A Review of Finger-vein Biometric Recognition

Ala Abdulhakim Alariki, Muqadas Faiz, Sanaullah Balagh, Christine Murray

***Abstract*—the widespread success of various biometric recognition systems has contributed to extensive exploration of new biometric modalities, expanding upon traditional fingerprint metrics. Finger-vein is one of the latest biometric traits that has attracted researchers because it promises to be an effective and reliable modality for implementation in biometric authentication systems. In this paper, a review of the current literature on finger-vein biometric authentication is given with the objective of finding out what features, classifiers, and methodologies are utilized by researchers in implemented systems. We find that vein pattern is the most widely used feature for finger-vein recognition. Also, in terms of usage, the hamming distance and Euclidean distance dominate as preferences over other finger-vein classifiers. Furthermore, in previous research in the finger vein authentication systems, there is a lack of comprehensive extraction and combined testing of all finger vein features. Based on this, we will develop the new finger vein authentication systems.**

***Index Terms*—Biometrics, Authenticating, Finger-vein, Features extraction, Classification.**

I. Introduction

Identity management with secure, reliable means is a crucial need for every society in today's globalized world. It is vital to be able to confirm or determine an individual's identity-claim. Such confirmation procedure is known as authentication or person recognition. According to O'Gorman [12], three methods are basic recognizing or authenticating an individual. First is via the individual's knowledge - what they know - such as password or PIN. Second, is via items they own extrinsically, such as ID card, passport, a USB token, or other external physical object. Third, is what they own intrinsically, their unique physical characteristics such as fingerprint, finger-vein, face, iris, gait, etc.

Manuscript received November 20, 2017; revised June 17, 2018. This work was supported in part by the American University of Afghanistan. A Review of Finger-vein Biometric Recognition.

A. A. Alariki is assistant professor in the Department of Information Technology and Computer Science, American University of Afghanistan, Kabul, Afghanistan (phone: +93-72986-3313; e-mail: aabdulaziz@auaf.edu.af).

M. Faiz is senior student in the Department of Information Technology and Computer Science, American University of Afghanistan, Kabul, Afghanistan (e-mail: mqasim.ug@auaf.edu.af).

S. Balagh is senior student in the Department of Information Technology and Computer Science, American University of Afghanistan, Kabul, Afghanistan (e-mail: sbalagh.ug@auaf.edu.af).

C. Murray is assistant professor in the Department of English and Humanities, American University of Afghanistan, Kabul, Afghanistan (e-mail: cmurray@auaf.edu.af).

The third method is known as biometric recognition, which is, for several reasons, considered a better approach over the other two more widely used methods. The knowledge-based authentication method leads to several widespread problems because it lacks the more deterministic features of biometric recognition. For example, passwords or PINs are easily forgotten, lost, shared, stolen, and guessed. Similarly, the second method has proven faulty: not only can identification items be forged, they have also proven to yield, via the same problems as knowledge-based authentication, a high measure of indeterminacy, thus an ultimate unreliability. Moreover, these widely used methods, in creating questions of unreliability while also being in widespread use, have limited ways and means of establishing alternative systems of identity management that can prevent duplicity and multiplicity in claims to identity. In contrast, the biometric recognition method offers prominent features that are more reliably deterministic, attributable, consistent in application and interpretation, as well as being based on nature's unique patterns of identity difference. Biometric traits are, then, extremely difficult to duplicate, lose, forget, or share [12].

Biometric authentication can be subdivided into two types, physiological and behavioral. The physiological biometrics account for body parts, such as fingerprints, finger-veins, palm-veins, hand-geometry, facial traits, retinal patterning, and so on. Behavioral traits refer to behavioral patterns of an individual, for example, voice, gait, typing patterns, etc. [13].

Indeed, the details and multiple uses of biometric recognition provide more reliable alternatives over the traditional authentication methods. However, the usefulness of biometric authentication will depend on what biometric modality (trait) is analyzed. Some biometric modalities have the advantage of providing more certainty than others. In this case, the finger-vein modality is considered exemplary since it has features of more certainty that is lacking in others. According to Yang, et al (2014) [1], it is most difficult to manipulate and forge finger-veins. This stands in remarkable contrast to exempla of fingerprint or voice modalities. Aside from general attributes that other biometric traits have, such as uniqueness yet universality, the finger-vein trait has discrete advantages. The individual must be alive for identity to register or be claimed. To illustrate this, in the capture process, the capture module of a finger-vein biometric system only captures the finger-vein images if there is blood circulation in the body of the individual. In addition to this condition of vitality, finger-vein modality has another advantage, which is internal biological properties. Finger-veins are very unlikely to become damaged. Consequently, these properties give finger-vein modality a much more desirable result over others [14].

