© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Security Enhanced Multi-Factor Biometric Authentication System Using FFF and KSVM

[1]P.Pandimeena, [2]N.Nanthini

[1]Research Scholar, Department of Computer Science, Sakthi College of Arts and Science for Women, Oddanchatram, India

[2]Assistant Professor, Department of Computer Science, Sakthi College of Arts and Science for Women, Oddanchatram, India

ABSTRACT

In this study we focus on multimodal biometric system by combining finger knuckle and finger vein using feature level fusion optimization. Biometric characteristics (Eyes, Finger vein, Finger Knuckle, Face, Ear, and Palm) like. Here used unique and secure password (like Finger Vein, Finger Knuckle). In this paper, the authors propose a multimodal biometric system by combining the finger knuckle and finger vein images at feature-level fusion using fractional firefly (FFF) optimization. Biometric characteristics, like finger knuckle and finger vein are unique and secure. Initially, the features are extracted from the finger knuckle and finger vein images using repeated line tracking method. Then, a newly developed method of feature-level fusion using FFF optimization is used. This method is utilized to find out the optimal weight score to fuse the extracted feature sets of finger knuckle and finger vein images. Thus, the recognition is carried out by the fused feature set using layered k-SVM (k-support vector machine) which is newly developed by combining the layered SVM classifier and k-neural network classifier. The experimental results are evaluated and the performance is analyzed with false acceptance ratio, false rejection ratio and accuracy. The outcome of the proposed FFF optimization system obtains a higher accuracy.

Keywords : Feature Level Fusion, FFF Optimization, Repeated Line tracking method, Layered K-SVM, K-neural network classifier.

I. INTRODUCTION

Nowadays, many of the multimodal biometric systems are in use and gained a lot of importance due to its uniqueness and effectiveness. The multimodal biometric systems include hand geometry, signature, retinal pattern, iris, voice-print, finger knuckle, fingerprint, finger vein, face and so on. The advantages and disadvantages of the biometric systems are based on the three main factors, such as user acceptance, accuracy and applicability. The accuracy of the iris pattern, retinal pattern and face is minimal, when compared to the finger knuckle and the finger vein traits. User acceptance is also very high for the finger knuckle and the finger vein compared to the other biometric traits.

The performance is also good for the finger knuckle and the finger vein due to the finger geometry. In addition to, security, non-traceability, speed, user friendly, accuracy and so on is the advantages of the finger vein. The integration of the feature sets is used to enhance the outcome of the recognition of the biometric system by the corresponding multiple modalities. The integration of the feature is done in three ways, such as feature-level fusion, score-level fusion and decision-level fusion. The integration of the feature set is difficult, when (i) the feature sets of multiple modalities are incompatible, (ii) unknown

relationship between the feature space of multiple modalities and, (iii) curse of dimensionality problem. Commonly, three level fusion before and after matching criteria are used for fusing the features. In score-level fusion, the integration of feature vector is done with the matching score output of the individual matches, and then, the feature vectors are accepted or rejected by an information

- Combining the fractional theory and firefly algorithm as fractional firefly (FFF) optimisation algorithm for feature-level fusion based on the finger knuckle and finger vein images.
- FFF optimisation algorithm is proposed to find out the optimal weight score level for the feature-level fusion. Thus, this optimisation is used to fuse the feature set of both finger knuckle and vein image by the weight score level.
- A new classifier called, k-SVM (k-support vector machine) is developed for the recognition of person by combining the k-NN (k-neural network) classifier and SVM classifier.

1.1 Challenges

On the basis of the literature review conducted, multimodal recognition have been actively studied with various machine learning techniques but for the unsurpassed recognition, the feature-level fusion-based recognition is the fine choice considering the matching score-level as well as the decision-level fusion. The developing of multimodal recognition techniques using feature-level fusion have not been studied much in the literature even though it contains more advantages than the score- and decision-level fusion. In feature-level fusion, the concatenation of the feature vector with reasonable accessibility is an important challenge in the biometric recognition system. Even if the features of the multimodalities are not compatible, the concatenation must be appropriate for the recognition.

Furthermore, fusion of the feature with the ultimate robust recognition is crucial challenge considerable in the multimodal biometric recognition system. While using feature-level fusion, the biometric recognition system must not degrade along with the quality of the feature sets. Proper processing over the feature must be employed for the thriving function of the recognition system. Another important challenge with respect to feature-level fusion is to develop the reliable recognition system. The fusion level must be selected in a way improving the recognition accuracy of the recognition system without degrading the system performance.

