Cryptosystem Based On Finger Vein Patterns Using Vas Algorithm

G.Kanimozhi, Dr. A. Shaik Abdul Khadir

Abstract: Cryptosystems based on biometrics authentication is developing areas in the field of modernize security schemes. Elastic distortion of fingerprints is one of the major causes for false non-match. While this problem affects all fingerprint identification function, it is especially dangerous in opposite identification function, such as note list and reduplication function. In such function, malicious possessors may purposely distort their fingerprints to evade identification. Distortion rectification (or equivalently distortion field estimation) is viewed as a regression problem, where the input is a distorted fingerprint and the output is the distortion field. The current document deals with the application of finger veins pattern as an approach for possessor confirmation and encryption key generation. The design of the optical imprison scheme by near infrared is described. We propose a step for the location of the vein crossing points and the quantification of the angles between the vein-branches, this information is used to generate a personal key that allows the possessor to encrypt information after the confirmation is approved. In order to demonstrate the potential of the suggested approach, and model of figure encryption is developed. All action: biometric imprison, figure presetting, key generation and figure encryption are performed on the identical hidden platform adding an important portability and diminishing the execution time.

Index Terms: Cryptosystem, hidden platform, biometrics, finger vein identification

1. INTRODUCTION

Biometrics is decided as the computerized identification of respective based on their behavioral and biological distinguishing (fingerprint, retina, voice, etc) [15]. Cryptography, on the other hand, concerns itself with the overhang of expectation with catching expectation from where it previous to where it is needed [2]. During the last decade Biometric has been considered as a promising option for cryptographic function [2]. Fingerprinting emerged [1] as a technological result to prevent irregular comfortable re-distribution. The reaction of low characteristic fingerprints counts on the type of the fingerprint identification scheme. A fingerprint identification scheme can be confidential as either a absolute or opposite scheme. In a absolute identification scheme, such as physical access mastery schemes, the possessor is supposed to be cooperative and desire to be identified. In a opposite identification scheme, such as identifying somebody in note lists and detecting multiple enrollments under different names, the possessor of interest (e.g., criminals) is supposed to be uncooperative and does not wish to be identified. In a absolute identification scheme, low characteristic will lead to false refuse of legitimate possessors and thus bring inconvenience. A typical Biometric based confirmation scheme is composed of two action, the enrollment step: first, a biometric model is taken from an respective; then, this biometric can be appear as an figure or as a set of information that is separated from the model this constitute the so called biometric pattern.

- *G. Kanimozhi Assistant professor, Department of computer science, B.D.U.C.C (W), Orathanadu, gkanimozhi24@gmail.com*
- *Dr. A. Shaik Abdul Khadir, Associate professor, Department of computer science, Khadir Mohideen College, Adirampattinam, Thanjavur (dt), asak_cs_kmc@ymail.com*

Decisively, the biometric information are placed on a information base (local or remotely) [11] and the confirmation step, in which the scheme scans an respective biometric information, extracts biometric aspect in the identical manner and compares them with the pattern of the possessor that the respective claims to be. Vein pattern identification in finger or palm is one of the biometrics approaches for confirmation. Hand vein geometry is based on the role that the vein pattern is distinctive for different respective. The veins under the skin surface absorb infrared light and thus have a darker pattern on the figure of the hand taken by an infrared camera. [1]. Multi authors have suggested several function that involve the use of their own designed schemes to imprison the vein pattern [7] as well as different steps to filter and make the characteristic extraction [20]. It is of elementicular interest the creation of robust and portable schemes that allow the use of hidden platforms as element of the result [6]. In the current document we describe the design, construction and testing of an hidden biometric cryptosystem. The first element of the document covers the creation of the biometric figure acquisition device based on near infrared, followed by the pattern stepping and the key creation this is performed by a suggested step that identifies the vein crossing points and measures the angles between the three branches involved in a common one. The second element of the document is focused on the cryptography application of the scheme to encrypting an figure as an model of its potential. Both action are developed in the identical hidden scheme, this allow us to consider this approach as a portable platform for future application in different environments for instance, the protection of patients information in the medical environment.

