ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

HAND VEIN BIOMETRIC RECOGNITION USING REPEATED LINE TRACKING METHOD

P.Jagadeesh[1], B.Bhuvaneswari[2]
[1,2]Assistant Professor Department of Electronics and Communication Engineering,
Saveetha School of Engineering, Saveetha University, Chennai-602105, India.
Email: pjagadeesh89@gmail.com

Received on: 10.08.2016 *Accepted on: 06.09.2016*

Abstract

The credential part of this project is to perform personal verification and identification based on hand geometry recognition. The previous system consists of the manual verification and identification of user information's like name, customer id, digital signature, photograph, etc. This enhances the accuracy of the design using MATLAB by measuring the length and width of the fingers. Using the palm recognition the enhancement is done where the length and width of the finger bone is measured and compared with the value which is already stored in the database. using canny edge detection algorithm. The length and width of the finger bone is measured. As it lies unique for each and every individual This proposal uses biometric-identification technique to measure the length and width of the finger bone . The main advantage of this system is to provide high security to the lockers and the Processing time required to do the operation is very less compared to the already previously system. The disadvantage with the existing system is that if the key is lost, replacement of key takes a long process until the user cannot access the locker. Changes for key to get stolen and hacking of locker also happens these all disadvantage is to overcome in our system.

Key Words: Repeated line tracking method, Canny edge algorithm, Booth multiplier

Introduction:

In the existing system lockers are opened using two keys, where one key is with bank manager and other with the user. If the user wants to open the locker then first the manager should key that is key1 should be used to open the locker and then the user's key that is key no 2 is used to open the locker. Once the manager inserts his key and opens the locker he leaves the user inside the room alone and goes out, only the room user knows what are the things available in the locker.

The things in the bank locker need not be given to the banker since it is a private locker only user has to know the things available so that there is no possibility of stealing of users belongings is really difficult for others it lies highly securable the advantages as user can open the locker only if the manager checks and verifies user details and opens the locker he acts as key 1 for the locker then user acts as key 2 and opens the lockers. The major disadvantage is that it takes long times because it is a manual, if key 2 is lost replacement takes a long process. Another disadvantage is that there may be a possibility of key to get lost or stolen. Once any other takes the key and try to open the locker it is not possible but also person who are in smuggling can go with other possibility of hacking options to open the locker. Hence in order to overcome all these disadvantages we are using a hand vein recognition system which is a new technology to be used in this field for security purposes. Finger recognition is also under the biometric recognition but it is commonly used hence to use a new concept we are going for hand vein recognition system.

Biometric Identification:

This process is very efficient because it deals with the parts of human beings for identification where it is unique for each and every individual. Our system also deals with one of the biometric features which are calculating the finger vein. The finger vein is different for each and every individual hence verification and identification using this biometric property lies efficiently and improves the security of human beings.

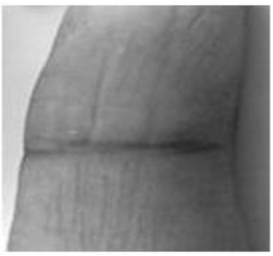

Figure 1 Model of Scanned Image.

The identification is done using vein. The hand is first scanned to obtain the image of the vein and using the vein the identification and recognition of an individual is being made.

Enrollment Process

The test subject's hand is scanned using an image capturing equipment like an x-ray scanner. The captured image is then normalized by converting into pixel values. The normalization of image is done so that the user can place his palm easily over the scanner no rules should be maintained by the user this really lies as a main advantage for the user. Hence taking

picture at each 10 degree can be cancelled. Taking extra images can be neglected so verification process takes only a small operation time.

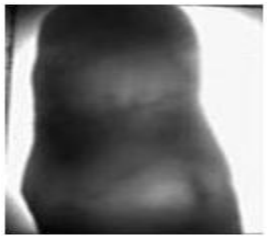

Figure 2 Captured Scan Image.