1.2 New FFF optimisation

A novel optimisation method is proposed for feature-level fusion using FFF optimisation, which comprises fractional theory and firefly algorithm. In the firefly algorithm, variation of light intensity and the formulation of attractiveness are the two significant issues. It is a meta heuristic algorithm for global optimisation, which is inspired by flashing behaviour of firefly insects. For simplicity, assume that the attractiveness of a firefly is determined by its brightness or light intensity, which in turn is associated with the encoded objective function. The brighter one will attract the other; so the less bright one is moved towards the brighter one. In the simplest case, for the optimisation problems, the brightness I of a firefly at a particular location x can be chosen as $I(x) \alpha f(x)$. In this paper, the fireflies are initialised randomly. For the next iteration, the fireflies are newly generated by finding the movement of firefly with another firefly, which is expressed using the fractional theory. The fractional theory can be rather interesting for filtering and edge detection and also enhance the quality of images. When differential and integral calculus plays a significant role in mathematics, experts investigated the computation of non-integer order derivatives and integrals. Thus, the integration of firefly optimisation and fractional theory is used here to calculate the appropriate value for α and β.

1.3 Deep Learning

In this paper, we do not focus on custom-tailored solutions. Instead, inspired by the recent success of Deep Learning in several vision tasks, and by the ability of the technique to leverage data, we focus on two general-purpose approaches to build image-based anti-spoofing systems with convolutional networks for several attack types in three biometric modalities, namely iris, face, and fingerprint. The first technique that we explore is hyper parameter optimization of network architectures that we hence forth call architecture optimization, while the second lies at the core of convolutional networks and consists of learning filter weights via the well-known back-propagation algorithm, here in after referred to as filter optimization. Fig. 1 illustrates how such techniques are used. The architecture optimization (AO) approach is presented on the left and is highlighted in blue while the filter optimization (FO) approach is presented on the right and is highlighted in red.

II. ARCHITECTURE OPTIMIZATION (AO)

AO is used to search for good architectures of convolutional networks in a given spoofing detection problem and uses convolutional filters whose weights are set at random in order to make the optimization practical. This approach assumes little a priori knowledge about the problem, and is an area of research in deep learning that has been successful in showing that the architecture of convolutional networks, by themselves, is of extreme importance to performance. In fact, the only knowledge AO assumes about the problem is that it is approachable from a computer vision perspective. FO is carried out with back-propagation in a predefined network architecture. This is a long standing approach for building convolutional networks that has recently enabled significant strides in computer vision, specially because of an understanding of the learning process, and the availability of plenty of data and process in power. Network architecture in this context is usually determined by previous knowledge of related problems.

In general, we expect AO to adapt the architecture to the problem in hand and FO to model important stimuli for discriminating fake and real biometric samples. We evaluate AO and FO not only in separate, but also in combination, i.e., architectures learned with AO are used for FO as well as previously known good performing architectures are used with random filters. This explains the crossing dotted lines in the design flow of Fig 1. As our experiments show, the benefits of evaluating AO and FO apart and later combining them to build anti-spoofing systems are twofold. First, it enables us to have a better comprehension of the interplay between these approaches, something that has been largely underexplored in the literature of convolutional networks. Second, it allows us to build systems with outstanding performance in all nine publicly available benchmarks considered in this work.

III. FILTER OPTIMIZATION (FQ)

The first three of such benchmarks consist of spoofing attempts for iris recognition systems, Biosec, Warsaw, and MobBIOfake. Replay-Attack and 3DMAD are the benchmarks considered for faces, while Biometrika, Cross Match, Italdata, and Swipe are the fingerprint benchmarks here considered, all them recently used in the 2013 Fingerprint Liveness Detection Competition (LivDet'13). Results outperform state-of-the-art counterparts in eight of the nine cases and observe a balance in terms of performance between AO and FO, with one performing better than the other depending on the sample size and problem difficulty. In some cases, we also show that when both approaches are combined, we can obtain performance levels that neither one can obtain by itself. Moreover, by observing the behaviour of AO and FO, we take advantage of domain knowledge to propose a single new convolutional architecture that

push performance in five problems even further, sometimes by a large margin, as in Cross Match (68.80%v.98.23%). The experimental results strongly indicate that convolutional networks can be readily used for robust spoofing detection. Indeed, we believe that data-driven solutions based on deep representations might be a valuable direction to this field of research, allowing the construction of systems with little effort even to image-based attack types yet to come. We organized the remainder of this work into five sections. Section II presents previous anti-spoofing systems for the three biometric modalities covered in this paper, while Section III presents the considered benchmarks. Section IV describes the methodology adopted for architecture optimization (AO) and filter optimization (FO) while Section V presents experiments, results, and comparisons with state-of-the-art methods.

