Robust Second Level Palm Vein Authentication for Digital Vault

Swarnaltha K
Associate Professor, Department of Information Science and Engineering
GSSS Institute of Engineering & Technology for Women, Mysuru
gururaj.k.s79@gmail.com

***Abstract* - There have been many researches that investigated the finger, hand, and palm vein recognition for automated personal identification. By using modern technology a person can control their personal information easily at any time and any place, but also there are risks that other people can take control of this information. Palm vein technology works by identifying the vein patterns in an individual's palm. When a user's hand is held over a scanner, a near-infrared light maps the location of the veins. The red blood cells present in the veins absorb the rays and show up as black lines, whereas the remaining hand structure shows up as white. This vein pattern is then verified against a preregistered pattern to authenticate the individual. As veins are internal in the body and have a wealth of differentiating features, attempts to forge an identity are extremely difficult, thereby enabling high level of security.**

***Keywords*—Palm vein, Pattern, Authenticate, Security.**

I. INTRODUCTION

A biometric system is a technological system that uses information about a person to identify that person. Biometric systems rely on specific data about unique biological traits in order to work effectively. A biometric system involves running data through algorithms for a particular result, usually related to a positive identification of a user or other individual. Biometrics is the automated method of recognizing a person based on a physiological or behavioural characteristic. Examples of behavioural characteristics are face recognition, fingerprints, hand geometry, signature verification, iris, retinal, finger/hand/palm vein recognition, ear recognition, and voice recognition. Palm Vein Authentication Technology is one of the newest biometric techniques researched today. Biometrics, such as with vein recognition, refers to methods for recognizing individual people based on unique Physical and behavioural traits. Palm vein authentication has high level of accuracy because it is located inside the body and does not change over the life and cannot be stolen. By using modern technology a person can control their personal information easily at any time and any place, but also there are some risks that other people can take control of this information. Compared with a finger or back of a hand, a palm has a broader and more complicated vascular pattern and thus contains a wealth of differentiating features for personal identification.

II. PROBLEM STATEMENT

Hand vein refers to the vascular pattern or blood vein patterns recorded from underneath the human skin .
The principal lines characterize the most distinguishable features on the palm. Most people have three principal lines, which are named as the heart line, head line, and life line Wrinkles are regarded as the thinner and more irregular line patterns. The wrinkles, especially the pronounced wrinkles around the principal lines, can also contribute for the distinguish the palm print. On the other hand, ridges are the fine line texture distributed throughout the palm surface. The ridge feature is less useful for discriminating individual as they cannot be perceived under poor imaging source.

III. METHODOLOGY

Fingerprints are used as a way of authentication for most of the security processes. They are the most widely used method of substantiation. They can be forged in many ways and may result in losing crucial information. There have been situations where cons have misused fingerprints and done away with fraud. Many existing fingerprint sensors acquire fingerprint images as the user's fingerprint is contacted on a solid flat sensor. Because of this contact, input images from the same finger can be quite different and there are latent fingerprint issues that can lead to forgery and hygienic problems.

In order to acquire fingerprint images with conventional touch-based sensors ,the user must place his finger on the flat window of the sensor. Because the skin of the finger is not flat, the user must apply enough pressure on the window to obtain sufficient size and achieve good image quality. However, this pressure produces unavoidable physical distortion in arbitrary directions, which is represented differently throughout every area of the same fingerprint image. Also, since the image varies with each impression, each fingerprint image from the same finger can appear quite different. Fig. 1 shows the images from touch-based sensor. Because of different pressure, the relative position and types of corresponding minutiae are different.

