Minutiae Extraction from a Finger Print for Efficient Biometric Cryptosystem

Jyoti Kesharwani
Department of Electronics and telecommunication, Chouksey Engineering College Bilaspur, India
jyoti_kesharwani@yahoo.com

Aarti Tiwari
Department of Electronics and telecommunication, Chouksey Engineering CollegeBilaspur, India
tiwaryaarti@yahoo.com

***Abstract*-Traditional cryptography provides powerful mechanisms to achieve information security but suffers from the key management problems. Biometrics has been an alternative measure for user authentication and identification based on physiological and behavioral characteristics of persons but still suffers from various biometric variations (due to wear-and-tear, accidental injuries, malfunctions, and path physiological development), improper acquisition and inconsistent representation of the biometric signal. Then comes the biometric cryptosystem which blends the cryptography and biometrics to reflect the combined strength of the two fields along with wiping out some common drawbacks in them. The key is dynamically generated from the biometric data instead of storing somewhere and used for authentication or input to cryptographic algorithms. In this paper, we have studied a previously proposed algorithm for biometric key generation from fingerprint, analyzed it, improved it and proposed a new divide and conquer method with distance based key generation algorithm for the same purpose. In this part we are explaining that how the process of minutiae extraction can be done and how the number of minutiae's can be counted from a image of finger print.**

Keywords: — Biometrics, Cryptography, Biometric Cryptosystem, Minutiae points, Image processing, , Divide and Conquer method

I. INTRODUCTION

A. Biometrics

The terms "Biometrics" and "Biometry" have been used since early in the 20th century to refer to the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. Statistical methods for the analysis of data from agricultural field experiments to compare the yields of different varieties of wheat, for the analysis of data from human clinical trials evaluating the relative effectiveness of competing therapies for disease, or for the analysis of data from environmental studies on the effects of air or water pollution on the appearance of human disease in a region or country are all examples of problems that would fall under the umbrella of "Biometrics" as the term has been historically used. The journal "Biometrics" is a scholarly publication sponsored by a non-profit professional society (the International Biometric Society) devoted to the dissemination of accounts of the development of such methods and their application in real scientific contexts.

Recently, the term "Biometrics" has also been used to refer to the emerging field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition. Neither the journal "Biometrics" nor the International Biometric Society is engaged in research, marketing, or reporting related to this technology. Likewise, the editors and staff of the journal are not knowledgeable in this area.

B. Principals of finger print biometrics

A fingerprint is made of a number of ridges andvalleys on the surface of the finger. Ridges are theupper skin layer segments of the finger and valleysare the lower segments. The ridges form so-calledminutia points: ridge endings (where a ridge end) andridge bifurcations (where a ridge splits in two). Manytypes of minutiae exist, including dots (very smallridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spacesbetween two temporarily divergent ridges), spurs (anotch protruding from a ridge), bridges (small ridgesjoining two longer adjacent ridges), and crossovers (two ridges which cross each other)

C. Cryptography

It is the practice and study of techniques for secure communication in the presence of third parties (called adversaries).More generally, it is about constructing and analyzing protocols that overcome the influence of adversariesand which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation.Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Modern Cryptography:Modern cryptography is a remarkable discipline. It is a cornerstone of computer and communications security, with end products that are imminently practical. Yet its study touches on branches of mathematics that may have been considered esoteric, and it brings together fields like number theory, computational-complexity theory, and probability theory. This course is your invitation to this fascinating field.

