International Journal of Gender, Science and Technology
ISSN: 2040-0748
UGC Care Group I Journal.
Vol-13 Issue-02 July 2024

Determining the Evaluation of Biometric Signal Processing Using Computational Approach

Dr Ranjith S[1], Dr Balachandran.G[2]
[1,2]Assistant professor,
[1,2]Department of Electronics and Communication Engineering,
[1,2]Jeppiaar Engineering College, OMR, Chennai.
Email- [1]ranjithsubramanian90@gmail.com, [2] balachandran@jeppiaarcollege.org

Abstract

This research provides the literature review on the research done on unimodal biometric systems that recognize retina, ear, face, palm, finger, and knuckle prints as well as fingerprints. Additionally, a summary of the work on multimodal biometrics that dealt with various characteristics and varying numbers of traits is offered in this research. The suggested method for picture preprocessing, feature extraction, and authentication is discussed in the following research. This Research also reviews several biometric categorization techniques. Research articles are gathered from a variety of sources, and the techniques used are characterized using a feature extraction and classification framework. The biometric imaging approaches are categorized as categorization methods based on the methodologies presented in the survey studies. Additionally, each of the current biometric authentication systems' research holes and problems are detailed.

Keywords: Biometric Authentication, classification, Feature Extraction, Identification.

Introduction

For the safe identification of users, biometric authentication is essential in many businesses. The demand for biometric authentication based on computational automated approach for accessing and identifying the user as well as limiting unlawful transactions is driven by the daily rise in transactional theft, fraud, and security level breaches. The answer is obtained through biometric authentication, which offers transactional data protection and confidentiality. Many industries, including as the military, state and federal governments, border management, law enforcement, and commercial systems, among others, have a requirement for biometric authentication.

The phrases "Biometric" and "Metric," which stand for "Measurement" and "Life," respectively, are derived from Greek. In computational methods, the word "authentication" refers to verifying users for trustworthy communication. Biometric authentication is thus trustworthy and user-friendly.

Alphonse M. Bertillon presented the first biometric identification method in 1883. The author distinguished users based on attributes including height, eye colour, middle finger length, breadth and length of the ear and skull, markings and scars, and middle finger length. Because of these factors, author Benry technology stopped by author Henry's for finger print biometric recognition. Lack of Determination, Anthropometric traits might change dramatically over time. Lack of Uniqueness, It is impossible to distinguish between various people from the same background based just

on their eye color. Lack of Training, More dependable takes more time and effort. The method for biometric authentication put out by the author Jain et al. is based on the six characteristics and corresponds to biometric applications.

Related Work

Face recognition has been a dynamic study in the area of biometrics since the 1970s. The recognition algorithm finds the faces in the dataset to separate the faces after receiving a face picture as input. Face recognition systems often execute face detection first to separate the faces in an input picture that has numerous faces. Each face is preprocessed, after which a dimensional illustration is sometimes produced. For economical categorization, a low dimensional picture is essential. The fact that the face is not a hard entity and that photographs of the face are often taken from a variety of angles presents difficulties for face identification.

In 2017, David Crouse et al. showed how to utilise a facial recognition system to identify specific lemurs in a huge group. As a result, long-term study is sometimes limited to a small number of taxa for certain animal lineages. The Madagascar-endemic class lineage of lemurs is not an exception. For many species, the long-term information needed to address biological process questions is inadequate. This is at least in part because it may be difficult to accumulate consistent information about well-known individuals over extended periods of time. In this study, they provide a replacement technique for lemur individual identification (LemurFaceID). A computer-assisted facial recognition system called LemurFaceID may be used to identify specific lemurs in supported photos. To define facial images, our method used MLBP features with Scale

Invariant Feature Remodel (SIFT) features. The high spatial quality of the SIFT features might be a perfect counterbalance to overfitting and the speed of the popularisation process. As a result, the usage of SIFT choices in the final recognition system was discontinued. When used in closed-set mode, LemurFaceID demonstrated a comparably high degree of identification accuracy (98.7%; 2-query picture fusion), whereas open set mode only achieved a 95% success rate. The OpenBR framework had to be used with this method.