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Because of the distinct benefits and advantages the finger-vein biometric brings to consideration, it has attracted a large body of researchers who have proposed various systems for implementation of finger-vein recognition systems. This paper reviews, then, the most important literature in finger-vein biometrics. The focus of this paper is on methods for feature extraction and classification, with an emphasis on performance. Section two, following here, details the summary review of related work conducted on finger-vein biometrics.

II. Related Work

In this section, related work in the finger-vein domain is reviewed.

Yang et al ,2014 [1] conducted an experiment on 156 subjects, presenting a framework with a new algorithm for the identification of finger-vein, which they claim can achieve much higher accuracy and can more consistently extract features from the finger-vein shapes and structures. In their study, they proposed new score level combination methods, namely, nonlinear and holistic, in order to effectively combine concurrently generated finger-vein and finger texture scores. The proposed framework utilizes vein patterns as the target feature and Hamming distance for classification. The overall performance results in %93.49 accuracy in the matching stage.

Yang et al, 2012 [2] has proposed a "simple but powerful" method, the Pyramid Histograms of Gray, Texture and Orientation Gradients (PHGTOG), to reflect information regarding extracted features, including gray, vein texture, and vein shape. In addition, they proposed PFS-PHGTOG as a subset of PHGTOG. They established that PFS-PHGTOG is superior to PHGTOG in terms of higher efficiency and lower computation complexity. Also, they conducted experiments to demonstrate the distinction between these two methods. They used gray, vein texture, and vein shape as extracted features and Euclidean distance as the classifier for their proposed systems with an accuracy of %0.0022 EER in terms of performance.

Raghavendra et al, 2014 [3] introduced a multimodal biometric sensor that is able to capture finger-vein and fingerprint samples at the same time. They have collected a database of 1500 finger-vein and fingerprint samples which was acquired from 41 subjects. They claimed that their extensive experiments on the database show a better performance over the conventional modern schemes when compared to their proposed biometric recognition scheme. According to their comparison score level fusion of finger-vein and fingerprint indicate the best performance with %0.78 EER accuracy. In this study, the vein pattern is utilized as the target feature and cross-correlation based comparator as the classifier with an accuracy of %1.74 EER accuracy.

A novel feature of the extraction method, Multi-Orientation Weighted Symmetric Local Graph Structure (MOW-SLGS), is proposed by Dong et al, 2015 [4] which takes into account location and direction information between the pixels of the image while the traditional Symmetric Local Graph Structure (SLGS) method only look at the relationship between the pixels of the image. MOW-SLGS sets weight to each edge based on the positional relationship between the target pixel and the edge. They have conducted their experiments on 106 subjects and used the Positional relationship between the edge and the target pixel as the desired feature and three different classifiers including 1-NN, Extreme Learning Machine (ELM) Neural Network, and VBELM with %0.9125 EER accuracy.

Another finger-vein identification method was proposed by Xi et al, 2013 [5] that is based on feature-point matching and is less vulnerable to deformation of vein patterns and shading. They claimed that matching of finger-vein images based on the proposed method of feature-point matching results in higher accuracy than the conventional finger-vein identification methods. They conducted their experiments on 676 subjects. They use the non-linear shape of the vein pattern as the default feature and Euclidean distance as the classification with an accuracy of %0.152 EER. However, this study acknowledge that their proposed method has issues including processing time and "normalization of a rotation angle around an optical axis and scale of a finger-vein image" which needs to be addressed in their future work.

Matsuda et al, 2016 [6] proposed a new method for finger-vein recognition that is based on $(2D)^2$ PCA and metric learning. They first extract the vein patterns feature by $(2D)^2$ PCA, and then, based on metric learning, a binary classifier is trained for each individual. They conducted their experiments on 80 subjects. They utilized K Nearest Neighbor (KNN) as classification with %99.17 of accuracy.

