric systems, such as fingerprint, iris and facial biometric systems [30].

FV biometrics has an inherent and natural connection with user verification and therefore does not require memorisation of any key [28]. FV biometrics has low levels of failure during individual enrolment [37]. It has high reliability for individual verification and low failure during enrolment and verification. FV patterns are highly reliable because of their low error rate, high levels of immunity against spoofing and user convenience [38], [51], [74], [75]. Accordingly, FV biometrics has elicited considerable attention from researchers because of its combined accuracy, speed, universality and cost efficiency [43]. Biometric information is highly available and obtainable by using cost-efficient sensor devices, unlike the information used in other types of verification systems. FV biometrics has several advantages over other biometric systems (e.g. face, voice, fingerprint and iris), such as low forgery rate, non-invasiveness and non-contact live-body detection [53], [54], [6].

The following additional advantages provide perfect motivations for using this technology.

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

FV 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 [73].

B. CHALLENGES

Previous studies have highlighted various challenges related to FV biometric applications. These challenges are classified into groups and discussed along with their references to enable readers to trace these sources and further discuss these challenges. These challenges are shown according to their nature in Figure 11.

1) CHALLENGES RELATED TO USER PERFORMANCE

This type of challenge involves factors that influence system performance and the result accuracy of matching. These factors are as follows.

- **User errors**: The shifting and rotation of the fingers in a sensor device during enrolment remain a major challenge in FV authentication [3], [44], [60]. This problem can reduce verification performance because such a movement significantly affects the matching results. Furthermore, during FV imaging, any movement or rotation of the fingers generates noise, which causes irregular luminance [55]. Consequently, different segments of the finger gain different amounts of light absorption, leading to processing errors.

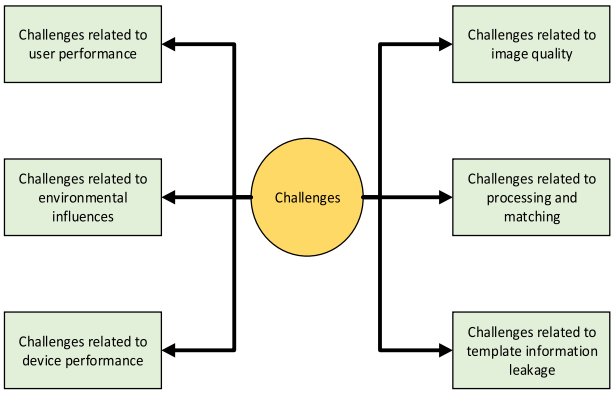

FIGURE 11. Categories of challenges grouped by nature.

- **Biometric finger features**: Another factor related to biometrics is finger features. According to Study [37], in addition to varying thickness, certain attributes related to finger skin affect image capture, such as pigmentation, thickness and hair. Moreover, we can obtain information by capturing images, such as the difference in thicknesses of finger muscles, bones and texture of networks surrounding the FVs, which produce a shadowy area [39]. Study [75] stated that the varying thickness of finger skin results in an unequal distribution of the light that passes through the fingers; consequently, high-quality vein patterns are difficult to capture 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 FV images remains a challenging task.

- **User gender**: The quality of vein lines during image capture is insufficient because certain females lack features that can be used during feature extraction and matching [48].

2) CHALLENGES RELATED TO ENVIRONMENTAL INFLUENCES

Images obtained during acquisition contain noise and unequal shadowy areas in addition to vein patterns [46], [55]. This noise can reduce the accuracy of the verification results. According to Study [25], the work environment influences authentication. Therefore, environmental noise must be eliminated because of the sensitivity of the verification process, thereby creating a critical trade-off between accuracy and usability. In addition, image acquisition is affected by venous pressure and body temperature changes; however, the centreline of the vein remains stable [5], [47]. FV image acquisition is naturally affected by the environment, surrounding temperature, light propagation in imaging FVs, physiological

changes and user performance [35]. Moreover, repeated and extended image acquisition changes the templates slightly because noise and environmental conditions, such as temperature and visible light confusion, occur due to non-uniform lighting, low local contrast and hair and skin conditions [37]. This section discusses the influence of the environment on image acquisition.

3) CHALLENGES RELATED TO DEVICE PERFORMANCE

The use of multi-biometrics in authentication systems may require additional acquisition sensors [49]. Dark lines extracted from FV images are unstable because the initial images obtained during enrolment have low contrast and include certain noise and non-uniform brightness [52], [53]. Typically, FV authentication techniques involve heavy and accurate computation and analyses [69]. Therefore, hardware devices and equipment are required to perform the process on FV data. Matching accuracy is generally poor when FV data contain large amounts of irrelevant information.

4) CHALLENGES RELATED TO IMAGE QUALITY

Noise elimination and other forms of image enhancement increase computational costs and lead to unacceptable processing rates [3], [5], [71]. Low-quality vein images affect system performance and result in slow processing, leading to poor system performance. Determining the same ROI using minimal cross or intersection points is difficult, and the accuracy of matching results is low. The most important factor in FV authentication is image quality because low-quality images produce fake or missing features simultaneously, thereby generating inaccurate results and decreasing verification accuracy [36], [42]. Furthermore, pattern quality is inherently affected by several factors that can be divided into two categories, as follows:

1. External factors related to environmental illumination, surrounding temperature, physiological changes, light penetration and unpleasant user behaviour;

2. Internal factors during the image pre-processing phase related to parameter inaccuracy, such as segmentation and enhancement processes applied on FV images. The quality of these images poses a serious challenge to the accuracy of matching results, security, scalability and privacy.

Vein images acquired using infrared light contain differently shaded areas produced from variations in skin thickness and finger bones and muscles. A significant challenge in vein biometrics is improving the verification performance and obtaining maximum immunity to false practices. Optical blurring, irregular shading or noise in low-quality vein images produces false extraction features or results in the loss of several vein features, leading to inaccurate verification results. The conflicts among various FV patterns in the same finger affect verification accuracy more seriously than the similarity of patterns of different fingers does [59]. In these patterns, areas can be stable or unstable, and performance accuracy is reduced. Thus, methods for improving the performance of these regular verification systems are required.

5) CHALLENGES RELATED TO PROCESSING AND MATCHING

The most important challenge in FV authentication systems is processing a large number of articles. Thus, frameworks (algorithm, methods and techniques) for enhancing system performance have been proposed. The challenges identified from the articles examined in the present study are discussed here. According to Studies [1], [53] and [61], the results of vein image segmentation become unsatisfactory and highly sensitive to noise due to low image quality. Moreover, segmenting a well-networked FV image is typically impractical when the image has low contrast. If the amount of input data is large, then the system will experience overload [2], [3], [70], [56]. Searching and verification requests in a large database consume additional processing time. Hence, if the database is large, then processing will become complex, and the number of patterns in the database will not affect the processing rate. The verification of an individual should not lead to the detection of other individuals to achieve privacy.

The verification process can lead to low accuracy when vein images have minimal vein intersection points [25], [57]. The most important problem is the accuracy of matching personal verification. When several patterns have low quality, the extraction and matching accuracies are influenced [38], [41]. The computation procedures during feature extraction from FV images are highly complex and time consuming [50]. Segmentation is affected by low-quality vein images [54]. The extracted features based on an inaccurate network lead to a decrease in the performance of the verification system. Collecting FV data from numerous users and maintaining the integrity of these data within FV authentication systems are challenging tasks [69]. Biometric authentication systems apply complex and heavy image processing algorithms [72]. Moreover, powerful computers are required to achieve suitable processing times. Biometric systems cannot constantly achieve the high processing speed required by real-time applications, such as in the military, which requires nearly pressing verification [73]. Two of the most important challenges in biometrics depend on enhancing verification performance to obtain resistance against any attack [76]. The main challenges include extracting robust vein features from vein images even when these images have irregular shading and noise and improving system efficiency.