According to a 2003 paper by Chang et al., 200 people's 3D and 2D photos were used in PCA-based recognition trials. Due of the probes, one experiment utilises one set of later photographs for each participant, while another experiment uses a larger collection of 676 probes. Results showed that for all studies, rank-one recognition for multi-modal 3D+2D was roughly 90%, for 3D alone it was 90%, and for 2D alone it was 89%. Utilizing a weighted total of the separate 3D and 2D face area distances, the combined result was achieved. The largest experimental investigation that has ever been reported in the literature, whether it be for a single 3D face or for multi-modal 2D+3D, is this one.

The closest adjacent pixel ratio approach, which Badrinath et al. (2011) introduced, is a revolutionary contributing methodology that confirms and matches the knuckle print for biometric identification. The scaling factor of the suggested approach is accelerated by using the accelerated robust features techniques. This experiment uses the PolyU Knuckle dataset with 7920 pictures for training and testing. Finally, this approach achieved a recognition accuracy rate of 99% and an error rate of 0.21%.

According to Amraoui et al. (2012), hybrid classifiers based on both micro texture and spatial domain have a fresh contribution to make. employing the micro texture and spatial domain approaches to extract the characteristics of the global and local information of the knuckle print. The findings are classified using machine learning methods, such as support vector machines. In this experimental approach, PolyU knuckle datasets are used. The most effective performance indicators were seen in the unique contribution.

Usha and Ezhilarasan (2013) created a novel technique for knuckle print biometric authentication called Finger Back Knuckle Surface. This method's primary goal is to extract the best characteristics, such the knuckle base point, knuckle edge points, and knuckle tip points. 120 picture samples from PolyU knuckle datasets are used in this experimental effort. This method found that there was little computing complexity and good accuracy.

Gao et al. (2014) used the Competitive Coding technique to extract features from knuckle prints. Texture information and orientation characteristics are contrasted using this approach. The knuckle picture is pre-processed using the Gabor filter, and the local and global parameters are also extracted. The outcome produced as the foundation for scoring and the highest score obtained for knuckle print verification.

Delicate and composed of neural cells, the retina is located in the rear of the eye in humans. Retinas are unique, even in identical twins, since the organ is complicated and gets blood from capillaries in distinct ways. Different people may experience different things with their left and right retinas, and these differences may be permanent. Using the morphological and crossing number methods for

feature extraction, the literature suggests an authentication system based on the retina. Before extracting retinal features from the retinal image, the blood vessel in the retina is divided from the retina picture. This process creates the foreground, background, and noisy area around the retina's border. The collected details, such bifurcation and crossover, form the basis of a matched template.

The 2019 method proposed by Gawande et al. uses iris and fingerprint data for individual authentication. First, features are extracted using the Haar wavelet from the fingerprint image's ROI. In the first step, the Haar wavelet splits the fingerprint image into four sub-bands: low frequency vectors on the left, high frequency vectors in the horizontal and vertical directions on the top left, and diagonal high frequency vectors on the top right. Subsequent decomposition get the LL component after the initial decomposition, and the process continues thereafter in the same manner. A downsized replica of the initial image is created after four stages of disintegration. From this, we get a feature vector with dimensions 1 x 60. Another application of segmentation is to remove unwanted features from an iris image, such as the eyelids, sclera, pupils, and eyelashes. Applying three-level decomposition utilizing Haar wavelet transform to the final normalized, enhanced image will provide a reduced feature vector. One x sixty-five is the final dimension of the retrieved feature vector. The authentication process begins with selecting the fingerprint as well as iris feature vectors that are most similar to one another, and then uses the con-variance matrix to calculate the Mahalanobis distance among the query feature and the stored feature. In the case of fingerprints and iris scans, the discrepancy between the feature under consideration and the vector that is most similar to it is determined. Tanh, make this difference standard. A fused feature vector of size 1 x 60 is obtained

by calculating the mean value of the difference vectors for the iris and fingerprint. This combined feature vector is SVM-trained. Function for the Radial Basis For the purpose of categorizing these combined characteristics, SVM and Poly SVM are used as the two kernels. Fusing fingerprint and iris data yields a GAR of 93%, whereas feature vectors created from fingerprint as well as iris data employing the Haar wavelet transform provide GARs of 88% and 87%, respectively.

