A Robust Palm Vein Authentication for Improving Safety and Security

Keerthi. C, Mrs. Savitha A.P, Dr M.B Anandaraju

Abstract- Biometrics is a technique that analyses and measure human body characteristics such as voice patterns, DNA, eye retinas, facial patterns, irises for authentication. A palm vein authentication system uses blood vessel patterns as key for personal identification. This paper intends to design architecture by palm vein analysis technique. Biometric analysis can be done with suitable looping algorithms like masking and mapping, a novel technique of extracting vein features out of palm which posses unique identity for different users. An IR-Illuminator is used to illuminate palm veins and is captured using image sensor. The raw image data so obtained should be pre-processed which includes segmentation of veins with respect to muscles, removal of noise, alignment of palm and orientation of veins. The pre-processing is simulated on MATLAB. A 2-level secure architecture for encoding and decoding process in Xilinx has been developed and can be dumped to FPGA also. The architecture takes bit data as input from MATLAB and performs verification of palm vein Region Of Interest (ROI) at individual levels and sends back the decoded bit to MATLAB for display on monitor for user. This project is robust in the sense image data acts as first level security and user input password converted to CRC-16 CCITT constructs a polynomial there by encoding image data this way a 2-level security and good authentication to the user is provided. In decoding process, the encoded polynomial is divided by image data set and if the reminder is zero the authentication to user is provided else a error message is displayed.

Key words: **palm vein, CCITT.**

. I. INTRODUCTION

Biometrics is automated methods for identifying a person based on a physiological or behavioral characteristic; among them are the features measurement of akin to face, handwriting, fingerprints, hand geometry, iris, palm vein, retinal, and voice. Palm vein biometric systems are more comprehensive because they provide a nontransferable means of recognizing people not just on cards or badges.

Manuscript received May 23, 2015.
Keerthi. C, P.G. Student, VLSI Design and Embedded System, B.G.S Institute of Technology, B.G.Nagar , Mandya-571448, Karnataka, India.
Mrs Savitha A.P, Assistant Professor, Department of Electronics and Communication Engineering, B.G.S.Institute of Technology, B.G.Nagar , Mandya-571448, Karnataka, India.

A key importance of palm vein biometric authentication is that, biometric information is based on human vein characteristics that stay constant throughout one's lifetime and are cumbersome to fake or change or forge.

II. PALM VEIN PATTERN

The biometric palm vein based identification system is based on statistical properties of palm vein pattern. Palm vein can be studied and is adopted for person identification and it is very difficult to forge.
Human skin is made up of three layers:
1) Epidermis 2) dermis and 3) sub cutis, as shown in Figure 1. Each layer will contain a different proportion of blood and fat.

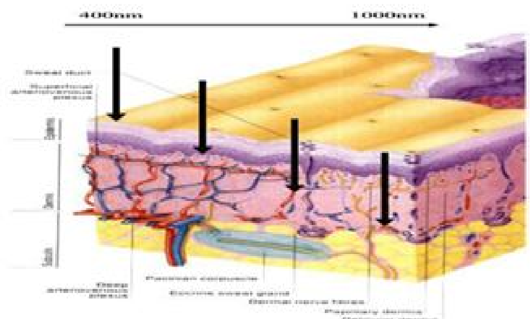

Figure 1: Cross sectional view of skin

Light from a source in the wavelength range of 700- to 1000-nm can penetrate human skin. Whereas 880–930 nm will give a good contrast of subcutaneous vein.
The epidermis also contains melanin, whereas the sub cutis contains veins. Light in different wavelengths range will penetrate to different layers of skin and illuminate in different spectra. NIR light penetrates human tissue further than visible light, and blood absorbs more NIR energy than the surrounding tissue (e.g., fat or melanin). The system acquires spectral information from all three dermal layers by using both near infrared (NIR) and visible bands.

III. METHODOLOGY

Palm vein pattern framework utilizes the goodness of both authentication and biometrics. In palm vein pattern framework, the secret key S is locked by G, where G is an unordered set from the biometric pattern. Polynomial P is composed by encoding the secret S. This polynomial is evaluated by all the elements of the unordered set G. A vault V is constructed by the union of unordered set G and chaff point set C which is not in G.

$$V = G \cup C \quad \ldots\ldots\ldots.. (1)$$

The union of the chaff point set hides the genuine point set from the adversary (attacker). Hiding the genuine point set secures the secret data S and user biometric template T. Vault V is unlocked with the query template T’. T’ is represented by another unordered set U’. The user has to separate sufficient number of points from the vault V by comparing U’ with V. The polynomial P can be successfully reconstructed if U’ overlaps with U and secret S gets decoded. If there is not substantial overlapping between U and U’ secret key S is not decoded. This construct is called palm vein because the vault will get decoded even for very close values of U and U’ and the secret key S can be retrieved. Therefore palm vein pattern construct becomes more appropriate for biometric data which possesses inherent fuzziness.