6) CHALLENGES RELATED TO TEMPLATE INFORMATION LEAKAGE

According to Studies [7] and [77], a crucial threat is the leakage of biometric information, such as when repetitive attacks are conducted using stolen information. Exchanging raw biometric information to forge biometric data after these data are stolen is infeasible. The security of authentication systems based on biometric technology is challenged because of the information leakage of biometric templates [28], [6]. Therefore, these systems require the security of multi-biometric templates [27]. All biometric patterns stored in a database that are extracted as biological biometrics through the authentication process should be secured and

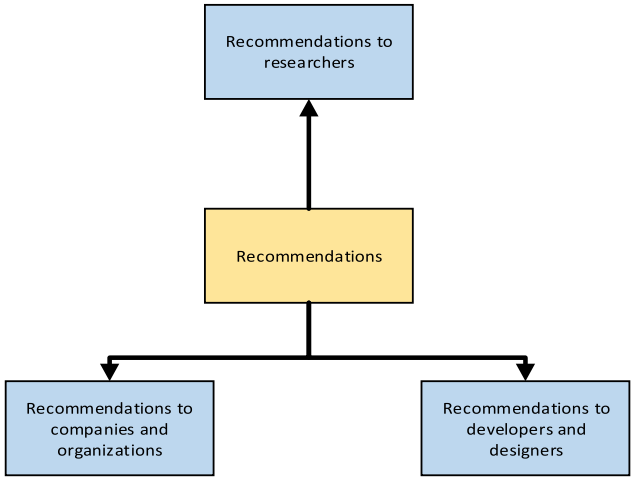

FIGURE 12. Categories of recommendations according to audience.

protected effectively from any attack. In the real world, billions of devices are connected through networks. The issue lies in protecting personal information and keeping these data secure; this challenge is widely discussed in all system types, especially authentication ones [51].

C. RECOMMENDTIONS

We briefly provide certain recommendations that were extracted from our survey. This section aims to mitigate the challenges encountered by developers and designers and help these individuals produce a robust and highly accurate FV biometric authentication system that satisfies the demands of companies and organisations. These recommendations are categorised into groups according to their audience, as shown in Figure 12.

1) RECOMMENDATIONS FOR RESEARCHERS

Researchers working on biometric authentication systems should follow various recommendations. In this section, we divide these recommendations into sub-categories as follows.

- Recommendations related to vein image enhancement

Studies on the vein intersection points of patterns for solving image quality problems may have provided false-positive verification results [25]. To create high-performance verification systems, additional processing can be implemented, thus enhancing the sharpness of FV images [5]. Therefore, improving low-quality FV features in the future is required [69].

- Recommendations related to authentication system protection

The most important aim of any authentication system is security. Therefore, researchers must focus on protecting systems from attackers and the leakage of biometric information. Moreover, security analysis can be improved through the accurate modelling of biometric feature distributions in FV databases [27]. According to Study [28], the efficiency and security of verification systems, especially in cloud computing, must be improved.

- Recommendations related to authentication problem optimisation

Searching for a method of obtaining an optimal subset from extracted features is beneficial for personal verification [1]. Thus, researchers must adopt problem optimisation approaches to address these concerns [64].

- Recommendations related to processing enhancement

Researchers are recommended to use various fusion methods together with vein shape features [46]. The entire verification system should be improved to achieve high performance and high matching accuracy. For the future extended use of modelling feature extraction methods, databases should be managed effectively, and matching methods and the entire verification system's performance using various levels of fusion should be evaluated to enhance matching accuracy [29], [35]. Furthermore, obtaining thorough information from binary FV patterns results in better performance than recent methods of predicting high and low FV patterns; it also reduces EER accordingly [42]. The present study identified various FV network feature extraction techniques [48]. However, research on corresponding verification algorithms remains insufficient. In addition, score-level fusion strategies other than maximum fusion should be investigated [49].

The use of other biometrics for the fusion of FVs as another multi-modal trait verification system has been proposed [52]. Reduction of the required computing time through exchange pixel-based chain code extraction with a convolution-based approach, reduction of selected reference points for dark lines in patterns during enrolment and reduction of the size of the feature vector are important. Study [41] discussed and addressed the dislocation problem. Studies should be conducted to determine whether OPM can evolve to improve its performance after extensive system run and to explore the capability of using neural network methodologies with other types of biometrics [59], [62]. Study [71] focused on the use of a greyscale intermediate filter. ROI detection and thinning consume most of the processing time of system hardware components.

2) RECOMMENDATIONS FOR 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, including FV biometric authentication. These recommendations can be applied when a high level of security is required, such as in military zone entry, confidential zones and ATMs [47]. Thus, researchers should focus on enhancing user identity and data security to reduce data system threats from any intruder and defence against cybercrimes.

3) RECOMMENDATIONS FOR DEVELOPERS AND DESIGNERS

This category is related to developers and designers who aim to develop biometric authentication systems.

Every proposed method should analyse security sufficiently [7]. Moreover, various fusion techniques can be applied to achieve improved model performance, and the number of shares can be expanded for enhanced verification levels [30]. Therefore, researchers should conduct security analyses under practical use cases. Developers and designers should focus on reducing the time cost through the proposed methods [38], learn to improve functions and examine whether FVs will change or not during the lifetime of an individual to enhance FV authentication system performance [39]. This topic should be given sufficient attention in future studies. Developers and designers should focus on developing the visual attributes of FVs together with DBC to improve performance further [41]. The accuracy of minutiae extraction algorithms and the use of several weighted fusion methods for feature combination should be improved [60]. In addition, SVDMM should be applied to other minutiae-based biometric verification schemes, such as fingerprint and palm vein identification. The system should be implemented on an FPGA platform using a highly powerful embedded processor, such as ARM, to achieve high-speed performance [56].

D. FUTURE DIRECTIONS

After reviewing the literature used for this study, we identified several directions for future studies suggested by previous authors. These new directions are classified in Figure 13. This section illustrates these suggested research directions, which will help researchers and developers work accordingly.

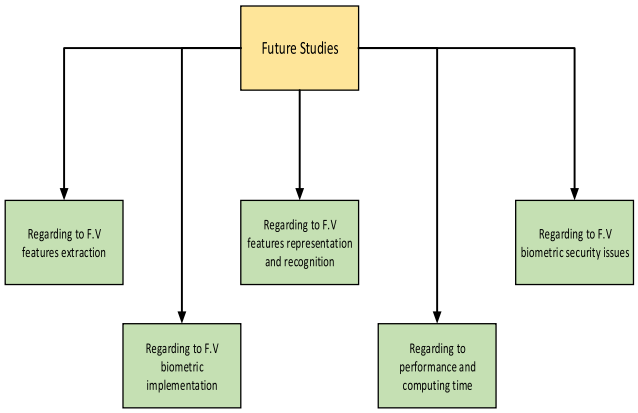

FIGURE 13. Future directions.

1) FV FEATURE EXTRACTION

Study [29] used different levels of fusion and enhanced the accuracy of feature extraction. This study stated that the databases of biometric patterns should be effectively managed to improve verification system performance. Study [66] suggested the use of new features of extraction methods and the creation of powerful HHsMs in the future to improve verification systems. The anatomical study proved the diameter of the FV difference from the fingertip to the finger root and from the sub-branch to the core branch. Therefore, this work focused on enhancing the matching and discrimination of FVs by dividing the width of the core vein branch and the sub-vein branch separately during the matching step [67]. Study [78] focused on FAR because of the misalignment between FV images during enrolment and rotation of the finger, which makes feature extraction challenging. To address this problem, a method for severe finger rotation and illumination variation should be used in future work. Furthermore, the capability to enhance computation through the combination of multi-modal recognition, which was proposed in this study, with scattering blur-restoration methods must be examined to illuminate noise in FV images.

2) FV FEATURE REPRESENTATION AND RECOGNITION

Studies [25] and [69] aimed to enhance FV images for people who lack vein intersection points to reduce false rejection results. Study [49] investigated the feasibility of applying score-level fusion strategies and compared the fusion of FV with that of multi-sample recognition systems. Determining the relationship between FV and finger dorsal with regard to recognition could be a future direction for the authors in Study [77].

3) FV BIOMETRIC SECURITY ISSUES

The authors in Study [7] suggested enhancing their proposed scheme to enable systems to restore raw biometric patterns and perform security analyses during actual use. The authors also suggested enhancing security analysis by accurately modelling FV biometric features in large finger multi-modal databases and re-estimating the suggested cryptosystems [27]. The future work for Study [28] could involve the means of using FV biometrics in various applications as a bio-key to enhance the security and efficiency of key management, especially in cloud computing. The future work for Study [31] could involve creating a large representative database with a small variation between real and forged patterns and conducting research using the proposed database to determine the requirements of applications. Furthermore, research in this area requires protecting matching algorithms [55].

4) FV BIOMETRIC IMPLEMENTATION

The WCCD features extracted from FV images are useful in identifying the operation to be used in selecting the optimal subset. Study [1] focused on determining the capability of using genetic programming and triangular norms in multi-modal based on FV biometrics. FV technology has important properties, such as security and reliability, compared with other biometric types. These properties provide an opportunity to implement this technology in various applications involving authentication and verification [40].