Kumar and Zhou, 2012 [7] suggest that the addition of soft biometric traits to finger-vein can enhance the recognition accuracy. They combined the width of the phalangeal joint in finger as a soft biometric with finger-vein patterns for this purpose. They developed three frameworks: hybrid framework, filter framework, and fusion framework to conduct the experiments on. Lu Yang et al claim that their experimental results show that the addition of the soft biometric trait to finger-vein perform better than the individual finger-vein modality. From among the developed frameworks, the hybrid framework works best. In their study, they used width of phalangeal joint in finger and vein pattern as the feature and Hamming distance as the classification with %8.08 accuracy. They conducted their experiments on 156 subjects.

Wu et al, 2011 [8] proposed a finger-vein pattern recognition system in which its feature extraction component is based on principal component analysis (PCA) and its classification component is based on Adaptive Neuro-Fuzzy Inference System (ANFIS). The PCA method is used to extract finger-vein features to reduce the computational load and remove noise and subsequently, the features are utilized in pattern identification and classification. In order to verify the efficiency and effectiveness of the proposed system, they have used Back-propagation (BP) network for comparison with ANFIS. Wu et al. conducted their experiment on 10 subjects. They have chosen vein pattern as the desired feature and ANFIS for the classification with %99 ANFIS accuracy. In section three, a comparison between the related work is presented.

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

III. Related Work Comparison

Table 1 is a comparison of the important components in finger-vein biometric recognition systems proposed or suggested by the research body. It includes the features and classifications used in different experiments and how well they contribute to performance in terms of accuracy. From the table we can deduce that Xi et al, 2013 [5] conducted their experiments on 676 subjects achieving a very high accuracy of %0.152 while Wu et al, 2011 [8] conducted their experiments on a group of 10 subjects achieving an accuracy of %99.

Although Kumar et al 2014 and Wu et al 2011 both cover Vein Pattern Feature, their answers differ. In Classification Kumar et al 2014 used hamming distance algorithm, while Wu et al 2011 used adaptive neuro-fuzzy inference. More significantly, the size of test group was 156 in Kumar et al 2014 and in Wu et al 2011 it was only 10 users. Yet, both achieved high authentication accuracy. This indicate that hamming distance algorithm is better than adaptive neuro-fuzzy inference. We can conclude from this result that hamming distance algorithm is more reliable for Classification. Additionally, achieving a high accuracy with a large body of users represents a more successful methodology in terms of feature extraction and classifier selection than a high accuracy with a handful of users.

Based on the studies in Table 1, there has been no comprehensive extraction and combined testing of all finger vein features. We further conclude, it is now necessary to develop a new, comprehensive authentication framework.

TABLE I
A COMPARISON OF RELATED WORK BY FEATURES AND PERFORMANCE

Author	Features	Classification	No of Users	Device	Performance
Kumar et al. [7]	Vein Pattern	Hamming distance	156	NA	%93.49 Accuracy
Xi et al. [5]	Gray, Vein Texture, Vein Shape	Euclidean distance	20	NA	%0.0022 EER
Raghavendra et al. [3]	Vein Pattern	cross-correlation based comparator	41	Fingerprint and Finger Vein Capture Device	%1.74 EER
Dong et al. [4]	Positional relationship between the edge and the target pixel.	1-NN, Extreme Learning Machine (ELM) Neural Network, VBELM	106	NA	%0.9125 EER
Matsuda et al. [6]	Non-linear Shape of the Vein Pattern	Euclidean distance	676	Imaging Device	%0.152 EER
Yang et al. [2]	Vein Pattern	K Nearest Neighbor	80	A computer with 2.4 GHz CPU and 4 GB Memory	%99.17 Accuracy
Lu Yang et al. [1]	Vein Pattern, Width of Phalangeal joint	hamming distance	156	Imaging Device	% 8.08 EER
Wu et al. [8]	Vein Pattern	Adaptive Neuro-Fuzzy Inference System (ANFIS)	10	NA	%99 ANFIS Accuracy

IV. Methodology

As with any biometric recognition system, finger-vein biometric systems are based on a generic framework that is composed of differing modules or building blocks, namely, image acquisition, feature extractor, storage, and matcher. Generally, the framework operates under a process that consists of two phases for the user registration and identification purposes. Theses phases are enrollment and authentication, respectively, as shown in Fig. 1.