Verification Process

The generate code is stored in a database. As and when required the database can be looked for verification. Whenever the person wants to be authenticated his hand is scanned again and pixel value is generated. The generated code is cross checked with that stored in the database. If it exists the person is authenticated else rejected. The block diagram for this process is shown below.

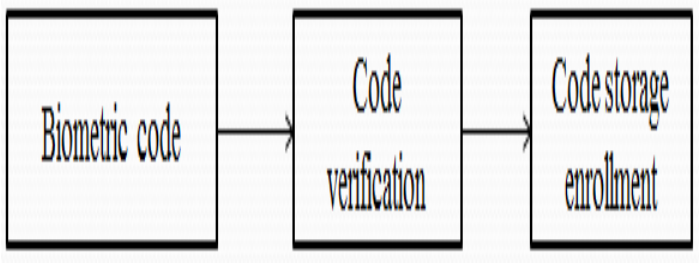

Figure 3 Block Diagram of Enrollment Process.

First the scanner which is a biometric device scans the hand image of the user and it does the process of enrollment and converts it into pixel value and is stored as a code when this code matches with the values in the database the user verification is done and is identified as correct person and opens the door else it rejects and leaves a warning message to the manager.

System Flow Diagram

For successful identification of a person, the person's hand should be scanned as an image within an acceptable resolution. Any image before processing is pre-processed by resizing. The scanned hand image is normalized by converting it into gray shade to reduce the matrix dimensions. Normalized image is processed further by converting it into pixel value using canny edge detection algorithm. This acts as a unique code for authentication. The first step in the process flow graph is that the image is scanned and to resize the image the normalization of the image. To extract only

the necessary parts in the image and to remove unnecessary parts and also to remove the noise in the image median filter is used to remove noise in the image.Normalization involves resizing and converting it into gray and binary images. Then Gaussian filter is used to remove noise in the picture and pixel value is calculated along with which the finger vein score value is calculated and is stored in the database. Further recognition and verification process takes place. All the vein is taken into consideration and score values is calculated for authentication. The veins are taken into consideration because one vein may lie similar for each and every individual.

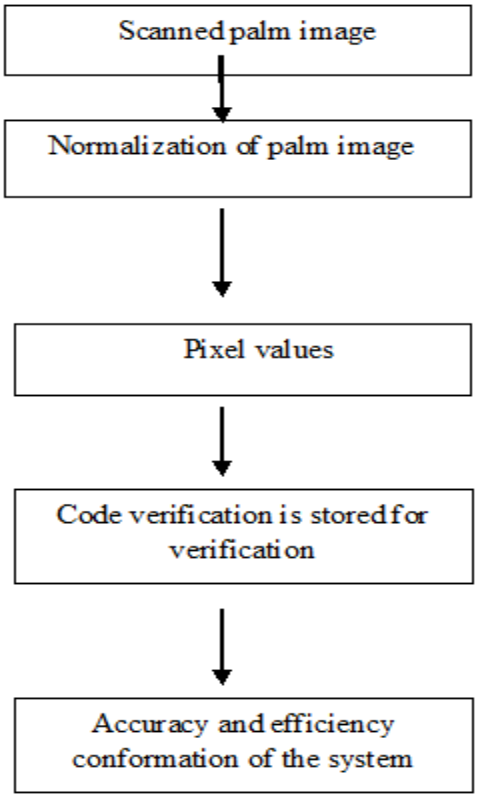

Figure 3 System Flow Graph.

Canny Edge Detection Algorithm

The purpose of edge detection in general is to significantly reduce the amount of data in an image, while preserving the structural properties to be used for further image processing. Several algorithms exists, and this worksheet focuses on a particular one developed by John F. Canny (JFC) in 1986. Even though it is quite old, it has become one of the standard edge detection methods and it is still used in research.

The aim of JFC was to develop an algorithm that is optimal with regards to the following criteria:

1. Detection: The probability of detecting real edge points should be maximized while the probability of falsely detecting non-edge points should be minimized. This corresponds to maximizing the signal-to-noise ratio.