IV. FUNCTIONS HIGH LEVEL DESIGN

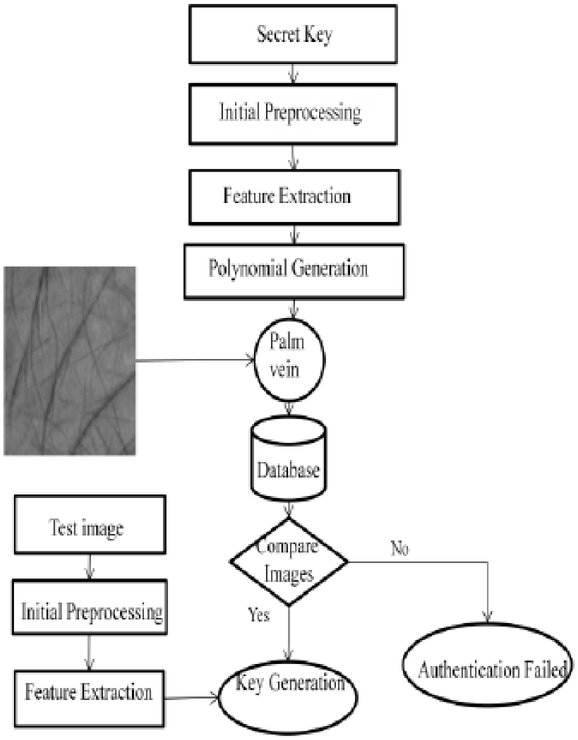


Fig 1-High Level Design

V. ENCODING

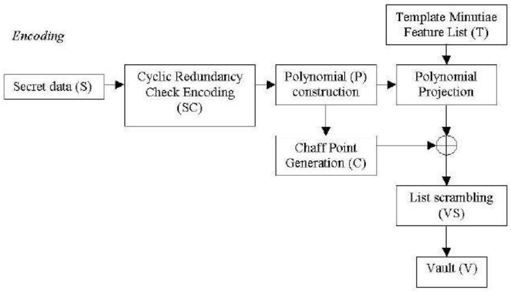

Encoding
Template Minutiae Feature List (T)
Secret data (S)
Cyclic Redundancy Check Encoding (SC)
Polynomial (P) construction
Polynomial Projection
Chaff Point Generation (C)
List scrambling (VS)
Vault (V)

Fig 2-Encoding Process

1) 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 a value of 0x1021 to form the CRC polynomial shown below

2)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 print minutiae of each user protect the secret such that as long as *n+1* number of palm vein print 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.

3) Lock Matrix Creation: The palm vein print 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.

4) 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 haff 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.

5) Palm vein pattern Creation: Combining the chaff points with the Code Matrix coordinates forms the palm vein pattern. The palm vein pattern matrix is the secure template that is stored in the system database. Neither the secret, nor the user's biometric data can be reproduced or stolen from the secure template.

VI. DECODING

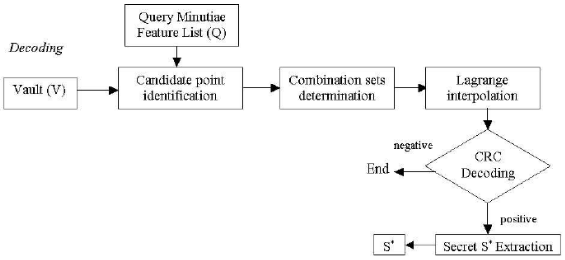


Fig 3-Decoding Process

1) Nearest Neighbour Detection: The minutiae values collected from the query image may not have the exact same coordinates as the values within the vault. Therefore, the nearest neighbour of the minutiae values must be found from the vault. This step creates a new set of x-coordinates that are used for subsequent procedures while the previous set of values from the minutiae is discarded.

2) 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.

3) 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.

Any Nth degree polynomial can be written in coefficient form as:

$$F(x) = a_0 + a_1x + \; a_2x^2 + \; \ldots + a_nx^n$$

where a0,…,an are real numbers.

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

5) 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*.

VII. IMPLEMENTATION

1. Authentication

During authentication, first the template and query palm vein prints are aligned using the high curvature points as described in. Then, r well separated and good quality minutiae are selected from the query and are coarsely matched with the points in the vault in order to filter out most of the chaff points. An XOR operation is applied between the descriptor (say D′) associated with each selected query minutia and the corresponding secure ordinate value to obtain a word C′. This word is then decoded to obtain the message, which represents the ordinate value corresponding to that minutia. If the ordinate value is correctly decoded for some minimum number (n + 1) of genuine points in the vault, the polynomial f can be correctly reconstructed indicating a successful match.

2. Analysis

A study showed that the min-entropy of the minutiae template MT given the vault V can be computed as

$$H_\infty(M^T|V) = -log\left(\frac{\binom{r}{n+1}}{\binom{r+s}{n+1}}\right),$$

If both the minutiae location and minutiae orientation are uniformly distributed. Here, r, n and s have the same meaning as defined earlier. The palm vein pattern implementation in uses the values of r = 24, s = 200and n = 8 for the typical vault construction. Based on the above analysis, the security of the palm vein print palm vein pattern implementation in is approximately 31 bits.

