Simulation of Biometric Encryption Using FP

POOJA UPPAL, MRS. AYUSHI
HINDU COLLEGE OF ENGINEERING, SONEPAT, HARYANA

Abstract- The biometric based security has been upgraded in this research paper. Here the advance three dimensional biometric system has been proposed. In case of traditional 2d system there were only single 2dimension image for comparison. But in traditional 3d there are two different 2 dimensional images for comparison. Thats why it was more secure. But it took more time as well as more space as compare to traditional 2d work. The best among them is canny based edge detection. The proposed work is fast during comparison process as only important edges have been compared.

Keywords- Biometrics, Matlab, Simulation, Figure Print

I. INTRODUCTION

Biometrics

The biometric based security has been divided on the bases of physiological and behavioural characteristics. The physiological characteristics consists of face, DNA, iris and finger recognition based biometric systems. But the behavioural characteristics involve keystroke, voice and signatures. The theme of this paper is to introduce the concept of security in cloud computer with biometric techniques.

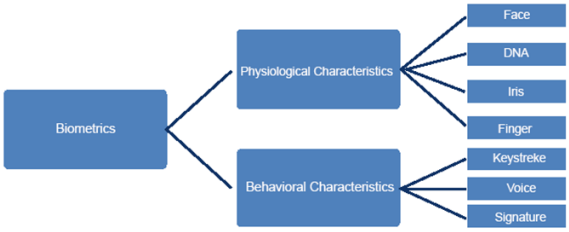

Fig.1: Physiological versus Behavioural characteristics

Finger Print

This system involve guide a fingerprint image of a human & records its advantage like arches, whorls, & loops along with outlines of edges, minutiae & furrows. Matching of Fingerprint could be attained in three ways, like minutiae, correlation & ridge

1. Minutiae based fingerprint matching stores a plane includes a set of points & set of points are corresponding in template & I/p minutiae.
2. Correlation based fingerprint matching overlays two fingerprint images & association among equivalent pixels is calculated.
3. Ridge feature based fingerprint matching is an innovative method that captures ridges, as minutiae based fingerprint capturing of fingerprint images is difficult in low quality.

To imprison fingerprints in current methods employ visual sensors that use a CMOS image sensor or CCD; solid state sensors work on principle of transducer technique using thermal, capacitive, piezoelectric sensors or electric field; or ultrasound sensors work on echography in which sensor sends acoustic signals through transmitter near finger & captures signals in receiver.

II. TOOLS & TECHNOLOGY

Edge Detection

In order to make the biometric detection fast we need the use of Edge detection mechanisms. These may be canny, sobel, prewitt and Robert. The best among them is canny based edge detection. The physiological characteristics are considered in this research the objective of research is to provide fast and more efficient biometric security to the cloud based systems.

In this system in canny based edge detection by John Canny contemplate mathematical difficulty of deriving an optimal smoothing strainer given criteria of detection, minimizing & localization multiple responses to a single edge. He showed that optimal filter given these assumptions is a sum of four rapidly growing terms.

He also showed that this filter could be well approximated by first-order unoriginal of Gaussians. Canny also introduced notion of non-maximum suppression, which means that given pre smoothing filters, edge points are as points where gradient magnitude assumes a local maximum within gradient direction.

The Expression for zero crossing of second derivative along pitch direction was first proposed by Haralick.[9] It took less than two decades to find a modern geometry variation meaning for that operator that links it to Marr–Hildreth (zero crossing of Laplacian) edge detector. That observation was presented by Ron Kimmel & Alfred Bruckstein.

III. PROPOSED WORK

In proposed work to provide security to the biometric data is acquired & analyzed & validated after transmission, signal processing, decision making & storing. Matlab has been used as simulation environment. In order reduce the size of image and comparison time edge detection techniques such as canny algorithm would be used to find edge of samples & get matrix representation of stored images of faces or Finger prints. Then various graphical techniques would be used to compare & comparison would be represented in form of Histograms.

Data Acquisition

Data collection involves use of sensors to detect & measure an individual's physiological or behavioural characteristics. Biometric feature must have following characteristics:- Universality, which means that every person should have characteristic, Uniqueness, two persons should not have same term or measurement of characteristic Permanence, characteristic should be invariant with time, Measurability.

Validity Of Test Data

Here, it checks for validity of processed data & decides whether person is authorized or not. Testing biometrics is difficult, because of extremely low error rates involved.

PROPOSED MODEL

In our proposed work we have integrate cloud with database, remote application with biometric based security. The objective of proposed work is to reduce the time consumption during sample comparison as well as the size of biometric samples.