5) PERFORMANCE AND COMPUTING TIME

Enhancing model performance can be useful for different fusion techniques and can increase the number of shares that support the accuracy of the identification results [30]. Considering the development of the visibility features of FV, this task

can be performed by combining these features with DBC and enhancing the performance of the verification system [41]. Study [52] focused on reducing processing time, which is achievable by replacing pixel-based chain code extraction with a convolution-based approach and selecting minimal points for vein line registration and comparison. Study [71] focused on using a greyscale median filter, detecting FV image ROI and reducing the computing time by using a thinning process accelerated in the hardware.

VI. NEW PROPOSED SOLUTION

Security service is necessary to prevent false data injection and several types of attacks in different domains [13], [79]–[100]. With the exception of the collected papers reviewed in this study, a new proposed solution is described in this section. According to what was presented in Subsection 4.2.1, 11 out of the 61 technical problems focused on security. This problem is considered a serious challenge in this type of technology, where the leakage of biometrics leads to serious risks by using the stolen FV templates in various attacks, such as spoofing and brute-force attacks. This problem affects the reliability of the verification framework and stakeholders' rights. To solve this problem, most previous studies used the cryptography technique, which pertains to securing biometric information against different threats. In general, encryption is insufficient for protecting against the vulnerabilities and threats arising from the weak design of systems and protocols [101]–[107]. Moreover, encrypted data are prone to intruders, who can decrypt secret information. Suppose that an attacker successfully gains access to a system from a vulnerable point. When the attacker finds unknown data (unreadable data), he becomes sure that sensitive information exists behind these unknown data because cryptography merely hides the content and meaning of data. The attacker can transfer these unknown data to another system or location and attempt to break the decryption of cipher text by using modern programmes and techniques [108]–[112]. Thus, the confidentiality of such information must be enhanced by using data hiding techniques, such as steganography or watermarking [17], [113]–[147]. The requirements needed to solve this problem according to the definition of information security by the international standard ISO/IEC 27002 (2005) should also be improved. This definition states that CIA of public information must be maintained to secure the information and concepts of the CIA triangle (confidentiality, integrity and availability). Moreover, the randomisation of FV features during the creation of user FV patterns needs to be increased. By achieving these requirements, FV information can be protected during the enrolment stage.

To perform such a study, two steps should be followed to develop a secure verification framework between the access point (enrolment device) and node databases in a decentralised network architecture without a central point. Firstly, a new hybrid biometric pattern model based on a merge algorithm could be proposed to combine radio frequency identification (RFID) and FV biometric features to increase the randomisation and security levels in pattern structures. Secondly, we could develop a combination of encryption, blockchain and steganography techniques for a hybrid pattern model. When a pattern is sent from an enrolment device (access point) to the node databases, this process ensures that the FV biometric verification system remains secure during authentication by meeting the information security standard requirements of confidentiality, integrity and availability.

Steganography and encryption techniques are used for confidentiality in transmission channels [148]–[155]. Blockchain technology is utilised to achieve data integrity and high availability [156]–[158]. The decentralised network architecture makes user information available to authorised persons in the case of network failure or disaster cases with high levels of security. Blockchain technology is proposed to eliminate the third party in terms of authentication. In other words, this architecture aims to eliminate node failure and reduce the communication and verification operations in FV biometric verification frameworks when users need to acquire services or simultaneously gain access to multiple nodes. This goal can be achieved by addressing the following functionalities: (1) user enrolment by FV patterns, (2) user membership validation, (3) validity verification of user FV biometrics and (4) user FV biometric cancellation from the network if needed.

During user authentication, the user sends his or her FV biometric pattern from the access point to the node (destination) by using blockchain technology because this technology was developed with full properties (such as hash, ledger and block of data). The user request is simultaneously sent to all nodes in the network. If more than 50% of the nodes verify this request, then the user gains access to the service. Each node has a ledger with which to verify the blockchain. If network failure is detected in the target node, then the request will be shifted to another node and will follow the same procedure. This design is beneficial for eliminating the central point. With regard to security analysis for this scenario, this design has the same resistance against spoofing and brute-force attacks. An attacker needs to hack 51% of all nodes in the network to gain access, as shown in Figure 14. The process between the access point and node databases is as follows:

Access point side

- FV images are pre-processed.
- FV features are extracted and converted into a binary string.
- RFID binary features extract and convert data into a binary string.
- Two binary strings (FV and RFID) are merged into one string with a random distribution by using the proposed merge algorithm.
- A hashing function is implemented on a copy of the hybrid pattern. Hashing is sent to the node side to achieve information integrity. This hash is transformed in the node side through the blockchain technique.

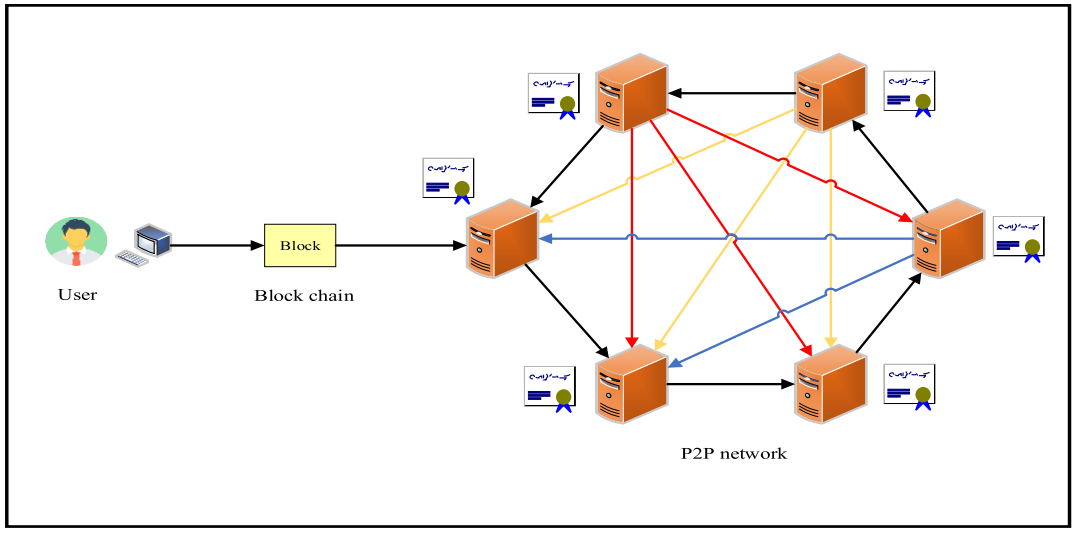

FIGURE 14. FV biometric verification framework in a decentralised network architecture.

- Another copy of the hybrid pattern is encrypted and sent to the node databases as a blockchain. This pattern is used during matching and decision-making to check if the user is authorised (authentication process).

Node side

- An encrypted copy of the hybrid pattern is already stored in the node databases prior to the receipt of the enrolment device request. The pattern is concealed using the steganography method.
- Upon receipt of the enrolment device request (encrypted pattern and hashing), the hashing in the blockchain is verified by matching the hashing with the ledger. This ledger is used to store the user's hashing individually in the node database side. The matching hashing operation is conducted for all users, except the first user (genesis user), thereby ensuring that the information is from a trusted source and the information has not been modified by unauthorised persons.
- When the matching of the hashing result is true (the next step proceeds), the hybrid pattern is decrypted, and the other processing steps proceed. Otherwise, an attack occurs in the system (user information is altered or this information is sent from an unauthorised location).
- A split operation is performed to split the FV features from the RFID features by using the proposed merge algorithm in reverse.

The process in the node database background is as follows:

- The hybrid pattern from the cover (stego-image), which exists in the node databases through steganalysis, is extracted. The encrypted hybrid pattern information is decrypted into plain text (binary).
- A split operation is performed to split the FV features from the RFID features by using the proposed merge algorithm in reverse.
- Two matching operations are performed between the FV feature from the enrolment device side and the FV feature extracted from the node databases; the same operation is performed for the RFID features.
- The user is identified and verified as authorised or unauthorised.

VII. STUDY LIMITATIONS

A limitation of this study is 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. The increasing progress in this field affects the timeliness of this study. Furthermore, the overview of research on 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 emphasise several problems that face FV biometric technology and need to be addressed by the research community.