2. LITERATURE REVIEW

2.1 HUMAN IDENTIFICATION USING FINGER IMAGES

Computerized human identification using physiological and/or behavioral distinguishing, i.e. biometrics, is increasingly mapped to new civilian function for commercial use. The anatomy of human fingers is quite complicated and largely responsible for the respective of fingerprints and

finger veins. The high respective of fingerprints has been attributed to the casual imperfections in the friction ridges and valleys which are commonly referred to as minutiae or level-2 fingerprint aspect [19]. The acquisition of such minutiae aspect typically requires imaging result higher than 400 dpi. The conventional level-1 fingerprint aspect, which illustrates macro finger details such as ridge flow and pattern type, can be separated from the low result fingerprint figures. Such aspects are useful for fingerprint classification, although the commercially available computerized fingerprint identification schemes barely utilize such level-1 aspect. The figures at such low result typically illustrate friction creases and also friction ridges but with varying clarity. Several biometrics technologies are susceptible to spoof attacks in which fake fingerprints, static palm prints, static face figures can be successfully employed as biometric models to impersonate the identification. Therefore several livens countermeasures to detect such sensor level spoof attacks had exited [1], [28]; for model finger response to electrical impulse [20], finger temperature and electrocardiographic signals [21], time varying perspiration patterns from fingertips [22], and percentage of oxygen saturated hemoglobin in the blood [23]. Despite variety of these suggestions only few have been found suitable for online fingerprint identification and these system require close contact of respective sensors with the fingers, which makes them unsuitable for unconstrained finger figures or when they appear fingers are not in close proximity with the sensors. In this context, the finger vein figures acquired from the near infrared or thermal infrared based optical imaging offers promising alternatives.

2.2 IMAGE REPRESENTATION

Two dimensions the frame criterion developed by Daubechies for one-dimensional wavelets, and it computes the frame bounds for the elementicular case of 2D Gabor wavelets. Completeness criteria for 2D Gabor figure recurrentations are important because of their increasing role in multi computer vision function and also in modeling biological vision, since recent neurophysiologic evidence from the visual cortex of mammalian brains suggests that the filter response profiles of the main class of linearly-responding cortical neurons (called simple cells) are best modeled as a family of self-similar 2D Gabor wavelets. They therefore derive the conditions under which a set of continuous 2D Gabor wavelets will provide a complete recurrentation of any figure, and we also find self-similar wavelet parameterizations which allow stable reconstruction by summation as though the wavelets formed an orthonormal basis. Approximating a “tight frame” generates redundancy which allows low-result neural responses to recurrent high-result figures, as they illustrate by figure reconstructions with severely quantized 2D Gabor coefficients.

2.3 PRIVACY AND SECRECY ASPECTS

These methods are seen to be elegant and interesting building blocks that can substitute or reinforce traditional cryptographic and personal confirmation schemes. However, as Schneier [34] pointed out, biometric information, unlike passwords and standard secret keys, if compromised cannot be canceled and easily substituted: people only have limited resources of biometric information. Moreover, stolen biometric information result in a stolen identity. Therefore, use of biometric information raises privacy concerns, as noted by Prabhakar et al. [30]. Ratha et al. [32] investigated vulnerability points of biometric secrecy schemes, and at the DSP forum [40], secrecy- and privacy-related problems of biometric schemes were discussed. Considerable interest in the topic of biometric secrecy schemes resulted in the proposal of different system over the past decade. Recent developments in this area led to methods grouped around two classes: cancelable biometrics and “fuzzy encryption.” Detailed summaries of these two approaches can be found in Uludag et al. [39] and in Jain et al. [20]. It is the objective of cancelable biometrics, introduced by Ratha et al. [32], [33], Ang et al. [3], and Maiorana et al. [25], to prevent storage of reference biometric information in the clear in biometric confirmation schemes. These methods are based on noninvertible transformations that preserve the statistical properties of biometric information and rely on the assumption that it is hard to exactly reconstruct biometric information from the transformed information and applied transformation. However, hardness of a problem is difficult to prove; and, in practice, the properties of these schemes are assessed using brute-force attacks. Moreover, visual inspection shows that transformed information, e.g., the distorted faces in Ratha et al. [33], still contain a lot of biometric information. In biometric secrecy schemes, a secret key is generated or chosen during an enrollment procedure in which biometric information are observed for the first time. This key is to be reconstructed after these biometric information are observed again during an attempt to obtain access (confirmation). Since biometric measurements are typically noisy, reliable biometric secrecy schemes also extract so-called helper information from the biometric observation at the time of enrollment. This helper information facilitates reliable reconstruction of the secret key in the confirmation step.