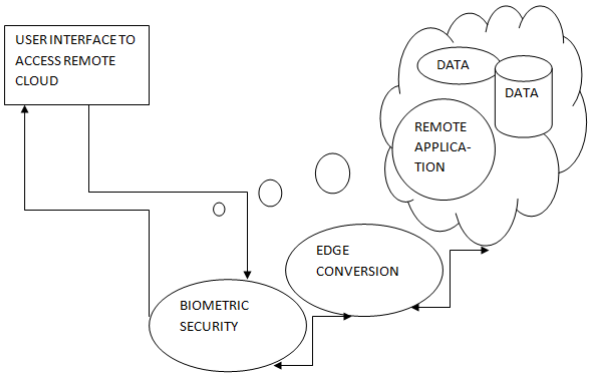

Fig.2: Proposed Model

IV. RESULT & DISCUSSION

The following window appears when we run the project. Here we could set the id, name, gender, address , contact no of person. The image of finger print is stored in image base from this interfaces. The images of finger print stored previously are compared with present finger prints. The time taken comparison in case of 2D, tradition 3d and proposed 3d is represented here. Moreover the size of file is also compared.

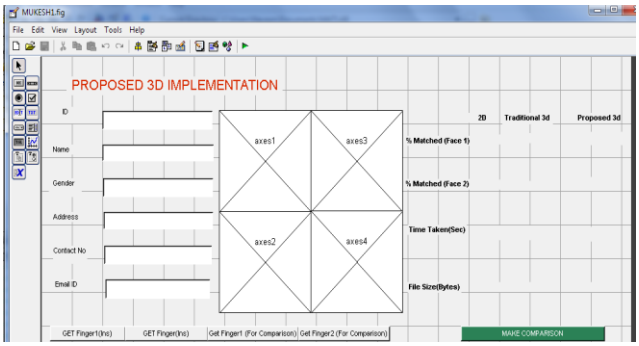

Fig.3: Design View of Proposed Work

In following window present the capturing of image and comparison is several cases.

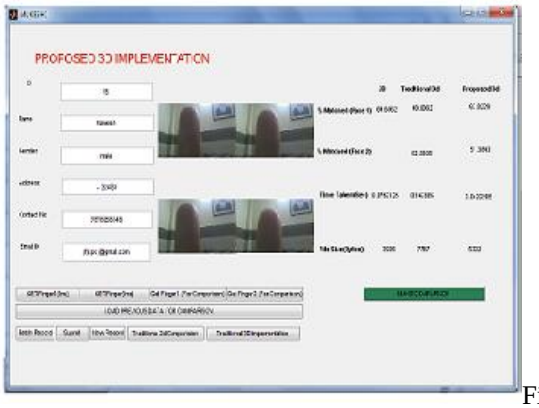

Fig .4: Implementation of Proposed Work

The following window represent the edge detection during comparison of image. This would reduce the size of image.

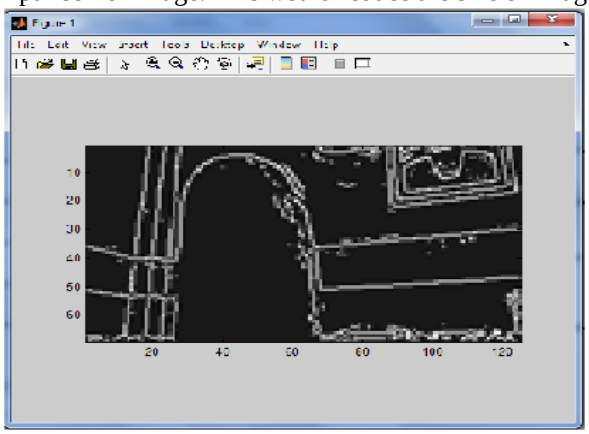

Fig.5: Edge detection applied during comparison

If the comparison is successful then the following window appears for encryption of image. This system would allow user to encrypt and decrypt image. User is free to choose image according to his choice

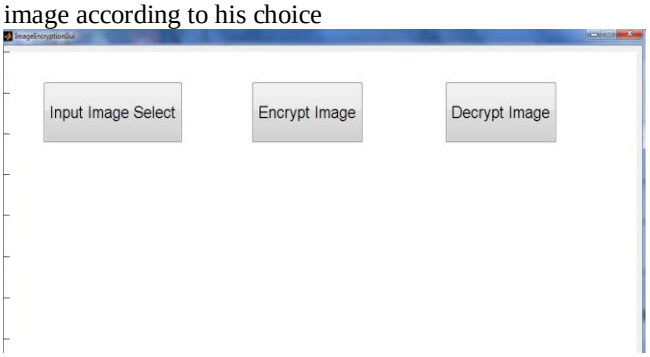

Fig.6: Design view of encyrption and decryption

This is the working process flow of image where image is selected and encrypted. After that image has been decrypted using common key.