VIII. CONCLUSION

Verification medical systems based on human biometrics are widely used in various medical applications that require reliable verification/identification schemes. Different platforms that utilise FV authentication systems with high levels of security and low verification error rates have attracted increasing attention. The present study contributes to extant research by producing a taxonomy of published literature. It differentiates the types of research conducted according to FV biometric systems in terms of development and classifies these studies into two categories (development of software- and hardware-based components). Researchers can use this taxonomy to determine gaps in FV biometric authentication system literature. We comprehensively analysed related articles by highlighting the number of publications, problem types, proposed solutions, best results, evaluation methods, available datasets, motivations, challenges and recommendations for future studies. Several recommendations for handling and controlling FV biometric authentication medical systems are also provided. These instructions must be

followed by developers and designers to help them create robust and highly accurate FV biometric authentication systems that meet the demands of companies and organisations in terms of information security. Furthermore, a newly proposed solution is explained. This solution can be implemented in the future to address the leakage of biometric information, which leads to serious risks when stolen FV templates are used. The proposed solution will be simulated and implemented in the future to serve as a guide for researchers who intend to verify secure framework-based decentralised network architectures in medical systems, including access points and various database nodes without a central point.

REFERENCES

[1] M. S. M. Asaari, S. A. Suandi, and B. A. Rosdi, "Fusion of band limited phase only correlation and width centroid contour distance for finger based biometrics," *Expert Syst. Appl.*, vol. 41, no. 7, pp. 3367–3382, Jun. 2014.

[2] J.-D. Wu and C.-T. Liu, "Finger-vein pattern identification using principal component analysis and the neural network technique," *Expert Syst. Appl.*, vol. 38, no. 5, pp. 5423–5427, May 2011.

[3] L. Dong, G. Yang, Y. Yin, F. Liu, and X. Xi, "Finger vein verification based on a personalized best patches map," in *Proc. IEEE Int. Joint Conf. Biometrics*, Sep./Oct. 2014.

[4] J.-D. Wu and S.-H. Ye, "Driver identification using finger-vein patterns with Radon transform and neural network," *Expert Syst. Appl.*, vol. 36, no. 3, pp. 5793–5799, Apr. 2009.

[5] M. Fayyaz, M. Hajizadeh-Saffar, M. Sabokrou, M. Hoseini, and M. Fathy, "A novel approach for Finger Vein verification based on self-taught learning," in *Proc. 9th Iranian Conf. Mach. Vis. Image Process. (MVIP)*, Nov. 2015, pp. 88–91.

[6] M. Jadhav and P. M. Nerkar, "Implementation of an embedded hardware of FVRS on FPGA," in *Proc. Int. Conf. Inf. Process. (ICIP)*, Dec. 2015, pp. 48–53.

[7] H. Suzuki, M. Suzuki, T. Urabe, T. Obi, M. Yamaguchi, and N. Ohyama, "Secure biometric image sensor and authentication scheme based on compressed sensing," *Appl. Opt.*, vol. 52, no. 33, p. 8161, Nov. 2013.

[8] K. Shaheed, H. Liu, G. Yang, I. Qureshi, J. Gou, and Y. Yin, "A systematic review of finger vein recognition techniques," *Information*, vol. 9, no. 9, p. 213, Aug. 2018.

[9] K. Syazana-Itqan, A. R. Syafeeza, N. M. Saad, N. A. Hamid, and W. H. B. M. Saad, "A review of finger-vein biometrics identification approaches," *Indian J. Sci. Technol.*, vol. 9, no. 32, pp. 1–9, 2016.

[10] E. Ting and M. Z. Ibrahim, "A review of finger vein recognition system," *J. Telecommun., Electron. Comput. Eng.*, vol. 10, nos. 1–9, pp. 167–171, 2018.

[11] A. A. Zaidan, B. B. Zaidan, O. S. Albahri, M. A. Alsalem, A. S. Albahri, Q. M. Yas, and M. Hashim, "A review on smartphone skin cancer diagnosis apps in evaluation and benchmarking: Coherent taxonomy, open issues and recommendation pathway solution," *Health Technol.*, vol. 8, no. 4, pp. 223–238, Sep. 2018.

[12] O. S. Albahri, A. A. Zaidan, B. B. Zaidan, M. Hashim, A. S. Albahri, and M. A. Alsalem, "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.*, vol. 42, no. 9, p. 164, 2018.

[13] A. S. Albahri, A. A. Zaidan, O. S. Albahri, B. B. Zaidan, and M. A. Alsalem, "Real-time fault-tolerant mHealth system: Comprehensive review of healthcare services, opens issues, challenges and methodological aspects," *J. Med. Syst.*, vol. 42, Jun. 2018, Art. no. 137.

[14] M. A. Alsalem, A. A. Zaidan, B. B. Zaidan, M. Hashim, O. S. Albahri, A. S. Albahri, A. Hadi, and K. I. Mohammed, "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.*, vol. 42, no. 11, 2018, Art. no. 204.

[15] A. A. Zaidan, B. B. Zaidan, M. Y. Qahtan, O. S. Albahri, A. S. Albahri, M. Alaa, F. M. Jumaah, M. Talal, K. L. Tan, W. L. Shir, and C. K. Lim, "A survey on communication components for IoT-based technologies in smart homes," *Telecommun. Syst.*, vol. 69, no. 1, pp. 1–25, Sep. 2018.

[16] A. H. Mohsin, "Real-time remote health monitoring systems using body sensor information and finger vein biometric verification: A multi-layer systematic review," *J. Med. Syst.*, vol. 42, no. 12, p. 238, 2018.

[17] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, S. A. bin Ariffin, O. S. Albahri, A. S. Albahri, M. A. Alsalem, K. I. Mohammed, and M. Hashim, "Real-time medical systems based on human biometric steganography: A systematic review," *J. Med. Syst.*, vol. 42, no. 12, p. 245, 2018.

[18] M. Talal, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, M. A. Alsalem, A. S. Albahri, A. H. Alamoodi, M. L. M. Kiah, F. M. Jumaah, and M. Alaa, "Comprehensive review and analysis of anti-malware apps for smartphones," *Telecommun. Syst.*, vol. 72, no. 2, pp. 285–337, Oct. 2019.

[19] M. Khatari, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, and M. A. Alsalem, "Multi-criteria evaluation and benchmarking for active queue management methods: Open issues, challenges and recommended pathway solutions," *Int. J. Inf. Tech. Decis. Making*, vol. 18, no. 4, pp. 1187–1242, Jul. 2019.

[20] A. Mohsin, A. Zaidan, B. Zaidan, O. Albahri, A. Albahri, M. Alsalem, and K. Mohammed, "Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication," *Comput. Standards Interfaces*, vol. 66, Oct. 2019, Art. no. 103343.

[21] E. M. Almahdi, A. A. Zaidan, B. B. Zaidan, M. A. Alsalem, O. S. Albahri, and A. S. Albahri, "Mobile patient monitoring systems from a benchmarking aspect: Challenges, open issues and recommended solutions," *J. Med. Syst.*, vol. 43, no. 7, p. 207, 2019.

[22] O. Zughoul, F. Momani, O. H. Almasri, A. A. Zaidan, B. B. Zaidan, M. A. Alsalem, O. S. Albahri, A. S. Albahri, and M. Hashim, "Comprehensive insights into the criteria of student performance in various educational domains," *IEEE Access*, vol. 6, pp. 73245–73264, 2018.

[23] K. Mohammed, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, M. A. Alsalem, A. S. Albahri, A. Hadi, and M. Hashim, "Real-time remote-health monitoring systems: A review on patients prioritisation for multiple-chronic diseases, taxonomy analysis, concerns and solution procedure," *J. Med. Syst.*, vol. 43, no. 7, p. 223, 2019.

[24] N. M. Napi, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, M. A. Alsalem, and A. S. Albahri, "Medical emergency triage and patient prioritisation in a telemedicine environment: A systematic review," *Health Technol.*, vol. 9, no. 5, pp. 679–700, Nov. 2019.

[25] J. Chavez-Galaviz, J. Ruiz-Rojas, A. Garcia-Gonzalez, and R. Fuentes-Aguilar, "Embedded biometric cryptosystem based on finger vein patterns," in *Proc. 12th Int. Conf. Elect. Eng., Comput. Sci. Autom. Control (CCE)*, Oct. 2015, pp. 1–6.

[26] T. Murakami, T. Ohki, and K. Takahashi, "Optimal sequential fusion for multibiometric cryptosystems," *Inf. Fusion*, vol. 32, pp. 93–108, Nov. 2016.

[27] J. Peng, Q. Li, A. A. A. El-Latif, and X. Niu, "Finger multibiometric cryptosystems: Fusion strategy and template security," *J. Electron. Imag.*, vol. 23, no. 2, Mar. 2014, Art. no. 023001.

