IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue2)
Available online at www.ijariit.com

An Innovation in Palm Vein Authentication for Biometric Privacy Preservation

M. Suganya
Rathnavel Subramaniam College of Arts & Science,
Sulur, Coimbatore - 402, TN, India
suganyam029@gmail.com

Dr. S. Suganya
Rathnavel Subramaniam College of Arts & Science,
Sulur, Coimbatore - 402, TN, India
suganya_cs@rvsgroup.com

Abstract: In real-time security applications, the image processing, and computer vision play a major part in determining the whole operation. The main advantages of biometric privacy are, to keep the information safe and secure, and access the information from anywhere at any time. In some traditional cases, the security systems are processed by passwords, personal identification numbers, and identification cards. In these cases, several problems occur due to the card was stolen and password hacking. Hence, to avoid such limitations it is necessary to implement the digital biometric data units in terms of face, iris, palm, fingerprints and voice. Among these data, the palm is considered in this work to explore the possibility of cryptography. Initially, the palm images are selected and stored in the database to cross-check the identity of private images which is considered as input, then the enrollment is made by comparing the public host images. The image is authenticated with the help of database with images. Finally, the decision is taken by matching the originally targeted palm image.

Keywords: De-identification, Privacy, Palm Vein Authentication, Visual Cryptography.

I. INTRODUCTION

Biometrics is one of the human characteristics, used for identification and security purposes. It has several advantages when compared with non-biometric applications, such as no external equipment is a need, there is a unique identification hence, data theft is avoided and biometric is always distinctive and made with characteristics. Some examples of biometric are listed as a fingerprint, palm veins, face recognition, DNA, palm print, recognition, retina, and scent.

Biometrics is defined as an automatic identification of an individual based on their behavioral or physiological characteristics. Some of the biometric applications are in entry controls in airport, ATMs and Government programs. Apart from these uses the biometric security is used for real-time applications such as internet banking, household applications and so on. Kataria et al., (2013) made a survey of the biometric techniques. In traditional cases the system is accessed by two step process, first, the process by which the user professes an identity by providing a username and a password used for the purpose of identification. Next, the verification process is made by authenticating the user. Biometric is well suited for both the type of identification and authentication. Commercially, biometric is used in workstations, for access the control over voice or face recognition system, for door security, for portable media such as mobile hard drives and USB sticks.

The biometric authentication system is used to process the registered user's image which is stored in the database. If a new user needs to access the system then it is necessary to register the detail by enrollment process, which is shown in figure 1. Here the information is characteristics by the person. The information stores the data by means of templates. After registration, the user data is collected as private image and recognized by verifying the image which is previously registered an image.

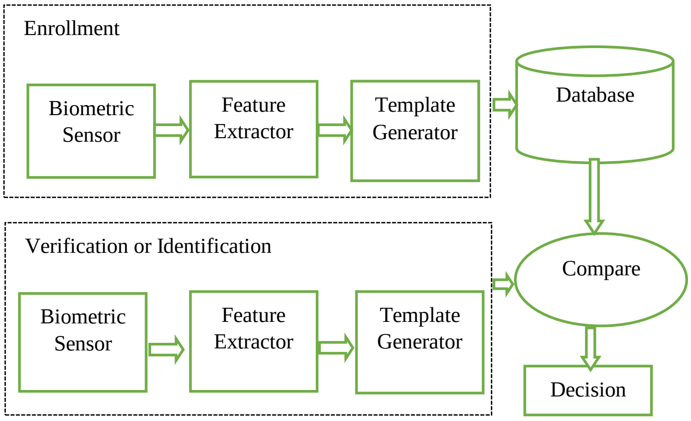

FIG.1. BIOMETRIC AUTHENTICATION PROCESS

The authentication process is common for all types of biometric process, in this research palm print is considered it is similar to fingerprints, palms of the human hands contain a unique pattern of ridges and valleys. Generally, the area of the palm is much larger than the area of a finger and compared with the result, palm prints are expected to be even more distinctive than the fingerprints.

