Finger-Vein as a Biometric -Based Authentication

Mohan D N[1], Mouna. G[2], Nagaveni. E[3]
[1]*Assistant Professor, Department of Information Science and Engineering, Nagarjuna college of Engineering and Technology, Banglore, India*
[2,3]*B.E. Student, Department of Information Science and Engineering, Nagarjuna College of Engineering and Technology, Banglore, India*

***Abstract*— With the evolution of consumer electronics, personal private information stored in the consumer Electronics (CE) devices are getting more valuable. To protect private information, Biometrics technology is subsequently equipped with the CE devices. Finger-vein is one of the biometric features, which is gaining popularity for identification recently. This article proposes a twofold finger-vein authentication system. The first stage of the identification process uses skeleton topologies to determine the similarities and differences between finger-vein patterns. Some extreme cases with ambiguous features cannot be successfully classified. Hence, the image quality assessment (IQA) is employed as the second stage of the system. Furthermore, to overcome the computational requirement of the algorithm, the GPU is adopted in our system.**

***Index Terms*—Consumer electronics, Image quality assement (IQA), Biometrics, Finger-vein**

1. INTRODUCTION

Personal identification technology is widely used in area access-control, e- control, e-commerce, and multimedia content in CE devices. Biometrics, which uses human physiological or behavioral features for identifying individuals, has attracted attention and is becoming one of the most popular and promising alternatives to the keys, PIN numbers, or traditional password. In the area of biometric identification, convenience and security of the system are important. In addition, the system requires high accuracy and fast response time. Thus, various types of human characteristics have been investigated as the keys of the biometrics, such as fingerprints,1 facial features,2 iris,3 voice, finger-vein,4 and palm print.

The finger-vein has the following features:
1)The vein is hidden inside the body and is mostly invisible to human eyes. 2) The no incursive capture method. 3) The finger-vein can be only taken from a live body. Hence, it is an intrinsic feature that is difficult to forge and steal. Similar to the iris biometrics, it has excellent performance an security. Therefore, the finger-vein recognition system is subsequently developed and is becoming one of the emerging technologies of the biometric authentication.

There are several approaches for finger- vein recognition systems, which have been proposed to improve both reliability and efficiency in recent years. A finger-vein matching method based on feature-level fusion and k-support vector machine classifier is available. However, the complicated mathematical operation requires that the execution time needs to be 5s for every frame. Therefore, we propose a twofold finger-vein recognition system, which incorporates the skeleton topology and the IQA to generate a better recognition performance with high efficiency. Furthermore, since the finger-vein matching time increases linearly with the size of the finger-vein database, the processing time will become unacceptably long when the system needs to provide a result in a short time. Hence, a many-core GPU is adopted to improve the matching process and keep the same accuracy.

2. DISADVANTAGES OF EXISTING SYSTEM

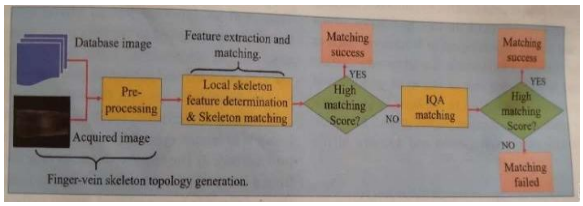
- Finger print- Using the fingerprint scanner does not take into consideration when a person physically changes.
  A person's finger changes sizes or form/pattern over time and the fingerprint scanner does not take this into consideration.
- The cost of computer hardware and software programs can be expensive.

- Using the fingerprint scanner can lead to false rejections. This biometrics device does not always read an individual's fingerprint accurately, could therefore refuse access to an employee. In certain cases, an employee may have not placed their fingerprint in the right spot or placed the left finger instead of the right and vice versa. During this scanner falsely rejects the employees fingerprint.
- Face recognition- 2D face recognition can be insecure and prone to spoofing.
  Exposed biometric modality. People can be recognized from a distance which can lead to privacy issues.
- Voice recognition – Prone to spoofing with recorded or imitated voice sample.
  May not be suitable for high security applications when used as only method of identification.
- Iris recognition- It is intrusive and expensive to setup, deforms non- elastically as pupil changes size.