- Symmetric-key cryptography
- Public-key cryptography

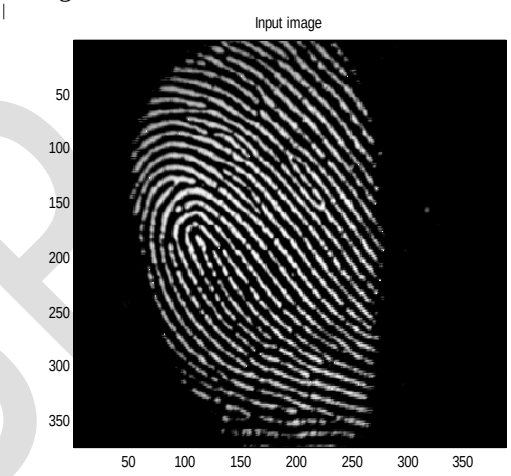
II.BIOMETRIC CRYPTOSYSTEM

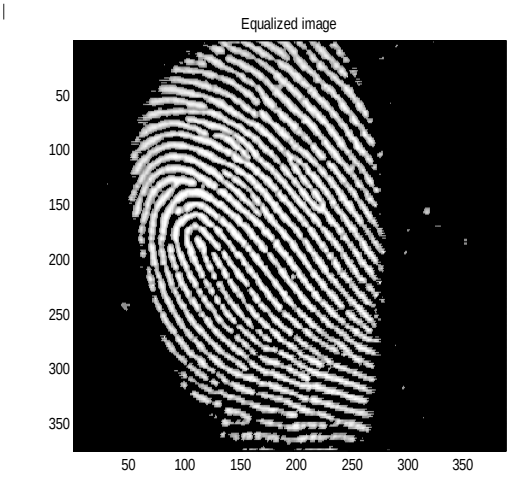
Despite of so many advantages, the Biometric systems also suffer from many drawbacks. Password-based authentication systems do not involve any complex pattern recognition techniques (passwords have to match exactly) and, hence, they almost always perform accurately as intended by their system designers. On the other hand, biometric signals and their representations (e.g., facial image and Eigen coefficients of facial image) of a person vary dramatically depending on the acquisition method, acquisition environment, user's interaction with the acquisition device, and (in some cases) variation in the traits due to various path physiological phenomena. Some of the common reasons for biometric signal/representation variations are- Inconsistent Presentation, Irreproducible Presentation and Imperfect Signal/Representational Acquisition. Biometric cryptosystem removes some common problems in the above two fundamental mechanisms and ensures the combined strength of the cryptography and biometrics. In such systems, while cryptography provides high and adjustable security levels, biometrics brings in no repudiation and eliminates the need to remember passwords or to carry tokens etc. There are different ways
to achieve the bio crypto system:- Biometric based

- Key release mode : In this mode the biometric template and the keys are stored as separate entities and the key is released only if the biometric matching is successful. .
- Key binding mode: In this mode the key and the template are monolithically bound within a cryptographic frame work.
- Key generation : In this mode the key is derived directly from the biometric data and is not stored in the database.

III.MINUTIAE EXTRACTION

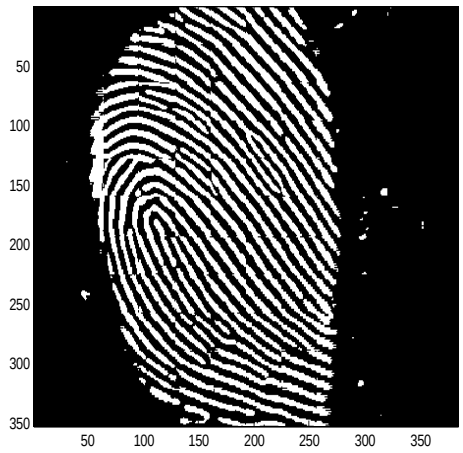
The minutiae points are extracted from the acquired fingerprint image through various image processing techniques. There are few steps to finding the exact number of minutiae from an image.First is to check that the image is RGB or not if it is RGB then we will have to convert it into gray. RGB to gray converts the RGB image to gray scale intensity image. It can be done by eliminating hue and the saturation information while retaining the luminance. To make the image more clear the image can be inverse. Then Histogram Equalization and Filters are used to enhance the contrast of an image.The Histogram Equalization block enhances the contrast of imagesby transforming the values in an intensity image so we will get the histogramof the output image which is approximately matches a specified histogram.Here shows you how to modify the contrast in intensityimages using the Contrast Adjustment and Histogram Equalization.