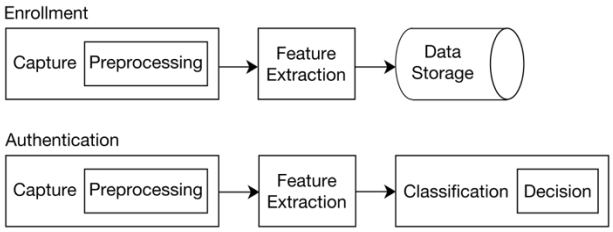

Fig. 1. Illustration of a typical finger-vein biometric recognition framework

A. Capture (Image acquisition)

Typically, the first operation in the enrollment phase is carried out by the image acquisition module (also called capture module). The image acquisition module captures an image of the finger veins. After that, the image goes through preprocessing stages to enhance and normalize the image so that the target features are easily extracted and are usable. In finger-vein biometric systems, a different approach is taken to capture the image by using a device that is different from the ones used for fingerprint biometric systems. A typical finger-vein capture device is composed of several components. An infrared light component that produce light on the finger dorsal – backside of the finger. Another component is the web camera or simply camera which captures the image of the finger veins which is made easy by the infrared light cast on the back side of the finger. A last component is the LED control that controls the amount of light needed for the capture.

B. Feature Extraction

The feature extractor module extracts the target features from the images captured in the previous stage of image acquisition. There are several desirable features that can be extracted from finger veins, and various research studies have recommended one or more of these features for implementation in finger-vein biometric recognition systems. According to Table 1, the researchers have used one or more of the following features in their proposed systems.

- Vein Pattern [1], [3], [6], [7], [8]
- Gray [2]
- Vein Texture [2]
- Vein Shape [2]
- Non-linear Shape of the Vein Pattern [5]
- Width of Phalangeal Joint [7]
- Relationship between the edge and pixels [4]

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

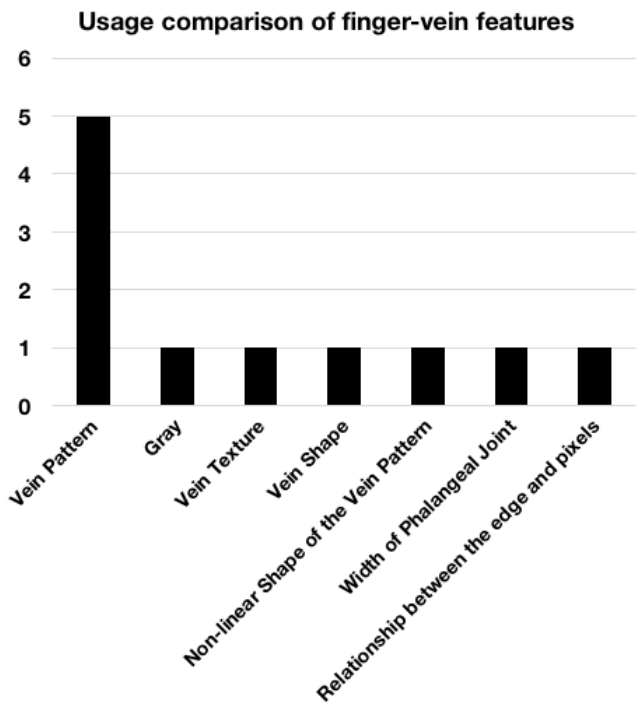

Fig. 2. A comparison of the common features used in finger-vein identification systems.

In Fig. 2, on one hand, Gray, Vein Texture, Vein Shape, Non-linear Shape of the Vein Pattern, and Width of Phalangeal Joint, each were used in one study. On the other hand, Vein Pattern was used by five different studies. Between individual people, Vein Pattern feature distinguishes uniqueness.

C. Storage

Biometric systems not only act as an identification management system, but also as a database of biometric information. In the enrollment phase, when the finger-vein image is captured, preprocessed, and the relevant features are extracted, it is then the job of the storage module – also called database module - to create a table and store the extracted features tied to specific users and save this table as a template. This template is later used in the authentication phase when a user claims identity to the system.