[28] Z. Wu, L. Tian, P. Li, T. Wu, M. Jiang, and C. Wu, "Generating stable biometric keys for flexible cloud computing authentication using finger vein," *Inf. Sci.*, vols. 433–434, pp. 431–447, Apr. 2018.

[29] D. Jagadiswary and D. Saraswady, "Biometric authentication using fused multimodal biometric," *Procedia Comput. Sci.*, vol. 85, pp. 109–116, Jan. 2016.

[30] A. Nandhinipreetha and N. Radha, "Multimodal biometric template authentication of finger vein and signature using visual cryptography," in *Proc. Int. Conf. Comput. Commun. Inform. (ICCCI)*, Jan. 2016, pp. 7–10.

[31] Y. Liu, J. Ling, Z. Liu, J. Shen, and C. Gao, "Finger vein secure biometric template generation based on deep learning," *Soft Comput.*, vol. 22, no. 7, pp. 2257–2265, Apr. 2018.

[32] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognit.*, vol. 78, pp. 242–251, Jun. 2018.

[33] X. Qiu, W. Kang, S. Tian, W. Jia, and Z. Huang, "Finger vein presentation attack detection using total variation decomposition," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 465–477, Feb. 2018.

[34] H. Qin, X. He, X. Yao, and H. Li, "Finger-vein verification based on the curvature in Radon space," *Expert Syst. Appl.*, vol. 82, pp. 151–161, Oct. 2017.

[35] H. Qin and M. A. El-Yacoubi, "Deep representation-based feature extraction and recovering for finger-vein verification," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1816–1829, Aug. 2017.

[36] F. Zhang, S. Guo, and X. Qian, "Segmentation for finger vein image based on PDEs denoising," in *Proc. 3rd Int. Conf. Biomed. Eng. Inform.*, vol. 2, Oct. 2010, pp. 531–535.
[37] P. Gupta and P. Gupta, "An accurate finger vein based verification system," *Digit. Signal Process.*, vol. 38, pp. 43–52, Mar. 2015.
[38] T. Liu, J. Xie, W. Yan, P. Li, and H. Lu, "Finger-vein pattern restoration with direction-variance-boundary constraint search," *Eng. Appl. Artif. Intell.*, vol. 46, pp. 131–139, Nov. 2015.
[39] Z. Liu, Y. Yin, H. Wang, S. Song, and Q. Li, "Finger vein recognition with manifold learning," *J. Netw. Comput. Appl.*, vol. 33, no. 3, pp. 275–282, May 2010.
[40] J.-D. Wu and C.-T. Liu, "Finger-vein pattern identification using SVM and neural network technique," *Expert Syst. Appl.*, vol. 38, no. 11, pp. 14284–14289, 2011.
[41] X. Xi, L. Yang, and Y. Yin, "Learning discriminative binary codes for finger vein recognition," *Pattern Recognit.*, vol. 66, pp. 26–33, Jun. 2017.
[42] H. Qin and M. A. El-Yacoubi, "Finger-vein quality assessment by representation learning from binary images," in *Proc. Int. Conf. Neural Inf. Process.*, vol. 9489, 2015, pp. 421–431.
[43] K. Parthiban, A. Wahi, S. Sundaramurthy, and C. Palanisamy, "Finger vein extraction and authentication based on gradient feature selection algorithm," in *Proc. 5th Int. Conf. Appl. Digit. Inf. Web Technol. (ICADIWT)*, Feb. 2014, pp. 143–147.
[44] J. Peng, N. Wang, A. A. A. El-Latif, Q. Li, and X. Niu, "Finger-vein verification using Gabor filter and SIFT feature matching," in *Proc. 8th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Jul. 2012, pp. 45–48.
[45] A. Hajian and D. A. Ramli, "Sharpness enhancement of finger-vein image based on modified un-sharp mask with log-Gabor filter," *Procedia Comput. Sci.*, vol. 126, pp. 431–440, Jan. 2018.
[46] B. A. Rosdi, C. W. Shing, and S. A. Suandi, "Finger vein recognition using local line binary pattern," *Sensors*, vol. 11, no. 12, pp. 11357–11371, Dec. 2011.
[47] N. Sugandhi, M. Mathankumar, and V. Priya, "Real time authentication system using advanced finger vein recognition technique," in *Proc. Int. Conf. Commun. Signal Process.*, Melmaruvathur, India, Apr. 2014, pp. 1183–1187.
[48] L. Zhichao, S. Dongmei, L. Di, and L. Hao, "Two modality-based bi-finger vein verification system," in *Proc. IEEE 10th Int. Conf. Signal Process.*, Oct. 2010, pp. 1690–1693.
[49] F. Saadat and M. Nasri, "A multibiometric finger vein verification system based on score level fusion strategy," in *Proc. Int. Congr. Technol., Commun. Knowl. (ICTCK)*. Mashhad, Iran: Islamic Azad Univ. Mashhad, Nov. 2015, pp. 11–12.
[50] A. William, T. S. Ong, S. H. Lau, and M. K. O. Goh, "Finger Vein verification using local histogram of hybrid texture descriptors," in *Proc. IEEE Int. Conf. Signal Image Process. Appl. (ICSIPA)*, Oct. 2015, pp. 304–308.
[51] Y. Lu, S. Wu, Z. Fang, N. Xiong, S. Yoon, and D. S. Park, "Exploring finger vein based personal authentication for secure IoT," *Future Gener. Comput. Syst.*, vol. 77, pp. 149–160, Dec. 2017.
[52] A. Pflug, D. Hartung, and C. Busch, "Feature extraction from vein images using spatial information and chain codes," *Inf. Secur.*, vol. 17, nos. 1–2, pp. 26–35, Feb. 2012.
[53] J. Yang, Y. Shi, and J. Yang, "Personal identification based on finger-vein features," *Comput. Hum. Behav.*, vol. 27, no. 5, pp. 1565–1570, Sep. 2011.
[54] L. Dong, G. Yang, Y. Yin, X. Xi, L. Yang, and F. Liu, "Finger vein verification with vein textons," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 29, no. 4, Jun. 2015, Art. no. 1556003.
[55] W. Song, T. Kim, H. C. Kim, J. H. Choi, H.-J. Kong, and S.-R. Lee, "A finger-vein verification system using mean curvature," *Pattern Recognit. Lett.*, vol. 32, no. 11, pp. 1541–1547, Aug. 2011.
[56] J.-D. Wu, C.-T. Liu, Y.-J. Tsai, J.-C. Liu, and Y.-W. Chang, "Development of neural network techniques for finger-vein pattern classification," in *Proc. 2nd Int. Conf. Digit. Image Process.*, vol. 7546, Feb. 2010, Art. no. 75460F.
[57] H. Huang, S. Liu, H. Zheng, L. Ni, Y. Zhang, and W. Li, "DeepVein: Novel finger vein verification methods based on deep convolutional neural networks," in *Proc. IEEE Int. Conf. Identity, Secur. Behav. Anal. (ISBA)*, no. 5, Feb. 2017.
[58] T. S. Ong, J. H. Teng, K. S. Muthu, and A. B. J. Teoh, "Multi-instance finger vein recognition using minutiae matching," in *Proc. 6th Int. Congr. Image Signal Process. (CISP)*, vol. 3, Dec. 2013, pp. 1730–1735.
[59] D. Tang, B. Huang, R. Li, W. Li, and X. Li, "Finger vein verification using occurrence probability matrix (OPM)," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jun. 2012, pp. 21–26.
[60] F. Liu, G. Yang, Y. Yin, and S. Wang, "Singular value decomposition based minutiae matching method for finger vein recognition," *Neurocomputing*, vol. 145, pp. 75–89, Dec. 2014.
[61] J. Wang, J. Xiao, W. Lin, and C. Luo, "Discriminative and generative vocabulary tree: With application to vein image authentication and recognition," *Image Vis. Comput.*, vol. 34, pp. 51–62, Feb. 2015.
[62] A. N. Hoshyar and R. Sulaiman, "Vein matching using artificial neural network in vein authentication systems," in *Proc. Int. Conf. Graphic Image Process. (ICGIP)*, vol. 8285, Oct. 2011, Art. no. 82850Z.
[63] J. Peng, A. A. A. El-Latif, Q. Li, and X. Niu, "Multimodal biometric authentication based on score level fusion of finger biometrics," *Optik*, vol. 125, no. 23, pp. 6891–6897, Dec. 2014.
[64] M. I. Razzak, R. Yusof, and M. Khalid, "Multimodal face and finger veins biometric authentication," *Sci. Res. Essays*, vol. 5, no. 17, pp. 2529–2534, 2010.
[65] J. Yang, Y. Shi, and G. Jia, "Finger-vein image matching based on adaptive curve transformation," *Pattern Recognit.*, vol. 66, pp. 34–43, Jun. 2017.
[66] J. Yang, J. Wei, and Y. Shi, "Accurate ROI localization and hierarchical hyper-sphere model for finger-vein recognition," *Neurocomputing*, vol. 328, pp. 171–181, Feb. 2019.
[67] L. Yang, G. Yang, Y. Yin, and X. Xi, "Finger vein recognition with anatomy structure analysis," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 8, pp. 1892–1905, Aug. 2018.
[68] R. B. Josephp and D. Ezhilmaran, "A smart computing algorithm for finger vein matching with affine invariant features using fuzzy image retrieval," *Procedia Comput. Sci.*, vol. 125, pp. 172–178, Jan. 2018.
[69] Y.-C. Cheng, H. Chen, and B.-C. Cheng, "Special point representations for reducing data space requirements of finger-vein recognition applications," *Multimedia Tools Appl.*, vol. 76, no. 9, pp. 11251–11271, May 2017.
[70] D. Tang, B. Huang, R. Li, and W. Li, "A person retrieval solution using finger vein patterns," in *Proc. 20th Int. Conf. Pattern Recognit.*, Aug. 2010, pp. 1306–1309.
[71] M. Khalil-Hani and P. C. Eng, "FPGA-based embedded system implementation of finger vein biometrics," in *Proc. IEEE Symp. Ind. Electron. Appl. (ISIEA)*, Penang, Malaysia, Oct. 2010, pp. 700–705.
[72] M. Khalil-Hani and P. C. Eng, "Personal verification using finger vein biometrics in FPGA-based system-on-chip," in *Proc. 7th Int. Conf. Elect. Electron. Eng.*, 2011, pp. II-171–II-176.
[73] M. Khalil-Hani and Y. H. Lee, "FPGA embedded hardware system for finger vein biometric recognition," in *Proc. 39th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Nov. 2013, pp. 2273–2278.
[74] R. Raghavendra, K. B. Raja, J. Surbiryala, and C. Busch, "A low-cost multimodal biometric sensor to capture finger vein and fingerprint," in *Proc. IEEE Int. Joint Conf. Biometrics*, Sep. 2014.
[75] R. Raghavendra, J. Surbiryala, K. B. Raja, and C. Busch, "Novel finger vascular pattern imaging device for robust biometric verification," in *Proc. IEEE Int. Conf. Imag. Syst. Techn. (IST)*, Oct. 2014, pp. 148–152.
[76] Y. Xin, Z. Liu, H. Zhang, and H. Zhang, "Finger vein verification system based on sparse representation," *Appl. Opt.*, vol. 51, no. 25, p. 6252, Sep. 2012.
[77] W. Yang, X. Huang, F. Zhou, and Q. Liao, "Comparative competitive coding for personal identification by using finger vein and finger dorsal texture fusion," *Inf. Sci.*, vol. 268, pp. 20–32, Jun. 2014.
[78] W. Kim, J. M. Song, and K. R. Park, "Multimodal biometric recognition based on convolutional neural network by the fusion of finger-vein and finger shape using near-infrared (NIR) camera sensor," *Sensors*, vol. 18, no. 7, p. 2296, Jul. 2018.
[79] Y. Y. A. Talib, B. B. Zaidan, A. A. Zaidan, and A. W. Naji, "Optimizing security and flexibility by designing a high security system for E-government servers," in *Proc. ICOCI*. Changlun, Malaysia: Univ. Utara Malaysia, 2009.
[80] M. Hussain, A. Zaidan, B. Zidan, S. Iqbal, M. Ahmed, O. Albahri, and A. Albahri, "Conceptual framework for the security of mobile health applications on Android platform," *Telematics Informat.*, vol. 35, no. 5, pp. 1335–1354, Aug. 2018.
[81] H. O. Alanazi, R. M. Noor, B. B. Zaidan, and A. A. Zaidan, "Intrusion detection system: Overview," *J. Comput.*, vol. 2, no. 3, pp. 130–133, 2010.