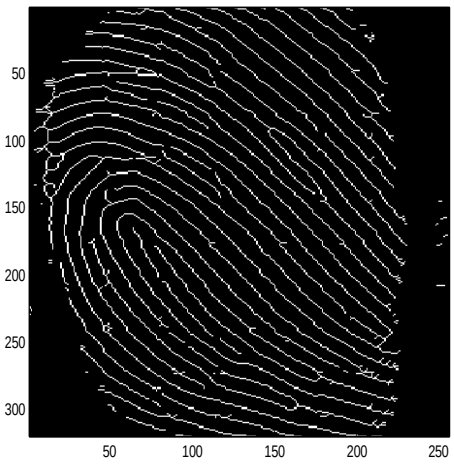


Here the above figure 1 is the input image and figure2 is the image after equalization. Both the images shows the changes in the input image and the equalized image as the figure 2 is more clear than the input image.
Binarization is the process which has been performed after histogram equalization. This process is done to convert the

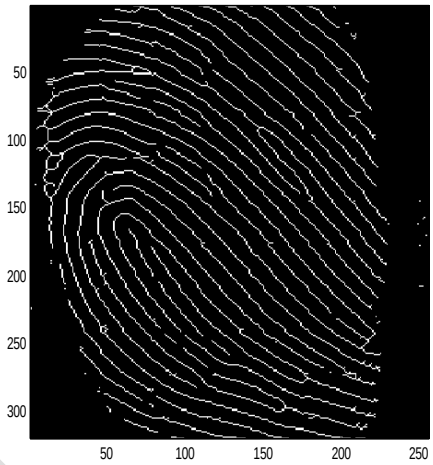
grey level image into a binary image it enhance the contrast between the ridges and valleys in a fingerprint image. It Convert the image to binary image, based on threshold. Here we are taking two values as 1 is for the white and 0 for the black Therefore,a level value of 0.5 is between black and white, regardless of class.in this we will have to define the class or level If we do not specify level, it usesthe value 0.5.Here the figure shows the process of binarization.



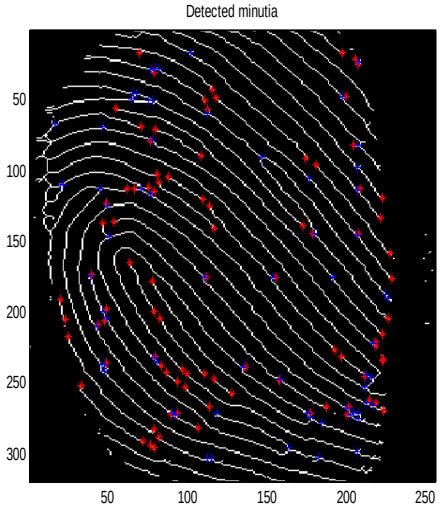
Morphological operation is used to find the region of interest.In region of interest (ROI) we are taking a portion of an image that we want to filter or perform some other operationon. We can define ROI by creating a binary mask. A binary mask is a binary image that is the same size as the image we wantto process with pixels that define the ROI set to 1 andall other pixels set to 0. After the morphological operation process of ridge thinning can be done.



It is performed to eliminate the redundant pixels of ridges and eliminate it till the ridges are just one pixel wide, in each scan of full fingerprint image.After fingerprint ridge thinning minutiae points are more cleared and can bemarked easily as shown in the figure. Thinning is the process to eliminate the redundant pixel but after this, still there is some noise is present in the image. To remove this noise and make the view of an image clearer we are performing the process of denoising. It is the process of removing noise and converting the image into double precision. It converts the intensity image into double precision so if the input image is of class double, theoutput image is identical. After removing the noise we get the clearer image of a finger print or we can say that to remove the false minutiae and make it more effective denoising is must. Here the image we get after denoising, in this all the minutiae's are shown clearly



After the process of denoising it is easy to detect the real minutiae's from the image. As all the minutiae's are now clearly shown so we can identify or detect the real minutiae's. These detected minutiae's are the actual number of minutiae which are present in a given image of fingerprint.