Proposed work

The accuracy of an optical review may be significantly increased by preprocessing the obtained pictures. Numerous filter approaches allow for the augmentation or diminution of a captured picture's intensity, allowing for a quicker and simpler image interpretation. With only a few clicks, an imperfect camera picture may be rectified. Image preprocessing may speed up identification while also increasing the likelihood of accurate recognition. As these photographs include a variety of undesired data for the identification process, the fresh image obtained from the digital camera is not appropriate for processing. Therefore, prior to examination, the photos are preprocessed to remove any unnecessary data. The preprocessing stage includes grey conversion, picture scaling, and binary of the image to improve image quality and create an image in which necessary characteristics can be accurately recognized.

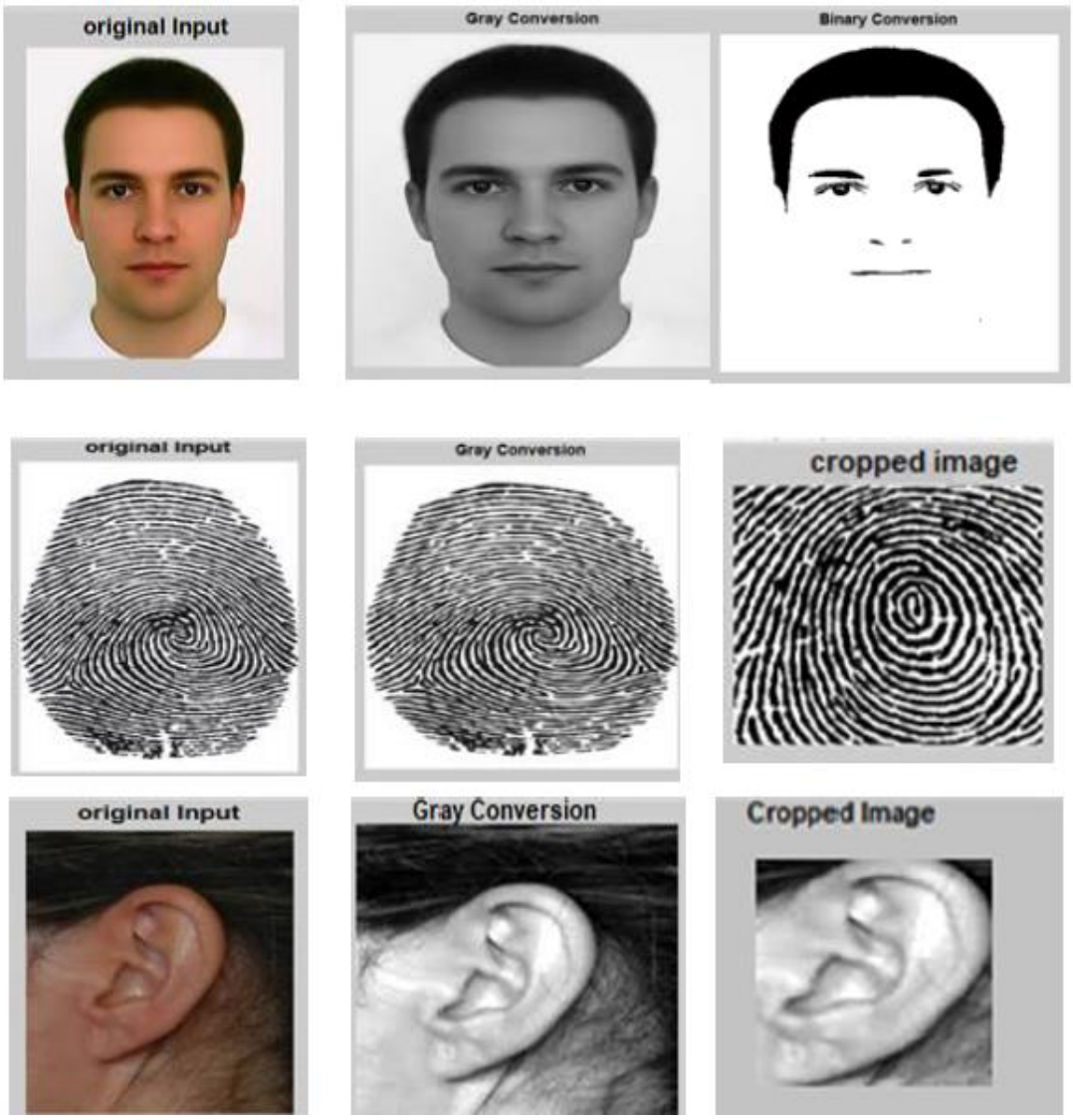

Figure 1 Sample preprocessed images RGB to Gray to Binary

Results & Discussion

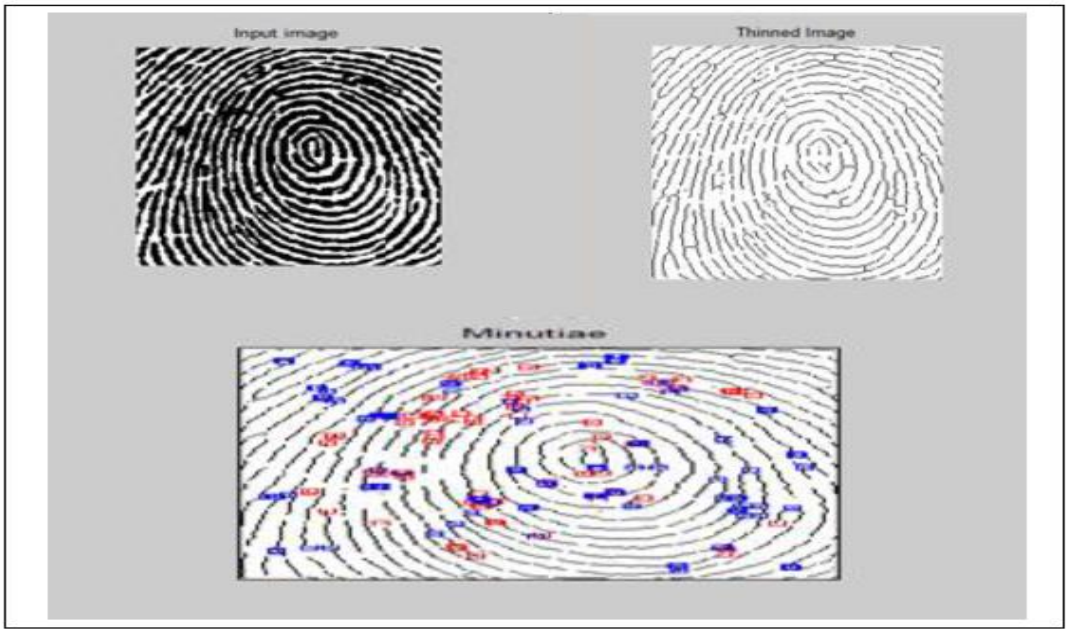

Figure 2 Resultant of Finger Print Feature Extractions (Similar for Knuckle and Palm)