IV. PROBLEM OF THE STATEMENT

Recognition or identification of human is very challenging problem in today's world. Here, the major challenge is to identify the human through finger knuckle and finger vein images. Let us assume that the input database of A having N persons and every person n1 have Q number of finger knuckles and finger veins.

$$A€n1; \{1 \le 1 \le N\}$$

$$n1 = \{qk; 1 \le k \le Q\}$$

Here, every person corresponding to qk is indicated as image Rij (knuckle image) and Sij (vein image) which are then utilized to recognize the person. The main problem considered here is to recognize N person separately through their finger knuckle and finger vein images.

V. METHODOLOGY

This research aims to developing a system for acquiring images of finger veins and processing them using MATLAB for the purpose of authentication. It includes designing of hardware for image acquisition, coding the matching algorithm for processing the finger vein pattern and training and testing of algorithm module. Typical Finger vein recognition system consists of image acquisition module, image preprocessing, feature extraction, and matching.

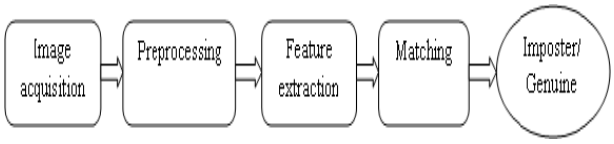

Figure-1: Authentication process

(i) Image acquisition: Finger Vein patterns can be viewed through an image sensor sensitive to infrared light. Infrared light passing through the tissues of the human body is blocked by hemoglobin. As hemoglobin exists densely in blood vessels, infrared light passing through veins appears as dark shadow lines in the captured image.

(ii) Pre-processing: The first step of the proposed multimodal biometric recognition is pre-processing which makes the input training images better suitable for the subsequent steps. The important processes such as, normalization, filtering and resizing are carried out under pre-processing steps. Once the input images are read out, it undergoes the normalization steps to convert the range of pixels within the particular range. The, median filtering is applied to smooth the input images which makes the input images much visible. Also, this process is helpful for the feature extraction to easily identify the vein parts. Then, resizing is performed to convert all the input images into fixed size through interpolation scheme.

Preprocessing step includes image segmentation in which captured image is divided into multiple parts. Each of the pixels in a segment will be similar with respect to some properties, such as color, texture or intensity. The aim of segmentation is to change the representation of an image into something that is easier to analyze. Image segmentation is used to locate objects and boundaries in an image. Segmentation is the process by which we are assigning a label to every

pixel in an image. Pixels sharing the same label will have certain similar visual characteristics.

5.1 Vein and Knuckle Print Extraction Using Repeated Line Tracking

In this method, the extraction of finger knuckle and vein print using a repeated line method is discussed. The line tracking operation starts at any pixel in the source image. We defined the current pixel position in an image as the current tracking point and this point is moved from pixel to pixel along the dark line direction in the finger knuckle and finger vein images. Thus, the method of feature extraction from the image is described as follows. F i, j is the intensity of the pixel i, j in the finger knuckle image. Similarly, F m, n is the intensity of the pixel m, n in the finger vein image. Zf_k and Zf_v are the set of pixels in the finger knuckle and finger vein images, respectively. S_1 is considered as the locus space. Thus, the knuckle and vein print are extracted by the following four steps:

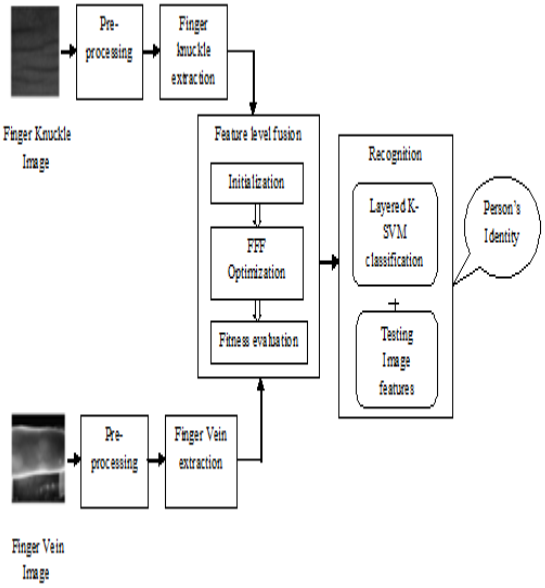

Figure-2: System Overview

The finger vein image features are extracted using wavelet transform and line detection. Wavelet transform is a mathematical function which divides a function into its different frequency components .Wavelet transform analyzes each individual component with a resolution that matches its scale. HAAR wavelet transform multiplies a function against the HAAR wavelet with various shifts and stretches. HAAR transform is easy to implement and is able to analyze the local features. These characteristics make HAAR wavelets applicable for Finger vein recognition algorithm. At last, matching with database is a final decision making step to get a result from the finger vein recognition algorithm. In the matching stage two types of errors are considered

- FAR (False Acceptance Rate)
- FRR (False Rejection Rate)
- EER (Equal Error Rate)

(i) FAR (FALSE ACCEPTANCE RATE)

FRR is the rate of occurrence of a scenario in which two fingerprints from same finger fails to match (the matching score is below the threshold) while

(ii) FRR (FLASE REJECTION RATE)

FAR is the rate of occurrence of a scenario in which two fingerprints from different fingers will match (matching score is greater than the threshold).

(iii) EER (EQUAL ERROR RATE)

EER is the error rate at which the FAR equals the FRR and is therefore, suitable for measuring the overall performance of biometric recognition system.

Sample image and its feature extracted image are shown below.

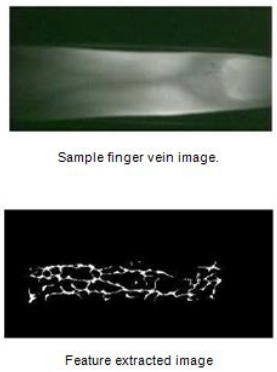

Figure-3: Feature extracted image

In the verification stage, newly captured finger vein image is applied to preprocessing stages, and at last vein image is replaced with the feature extracted image. Finally that extracted image is sent to an

authentication stage. This stage will match the newly feature extracted image with the database image, after matching it will create a match score of each finger vein images in the database. Depending on the match score authentication is carried out. This project implements a highly secured authentication system based on using finger vein recognition.

5.2 Feature-level fusion by FFF optimisation

Fusion at the feature level is least explored even though they are expected to provide better recognition results and much easier to compute. The matching score-level and decision-level supplies less information to be exploited for personnel authentication than the feature-extraction level. Also, the feature-level fusion carries much richer information about the raw biometric data than the matching score or decision level. This is the driving force for the proposed scheme.

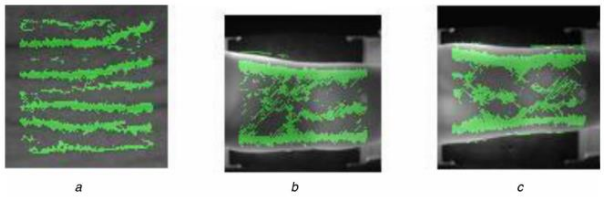

Fig.4 Vein extracted image

5.3 Recognition using layered k-SVM classifier

The extracted features of finger knuckle and finger vein are fused by the FFF optimisation. Then, the classification is performed using layered k-SVM classifier. Here, SVM classifier and k-NN classifier are combined to perform binary classification and then, N – 1 k-SVM classifiers are connected serially to perform multi-level classification. Here, SVM classifier is a binary classifier which is classified by either 0 or 1. Similarly, k-NN classifier is popular technique for data classification based on the neighbours of the input test data. The reason of selecting the k-NN classifier is that it can perform better for multi-classification because the classification is purely based on the distance between the training data and test sample. Also, SVM is preferably chosen here because of the good performance for the high dimensional data. In proposed work, we used an N number of persons for biometric recognition. Thus, recognition is done by the layered k-SVM classifier which consists of N – 1 number of classifiers.

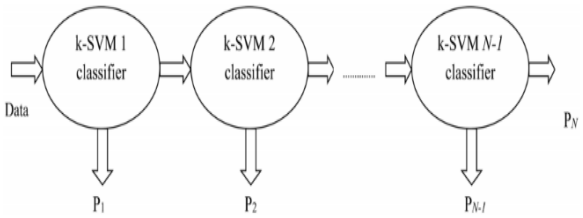

Figure-5: Architecture of layered k-SVM classifier

VI. RESULTS AND DISCUSSION

6.1 Registration Process

Select input images for registering training data, these users can only access the accounts.