In the proposed palm vein print palm vein pattern the true ordinate values can be obtained in two ways. (i) Directly guessing the 16-bit ordinate values. Since the ordinate values of the genuine points are obtained through evaluation of a randomly generated secure polynomial, it is reasonable to assume that the difficulty of directly guessing an ordinate value is approximately 16 bits (assuming there are more than 16 information bits in the error correcting code). Also since the adversary has to simultaneously guess (n + 1) ordinate values correctly ,this corresponds to approximately 16(n + 1) bits of security.(ii) Guess the descriptors associated with each minutia. Although the length of descriptor is N bits(N = 511 here), there is a strong correlation between the descriptor bits. Suppose that the entropy of a minutia descriptor D is Id bits and ρ = (119 × Id)/511 ≈Id/4 bits should be corrected. As shown by Hao et al., the difficulty in guessing a minutiae descriptor is approximately

$$R = \log\left(2^{I_D} / \binom{I_D}{\lceil\rho\rceil}\right)$$

Bits. Since the adversary has to simultaneously guess (n+1)minutiae descriptors correctly, using minutiae descriptors provides approximately (n + 1)R bits of security. For instance ,if n = 8 and ID = 6 bits, then R ≈ 2 bits. In this scenario, the proposed scheme increases the security of the palm vein pattern by approximately 16 bits and the overall security is 47 (31 + 16) bits.

The above security analysis assumes the use of a perfect error correction coding scheme (a w-error correcting binary code of size 2N is said to be perfect if for every word C

, there is a unique codeword C such that the Hamming distance between C and C' is at most w bits).If the coding scheme is not perfect, some of the words may result in a decoding failure which would indicate a correct minutia descriptor being used to de-commit the ordinate value. Note that even if all the incorrect descriptors lead to decoding failure, which is very unlikely, the security is at least as good as the security of the original palm vein pattern. Non-perfect codes may reduce the effective value of R, thereby limiting the additional security that can be achieved using descriptors. While our current implementation uses non-perfect codes, we are exploring the possibility of using available perfect codes (the class of

Hamming codes and Gray code) to achieve the required error correction capability.