The security of the palm vein pattern depends on the infeasibility of the polynomial reconstruction. The vault performance can be improved by adding more number of chaff points C to the vault. First, the user has to subject his palm to the palm vein sensor which consists of near infrared led ,which will provide the view of veins in the palm and camera which will capture the image of it. The image is then pre-processed (which involves normalization, segmentation, binarization, image thinning, size selection) using MATLAB as a tool after this the user has to enter the 16 bit secret key or password. During authentication, the encoding and decoding will be performed by using Xilinx ISE design suite. In encoding, the palm vein image and secret key will be encoded and while decoding if the correct user palm is provided then only authentication/ access to the system will be provided or else authentication will be denied.

IV. PRE –PROCESSING OF PLAM VEIN

Pre-processing is the technique of enhancing data images prior to computational processing. Pre-processing the images involves eliminating low-frequency background noise, masking certain portions of images, normalizing the intensity of the individual particles images and removing reflections. Steps in pre-processing includes:

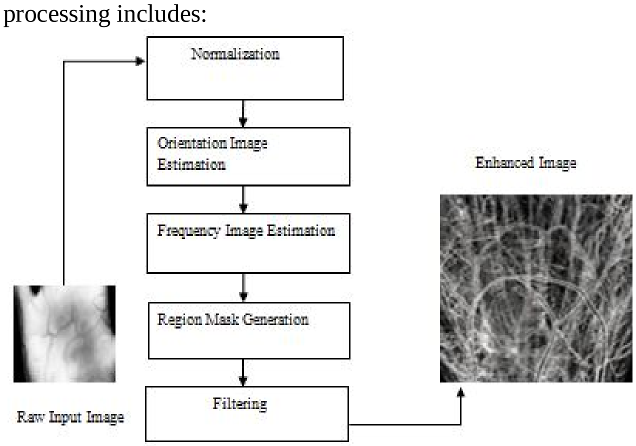

Figure 2 : Block Diagram Involving Steps Of Pre-Processing.

(a)Normalization: Normalization is a process that changes the range of pixel intensity values. The goal is to obtain a standard image with no artifacts arising from the specific conditions in which a particular image was take. Image normalization refers to eliminating image variations (such as noise, occlusion or illumination) that are related to conditions of image acquisition and are irrelevant to object identity. For example, if the intensity range of the image is 10 to 170 and the desired range is 0 to 255 the process entails subtracting 10 from each of pixel intensity, making the range 0 to 160.
Then each pixel intensity is multiplied by 255/160, making the range 0 to 255.

(b) Image Segmentation: The goal of image segmentation is to cluster pixels into salient image regions. Image segmentation is the process of assigning a label to every pixel in an image such that pixels with the same label share certain characteristics. Segmentation could be used for occlusion boundary estimation within motion or stereo systems, object recognition, image compression, image database look-up or image editing. The result of image segmentation is a set of segments that collectively cover the entire image or a set of contours extracted from the image.

(c) Image Binarization : In Binarization, the grey scale image is converted into binary image. Binary images are easy to process. The basic principle of converting an image into binary is to decide a threshold value, and then the pixels whose value are more than the threshold are converted to white pixels, and the pixels whose value are below or equal to the threshold value are converted to black pixels.

(d) Orientation Image Estimation: Computing a reliable orientation map is a critical step. The accuracy of orientation measurement is also a primary concern. Image orientation is central to many tasks in image processing which includes the extraction of lines, edges and curves and image enhancement. Each time a user subjects the palm to the vein sensor, the orientation that the user place the palm may be different. Sometimes the user cannot remember the orientation, this may be indicated as error or the feature required may not be captured accurately. Therefore the design for orientation based image estimation requires defining a window or square area where the features are distinct and complex which would be independent of the orientation the user places the palm.

(e) Noise Elimination**:** There are many small unwanted portions that are unnecessary for further processing, but these portions if exist may lead to incorrect minutiae detection. Usually a sequence of data may involve useful data, inconsistent data and noisy data. Pre-processing may reduce the noisy and inconsistent data. The data corrupted with noise can be recovered with pre-processing techniques. These portions usually consist of around 20 to 25 pixels.

V. IMPLEMENTATION

1. Encoding

Figure 3 shows the block diagram of the encoding process. In encoding, secret key(s) or password and palm vein are encoded to form a polynomial this is considered as vault(v).