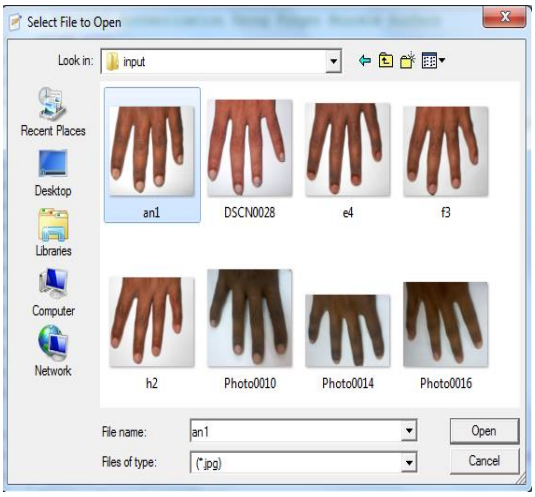

Figure-2: Registration process

6.2 Binary Image

After that selection the user hand converted into binary images.

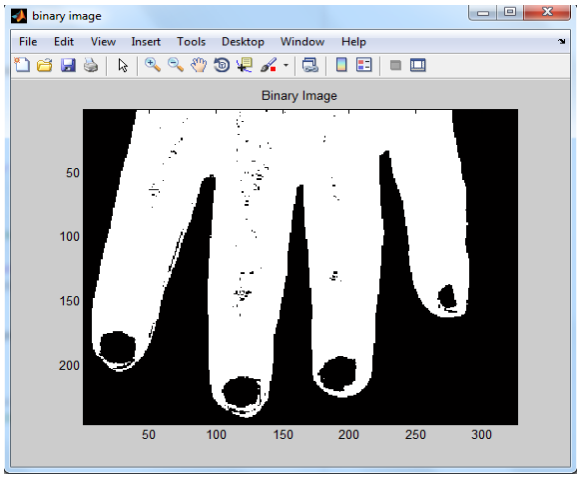

Figure-3: Binary image

6.3 Canny Edge Detection

Binary images are converted into contours images and also calculate the distance peak values from the given images, after that canny edge detection the registered finger knuckle are extracted from the training image.

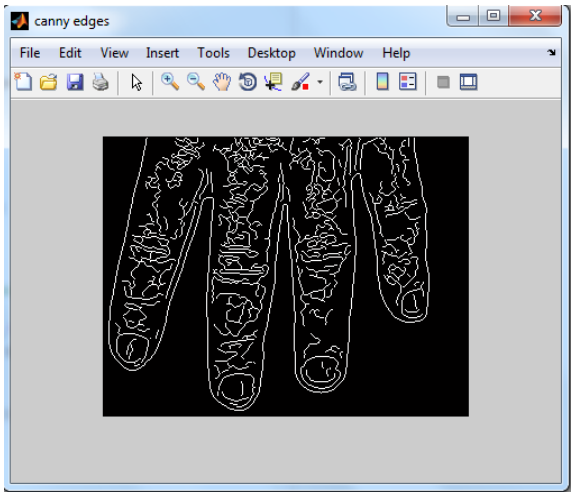

Figure-4: Canny edge detection

6.4 Knuckle Extraction

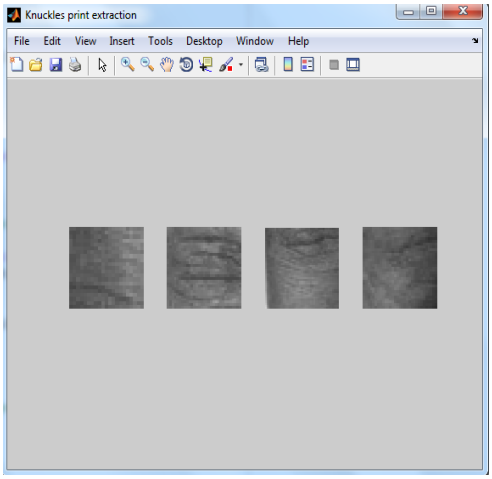

Figure-5: Knuckle extraction

Training images extracted details are stored in temporary database, given user finger as a test user finger which is processed using above methods after that getting extracted value is compared to the training data values, then only get the result user is authorized or not.

6.5 Authorization Process

Whether the results are verified using predefined training details.

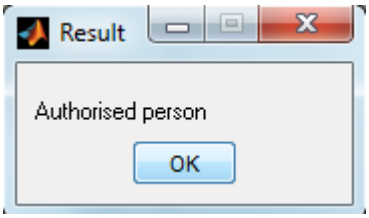

Figure-5: Authorization process

6.6 Finger Vein Extraction Process

Represents the finger vein extracted image. Training images extracted details are stored in temporary database. Then only get the result user is authorized or not.