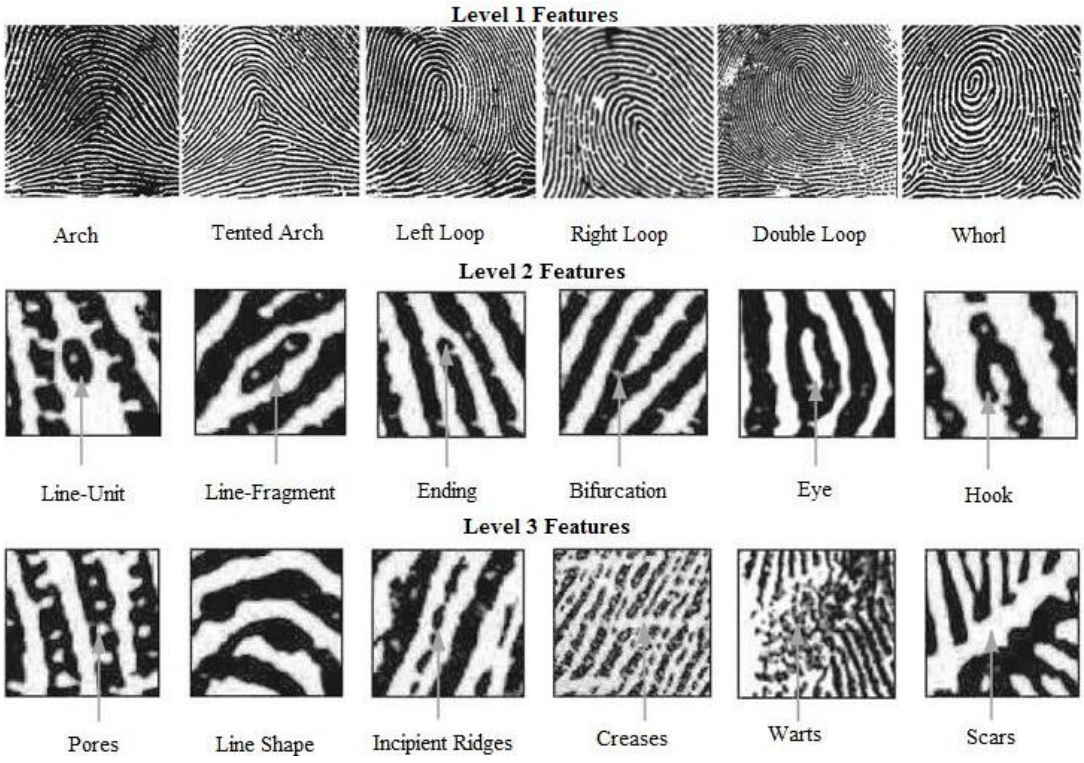

Figure 3. Level 1, 2, 3 features in Finger Prints

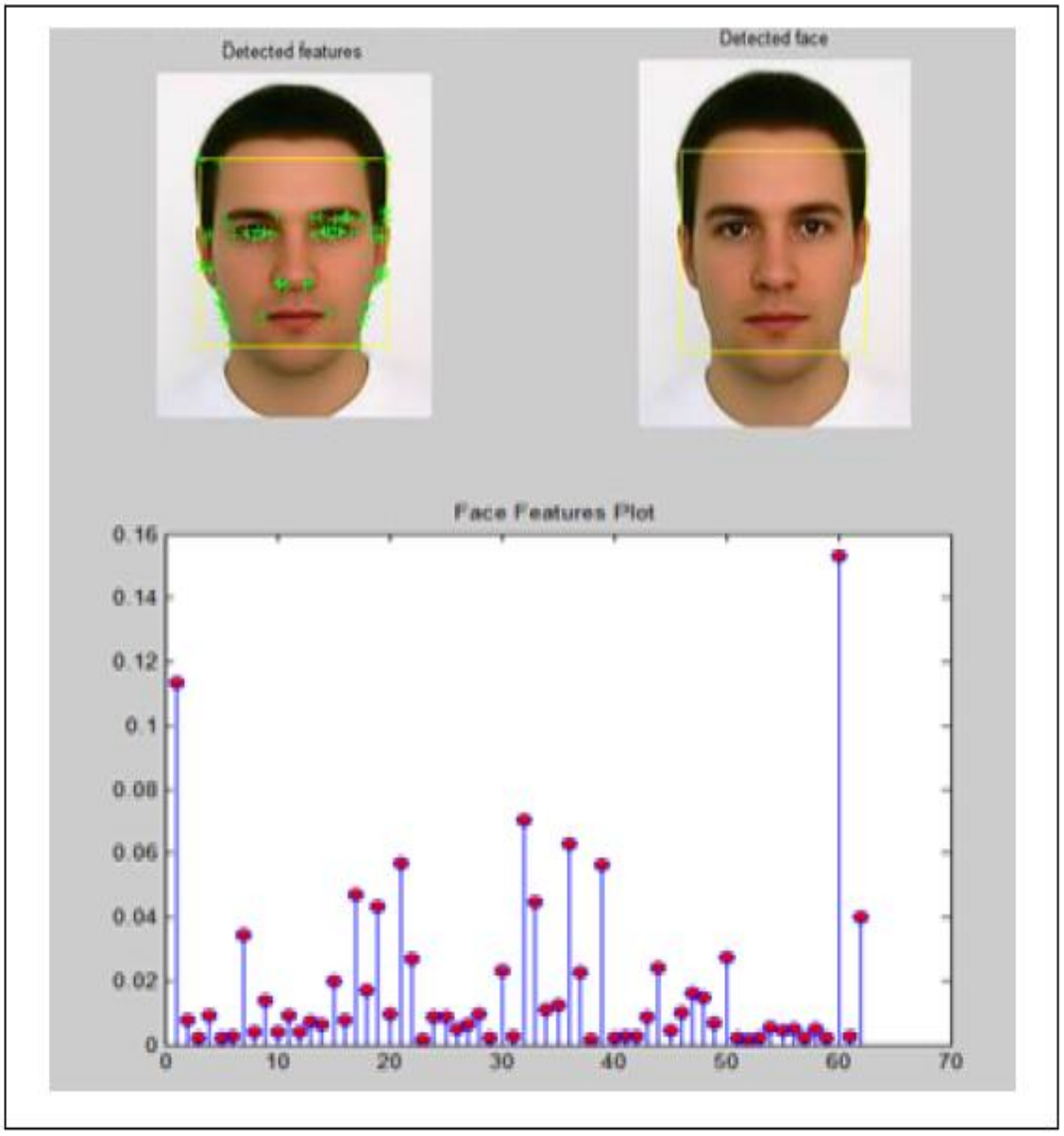

Figure 4 Resultant of Face Feature Extractions

Conclusion

This research discusses several feature extraction methods and approaches in addition to evaluating data comparisons with database templates and decision-making processes for authentication. According to the report, there have been very few attempts to authenticate someone using several biometric features. The literature review adds to the discussion of numerous methodologies used by various researchers for retina, face identification, finger print recognition, palm print recognition, knuckle print recognition, and ear recognition. However, there are several feasible, tested approaches to improve identification precision while simultaneously speeding up authentication. These techniques are noted and used in this study. The suggested method for picture preprocessing, feature extraction, and authentication is discussed in the following Researchs. This Research also reviews several biometric categorization techniques. Research articles are gathered from a variety of sources, and the techniques used are characterized using a feature extraction and classification framework. The biometric imaging approaches are categorized as categorization methods based on the methodologies presented in the survey studies. Additionally, each of the current biometric authentication systems' research holes and problems are detailed.

Reference

1. Almabdy S and Elrefaei L. 2021. An Overview of Deep Learning Techniques for Biometric Systems Artificial Intelligence for Sustainable Development: Theory, Practice and Future Applications. 10.1007/978-3-030-51920-9_8, (127-170).
2. Surabhi Hom Choudhury, Amioy Kumar, Shahedul Haque

Laskar, Biometric Authentication through Unification of Finger Dorsal Biometric Traits, Information Sciences, Volume 497, 2019, Pages 202-218.