[82] H. O. Alanazi, H. A. Jalab, M. A. Gazi, B. B. Zaidan, and A. A. Zaidan, "Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance," *J. Med. Plants Res.*, vol. 4, no. 19, pp. 2059–2074, Jul. 2016.

[83] B. B. Zaidan, A. Haiqi, A. A. Zaidan, M. Abdulnabi, M. L. M. Kiah, and H. Muzamel, "A security framework for nationwide health information exchange based on telehealth strategy," *J. Med. Syst.*, vol. 39, no. 5, p. 51, 2015.

[84] M. L. M. Kiah, S. H. Al-Bakri, A. A. Zaidan, B. B. Zaidan, and M. Hussain, "Design and develop a video conferencing framework for real-time telemedicine applications using secure group-based communication architecture," *J. Med. Syst.*, vol. 38, no. 10, p. 133, Oct. 2014.

[85] O. S. Albahri, A. S. Albahri, K. I. Mohammed, A. A. Zaidan, B. B. Zaidan, M. Hashim, and O. H. Salman, "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.*, vol. 42, no. 5, p. 80, 2018.

[86] M. S. Nabi, M. L. M. Kiah, A. A. Zaidan, and B. B. Zaidan, "Suitability of adopting S/MIME and OpenPGP email messages protocol to secure electronic medical records," in *Proc. 2nd Int. Conf. Future Gener. Commun. Technol. (FGCT)*, Nov. 2013, pp. 93–97.

[87] S. Iqbal, M. L. M. Kiah, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, and M. A. Alsalem, "Real-time-based E-health systems: Design and implementation of a lightweight key management protocol for securing sensitive information of patients," *Health Technol.*, vol. 9, no. 2, pp. 93–111, Mar. 2019.

[88] O. Enaizan, A. A. Zaidan, N. M. Alwi, B. B. Zaidan, M. A. Alsalem, O. S. Albahri, and A. S. Albahri, "Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis," *Health Technol.*, vol. 7, pp. 1–28, Nov. 2018.

[89] H. O. Alanazi, A. A. Zaidan, B. B. Zaidan, M. L. M. Kiah, and S. H. Al-Bakri, "Meeting the security requirements of electronic medical records in the ERA of high-speed computing," *J. Med. Syst.*, vol. 39, no. 1, p. 165, 2015.

[90] N. Raad, G. Alam, B. Zaidan, and A. Zaidan, "Impact of spam advertisement through E-mail: A study to assess the influence of the anti-spam on the E-mail marketing," *Afr. J. Bus. Manage.*, vol. 4, no. 11, pp. 2362–2367, Sep. 2010.

[91] B. Zaidan, A. Zaidan, and M. M. Kiah, "Impact of data privacy and confidentiality on developing telemedicine applications: A review participates opinion and expert concerns," *Int. J. Pharmacol.*, vol. 7, no. 3, pp. 382–387, Mar. 2011.

[92] M. L. Shuwandy, B. B. Zaidan, A. A. Zaidan, and A. S. Albahri, "Sensor-based mHealth authentication for real-time remote healthcare monitoring system: A multilayer systematic review," *J. Med. Syst.*, vol. 43, no. 2, p. 33, 2019.

[93] M. Talal, A. A. Zaidan, B. B. Zaidan, A. S. Albahri, A. H. Alamoodi, O. S. Albahri, M. A. Alsalem, C. K. Lim, K. L. Tan, W. L. Shir, and K. I. Mohammed, "Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review," *J. Med. Syst.*, vol. 43, no. 3, p. 42, Mar. 2019.

[94] A. Medani, A. Gani, O. Zakaria, A. A. Zaidan, and B. B. Zaidan, "Review of mobile short message service security issues and techniques towards the solution," *Sci. Res. Essays*, vol. 6, no. 6, pp. 1147–1165, 2011.

[95] A. W. Naji, A. S. Housain, B. B. Zaidan, A. A. Zaidan, and S. A. Hameed, "Security improvement of credit card online purchasing system," *Sci. Res. Essays*, vol. 6, no. 16, pp. 3357–3370, Jun. 2016.

[96] M. Hussain, A. Al-Haiqi, A. Zaidan, B. Zaidan, M. M. Kiah, N. B. Anuar, and M. Abdulnabi, "The rise of keyloggers on smartphones: A survey and insight into motion-based tap inference attacks," *Pervasive Mobile Comput.*, vol. 25, pp. 1–25, Jan. 2016.