IV. RESULT

After doing all the operations we will get the real minutiae from an image of a finger print. Here in figure the real minutiae's can be shown or the number of termination bifurcation can be easily find. According to the structure of minutiae or by calculating the number of bifurcation and termination we can easily find out the real minutiae's. After performing all the operation the real number of minutiae can be counted and then it is used for generating the key for the biometric cryptosystem. We are now able to apply the different methods for generating key from these minutiae. In the next section we will see how the different approaches are applying on these minutiae's and key generation can be done.

Real Minutia

REFERENCES

[1] A. K. Jain, A. Ross, S. Pankanti, "Biometrics: A Tool for Information Security", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 1, NO. 2, JUNE 2006.

[2] F. Hao, R. Anderson, J. Daugman, "Combining Crypto with Biometrics Effectively", IEEE TRANSAC TIONS ON COMPUTER S, VOL. 55, NO. 9, SEPTEMBER 2006.

[3] N. Ratha, J. Connell, R. M. Bolle, S. Chikkerur, "Cancelable Biometrics: A Case Study in Fingerprints", The 18th International Conference on Pattern Recognition (ICPR'06) 2006.

[4] K. Nandakumar, "Multibiometric Systems: Fusion Strategies and Template Security", A Dissertation Submitted to Michigan State University in partial ful¯llment of the requirements for the degree of Ph..D., 2008

[5] Dr. R.Seshadri, T.RaghuTrivedi, "Generation of key for Session key Distribution Using Bio-Metrics", International Journal on Computer Science and Engineering Vol. 02, No. 06, pp. 1992-1995, 2010

[6] S.V. K. Gaddam1 and M. Lal2, "Effecient Cancellable Biometric Key Generation Scheme for Cryptography" International Journal of Network Security, Vol.11, No.2, pp. 57-65, Sep. 2010.

[7] Dr. R. Seshadri, T.RaghuTrivedi, "Efficient Cryptographic Key Generation using Biometrics", Int. J. Comp. Tech. Appl., Vol 2 (1), 183- 187,2012

[8] A. Jagadeesan, T. Thillaikkarasi, Dr. K. Duraiswamy, "Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature ", International journal of computer science, vol. 2 no. 6, pp. 16-26, 2011

[9] R. Bais, K. K.Mehta , "Biometric Parameter Based Cryptographic Key Generation", international Journal of Engineering and Advanced Technology ,Vol. 1, pp. 158-160, 2012

[10] Mr. P .Balakumar , Dr. r. venkateshan, "A Survey on Biometrics based Cryptographic Key Generation Schemes", International Journal of Computer Science and Information Technology & Security, vol. 2, no. 1, pp. 80-85, 2012

[11] K.Kavitha, Dr.K.Kuppusamy, "A Hybrid biometric authentication algorithm", International Journal of Engineering Trends and Technology-, Vol. 3, 2012

[12] S. Kaur. "Enhancing Template Security by a Biometric key Generating Cryptosystem: A Review", International Journal of Advanced Research in Computer Science and Software Engineering , vol.3, pp. 973-976, 2013

[13] M. ShahnawazNasir, P. Kuppuswamy ," Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm ", International Journal of Innovative Research in Computer and Communication Engineering , Vol. 1, pp. 1741-1748, 2013

[14] K. H Solanki, C. patel "Biometric Key Generation In Digital Signature Of Asymmetric Key Cryptographic To Enhance Security Of Digital Data" , International Journal of Engineering Research & Technology (IJERT), Vol 2, pp. 1-7, 2013

[15] R. Ranjan, S. Kumar singh, "Improved and Innovative Key Generation Algorithms for Biometric Cryptosystems" IEEE International Advance Computing Conference (IACC), pp. 944-946, 2013