2. Localization: The detected edges should be as close as possible to the real edges.

3. Number of responses: One real edge should not result in more than one detected edge

Results and Discussions

Codes generated from the image are pixel, vein score values. These values are stored in MATLAB database. Since the scanned palm images used for verification are the same, the codes generated are the same. The same code is compared with that in the database. The score values and the threshold values are already stored in the database. The threshold value is an 8 bit value which lie between 0 to 255. All the veins in the image is calculated and taken into consideration to calculate the score value and threshold value. Only one vein can be taken into consideration but it may lie same for some individuals in order to overcome that all the veins are taken into consideration to calculate the score value and for verification and identification process. Only the values of the images stored in the database can be used for matching and if any changes should be made the user has to update the information. If the image matches with the image in the database, the user is allowed (i.e.) authenticated checkbox will be displayed on the screen and if the image does not matches, unauthenticated check box is displayed on the screen and the alarm alarms.

Output

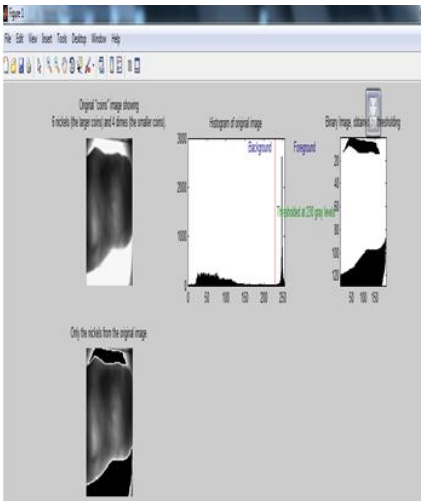

Figure 4 Different Types of Images Conversion.

Code Comparison

Biometric identification fits squarely in the classical framework of statistical decision theory. Yes/No pattern recognition decision have four possible outcomes: both a given pattern is, or is not, in fact the target; and in either case, the decision made by the recognition algorithm may be either the correct or the incorrect one. In a biometric decision context the four

possible outcomes are normally called-false accept (FA), correct accept (CA); false reject (FA) and correct reject (CR). Obviously the first and third outcomes are errors (called type I and type II respectively), whilst the second and fourth outcomes are the ones sought. By manipulating the decision criteria as required, the relative probabilities of these four outcomes can be adjusted in a way that reflects their associated costs and benefits. These may be varying in different applications. In a business point of view the customer cost of a FR error, whereas just the opposite may be true in a military or nuclear context.

Conclusion

The system developed was able to compute pixel values with the precision, but the reconstructed image produces a high accuracy. The image values are calculated and the calculated threshold and score values are stored in the database. The database values are stored in the database for identification and verification process. The verification is done in such a way that all the veins are taken into consideration in order to do authentication process. All the veins are taken into consideration for the cause that one vein may lie same for each and every individual will leads to wrong authentication of user hence all these veins are taken into consideration for accurate authentication of the user. The accuracy in the system is increased up to above 99% in this technique.

Figure 5 vein detection image.

The extracted parts in the image are done under a process of Gaussian filter to remove the noise in the figure to remove the unwanted portions in the filter. When the score values of veins get stored in the database the vein values are calculated and compared with the values in the database for verification andidentification process. The images value gets stored in the database and if the new image appears it get compared and verification and identification is done and authentication is done. If the authentication is done a checkbox appears as access is allowed and if the images does not matches with the value stored in the database and checkbox appears as access is denied and the alarm alarms. The extracted vein image looks as the output.