3. PROPOSED DESIGN

3.1. DEVICE OVERVIEW

The device is composed by three main hardware components: figure acquisition module, steps module, and physical possessor interface. The figure acquisition module imprisons the figure to be steps and also ensures the identical conditions for any possessor. The steps module is the core of the scheme since it executes finger-vein identification, vein crossing points location and angles quantification between vein branches, the key generation step (during the enrollment step) and the confirmation. It also executes cryptosystem steps to cipher/decipher information as well as handling of inputs/outputs from/to real world. Physical possessor interface is used as the bridge to the real world, it provides inputs to steps module (possessor requests) and also it allows the steps module to display results to the possessor. The steps module is divided into three blocks: Possessor interface, Acquisition sub scheme and Security sub scheme. Acquisition sub scheme is the software component responsible for capturing, presetting, stepping and extract finger vein pattern aspect from possessor. Security subschema is the scheme component that verifies that possessor is allowed

to access the scheme and also it provides the means to cipher/decipher information, adding an extra security level to the scheme.

3.2. BIOMETRIC ACQUISITION

This module is the subschema in charge of the figure acquisition and finger vein pattern stepping, which is shown in Fig. 1.

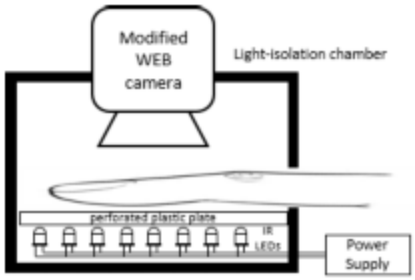


Fig. 1: *Suggested acquisition scheme*

3.3 VAS (VEIN ACQUISITION SYSTEMS) ALGORITHM

Low cost vein acquisition schemes have been developed by different authors for subject identification.

Step: 1 Figure acquisition

We create our own figure acquisition device integrating an infrared web camera, an isolation chamber and a set of 850nm infrared LEDs. Finger vein trans illumination method is adopted to obtain figures where the finger veins appear as a dark pattern.

Step: 2 Figure presets

For an easier and faster subsequent figure steps and feature extraction stages, an figure presets procedure is adopted with the aim to remove noise from the input figure, discard the background from it and accelerate posterior digital steps.

Step: 3 region of interest (ROI)

This procedure consists of a region of interest (ROI) extraction, figure ROI resizing, Gaussian filtering smoothing and background removal using Otsu's segmentation step. Region of interest extraction the input figure is converted to a gray-scale figure to extract a ROI. This prevents working with unwanted information and facilitates digital steps by the hidden platform. Also, ROI is resized in order to speed up sub scheme steps execution.

Step: 4 Input noise removals.

In order to remove noise from the input figure, a Gaussian filter is applied to smooth the ROI. This can be considered as a spatial low pass filter that reduces the figure's high frequencies components.

Step: 5 Gaussian filters

A Gaussian filter is reappear as $G(x, y, \sigma) = K\, e^{x2+y2/2\sigma}$ where σ determines the width of the Gaussian kernel and $K=\frac{1}{2\pi\sigma 2}$ is the normalization constant. Assuming that I (x, y) denotes the ROI, F_G (x, y) denotes the Gaussian filtered I(x, y), we can obtain

$$F_G(x, y) = G(x, y; \sigma) * I(x, y) \qquad (1)$$

Where * denotes convolution function in two dimensions.

Step: 6 Background removals

Multi system has been applied so that background pixels are removed from acquired vein figures [19]. Here, Otsu's segmentation step [12] is used to remove the background from the finger vein figures. It was decided to threshold the Gaussian filtered figure in order to separate the pixels into two classes: C_1, the finger pixels, and C_2, the background. Assuming that $F_R(x; y)$ denote the Gaussian filtered figure $F_G(x; y)$ with background removed by the Otsu's step, we can express the finger vein segmentation as

$$F_R(x,y)=\begin{cases} Fg(x,y), \text{if } Fg(x,y) \geq u; \\ 0, \qquad \text{otherwise} \end{cases} \qquad (2)$$

Where u = [0,255] is the threshold value that maximizes the Otsu's cost function for the binary separation.

Step: 7 Figure Steps

In order to extract efficiently the finger vein network figure, enhancement must be applied. Guided filtering followed by Gabor filtering is applied. Because of the enhancement filtering performance, a simple global threshold segmentation is required to binaries the figure. A thinning step is implemented to get the vein skeleton for a properly feature extraction.