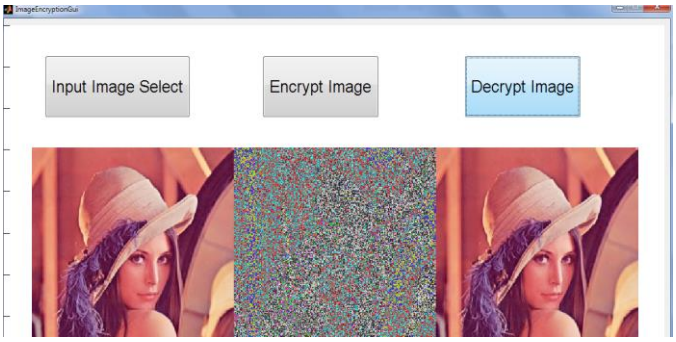

Fig..7: Implementation of encryption and decryption

V. CONCLUSION

In case of traditional 2d system there were only single 2dimension image for comparison. But in traditional 3d there are two different 2 dimensional images for comparison. Thats why it was more secure. But it took more time as well as more space as compare to traditional 2d work. The proposed work is better than tradition work as this is less time consumming as well as less space consuming as compare to traditional work. As proposed system does not take image as it is. It convert image to edge base then make comparison . This reduces the comparison time as well as space taken by image. This system is also more secure as compare to tradition work.

VI. REFERENCES

[1]. A. K. Jain, A. Ross, & S. Pankanti, "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics & Security, Vol. 1, No. 2, 2006, pp. 125-143.

[2]. J. Daugman, "New Methods within Iris Recognition", IEEE Trans. on Systems, Man, & Cybernetics, Vol. 37, No. 5, 2007, pp. 1167-1175.

[3]. R. Wildes, "Iris Recognition: an Emerging Biometric Technology", Proceedings of IEEE, Vol. 85, No. 9, 1997, pp. 1348-1363.

[4]. W. Boles, & B. Boashash, "A Human Identification Technique Using Images(pictures) of Iris & Wavelet Transform", IEEE Trans. on Signal Processing, Vol. 46, No.4, 1998, pp. 1185-1188.

[5]. W. Kong, & D. Zhang, "Accurate Iris Segmentation Based on Novel Reflection & Eyelash Detection Model", within International Symposium on Intelligent Multimedia, Video & Speech Processing, 2001, pp. 263-266.

[6]. L. Ma, & T. Tisse, "Personal Recognition Based on Iris Texture Analysis", IEEE Trans. on PAMI, Vol. 25, No. 12,2003, pp. 1519-1533.

[7]. N. Schmid, M. Ketkar, H. Singh, & B. Cukic, "Performance Analysis of Iris Based Identification System Matching Scores Level", IEEE Transactions on Information Forensics & Security, Vol. 1, No. 2, 2006, pp. 154-168.

[8]. V. Dorairaj, A. Schmid, & G. Fahmy, "Performance Evaluation of Iris Based Recognition System Implementing PCA & ICA Encoding Techniques", within Proceedings of SPIE, 2005, pp. 51-58.

[9]. C. Fancourt, L. Bogoni, K. Hanna, Y. Guo, & R. Wildes, & N. Takahashi, & U. Jain, "Iris Recognition at a Distance", within Proceedings of International Conference on Audio & Video-Based Biometric Person Authentication, 2005, pp. 1-13.

[10]. "CASIA Iris Image Database", Chinese Academy of Sciences Institute of Automation. http://www.sinobiometrics.com

[11]. A. E. Yahya, & M. J. Nordin, "A New Technique for Iris Localization within Iris Recognition System", Information Technology Journal, Vol. 7, No. 6, 2008, pp. 924-928.

[12]. L. Masek, "Recognition of Human Iris Patterns for Biometric Identification", Measurement, Vol. 32, No. 8, 2003, pp. 1502-1516.

[13]. M. Clark, A. C. Bovik, & W. S. Geisler, "Texture segmentation using Gabor modulation/demodulation",Pattern Recognition Letters, Vol. 6, No. 4, 1987, pp. 261-267.

[14]. M. R. Turner, "Texture discrimination by Gabor functions",Biological Cybernetics, Vol. 55, No. 2, 1986, pp. 71-82.

[15]. A. Poursaberi, & B. N. Araabi, "An iris recognition system based on Daubechies's wavelet phase", within Proceedings of 6th Iranian Conference on Intelligent Systems, 2004.

[16]. Y. Chen, M. Adjouadi, A. Barreto, N. Rishe, & J.Andrian, "A Computational Efficient Iris Extraction Approach within Unconstrained Enviroments", within BTAS'09 Proceedings of IEEE International Conference on Biometrics: Theory, Applications & Systems, 2009, pp.17-23.

[17]. S. Shah, & A. Ross, "Iris Segmentation Using Geodesic Active Contours", IEEE Trans. on Information Forensics and Security, Vol. 4, No. 4, 2009, pp. 824-836.