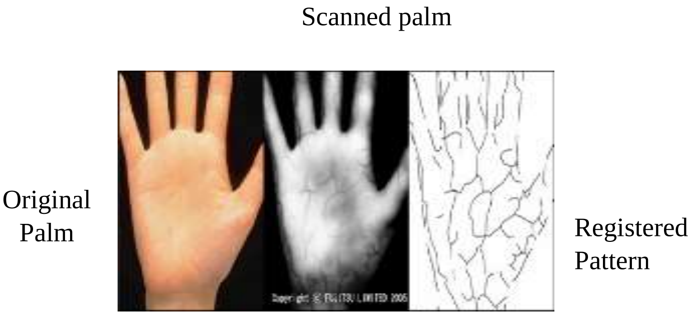

FIG.2. PROCESS OF REGISTRATION

The registered palm pattern is stored in the database along with the personal details of the client, as shown in figure 2, if a palm is placed in the scanner then the special characteristic of the reduced hemoglobin coursing through the palm veins is absorbed near-infrared light. This process takes a snapshot of the outer skin, hence, it is very hard to read or steal.

The scanners used for palm print need to capture a large area, hence, it is bulkier and more expensive than the fingerprint. Human palms also contain additional features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, it results in cheap. If a high-resolution palmprint scanner is used then the geometry features such as width, length, and area of a palm, ridge and valley features such as minutiae and singular points such as deltas, principal lines, and wrinkles may be combined to build a highly accurate biometric authentication system. Generally, in palm print based authentication system hand image of an individual is collected and then processed by preprocessing steps like image thresholding, border tracking, segmentation, and ROI location are sequentially executed to obtain a square region which possesses the palm-print data.

This section illustrated about basic palm registration process and general biometric applications. Section 2 reviews some traditional methods and applications implemented in several applications. Section 3 state's methodology with visual cryptography, in section 4, the experimental results were made for proposed design evaluation. Finally, the paper is summarized in section 5.

II. LITERATURE SURVEY

The automated biometric authentication system is recently developing rapidly, but since it is necessary to enhance the system to outperform the task. This section reviewed in detail about the biometric applications and implementation.Past many researchers were focused on security applications and stated a lot of challenges in biometric. An introduction to biometric authentication systems is made by Wayman et al., (2005), they stated generic biometric system with some of the applications. They also stated some of the security and privacy issues.

Lin and Fan (2004) presented an approach for personal verification using palm-dorsal vein thermal images in patterns. The characteristics of this method is that has no prior knowledge about the objects and the parameters can be set automatically. They have adopted an Infrared (IR) camera to capture the thermal images of the palm-dorsa. Feature Points of the Vein Patterns (FPVPs) are extracted within the region of convergence by modifying the basic tool of watershed transformation based on the properties of thermal images. Finally, the hierarchical integrating function is applied to integrate multiple features and multi-resolution representations. They have made a logical and reasonable method to select a trained threshold for verification.

In biometric technology, the finger vein authentication plays a major role in security and convenience. The image captured by the camera under IR light consists of veins and its backgrounds such as muscles, bones, and tissues. Mulyono and Jinn (2008) proposed a method to enhance the image quality. The noise produced by the camera and the light effect reduces the quality of the Image. They processed the image with adaptive threshold method and matched them using improved template matching.

Based on the real-time applications, to ensure customer security, Suruga bank launched its “Bio Security Deposit” in July (2004), the world’s first financial service to use Palm Secure. This service features high security for customers using vein authentication, it does not require a bank card or passbook and prevents withdrawals from branches other than the registered branch and ATMs thereby minimizing the risk of fraudulent withdrawals. Zhang et al., (2007) proposed personal authentication using palm vein. They included infrared palm images capture, detection of Region of Interest, Palm vein extraction by multi-scale filtering and matching.

Wang and Leedham (2006) made a near and far-infrared imaging for vein pattern biometrics. Badawi (2006) made a hand vein biometric verification prototype for testing performance and patterns similarity. Li et al., (2010) made a palm vein biometric recognition based on curvelet. Wang et al., (2008) presented a person recognition system by fusing palmprint and palm vein images based on “Laplacianpalm” representation. Wang et al., (2007) made an infrared imaging of hand vein patterns for biometric purposes.

Noh et al., (2016) represented some overview and challenges of palm vein biometric system. Akbar et al., (2016) made a palm vein biometric identification system using local derivative pattern.Lu et al., (2016) palm vein recognition using directional features derived from local binary patterns.Lan et al., (2010) made a design based on FPGA-based palm vein acquisition system. Dere et al., (2016) designed a human identification model using palm vein images.