3.4 IMAGE ENHANCEMENT

Adaptive threshold segmentation system have been employed for vein pattern extraction [10]. Nevertheless the noise generation by its use makes it an undesirable technique by itself. Here, a combination of guided filtering followed by multichannel Gabor filtering [17] is the used method so that finger veins are enhanced. Guided filter [3] is a recently alternative suggested as an edge-preserving smoothing operator. A guided filtered figure is obtained by considering the comfortable of a guidance figure, which can be another figure or even the input figure itself. Currently guided filtering has been used to enhance finger vein figures. Assuming that G is the guided filter output in a square window w of radius r centered at the pixel k:

$$G_i = a_k L_i + b_k, \forall i \in w_k \qquad (3)$$

Where L_i is guidance figure and (a_k, b_k) are some linear coefficient assumed to be constant in w_k. This model ensures that G has an edge only if L has an edge, because $\nabla G = \alpha \nabla L$. This linear coefficients are calculated as in [17]. Gabor filter has been suggested as a band pass filter with an excellent performance for noise removal while ridge preservation. A set of three even-symmetric Gabor filters [18] with specific orientations are used so that a enhanced finger vein pattern is suitable to apply a segmentation method. The even-symmetric Gabor filter is reappear as:

$$G_{ak}(x,y)=Ke^{-1/2(x_6{}^2+{}^{y}{}_6{}^2/\sigma 2)} \cos(2\pi f_k x \theta_k) \qquad (4)$$

Where

$$\begin{bmatrix} x\theta \\ y\theta \end{bmatrix} = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

$K=1/2\pi\sigma^{2,}$ k = (1, 2, 3) is the channel index, θ_k and f_k respectively denote the orientation and the center frequency at each channel. Here only three directional Gabor filters were applied in order to reduce computational load, and to prevent redundant information by the application of more directional filters. Assuming that G(x; y) denotes the guided filtered finger vein figure and F (x; y) recurrent the filtered Gabor figure in the kth channel we have,

$$F_k(x,y) = G(x,y) * G_{ak}(x,y) \qquad (5)$$

Where * denotes convolution function in two dimensions. To determine the σ and f_k parameters, the scheme suggested in [9] was used. From the set of Gabor filtered figures F(x; y), the criteria described in [18] was used with the aim to get an integrated Gabor filtered figure.

3.5 IMAGE SEGMENTATION AND THINNING

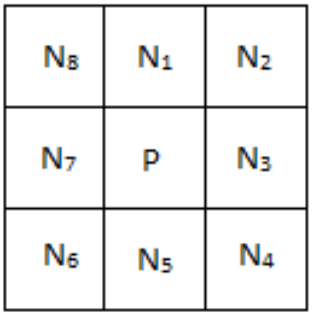
Due to the figure enhancement step, the filtered finger vein figure currents two classes of pixels (finger veins and rest) with a constant tone separation between them. A general global segmentation is used so that a binaries figure is generated. To reduce segmentation noise, morphological opening functions were applied to the segmented figure. For a proper feature extraction from the binaries vein network, a thinning step must be used. The criteria used to thin an figure is described in [8]. The methodology in [8] must be followed so that the feature extraction stage has the desired performance.

4. INDIVIDUAL ENROLLMENT

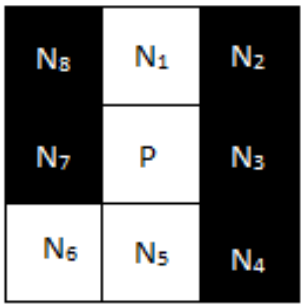
To grant access and encryption/decryption can be performed, a key depending on respective confirmation must be used. Identity verification is necessary so that a registered respective uses the generated key to trigger encryption/decryption action. This confirmation is based on information matching between current and previous registered patterns. For identity verification [13], information like, geometric measurements, corner points and Euclidean distance between figure points, have been used as feature information for information matching. In this work, the crossing points between veins and angles between the branches at those locations are used so that confirmation can be accomplished. The pattern is confirmed by a list of coordinates of each crossing point and the values of the angles between branches, all this information are set in a vector K that recurrent the biometric pattern for the possessor, also the key could obtained from this vector. These sections include the step to find out the crossing points and calculate the described angles shown in Fig. 3, in order to form the pattern.

4.1 INTERSECTION POINTS LOCATION

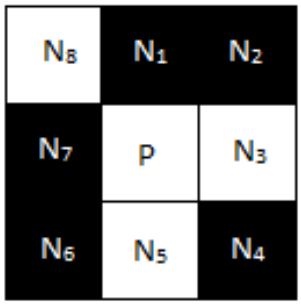
To locate these points, 8 neighborhood connectivity criteria were used. Due to the distinguishing appear in the thinned figure B, a simple procedure is applied in order to trace these locations. Assuming a pixel neighborhood showed in Fig. 2, a vein pixel P is an crossing point candidate if it has 3 pixels vein neighbors N_w, it means three white pixels. To determine that a candidate is a real crossing point, N_w pixels must not be adjacent between them as illustrated in Fig. 2. The difference between a false and a real crossing point can be appreciated in Fig. 2b, and 2c.