As it is the case with most technology powered systems, biometric identification has its own set of advantages and disadvantages. However, it always depends on a particular use case that it will be more advantageous or disadvantageous if deployed. As more and more biometric systems are deployed, they are expected to become even cheaper with increased production and economy of scale.

3. PROPOSED FINGER-VEIN RECOGNITION METHOD

The entire procedure of the proposed system has three steps. 1) Finger-vein skeleton topology generation. 2) Feature extraction and matching. 3) IQA matching. The first stage is preprocessing and finger-vein skeleton generation for the input image and entire database. In the second step, most of the finger-vein patterns are matched with the input. The third step adopts IQA to determine the ambiguous cases.



Finger-Vein skeleton topology Generation.

The figure below has the overview of the vein skeleton generation process. Before the matching, the finger-vein image is separated from its background in the preprocessing stage. Subsequently, the ROI is extracted based on the contour of the finger. For a given image I(u,v) with the size of hxw, the ROI extraction is defined as:

$I(u,v)= \{ I(u,v),$

$\{ \text{If } \text{Argmin}u(Ic)<=u<=\text{Argmax}u(Ic)$

$\{ 0, \text{otherwise}$

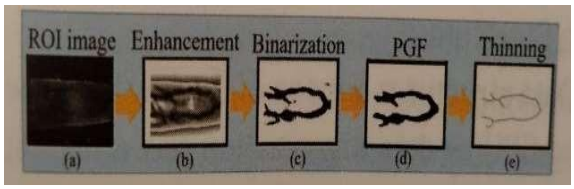


Fig 3.1

In the above mentioned expression, u and v denote the row and column index of the pixel; *h* and *w* denote the height and width of the image. Ic =1,…..,w denotes each column of the image. For ecan column of the image, the minimal and maximal differences, min(Ic) and max(Ic), between two neighboring pixels are computed. min(Ic) and max(Ic) represent the top and bottom contours of the finger for each column, respectively. The pixels between two contours belong to the ROI of the image, termed Iroi.

After ROI extraction, the segmented finger-vein image is then enhanced by using local histogram equalization to improve its contrast, as shown in fig 3.1(b). Subsequently, the binarization is applied to generate the binary vein patterns for the further extraction of the vein skeleton. The peer group filter is typically used to reduce noises in the image processing, and it is adopted to refine the binary vein patterns by removing those unwanted noises; fig 3.1(d) shows an example of denoising process. Afterward, the morphological thinning algorithm is applied for obtaining the vein skeletons topology.

Feature Extraction and Matching.

To recognize the skeleton topologies, the detection method is adopted from the work for feature points detection i.e., determining end points and a bifurcation point. For an image, the skeleton is composed of a node Ni and its connectivity, which can be defined by a ring operation, Ne(Ni).

Subsequently, the sum of Euclidian distances between Ni and Ne(Ni) is computed and employed for the further comparison between the input sources and database. In figure 3.2(c)below, the left most skeleton pixel(green circle)is first detected as the start point s and origin of coordinate(0,0). Every bifurcation and ending point are detected for calculating the distance. If the locations of the bifurcation or ending points of the input and database images are nearby, the coordinates of these locations are collected to generate the sum of Euclidean distances(purple arrow), as shown in the fig 3.2(d).

