International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

A Literature Review on 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

Department of ECE, Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu, India

ABSTRACT

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 s 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 are the advantages of the finger vein.

CSEIT1833231 | Received : 12 March 2018 | Accepted : 24 March 2018 | March-April-2018 [(3) 3 : 417-425]

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.

A. 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.

B. New FFF Optimization

A novel optimization 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.

II. METHODOLOGIES USED FOR MULTIMODAL BIOMETRIC SYSTEM

A. Authentication using finger vein recognition based on Matlab

This thesis 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.

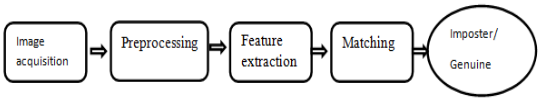


Figure-1: Authentication Processing

B. 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.

C. 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.

D. 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. Zfk and Zfv are the set of pixels in the finger knuckle and finger vein images, respectively. S1 is considered as the locus space. Thus, the knuckle and vein print are extracted by the following four steps:

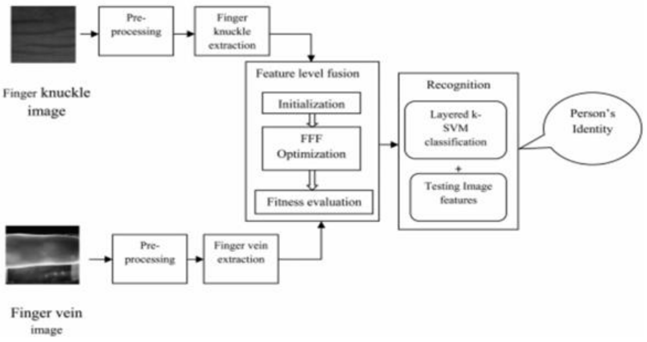
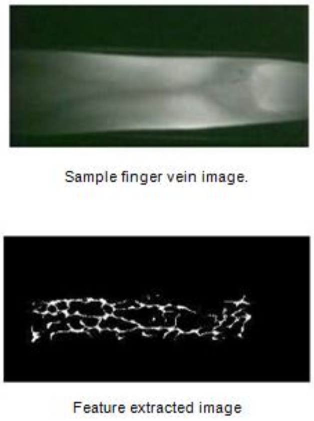


Figure-2 Block diagram of the proposed methodology

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

Sample image and its feature extracted image are shown below.


Sample finger vein image.

Feature extracted image

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.

E. 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.

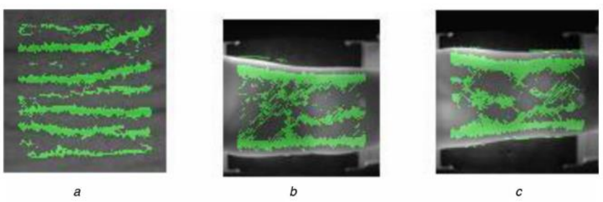


Figure-4: Vein extracted image

F. 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.

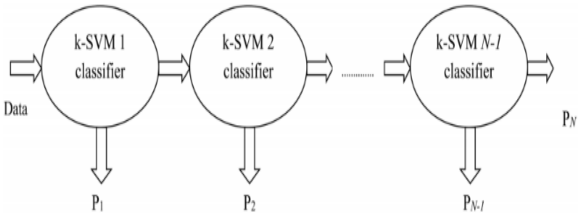


Figure-5:Architecture of layered k-SVM classifier

Table-1: Comparison table on the literature survey

S.No	Title	Description	Merit	Demerit
1	Spoof Attacks on Multimodal Biometric Systems	In addition, latest results have questioned that, contrary to a common claim, multimodal systems can be cracked by spoofing only one trait. Those results were obtained using simulated.	Investigate this significant security issue, focusing on behavior of fixed and trained score fusion rules, using real spoof attack samples under different spoof attack scenarios.	In particular, most widely used fixed rules can be less robust, even if the quality of fake biometric trait is low.
2	Presentation Attack Detection Algorithm for Face and Iris Biometrics	A novel solution to detect a presentation attack based on exploring both statistical and Cepstral features.	Binarized Statistical Image Features (BSIF) and Cepstral features that can reflect the micro changes in frequency using 2D Cepstrum analysis.	Generating face and iris artifacts is not only easy but also cost effective.
3	Fake Biometric Detection to Iris, Fingerprint using Image Quality Assessment	To make sure the actual presence of a true legitimate attribute in distinction to a faux self –manufactured artificial or reconstructed sample may be a significant drawback in biometric	The target of the planned system is to boost the safety of biometric recognition frameworks, by adding animate ness assessment during a quick, easy, and non-	Low complexness options are most well-liked over those that need a high machine load. Unknown, because the detection system solely has access to

		identification, which needs the event of recent and efficient protection measures.	intrusive manner, through the utilization of image quality assessment.	the input sample.
4	Biometrics In Abc: Counter-Spoofing Research	Automated Border Control (ABC) is concerned with fast and secure processing for intelligence-led identification.	It indicates that the new developing trend is fusion of multiple biometrics against spoofing attacks.	Ideal ABC may have a nature of non-intrusive, efficiency, and effectiveness.
5	Fake Biometric Detection for Iris, Fingerprint and Face Recognition	To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures.	Novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts.	The problem of fake biometric detection can be seen as a two-class classification problem where an input biometric sample has to be assigned to one of two classes: real or fake.
6	A Survey Based on Fingerprint, Face and Iris Biometric Recognition System, Image Quality Assessment and Fake Biometric	This paper introduce three biometric techniques which are face recognition, fingerprint recognition, (Multi Biometric System) and also introduce the attacks on that system and by using Image Quality Assessment for Liveness Detection how to protect the system from fake biometrics.	Hardware –based schemes generally present a higher fake detection rate, at the same time software-based techniques are in general less expensive (like no extra device is needed), and less intrusive since their implementation is clear to the user.	Fingerprints have been used from long time for identifying individuals.
7	Fingerprint Liveness Detection in the Presence of Capable Intruders	Fingerprint Liveness detection methods have been developed as an attempt to overcome the vulnerability of fingerprint biometric	The design by modeling the distribution of the live samples and predicting as fake the samples very unlikely	Traditional approaches have been quite optimistic about the behavior of the intruder assuming the use of a previously