III. RESEARCH METHODOLOGY

From the literature, it is noticed that biometric privacy is improved by the various recognition system, identification model and implemented in some real time systems. This section gives the brief explanation of visual cryptography and methodology used for palm vein based biometric system. The biometric units may differ according to the applications, in this research palm vein is considered for the process. The proposed approach is made with palm vein processing, initially, enrollment process for accessing the secure resource is shown in figure 3.The image is captured by the scanner and stored in the format of the image. The scanned image is a digital image, there is a need to make it as multiple segments called as super-pixels. Then normalization process taken place for changing the range of pixel intensity values, it is carried by sheet models. Finally, the feature extraction is made by convolving the normalized palm vein pattern into one-dimensional wavelet.

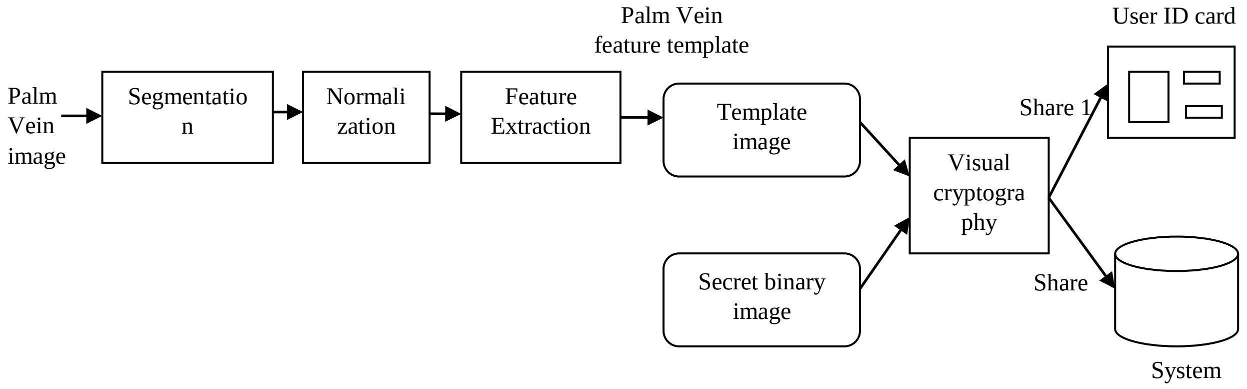

FIG.3. ENROLLMENT PROCESS OF PALM VEIN PROCESSING

After template image generation the secret binary image is compared with the template image to encrypt the pictures. This process is done by a cryptographic technique called as visual cryptography. The encrypted and decrypted images are transferred through this unit and stores the data in the database.A simple algorithm for visual cryptography is given by encrypted images.

Step 1: Create an image of random pixels with the same size and shape as original image consider it as random1.

Step 2: create a second image whose pixels are matched with XOR of first image and original image, it is represented as $random2 = \mathrm{random1} \oplus \mathrm{random2}$

Step 3: Finally, the step1 and Step2 are merged with XOR operation and listed as,$\mathrm{random1} \oplus \mathrm{random2} = \mathrm{random1} \oplus (random1 \oplus original) = original$.

Figure 4 shows the block diagram of the proposed approach for palm vein biometric modalities. The enrollment process made by collecting the private biometric data and sent to a trusted third-party entity.