D. Classification

The classification or matching module carry out the job of comparing a sample template or query with the stored template in the database to produce a matching score and by that determine whether the templates data agree. The higher the matching score is the more similar the templates are. In finger-vein recognition systems, various classifiers are proposed by researchers to do the matching between the query and the stored template data. According to Table 1, the researchers have implemented one or more of the following Classifiers in their proposed systems:

- Hamming distance [1], [7]
- Euclidean distances [2], [5]
- Cross-correlation based comparator [3]
- Extreme Learning Machine (ELM) Neural Network [4]
- K Nearest Neighbor [6]
- Back-propagation (BP) Network, Adaptive Neuro-Fuzzy Inference System (ANFIS) [8]

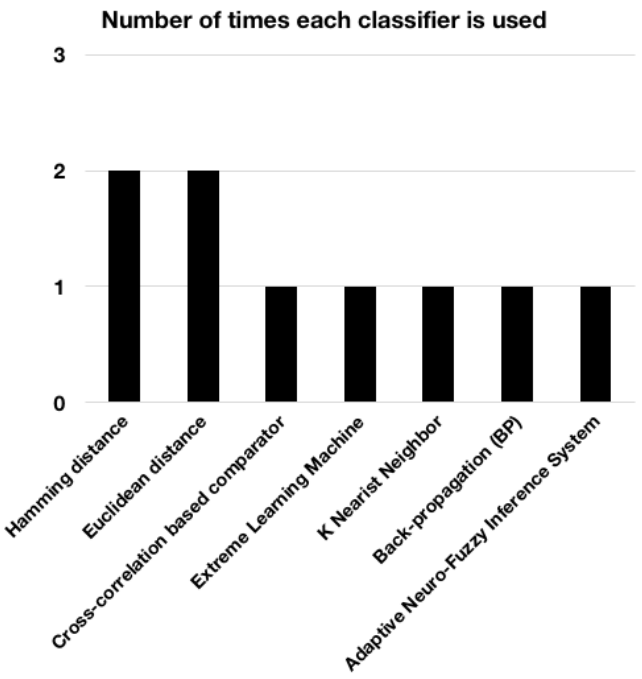

Fig. 3. Finger-vein classifiers usage comparison

The results in Fig. 3, suggest that the Hamming Distance and Euclidean distance algorithms are more effective and practical than other classifiers.

V. Performance Measurement

A. Evaluation of Biometrics Scheme

For a specific biometric system to be evaluated, three important error rates need to be taken into consideration, namely: False Rejection Rate (FRR), False Acceptance Rate (FAR), Equal Error Rate (EER) and accuracy. Pattern classifier output is sensitive to many factors, including algorithm choice, amount of training data and the chosen features in the feature vector. These factors have effects on the performance metrics computed for each classifier [10].

The different types of measures to be considered when evaluating any pattern classifier are shown in Table 2.4. It shows all the possible results in a two-class problem, with the class decisions made by the classifier in the columns, and the true, known classes in the rows. The diagonal from top left to bottom right shows the number of correctly classified patterns. True accept and true reject are seen when the classifier produces the same result as the known classification for the pattern. False accept and false reject are when the classifier produces the opposite result to the known classification. According to Crawford, several different types of error rates are commonly reported in biometrics which are listed in Table II.

TABLE II
CONFUSION MATRIX FOR TWO-CLASS PROBLEM

		Predicted Class	
		Positive	**Negative**
True Class	Positive	True Accept	False Reject
	Negative	False Accept	True Reject

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

B. False Rejection Rate (FRR)

It is a statistic that represents the number of times the system results into a false rejection (in terms of percentage). A false rejection occurs when an authorized user sample of a biometric is not matched with the stored template and then rejected by the system. Let false reject (FR) represent the number of false rejects from the classifier output and NA be the number of authorized user patterns. Then FRR is calculated using (1).

$$FRR = \frac{Number\ of\ genuine\ rejects}{Number\ of\ genuine\ attempts} = \frac{FR}{NA} \quad (1)$$

C. False Acceptance Rate (FAR)

This is a statistic that represents the number of times (percentage) the system results into a false accept. This result occurs when an imposter sample biometric is matched with a stored template biometric, hence accepted by the system. Let FA be the number of false accepts and NI be the number of impostor patterns. FAR is calculated as in (2).

$$FAR = \frac{Number\ of\ imposter\ accepts}{Number\ of\ imposter\ patterns} = \frac{FA}{NI} \quad (2)$$

D. Equal Error Rate (EER)

EER is the point at which the plotted curves of TAR (1-FRR) and FAR meet. According to Crawford, 2012 [10], EER can be determined by plotting the ROC curve for the classifier; and determining its abscissa by plotting a diagonal line from the upper left to the lower right corners and observing where the two lines cross [9].