VIII. RESULTS AND DISCUSSIONS

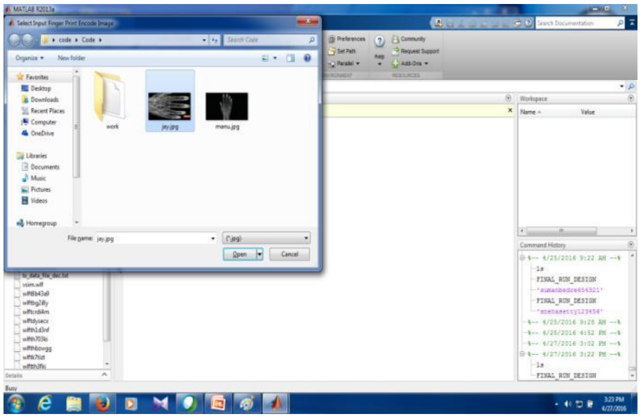


Fig 4: Input image

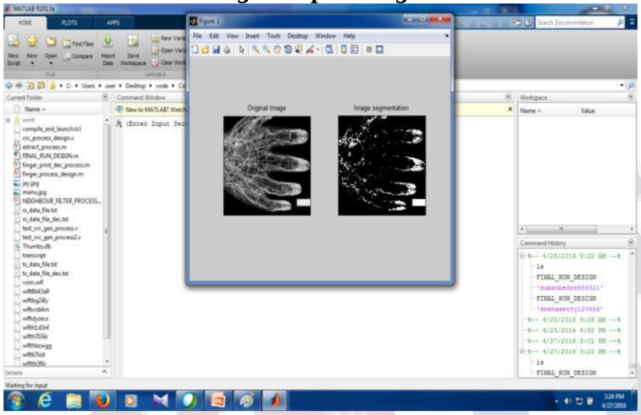


Fig 5: Image Segmentation

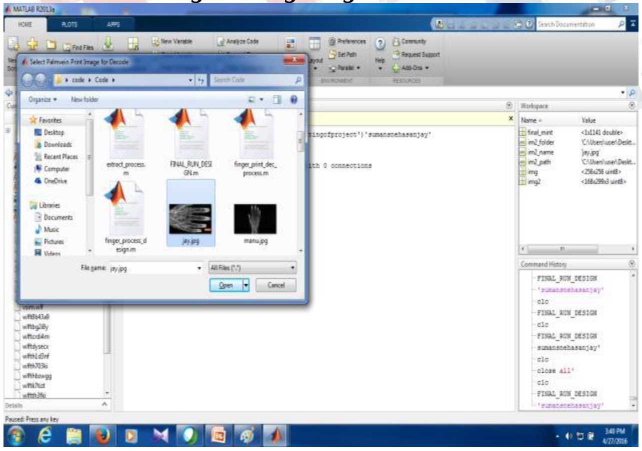
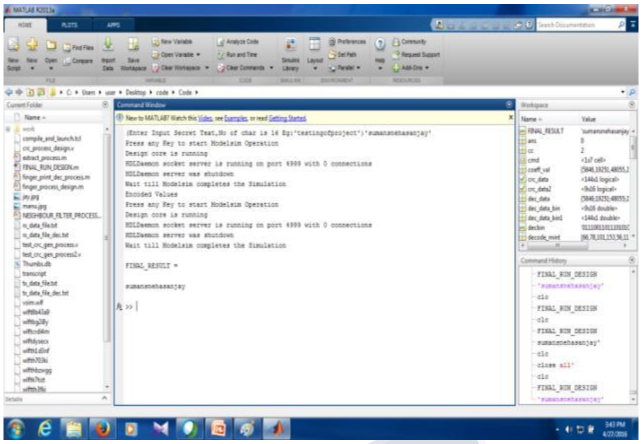


Fig 6:Decoding input



```
(Enter Input Secret Text,No of char is 16 Eg:'testingofproject')'sumansnehasanjay'
Press any Key to start Modelsim Operation
Design core is running
HDLDaemon socket server is running on port 4999 with 0 connections
HDLDaemon server was shutdown
Wait till Modelsim completes the Simulation
Encoded Values
Press any Key to start Modelsim Operation
Design core is running
HDLDaemon socket server is running on port 4999 with 0 connections
HDLDaemon server was shutdown
Wait till Modelsim completes the Simulation

FINAL_RESULT =

sumansnehasanjay

>>
```

Fig 7:Authenticated output

IX. CONCLUSION

Palm vein biometric systems are superior because they provide a non transferable means of identifying people not just cards or badges. A key advantage of palm vein biometric authentication is that, biometric data is based on human vein characteristics that stay constant throughout one's lifetime and are difficult to fake or change.

The developed system provides second level security. The project can be implemented in areas where authentication is crucial. The system can be useful in the field of medicine, banking, airports, forensic department.

REFERENCES

[1] Mona A. Ahmed, Hala M. Salem, El-Sayed M. El-Horbaty, Abdel-Badeeh M. Salem, "Analysis of Palm Vein Pattern Recognition Algorithms and Systems", International Journal of Bio-Medical Informatics and e-Health, Vol.1, No.1, June-July 2

[2] Sarah Benziane and Abdelkader Benyettou, "Biometric Technology Based on Hand Vein", Oriental Journal of Computer Science and Technology, Vol.6,No.4,December-2013.

[3] Yingbo Zhou and Ajay Kumar, "Human Identification Using Palm-Vein Images", IEEE Transactions on Information Forensics and Security, Vol.6, No.4, December 2011.

[4] Dileep Kumar and Yeonseung Ryu, "A Brief Introduction of Biometrics and Fingerprint. Payment Technology", International Journal of Advanced Science and Technology, Vol.4, March-2009.

[5] Mi Pan and Wenxiong Kang, "Palm Vein Recognition Based on Three Local Invariant Feature Extraction Algorithms", Biometric Recognition, Vol.7098, 2011.

[6] Yi-Bo Zhang,Qin Li, Jane You and Prabir Bhattacharya," Palm Vein Extraction and Matching for Personal Authentication ",G. Qiu et al. (Eds.): VISUAL 2007, LNCS 4781, pp. 154–164, 2007.

[7]. Wang Lingyu and Graham Leedham," Near- and Far-Infrared Imaging for Vein Pattern Biometrics", Proceedings of the IEEE International Conference on Video and Signal Based Surveillance (AVSS'06).

[8]. Masaki Watanabe, Toshio Endoh, Morito Shiohara, and Shigeru Sasaki," Palm vein authentication technology and its applications". Armin Gruen and Haihong Li, "Semi-Automatic Linear Feature Extraction by Dynamic

[9]. Armin Gruen and Haihong Li, "Semi-Automatic Linear Feature Extraction by Dynamic Programming and LSB-Snakes", Photogrammertric Engineering and Remote Sensing, VOL.63 NO.8.