		systems to spoofing attacks.	according to that model.	known material.
8	Face Spoof Detection with Image Distortion Analysis	Automatic face recognition is now widely used in applications ranging from de-duplication of identity to authentication of mobile payment.	Popularity of face recognition has raised concerns about face spoof attacks (also known as biometric sensor presentation attacks), where a photo or video of an authorized person's face could be used to gain access to facilities or services.	Different classifiers needed for different spoof attacks.
9	Image Quality Assessment for Fake Biometric Detection: Application to Face and Fingerprint Recognition	Develop a system to enhance the security of biometric recognition framework, by providing a two stage security using finger print and face detection applications.	High level security. More efficient and accurate. Protection against the fake biometric traits. Varied usability, right from small scale companies to the government organizations.	Poor generalization ability (vulnerable to the variations in acquisition conditions).
10	Biometric Anti spoofing Methods: A Survey in Face Recognition	Spoofing, referred to by the term presentation attack in current standards, is a purely biometric vulnerability that is not shared with other IT security solutions.	It refers to the ability to fool a biometric system into recognizing an illegitimate user as a genuine one by means of presenting a synthetic forged version of the original biometric trait to the sensor.	The spoofing artefact is a 3D mask of the genuine client's face, increasing the difficulty to find accurate counter measures against them.

III. 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 analysed 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.

IV. 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

[11]. Yang, W., Huang, X., Zhou, F., et al.: 'Comparative competitive coding for personal identification by using finger vein and finger dorsal texture fusion',Inf. Sci., 2014, 268, pp. 20–32

[12]. Park, G., Kim, S.: 'Hand biometric recognition based on fused hand geometry and vascular patterns', Sensors, 2013, 13, pp. 2895–2910.

[13]. Rattani, A., Kisku, D.R., Bicego, M., et al. 'Feature level fusion of face and fingerprint biometrics'. Proc. of Int. Conf. on BTAS, 2007, pp. 1–6.

[14]. Srivastava, D.K., Bhambhu, L.: 'Data classification using support vector machine', J. Theor. Appl. Inf. Technol., 2009, 12, (1), , pp. 1–7

[15]. Dass, S.C., Nandakumar, K., Jain, A.K.: 'A principled approach to score level fusion in multimodal biometric systems'. Proc. of Audio- and Video-Based Biometric Person Authentication, 2005, pp. 1049–1058

[16]. Feifei, C.U.I., Gong ping, Y.A.N.G.: 'Score level fusion of fingerprint and finger vein recognition', Comput. Inf. Syst., 2011, 7, (16), pp. 5723–5731

[17]. Jain, A.K., Ross, A., Prabhakar, S.: 'An introduction to biometric recognition', Circuits Syst. Video Technol., 2004, 14, (1), pp. 4–20

[18]. Yang, J., Zhang, X.: 'Feature-level fusion of fingerprint and finger-vein for personal identification', Pattern Recogn. Lett., 2012, 33, pp. 623–628

[19]. Park, Y.H., Tien, D.N., Lee, E.C., et al.: 'A multimodal biometric recognition of touched

fingerprint and finger-vein'. Proc. of Int. Conf. on Multimedia and Signal Processing, 2011, vol. 1, pp. 247–250

[20]. Miura, N., Nagasaka, A., Miyatake, T.: 'Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification', Mach. Vis. Appl., 2004, 15, pp. 194–203

[21]. Kumar, A., Ravikanth, C.: 'Personal authentication using finger knuckle surface', IEEE Trans. Inf. Forensics Sec., 2009, 4, (1), pp. 98–110

[22]. Kumar, A., Zhou, Y.: 'Human identification using finger images', IEEE Trans. Image Process., 2012, 21, (4), pp. 2228–2244

[23]. Miura, N., Nagasaka, A., Miyatake, T.: 'Extraction of finger vein patterns using maximum curvature points in image profiles', IEICE Trans. Inf. Syst.,2007, 8, pp. 1185–1194

[24]. Yang, W., Yu, X., Liao, Q.: 'Personal authentication using finger vein pattern and finger-dorsa texture fusion'. Proc. of the 17th ACM Int. Conf. on Multimedia, 2009, pp. 905–908

[25]. Prabhakar, S., Pankanti, S., Jain, A.K.: 'Biometric recognition: security and privacy concerns', IEEE Secur. Priv., 2003, 1, (2), pp. 33–42

[26]. Deepak, A., Shirsat, S.: 'Multimodal biometric recognition system'. Proc. Of Int. Conf. on recent Innovations in Engineering and Management, 2016, pp.237–244

[27]. Yang, X.-S.: 'Firefly algorithm, stochastic test functions and design optimisation', Int. J. Bio-Inspired Comput., 2010, 2, (2), pp. 78–84