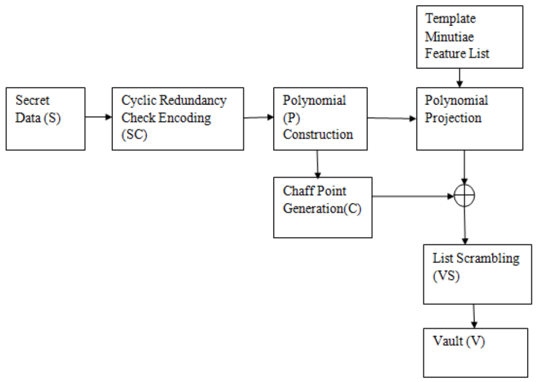

Figure 3: Block Diagram Of Encoding.

(a)Secret Key (S): The secret key (s) is the user password that is used during authentication. The user password may be alphabetic or numerical or a combination of both. The user password is 16-bit which would be difficult for adversary to guess.

(b) CRC Encoding: Firstly, the secret, *S* is encoded using CRC and the CRC value is concatenated at the end of the secret to form a secret', *S'*. For this purpose we have used CRC-16-CCITT with polynomial shown below

$$x^{16} + x^{15} + x^2 + 1 \quad \text{......... (2)}$$

(c) Polynomial Encoding: To hide the secret in the palm vein pattern, the secret is divided into *(n+1)* parts and the parts become the coefficients of an *n* degree polynomial. The palm vein minutiae of each user protect the secret such that as long as *n+1* number of palm vein minutiae are found, the secret can be reconstructed from the palm vein pattern. However, if there are less than *n+1* correct minutiae, it becomes computationally infeasible to re-produce the secret.

(d) Lock Matrix Creation: The palm vein minutiae coordinates are concatenated to form the Lock Matrix for this palm vein pattern.
The minutiae coordinates form the x-coordinate values and the Horner's method is used to evaluate the polynomial to find the equivalent y-coordinate values. The x and y-coordinates are then stored in a matrix known as the Lock Matrix. With this step, the polynomial can be discarded and now the secret can only be re-created using this Lock Matrix.

(e) Chaff Point Generation: The next step is to generate chaff points to cover the complete range of the palm vein pattern but not overlap with the Lock Matrix coordinates. To perform chaff generation we have used an algorithm similar to Rényi's random space filling method described in. The algorithm generates random points in the 2-dimensional plane (xi, yi) that have a certain minimum distance from the points that already exist on the plane. This distance is also known as the Euclidian distance. The algorithm is iterated until a sufficiently large set is created and the Code Matrix elements are adequately hidden.

2. Decoding

The decoding process for the Palm vein pattern is the opposite of the encoding process with some differences which is depicted in Figure 4. During decoding process, a user tries to unlock by using the query minutiae features and if it matches to that encoded then authentication is provided or denied.

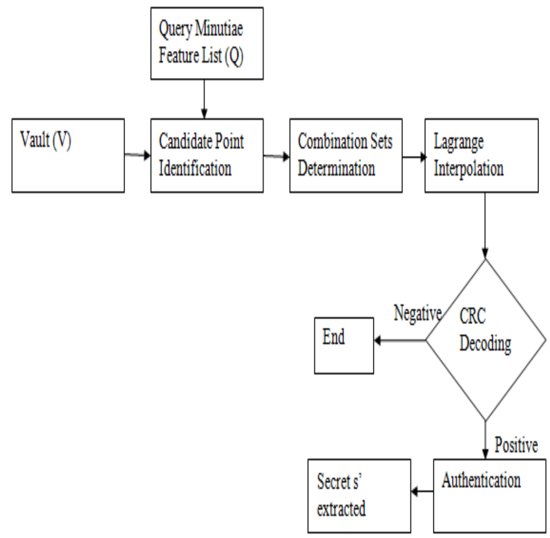

Figure 4: Block Diagram Of Decoding.

(a)Unlock Matrix Creation: The equivalent y-coordinate value can also be read from the palm vein pattern matrix. Together these coordinate sets from the Unlock Matrix.

(b)Polynomial Reconstruction: Polynomial interpolation is used to reconstruct candidate polynomials based on the Unlock Matrix. Gauss Elimination is used to deflate the polynomial. The Unlock Matrix is evaluated iteratively to produce all possible polynomial candidates.
An Nth degree polynomial can be written in coefficient form as:

$$F(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \quad \text{... (3)}$$

where a0,…,an are real numbers.