Next, a reasonable search radius is defined to reduce the search time and enhance the recognition accuracy rate. The position of the search radius corresponds to coordinates of the input skeleton node. First, the search radius is useful for matching each local skeleton feature in the input topology; when the number of matched local skeleton features is low, the computation time can be reduced considerably. Second, the skeleton topology can be successfully matched to various patterns through a large number of the mismatched nodes. In addition, some nodes exhibit the same topology, but such nodes are discarded if they are out of the search radius. Therefore, a search radius is defined to limit the position of skeleton nodes for preventing the mismatch caused by the similarity in the local skeleton features. Subsequently, the minimum difference between each skeleton node and its comparison candidates is determined by matching the local skeleton features between the input and database images. The difference of length of the Skelton is denoted as Di, which is obtained by calculating the difference of Ei belonging to the corresponding skeleton nodes as

Di = *min abs(Eiin – E* ^{db}*) EKdb € SC(Ni)*

where Eiin and Ekdb are the Euclidean distances of input and database

SC(Ni) indicates the local skeleton features in the search radius belonging to the input skeleton nodes Ni. If Di is lower than the user defined threshold Td, the input skeleton node is considered as a matched node; otherwise, it is not matched. The skeleton matching score Svskm is defined as: Svskm =nm/nall, where n all denotes the number of skeleton nodes extracted from an image, nm denotes the number of the matched skeleton nodes after the minimal difference is determined.

There are some extreme case that may affect the generated skeletons due to the design of the device and the finger displacement during image acquisition by the user, which may lead to method is adopted to yield a more stable and precise recognition result.

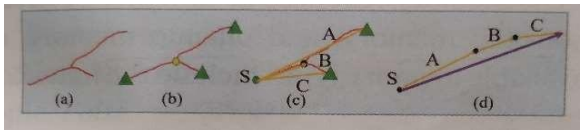


Fig 3.2 (a) Skeleton image. (b)Point detection. (c)Ring operation of a node.(d)Sum of Euclidean distances.

4. PERFORMANCE EVALUATION

Accuracy is a measure of how well the system is able to correctly match the biometric information from the same person and avoid falsely matching biometric information from different people. False acceptance rate (FAR) measure represents the degree or frequency where biometric information from one person is falsely reported to match the biometric information from another one. False rejection rate (FRR) measure represents the frequency of cases when biometric information is not matched against any records in a database when it should have been matched because the person is in the database. Therefore, for accuracy, FAR and FRR must be low. The point at which FAR and FRR intersects, that value is called Equal Error Rate (EER). EER of any system gives system performance independent of the threshold. Hence, lower the EER, better the system performance.

In the skeleton matching and IQA matching, the corresponding EER is 1.88% and 3.77%. After combining these two methods, the hybrid scheme achieved an EER of 0.94%. The proposed IQA algorithm adequately compensated for the weakness of the proposed skeleton matching and improved the performance of the overall recognition system. Furthermore, the hybrid scheme registered a competitive EER compared with other methods. In Table evaluation, although the EER of the method in is better, the proposed method offers up to five times faster on recognition speed, which indicates that the proposed method performs better under similar recognition accuracy.

5. CONCLUSION

The proposed system employs the vein skeletons and the IQA to recognise the similarity of the finger-vein patterns of individuals. The experiment results demonstrated that the presented system achieves higher performance levels compared with other finger-vein recognition systems. Furthermore, the system takes the advantage of GPU to improve the matching process in a reasonable amount of time for the large database with the same accuracy.

REFERENCES

[1] A. Majumder, J. Goswani, S. Ghosh, R. Shrivastawa, S. P. Mohanty and B. K. Battacharya, "Pay-Cloak: A biometric back cover for smart phones: facilitating secure contactless payments and identity virtualization at low cost to end users," IEEE consum. Electron. Mag., vol. 6, no. 2, pp. 78-88, Apr.2017.

[2] J. Chen, F. Shen, D. Z. Chen, and P. J. Flynn, "Iris recognition based on human-interpretable features,"

[3] S.Veluchamy and L. R. Karlmarx, "System for multimodal biometric recognition based on finger knuckle and finger vein feature-level fusion and K- support vector machine classifier," IET (Inst.Eng. technol.)Biometrics vol.6,pp. 232-242, 2017.

[4] D. Wang, J. Li, and G. Memik, "User identification based on finger-vein patterns for consumer electronics devices," IEEE Trans. Consum. Electron. Vol.56, no. 2,pp. 799-804, May 2010.