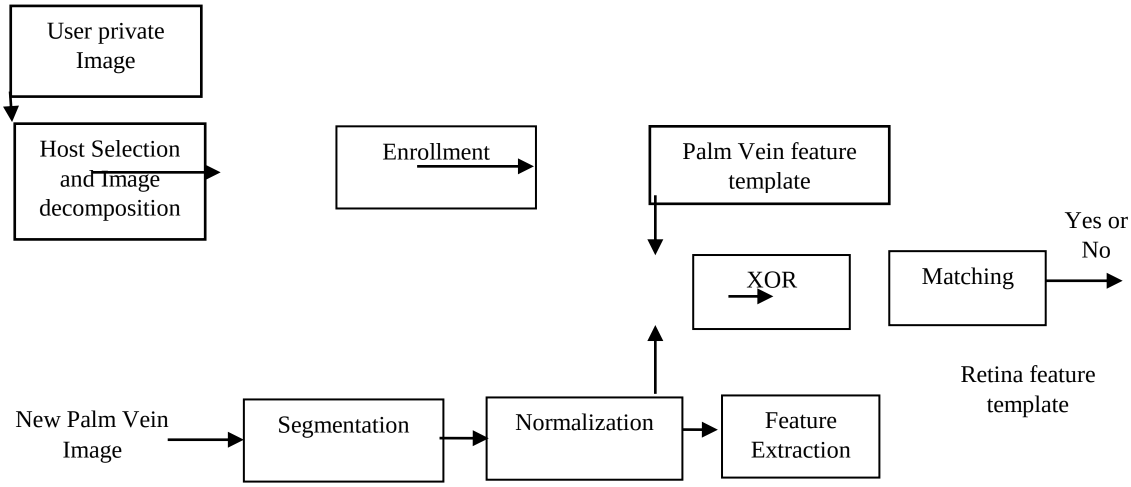

FIG.4. Proposed Approach for De-Identifying and Storing a Palm Vein Image

Once the trusted entity receives the image, then the biometric data is decomposed into two images and the original data is rejected. The use of palm vein as hosts for a private palm vein image has several benefits in the context of biometric applications. First, the demographic attributes of the private palm vein images such as a vein, muscles, extra skin surface in the palm, etc. can be retained in the host images. Second, a set of public palm veins images may be used to host the private palm vein database. Here a small set of public palm vein images can be used to encrypt the entire set of private palm vein images. Finally, the feature template is XOR-logic with the palm vein template from the original database. The last condition states that the matching will be done in a similar manner.Visual Cryptography (VC) is a method used for secret sharing, in this research a secret image called palm vein image is encoded into transparencies, and the stacking of any out of transparencies reveals the secret image. After encryption, there is no way to decrypt-except visual cryptography. Hence, this system is secure for image processing applications. It is one of the best technique used to protect the data such as biometric templates. Naor and Shamir (1994) introduced the visual cryptography scheme (VCS) to allow the secret sharing of images without any cryptographic computations in simple and easy manner.

IV. EXPERIMENTAL RESULTS

The performance analysis for palm vein is made with real time data which is collected and shown in figure 5, here the frame is segmented and processed by the encoding scheme. The overall implementation process is made by MATLAB open source unit.

Table I
Equal error rates (%) at different threshold values

Sl.No	Threshold Values (TH)	Equal Error Rate (EER) (%)
1	131	32.1
2	164	19.2
3	176	7.14

The experimental results were analyzed with the Equal Error Rate (EER) with respect to the threshold value. In the case of palm vein image templates, the proposed method encrypt and send the data over an enrollment process and retrieved by the de-identification unit. The table I shows the result of reconstructed palm vein images with the threshold value of 176 and its error rate is almost 7.14%, these results provides the exact securing of palm vein images.

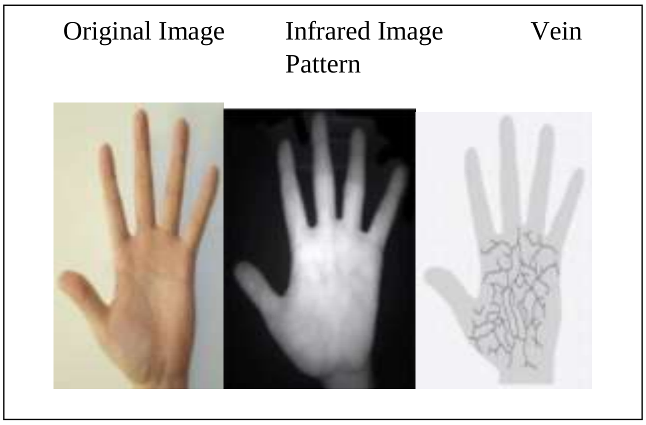

FIG.5. Original Image versus Vein Patterns

TABLE II
EXPERIMENTAL RESULTS FOR INDIVIDUAL SHEET IMAGES

	EER (%)
Reconstructed vs Reconstructed	3.1
Sheet 1 vs Sheet 1	42.1
Sheet 2 vs sheet 2	41.4

The main aim of measuring the error rate is to improve the reconstruction of the original image and to make a secure biometric authentication unit. From the results, it is summarized that the proposed method with visual cryptography is effective for implementing secure biometric authentication unit.