E. Accuracy

In as much as a confusion matrix gives all the information required, to evaluate the performance of a classification model, aggregation would be more preferable, so that it can be easier to compare different models' performances. The confusion matrix provides the results to calculate the accuracy. It is specified as follows in (3).

$$Accuracy = \frac{Number\ of\ correct\ predictions}{Total\ number\ of\ predictions} \quad (3)$$

In most cases classification algorithms look for models that can give the highest accuracy or give the lowest error rate when applied to a training set.

VI. Conclusion

In this paper, we have reviewed the most important literature on finger-vein authentication, describing various methods for both feature extraction and classification as proposed by the body of research. We drew comparisons between the proposed features and classifiers, deducing that vein patterning is the most widely used feature of finger-vein authentication, whereby usage of hamming distance and Euclidean algorithms dominate other classifiers. Furthermore, we note that, aside from what classifications and features are prevalently used in experiments conducted by researchers, there is a lack of comprehensive extraction and combined testing of all finger vein features.

Thus, it is necessary to state that our future work will focus on ways of combining all the finger-vein features, seeking ways to synthesize and implement them into one unified system. The hamming distance and Euclidean distance are selected as the most reliable classification with the highest performance accuracy, hence, the number of participants or users should be considered highly with respect to the number of samples. Therefore, the finger-vein authentication mechanism need to be experimented in realistic circumstances. Additionally, the wearable device as a favorite finger-vein authentication mechanism could be chosen a major research tool with Android interface software. As a result, for future exploration to propose a system for finger-vein authentication, all the mentioned points should be considered with their mechanism to have the best efficiency regarding identifying the correct and accurate result from the subject's finger-vein.

Acknowledgment

This work is supported by the American University of Afghanistan. The authors would like to thank the Department of Information Technology and Computer Science for its support and encouragement.

References

[1] Yang, L., Yang, G., Yin, Y., and Xi, X.: 'Exploring soft biometric trait with finger vein recognition', Neurocomputing, 2014, 135, pp. 218-228.
[2] Yang, G., Xi, X., and Yin, Y.: 'Finger vein recognition based on (2D) 2 PCA and metric learning', BioMed Research International, 2012, 2012.
[3] Raghavendra, R., Raja, K.B., Surbiryala, J., and Busch, C.: 'A low-cost multimodal biometric sensor to capture finger vein and fingerprint', in Editor (Ed.)^(Eds.): 'Book A low-cost multimodal biometric sensor to capture finger vein and fingerprint' (IEEE, 2014, edn.), pp. 1-7.
[4] Dong, S., Yang, J., Chen, Y., Wang, C., Zhang, X., and Park, D.S.: 'Finger Vein Recognition Based on Multi-Orientation Weighted Symmetric Local Graph Structure', KSII Transactions on Internet & Information Systems, 2015, 9, (10).
[5] Xi, X., Yang, G., Yin, Y., and Meng, X.: 'Finger vein recognition with personalized feature selection', Sensors, 2013, 13, (9), pp. 11243-11259.
[6] Matsuda, Y., Miura, N., Nagasaka, A., Kiyomizu, H., and Miyatake, T.: 'Finger-vein authentication based on deformation-tolerant feature-point matching', Machine Vision and Applications, 2016, 27, (2), pp. 237-250.
[7] Kumar, A., and Zhou, Y.: 'Human identification using finger images', IEEE Transactions on image processing, 2012, 21, (4), pp. 2228-2244.
[8] Wu, J.-D., and Liu, C.-T.: 'Finger-vein pattern identification using principal component analysis and the neural network technique', Expert Systems with Applications, 2011, 38, (5), pp. 5423-5427.
[9] Clarke, N. L., Furnell, S. M., and Reynolds, P. L.: 'Biometric authentication for mobile devices', 'Proceeding of 3rd Australian Information Warfare and Security Conference', 2002, pp. 61-69.
[10] Crawford, H. A., 'A framework for continuous, transparent authentication on mobile devices', 'University of Glasgow, United Kingdom, PhD Thesis', 2012.
[11] Saevanee, H., 'Continuous User Authentication Using Multi-Modal Biometrics', 'School of Computing and Mathematics', 'Plymouth University, England, PhD Thesis', 2014.
[12] O'Gorman, L., 'Comparing Passwords, Tokens, and Biometrics for User Authentication', Avaya Labs, 2003, pp. 6.
[13] Weaver, A., 'Biometric Authentication', 'University of Virginia', 2006.
[14] Yang, L.,Yang, G., Yin, Y., Zhou, L., 'A survey of finger vein recognition', 'School of Computer Science and Technology, Shandong University', 2014.