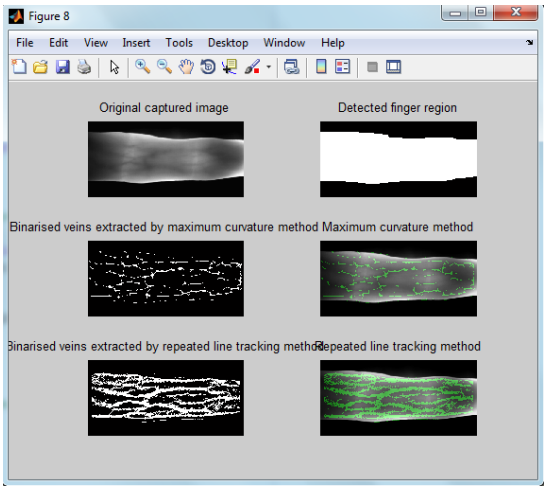

Figure-6: Finger vein extraction process

VII. CONCLUSION AND SCOPE OF FUTURE WORK

Conclusion

In this paper, a multimodal biometric recognition system based on the finger knuckle and finger vein was proposed. An important aspect of the proposed system was the development of FFF optimisation for feature-level fusion. After input images were pre-processed, the FKP was extracted from the knuckle image and vein was extracted from finger vein images using the repeated line tracking method. Then, the features were extracted from the finger knuckle and vein by applying the grid operation to the image. Subsequently, the proposed system was fused the obtained feature set with the help of weight score level, which was obtained by feature-level fusion using FFF optimisation method. Then, recognition was performed by the fused feature set using layered k-SVM classifier. The proposed system was evaluated with the existing systems and the performance was analyzed by the metrics, FAR, FRR, EER and accuracy. From the outcome, we found that the accuracy was obtained for the proposed method. In future, the proposed method can be extended to develop the different objective functions to find the optimal weight score.

Future Work

In our future work, we intend to evaluate such datasets using the proposed approaches here and also consider other biometric modalities such as palm, vein, and gait. Finally, it is important to take all the results discussed here in with a grain of salt. We are not presenting the final word in spoofing detection. In fact, there is important additional research that could finally take this research another step forward. We envision the application of deep learning representations on top of pre-processed image feature.

VIII. REFERENCES

[1]. Jain, A.K., Hong, L., Kulkarni, Y.: 'A multimodal biometric system using fingerprint, face and speech'. Proc. of Int. Conf. on Audio-and Video-based Biometric Person Authentication, 1999, pp. 182–187.

[2]. Saini, R., Rana, N.: 'Comparison of various biometric methods', Adv. Sci. Technol., 2014, 2, (1), pp. 24–30.

[3]. Perumal, E., Ramachandran, S.: 'A multimodal biometric system based on palmprint and finger knuckle print recognition methods', Inf. Technol., 2015, 12, (2), pp. 118–127.

[4]. Neware, S., Mehta, K., Zadgaonkar, A.S.: 'Finger knuckle surface biometrics', Eng. Technol. Adv. Eng., 2012, 2, (12), pp. 452–455.

[5]. Lu, L., Peng, J.: 'Finger multi-biometric cryptosystem using feature-level fusion', J. Signal Process., Image Process. Pattern Recogn., 2014, 7, (3), pp. 223–236.

[6]. Kale, K.V., Rode, Y.S., Kazi, M.M., et al.: 'Multimodal biometric system using fingernail and finger knuckle'. Proc. of Int. Symp. on Computational and Business Intelligence, 2013, pp. 279–283.

[7]. Jacob, A.J., Bhuvan, N.T., Thampi, S.M.: 'Feature level fusion using multiple fingerprints', Comput. Sci.-New Dimens. Perspect., 2011, 4(1), pp. 13–18.

[8]. Kang, B.J., Park, K.R.: 'Multimodal biometric method based on vein and geometry of a single finger', IET Comput. Vis., 2010, 4, (3), pp. 209–217.

[9]. Michael, G.K.O., Connie, T., Teoh, A.B.J.: 'A contactless biometric system using multiple hand features', Visual Commun. Image Represent., 2012, 23, pp. 1068–1084.

[10]. Ross, A., Govindarajan, R.: 'Feature level fusion in biometric systems'. Proc. of Biometric Consortium Conf. (BCC), 2004.