CONCLUSION

The design of the novel biometric system is essential in recent days to eliminate the smart cards and passwords. Hence, it requires a special unit to design the biometric system. This research gives a new direction in the field of biometric cryptosystems analyzed with the palm vein image templates. The experimental results were shown that error rate is reduced if the threshold value increases. The comparison of the previously stored image is compared with the new image which is captured by a camera or by the scanner. The scope of future work is, to implement this proposed method in a real time end to end processing by reducing the error rates.

REFERENCES

[1]. Kataria, A. N., Adhyaru, D. M., Sharma, A. K., & Zaveri, T. H. (2013, November). A survey of automated biometric authentication techniques. In 2013 Nirma University International Conference on Engineering (NUiCONE) (pp. 1-6). IEEE.

[2]. Wayman, J., Jain, A., Maltoni, D., &Maio, D. (2005). An introduction to biometric authentication systems (pp. 1-20). Springer London.

[3]. Lin, C. L., & Fan, K. C. (2004). Biometric verification using thermal images of palm-dorsa vein patterns. IEEE Transactions on Circuits and systems for Video Technology, 14(2), 199-213.

[4]. Mulyono, D., & Jinn, H. S. (2008, April). A study of finger vein biometric for personal identification. In Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on (pp. 1-8). IEEE.

[5]. Zhang, Y. B., Li, Q., You, J., & Bhattacharya, P. (2007, June). Palm vein extraction and matching for personal authentication. In International Conference on Advances in Visual Information Systems (pp. 154-164). Springer Berlin Heidelberg.

[6]. Wang, L., &Leedham, G. (2006, November). Near-and far-infrared imaging for vein pattern biometrics. In 2006 IEEE International Conference on Video and Signal Based Surveillance (pp. 52-52). IEEE.

[7]. Badawi, A. M. (2006). Hand Vein Biometric Verification Prototype: A Testing Performance and Patterns Similarity. IPCV, 14, 3-9.

[8]. Li, Q., Zeng, Y. A., Peng, X., & Yang, K. (2010). Curvelet-based palm vein biometric recognition. Chinese Optics Letters, 8(6), 577-579.

[9]. Wang, J. G., Yau, W. Y., Suwandy, A., & Sung, E. (2008). Person recognition by fusing palmprint and palm vein images based on “Laplacianpalm” representation. Pattern Recognition, 41(5), 1514-1527.

[10]. Wang, L., Leedham, G., & Cho, S. Y. (2007). Infrared imaging of hand vein patterns for biometric purposes. IET computer vision, 1(3/4), 113.

[11]. Noh, Z. M., Ramli, A. R., Saripan, M. I., & Hanafi, M. (2016). Overview and challenges of palm vein biometric system. International Journal of Biometrics, 8(1), 2-18.

[12]. Akbar, A. F., Wirayudha, T. A. B., &Sulistiyo, M. D. (2016, May). Palm vein biometric identification system using local derivative pattern. In Information and Communication Technology (ICoICT), 2016 4th International Conference on (pp. 1-6). IEEE.

[13]. Lu, W., Li, M., & Zhang, L. (2016). Palm Vein Recognition Using Directional Features Derived from Local Binary Patterns. Structure, 9(5).

[14]. Lan, X., Chen, P., & Sun, Z. (2015, May). The design of FPGA-based palm vein acquisition system. In Computer Science and Applications: Proceedings of the 2014 Asia-Pacific Conference on Computer Science and Applications (CSAC 2014), Shanghai, China, 27-28 December 2014 (p. 251). CRC Press.

[15]. Dere, S. N., Gurjar, A. A., &Sipna, C. O. E. T. (2016). Human Identification Using Palm-Vein Images: A New Trend in Biometrics. International Journal of Engineering Science, 2298.

[16]. Naor, M., & Shamir, A. (1994, May). Visual cryptography. In Workshop on the Theory and Application of-of Cryptographic Techniques (pp. 1-12). Springer Berlin Heidelberg.