(c)Polynomial Interpolation: In order to actually reconstruct the secret locked within the palm vein pattern, the points in the unlocking set must be used to interpolate a polynomial. The unlocking set will contain both real points and chaff points. The simplest mechanism for recovering the polynomial is a brute-force search, where various k+1 element subsets of the unlocking set are used to interpolate a degree k polynomial, using Newtonian Interpolation method.

(d)Polynomial Decoding: Polynomial decoding is performed where all the coefficients of the polynomial are concatenated to re-form the secret', *S'*.

***(e)*CRC Error Detection:** CRC values are calculated for the first part of each possible *S'* candidate and compared to the last 16-bits. If the CRC value and the last 16 bits are the same, then the secret', *S'* has been successfully identified. Discarding the last 16 bits will give us the original secret, *S*.

VI. Simulation Result

After pre-processing, 16 bit secret key is entered by the user. The palm vein images and the secret key will be encoded to construct a polynomial and during decoding correct palm is provided then authentication is provided or a error message is indicated. The original image is obtained from the sensor.

1. Simulation Results Of Pre-Processing

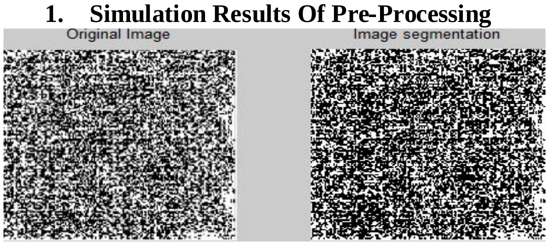

Figure 5 : Image Segmentation Of Original Image

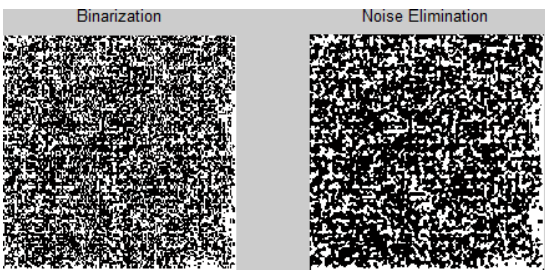

Figure 6: Binarization And Noise Elimination Of The Original Image

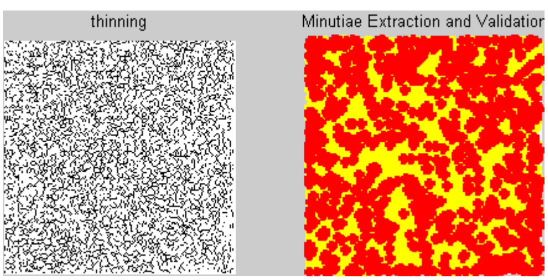

Figure 7 : Thinning And Minutiae Extraction And Validation Operation

From Figure 7 the view of the veins and the minutiae points(red color) and chaff points(yellow) is obtained.

2. Simulation result obtained during encoding

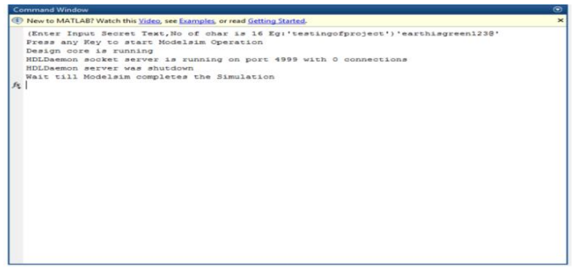

Figure 8: simulation In MATLAB Command Window

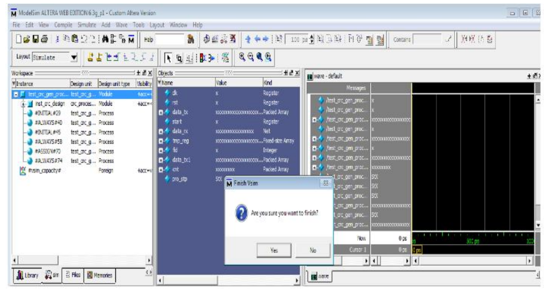

Figure 9: Encoding In Modelsim

Next operation is decoding, if the correct palm vein is given then authentication to the system will be provided and the 16-bit password will be returned and is displayed to the user on command window.