References

1. R. P.Wildes, “Iris recognition: An emerging biometric technology,” *Proc.IEEE*, vol. 85, no. 9, pp. 1348–1363, Sep. 1997.
2. K. R. Park and J. Kim, “A real-time focusing algorithm for iris recognition camera,” *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 35, no. 3,pp. 441–444, Aug. 2005.
3. T. Tan, Y. Zhu, and Y. Wang, “Iris Image Capture Device,” Chinese Patent 2 392 219, Jul. 22, 1999.
4. CASIA Iris Image Database. [Online]. Available: http://www.cbsr.ia.ac.cn/IrisDatabase.htm
5. P. Shi, L. Xing, and Y. Gong, “A Quality Evaluation Method of Iris Recognition System,” Chinese Patent 1 474 345, May 22, 2003.
6. “Iris recognition in focus,” *Biom. Technol. Today*, vol. 13, no. 2, pp. 9–11, Feb. 2005.
7. [Online]. Available: http://www.iriscan.com/index.php
8. [Online]. Available: http://www.oki.com/jp/FSC/iris/en/
9. [Online]. Available: http://www.lgiris.com
10. Polat, Yıldırım, "Hand Geometry Identification without Feature Extraction by General Regression Neural Network", Expert Systems with Applications: An International Journal, Vol .34, No.2, pp. 845-849,February 2008.
11. X. He, J. Yan, G. Chen, and P. Shi, “Contactless autofeedback iris capturedesign,” *IEEE Trans. Instrum. Meas.*, vol. 57, no. 7, pp. 1369–1375,Jul. 2008.
12. M.Adan, "Biometric verification/identification based on hands naturallayout", Image and Vision Computing, Vol.26, No.4, pp. 451-465, 2008.
13. A. Ross, R. Pasula, and L. Hornak, “Exploring multispectral iris recognition beyond 900 nm,” in *Proc. Conf. Comput. Vis. Pattern Recognit. Workshop*, 2006, pp. 1–8.
14. M. Vilaseca, R. Mercadal, J. Pujol, M. Arjona, M. de Lasarte, R. Huertas,
15. M. Melgosa, and F. H. Imai, “Characterization of the human iris spectralreflectance with a multispectral imaging system,” *Appl. Opt.*, vol. 47,pp. 5622–5630, Oct. 2008.

16. M. J. Burge and M. K. Monaco, “Multispectral iris fusion for enhancement, interoperability, and cross wavelength matching,” in *Proc.SPIE—Algorithms Technologies Multispectral, Hyperspectral, Ultraspectral Imagery XV Conf.*, Orlando, FL, Apr. 13, 2009, vol. 7334, pp. 73341D-1–73341D-8.
17. H. T. Ngo, R. W. Ives, J. R. Matey, J. Dormo, M. Rhoads, andD. Choi, “Design and implementation of a multispectral iris capture system,”in *Proc. 43rd Asilomar Conf. Signals, Syst. Comput. Conf. Rec.*, 2009, pp. 380–384.
18. Y. Gong, D. Zhang, P. Shi, and J. Yan, “High-speed multispectral iris capture system design,” *IEEE Trans. Instrum. Meas.*, vol. 61, no. 7,pp. 1966–1978, Jul. 2012.
19. [Online]. Available: http://www.crossmatch.com/i-scan-2.php
20. [Online]. Available: http://www.iritech.com/products/IriTerminal.html
21. [Online]. Available: http://www.cogentsystems.com/cis202.asp
22. [Online]. Available: http://www.newscaletech.com/M3-F.html
23. J. R. Matey, O. Naroditsky, K. Hanna, R. Kolczynski, D. LoIacono,S. Mangru, M. Tinker, T. Zappia, and W. Y. Zhao, “Iris on the move: Acquisitionof images for iris recognition in less constrained environments,” *Proc. IEEE*, vol. 94, no. 11, pp. 1936–1947, Nov. 2006.
24. K. Hollingsworth, K. Bowyer, and P. Flynn, “Pupil dilation degrades irisbiometric performance,” *Comput. Vis. Image Understand.*, vol. 113, no. 1, pp. 150–157, Jan. 2009.
25. Marcos Faundez-Zanuy, "Authentication of Individuals Using Hand Geometry Biometrics: A Neural Network Approach", Neural Processing Letters, Vol.26, No.3, pp.201-216, 2007.