[97] H. O. Alanizi, M. M. Kiah, A. Zaidan, B. Zaidan, and G. M. Alam, "Secure topology for electronic medical record transmissions," *Int. J. Pharmacol.*, vol. 6, no. 6, pp. 954–958, Jun. 2010.

[98] M. Hussain, A. Al-Haiqi, A. Zaidan, B. Zaidan, M. Kiah, S. Iqbal, S. Iqbal, and M. Abdulnabi, "A security framework for mHealth apps on Android platform," *Comput. Secur.*, vol. 75, pp. 191–217, Jun. 2018.

[99] M. A. Watari, A. A. Zaidan, and B. B. Zaidan, "Securing m-government transmission based on symmetric and asymmetric algorithms: A review," *Asian J. Sci. Res.*, vol. 8, pp. 80–94, Oct. 2013.

[100] M. S. A. Nabi, M. M. Kiah, B. Zaidan, A. Zaidan, and G. M. Alam, "Suitability of using SOAP protocol to secure electronic medical record databases transmission," *Int. J. Pharmacol.*, vol. 6, no. 6, pp. 959–964, Jun. 2010.

[101] M. Abomhara, O. Zakaria, O. O. Khalifa, A. Zaidan, and B. Zaidan, "Enhancing selective encryption for H. 264/AVC using advanced encryption standard," *Int. J. Comput. Elect. Eng.*, vol. 2, no. 2, p. 223, 2010.

[102] H. O. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, M. Shabbir, and Y. Al-Nabhani, "New comparative study between DES, 3DES and AES within nine factors," *J. Comput.*, vol. 2, no. 3, pp. 1–6, 2010.

[103] Y. Salem, M. Abomhara, O. O. Khalifa, A. Zaidan, and B. Zaidan, "A review on multimedia communications cryptography," *Res. J. Inf. Technol.*, vol. 3, no. 3, pp. 146–152, Mar. 2011.

[104] M. Abomhara, O. O. Khalifa, O. Zakaria, A. Zaidan, B. Zaidan, and H. O. Alanazi, "Suitability of using symmetric key to secure multimedia data: An overview," *J. Appl. Sci.*, vol. 10, no. 15, pp. 1656–1661, Dec. 2010.

[105] S. H. Al-Bakri, M. L. M. Kiah, A. A. Zaidan, B. B. Zaidan, and G. M. Alam, "Securing peer-to-peer mobile communications using public key cryptography: New security strategy," *Int. J. Phys. Sci.*, vol. 6, no. 4, pp. 930–938, 2011.

[106] M. Abomhara, O. O. Khalifa, A. A. Zaidan, B. B. Zaidan, O. Zakaria, and A. Gani, "An experiment of scalable video security solution using H. 264/AVC and advanced encryption standard (AES): Selective cryptography," *Int. J. Phys. Sci.*, vol. 6, no. 16, pp. 4053–4063, 2011.

[107] M. L. M. Kiah, M. S. Nabi, B. B. Zaidan, and A. A. Zaidan, "An enhanced security solution for electronic medical records based on AES hybrid technique with SOAP/XML and SHA-1," *J. Med. Syst.*, vol. 37, no. 5, p. 9971, Oct. 2013.

[108] G. M. Alam, M. Kiah, M. L. M. Kiah, B. B. Zaidan, A. A. Zaidan, and H. O. Alanazi, "Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study," *Sci. Res. Essays*, vol. 5, no. 21, pp. 3254–3260, 2010.

[109] A. A. Zaidan, B. B. Zaidan, Y. A. Taqa, M. K. Sami, G. M. Alam, and A. H. Jalab, "Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem," *Int. J. Phys. Sci.*, vol. 5, no. 11, pp. 1776–1786, 2010.

[110] B. B. Zaidan, A. A. Zaidan, A. Taqa, G. M. Alam, M. L. M. Kiah, and A. H. Jalab, "StegoMos: A secure novel approach of high rate data hidden using mosaic image and ANN-BMP cryptosystem," *Int. J. Phys. Sci.*, vol. 5, no. 11, pp. 1796–1806, 2010.

[111] A. W. Naji, A. A. Zaidan, B. B. Zaidan, and I. A. S. Muhamadi, "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.*, vol. 56, no. 5, pp. 498–502, 2010.

[112] A. W. Naji, S. A. Hameed, W. F. Al-khateeb, O. O. Khalifa, and T. S. Gunawan, "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.*, vol. 3, no. 1, pp. 1–6, 2009.

[113] B. B. Zaidan, A. A. Zaidan, and F. Othman, "Enhancement of the amount of hidden data and the quality of image," Fac. Comput. Sci. Inf. Technol., Univ. Malaya, Kuala Lumpur, Malaysia, Tech. Rep., 2008.

[114] B. Zaidan and A. Zaidan, "Comparative study on the evaluation and benchmarking information hiding approaches based multi-measurement analysis using TOPSIS method with different normalisation, separation and context techniques," *Measurement*, vol. 117, pp. 277–294, Mar. 2018.

[115] A. A. Z, A. W. Naji, S. A. Hameed, F. Othman, and B. B. Zaidan, "Approved undetectable-antivirus steganography for multimedia information in PE-file," in *Proc. Int. Assoc. Comput. Sci. Inf. Technol. Spring Conf.*, 2009, pp. 425–429.

[116] M. A. Ahmed, M. L. M. Kiah, B. Zaidan, and A. Zaidan, "A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm," *J. Appl. Sci.*, vol. 10, no. 1, pp. 59–64, Jan. 2010.

[117] A. Al-Frajat, H. Jalab, Z. Kasirun, A. Zaidan, and B. Zaidan, "Hiding data in video file: An overview," *J. Appl. Sci.*, vol. 10, no. 15, pp. 1644–1649, Dec. 2010.

[118] A. W. Naji, A. A. Zaidan, B. B. Zaidan, and I. A. Muhamadi, "New approach of hidden data in the portable executable file without change the size of carrier file using distortion techniques," *Proc. World Acad. Sci. Eng. Technol.*, vol. 9, no. 7, pp. 493–497, Jul. 2009.

[119] M. E. Eltahir, L. M. Kiah, B. B. Zaidan, and A. A. Zaidan, "High rate video streaming steganography," in *Proc. Int. Conf. Inf. Manage. Eng.*, 2009, pp. 550–553.

[120] B. B. Zaidan, A. A. Zaidan, H. A. Karim, and N. N. Ahmad, "A new digital watermarking evaluation and benchmarking methodology using an external group of evaluators and multi-criteria analysis based on 'large-scale data,"' *Softw. Pract. Exper.*, vol. 47, no. 10, pp. 1365–1392, Oct. 2017.

[121] B. B. Zaidan and A. A. Zaidan, "Software and hardware FPGA-based digital watermarking and steganography approaches: Toward new methodology for evaluation and benchmarking using multi-criteria decision-making techniques," *J. Circuit Syst. Comput.*, vol. 26, no. 7, Jul. 2017, Art. no. 1750116.

[122] F. Othman, L. Maktom, A. Y. Taqa, B. B. Zaidan, and A. A. Zaidan, "An extensive empirical study for the impact of increasing data hidden on the images texture," in *Proc. Int. Conf. Future Comput. Commun.*, Apr. 2009, pp. 477–481.

[123] A. A. Zaidan, B. B. Zaidan, O. H. Alanazi, A. Gani, O. Zakaria, and G. M. Alam, "Novel approach for high (secure and rate) data hidden within triplex space for executable file," *Sci. Res. Essays*, vol. 5, no. 15, pp. 1965–1977, 1965.

[124] A. A. Zaidan and B. B. Zaidan, "Novel approach for high secure data hidden in MPEG video using public key infrastructure," *Int. J. Comput. Netw. Secur.*, vol. 1, no. 1, pp. 1553–1985, 2009.

[125] B. Zaidan, A. Zaidan, F. Othman, R. Z. Raji, S. Mohammed, and M. Abdulrazzaq, "Quality of image vs. quantity of data hidden in the image," in *Proc. IPCV*, vol. 6, 2009, pp. 343–350.

[126] A. W. Naji, T. S. Gunawan, S. A. Hameed, B. B. Zaidan, and A. A. Zaidan, "'Stego-analysis chain, session one' investigations on steganography weakness vs stego-analysis system for multimedia file," in *Proc. Int. Assoc. Comput. Sci. Inf. Technol. Spring Conf.*, 2009, pp. 405–409.