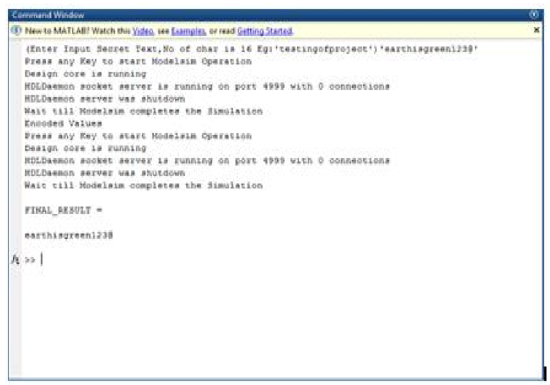

Figure 10: Authentication To The System

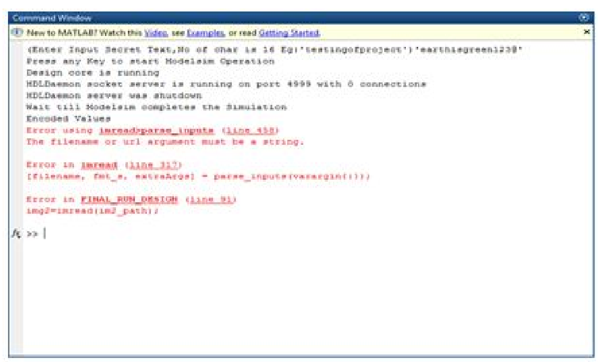

Figure 11: Denied Authentication.

VII. CONCLUSION

The importance of palm vein authentication for improved safety and security was studied and implemented in this paper. Palm vein properties and the construction of the palm vein sensor was explored that provided a vast knowledge of the superior vein authentication system. The disadvantages and cost concern of other biometric technique provided striking idea of developing authentication system using palm vein. The truth that vein patterns are internal to the body and difficult to duplicate stands as the route.

The system developed provides a 2-level protection one is the 16- bit secret key other is the palm vein in which 28 minutiae points matching is considered. Different pre-processing steps was studied which provides the enhanced features for identification. The MATLAB software plays an important role in pre-processing. The 16-bit CRC implemented using CCITT is a error detection algorithm, which is simulated on Xilinx, that helped in polynomial extension. The operation of encoding and decoding used in the paper was analyzed, implemented and the results are collected.

REFERENCES

[1] Saravanan.A and Dr. M. Ramkumar Prabhu, "Palm-Vein Image Recognition of Human Using Discrete Enhancement", Head of the Department, Department of Electronics and Communication Engineering SRM University, Chennai, TN, India. International Journal of Electronics and Communication Engineering.ISSN 0974-2166 Volume 6, Number 3 (2013), pp. 267-275

[2] Mona A. Ahmed, Hala M. Ebied, El-Sayed M. El-Horbaty, Abdel-Badeeh M. Salem," Palm Vein Preprocessing Image based on Homomorphic Filtering", Computer Science Department, Faculty of Computer and Information Sciences Ain Shams University, Cairo, Egypt. Volume 3, Issue 5, September-October 2014 ISSN 2278-6856.

[3] Ali Mohsin Al-juboori1, Wei Bu3 Xiangqian Wu, and Qiushi Zhao," Palm Vein Verification Using Multiple Features and Isometric Projection", Department of Media Technology and Art, Harbin Institute of Technology, Harbin, 150001, China. International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.7, No.1 (2014), pp.33-44.

[4] A. Juels and M. Wattenberg, "A Palm vein Commitment Scheme", In G. Tsudik, Ed., Sixth ACM Conf. Computer and Comm. Security, pp. 28-36, 1999.

[5] S. Lin, An Introduction to Error-Correcting Codes, Prentice-Hall, 1970.

[6] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure Smartcard-Based Palm veinprint Authentication",Proc. ACM SIGMM 2003 Multim., Biom. Met.& App., pp. 45-52, 2003.

[7] . J.-P. Linnartz and P. Tuyls, "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates", Proc. 4th Int'l Conf. Audio- and Video-based Biometric Person Authentication, pp. 393-402, 2003.

[8] Yuhang Ding, Dayan Zhuang and Kejun Wang, "A Study of Hand Vein Recognition Method", The IEEE International Conference on Mechatronics & Automation Niagara Falls, Canada, July 2005.

KEERTHI C pursuing 4th semester M.Tech in VLSI Design and Embedded System in B.G.S. Institute of Technology, B. G. Nagar, Mandya , Karnataka, India. She Received her B.E (Instrumentation Technology) degree from GSSS college of Engineering, Mysore in 2013.She had presented her paper in National conference on Emerging trends in Electronics and Communication (NCETEC-15) and the paper was selected as the best paper of the session.

Savitha A P received B.E Degree in Electronics and Communication from Mysore University, India in the year 2000 and M.Tech Degree in VLSI and Embedded systems from VTU, India in the year 2007.She is now working at BGS Institute of Technology, B G Nagar. Her field of interest is image processing, biometrics. Currently doing research in biometrics.