3. Laimeche L, Meraoumia A, Houam L and Bouchemha A. 2021. An Effective Framework for Secure and Reliable Biometric Systems Based on Chaotic Maps Pattern Recognition and Artificial Intelligence. 10.1007/978-3-030-71804-6_23, (314-328).
4. Hammad, M.,and Wang, K. (2019), "Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network", Computers & Security, Vol. 81, pp. 107–122.
5. Conti V, Rundo L, Militello C, Salerno V, Vitabile S and Siniscalchi S. (2020). A multimodal retina-iris biometric system using the Levenshtein distance for spatial feature comparison. IET Biometrics. 10.1049/bme2.12001.
6. Shahreza H and Marcel S. (2021), Towards Protecting and Enhancing Vascular Biometric Recognition Methods via Biohashing and Deep Neural Networks. IEEE Transactions on Biometrics, Behavior, and Identity Science. 10.1109/TBIOM.2021.3076444, 3:3, (394-404).
7. Choras, M. and Kozi, R. (2012), "Contactless palmprint and knuckle biometrics for mobile devices", Journal of theoretical advances, Vol.7, pp.73-85.
8. Connolly, J.F., Granger, E. and Sabourin, R. (2012), "An adaptive classification system for video-based face recognition", Journal of

information sciences, Vol.192, pp.50-70.

", International Journal of Biometrics, Vol.11, No.3, pp.257 – 273.

9. Subhashini, K.R. and Satapathy, J.K., (2017), "Development of an Enhanced Ant Lion Optimization Algorithm and its Application in Antenna Array Synthesis", Applied Soft Computing, Vol. 59, pp.153-173.
10. Arora S and Bhatia M. 2021. Challenges and opportunities in biometric security: A survey. Information Security Journal: A Global Perspective. 10.1080/19393555.2021.1873464, (1-21).
11. Zhang L, Zhang L and Zhang D (2010), "Monogenic code: a novel fast feature coding algorithm with applications to finger-knuckle-print recognition", Journal of pattern recognition, Vol.1, pp.1-4.
12. Zhang L, Zhang L, Zhang D and Guo Z (2012), "Phase congruency induced local features for finger-knuckle-print recognition", Journal of pattern recognition, Vol.45, pp.2522-2531.