[127] B. B. Zaidan, A. A. Zaidan, A. Taqa, and F. Othman, "Stego-image vs stego-analysis system," *Int. J. Comput. Elect. Eng.*, vol. 1, no. 5, pp. 1793–8163, 2009.

[128] A. Zaidan, B. Zaidan, A. K. Al-Fraja, and H. A. Jalab, "Investigate the capability of applying hidden data in text file: An overview," *J. Appl. Sci.*, vol. 10, no. 17, pp. 1916–1922, Dec. 2010.

[129] B. B. Zaidan, A. A. Zaidan, H. A. Karim, and N. N. Ahmad, "A new approach based on multi-dimensional evaluation and benchmarking for data hiding techniques," *Int. J. Inf. Technol. Decis. Making*, vol. 16, pp. 1–42, Mar. 2017.

[130] A. K. Hmood, B. Zaidan, A. Zaidan, and H. A. Jalab, "An overview on hiding information technique in images," *J. Appl. Sci.*, vol. 10, no. 18, pp. 2094–2100, Dec. 2010.

[131] A. Zaidan, B. Zaidan, and F. Othman, "New technique of hidden data in PE-file with in unused area one," *Int. J. Comput. Elect. Eng.*, vol. 1, no. 5, pp. 642–650, 2009.

[132] A. Hamdan, H. A. Jalab, A. A. Zaidan, and B. B. Zaidan, "New frame work of hidden data with in non multimedia file," *Int. J. Comput. Netw. Secur.*, vol. 2, no. 1, pp. 46–54, 2010.

[133] A. W. Naji, S. A. Hameed, M. R. Islam, B. B. Zaidan, T. S. Gunawan, and A. A. Zaidan, "'Stego-analysis chain, session two' novel approach of stego-analysis system for image file," in *Proc. Int. Assoc. Comput. Sci. Inf. Technol. Spring Conf.*, 2009, pp. 410–413.

[134] A. H. Ali, L. E. George, A. A. Zaidan, and M. R. Mokhtar, "High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain," *Multimedia Tools Appl.*, vol. 77, no. 23, pp. 31487–31516, Dec. 2018.

[135] A. Naji, A. Zaidan, and B. Zaidan, "Challenges of hidden data in the unused area two within executable files," *J. Comput. Sci.*, vol. 5, no. 11, pp. 890–897, Nov. 2009.

[136] A. K. Hmood, H. A. Jalab, Z. Kasirun, B. Zaidan, and A. Zaidan, "On the capacity and security of steganography approaches: An overview," *J. Appl. Sci.*, vol. 10, no. 16, pp. 1825–1833, Dec. 2010.

[137] H. Alanazi, A. A. Zaidan, B. B. Zaidan, H. A. Jalab, and Z. K. Al-Ani, "New classification methods for hiding information into two parts: Multimedia files and non multimedia files," *J. Comput.*, vol. 2, no. 3, pp. 1–8, 2010.

[138] H. A. Jalab, A. A. Zaidan, and B. B. Zaidan, "Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation," *J. Comput.*, vol. 1, no. 1, pp. 108–113, Dec. 2009.

[139] M. Elnajjar, A. A. Zaidan, B. B. Zaidan, M. E. M. Sharif, and H. Alanazi, "Optimization digital image watermarking technique for patent protection," *J. Comput.*, vol. 2, no. 3, pp. 1–8, 2010.

[140] Z. K. Al-Ani, A. A. Zaidan, B. B. Zaidan, and H. O. Alanazi, "Overview: Main fundamentals for steganography," 2010, *arXiv:1003.4086*. [Online]. Available: https://arxiv.org/abs/1003.4086

[141] M. L. M. Kiah, B. B. Zaidan, A. A. Zaidan, A. M. Ahmed, and S. H. Al-bakri, "A review of audio based steganography and digital watermarking," *Int. J. Phys. Sci.*, vol. 6, no. 16, pp. 3837–3850, 2011.

[142] Y. Al-Nabhani, A. Zaidan, B. Zaidan, H. A. Jalab, and H. Alanazi, "A new system for hidden data within header space for EXE-File using object oriented technique," in *Proc. 3rd Int. Conf. Comput. Sci. Inf. Technol.*, vol. 7, Jul. 2010, pp. 9–13.

[143] S. S. Nassar, N. M. Ayad, H. M. Kelash, H. S. El-Sayed, M. A. M. El-Bendary, F. E. A. El-Samie, and O. S. Faragallah, "Secure wireless image communication using LSB steganography and chaotic baker ciphering," *Wireless Pers. Commun.*, vol. 91, no. 3, pp. 1023–1049, Dec. 2016.

[144] A. K. Hmood, Z. M. Kasirun, H. A. Jalab, G. M. Alam, A. A. Zaidan, and B. B. Zaidan, "On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates," *Int. J. Phys. Sci.*, vol. 5, no. 7, pp. 1054–1062, 2010.

[145] H. A. Jalab, A. A. Zaidan, and B. B. Zaidan, "New design for information hiding with in steganography using distortion techniques," *Int. J. Eng. Technol.*, vol. 2, no. 1, pp. 72–77, Jan. 2014.

[146] A. Majeed, L. M. Kiah, H. T. Madhloom, B. B. Zaidan, and A. A. Zaidan, "Novel approach for high secure and high rate data hidden in the image using image texture analysis," *Int. J. Eng. Technol.*, vol. 1, no. 2, pp. 63–69, 2009.

[147] B. B. Zaidan, A. A. Zaidan, A. Y. Taqa, and F. Othman, "An empirical study for impact of the increment the size of hidden data on the image texture," in *Proc. ICFCC*, 2009.

[148] B. Zaidan, A. Zaidan, A. Al-Frajat, and H. Jalab, "On the differences between hiding information and cryptography techniques: An overview," *J. Appl. Sci.*, vol. 10, no. 15, pp. 1650–1655, Dec. 2010.

[149] A. A. Zaidan, F. Othman, B. B. Zaidan, R. Z. Raji, A. K. Hasan, and A. W. Naji, "Securing cover-file without limitation of hidden data size using computation between cryptography and steganography," in *Proc. World Congr. Eng.*, vol. 1, 2009.

[150] A. A. Zaidan, B. B. Zaidan, and A. Majeed, "High securing cover-file of hidden data using statistical technique and AES encryption algorithm," in *Proc. World Acad. Sci., Eng. Technol.*, vol. 54, 2009, pp. 468–479.

[151] A. A. Zaidan, B. B. Zaidan, M. M. Abdulrazzaq, R. Z. Raji, and S. M. Mohammed, "Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography," in *Proc. Int. Assoc. Comput. Sci. Inf. Technol. (IACSIT)*, vol. 20, 2009.

[152] O. O. Khalifa, A. W. Naji, A. A. Zaidan, B. B. Zaidan, and S. A. Hameed, "Novel approach of hidden data in the (unused area 2 within EXE file) using computation between cryptography and steganography," *Int. J. Comput. Sci. Netw. Secur.*, vol. 9, no. 5, pp. 294–300, 2010.

[153] A. W. Naji, A. A. Zaidan, B. B. Zaidan, S. A. Hameed, and O. O. Khalifa, "Novel approach for secure cover file of hidden data in the unused area within exe file using computation between cryptography and steganography," *J. Comput. Sci.*, vol. 9, no. 5, pp. 294–300, 2009.

[154] A. Taqa, A. A. Zaidan, and B. B. Zaidan, "New framework for high secure data hidden in the MPEG using AES encryption algorithm," *Int. J. Comput. Elect. Eng.*, vol. 1, no. 5, pp. 566–571, Nov. 2013.

[155] A. A. Zaidan, B. B. Zaidan, and H. A. Jalab, "A new system for hiding data within (unused area two+image page) of portable executable file using statistical technique and advance encryption standared," *Int. J. Comput. Theory Eng.*, vol. 2, no. 2, pp. 218–225, 2010.

[156] A. Mohsin, A. Zaidan, B. Zaidan, O. Albahri, A. Albahri, M. Alsalem, and K. Mohammed, "Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions," *Comput. Standards Interfaces*, vol. 64, pp. 41–60, May 2019.

[157] A. Mohsin, A. Zaidan, B. Zaidan, O. Albahri, A. Albahri, M. Alsalem, and K. Mohammed, "Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication," *Comput. Standards Interfaces*, vol. 66, Oct. 2019, Art. no. 103343.

[158] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, and K. I. Mohammed, "Based medical systems for patient's authentication: Towards a new verification secure framework using CIA standard," *J. Med. Syst.*, vol. 43, no. 7, p. 192, 2019.