(a) Neighborhood Connectivity



(c) Not an intersection point



(c) A real intersection point

Fig. 2: *Intersection Point Localization N_1, N_2, N_3,... N_8 ,are the neighbors candidate pixel P*

4.2 ANGLES MEASUREMENT

To calculate the angles between the branches at a crossing point, the scheme showed in Fig. 3 is adopted. A circle of variable radius is drawn around the crossing point in order to detect those sites where the circle intersects the vein branches. Once identified these sites, it is calculated the Euclidean distance between them. When a circle includes more than one crossing point, its radius is decreased until only one is surrounded. With this, 3 triangles of measured sides (a; b; c) are generated around each crossing point. To calculate the angle between the branches, equation (6) is used. Here is assumed that angles are measured at vertex

A which corresponds to the crossing location as showed in Fig. 3.

$$\theta_i=\arccos (b^2+c^2-a^2)/2bc \ \forall I =1, 2, 3 \qquad (6)$$

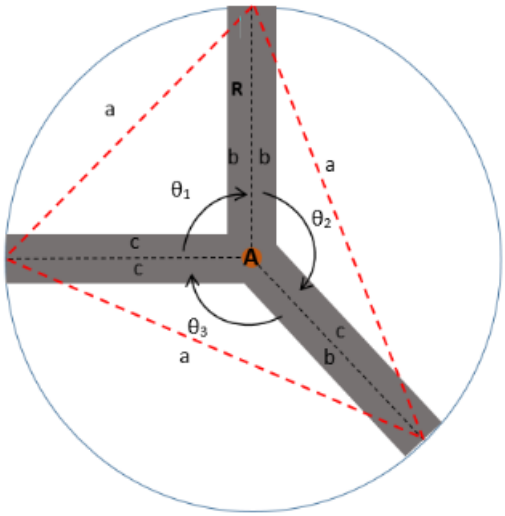


Fig. 3: *Feature Extraction and Angles Measurement Scheme*

When a new vein pattern is registered, a key K is generated using the pattern information. The key for a new respective is reappear as

$$K_u = [x_{r1},y_{r1},\theta_{0r1},\theta_{1r1},\ \theta_{2r1}...x_{rn},y_{rn},\ \theta_{0rn}\ ,\theta_{2rn} \qquad (7)$$

Where n recurrent the number of crossings points detected. For this element work, only the first 16 elements of K are used as the key.

5. SECURITY

5.1 AUTHENTICATION

Once the pattern is obtained from the possessor, it is necessary to compare it against some other already existing in a information base, in this way, the key is revealed and access can be granted to encryption / decryption functions.

The first step is to calculate the Euclidean distance:

$$\sum_{i=0}^{N} \sqrt{(\mathrm{xri}-\mathrm{xci})2+(\mathrm{yri}-\mathrm{yci})2}$$

Where x_{ri} and Y_{ri} are the location of the crossing points of the registered respective and x_{ci} and Y_{ci} are the point from the current possessor. If A < 2 < then equation (8) is applied to calculate the error e between the current pattern K and the registered one K_{ut}

$$\|\mathrm{Kut}-\mathrm{Kuc}\| \qquad (8)$$

Once calculated (8), a threshold value is used to determine if subject is authenticated or not.

5.2 CRYPTOSYSTEM

In order to test the suggested biometric cryptosystem, an figure was ciphered/deciphered using different vein patterns. The first step after subject confirmation is the encryption, the so called Information Encryption Standard (DES) step is used to cipher/decipher information provided by scheme possessors, in this case a figure. DES is a symmetric encryption method based on mixing functions like Advanced Encryption Standard (AES), rather than complex mathematical problems and it is widely used because it is much faster than asymmetric ciphers [4]. For this document BMP figures were used to be encrypted, because this is a raw format and not much step must be done in order to get pixel values. Relevant information of BMP file like width, height, header size and bits per pixel can be obtained from the header of the figure.

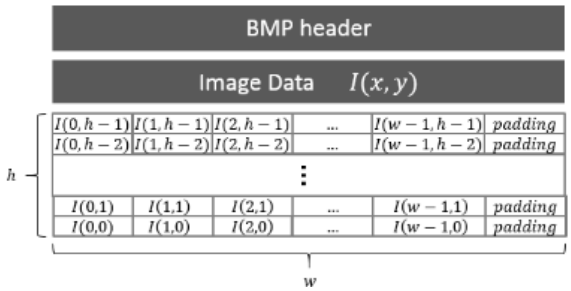


Fig. 4: *BMP File format*

In Fig.4 is shown the basic structure of a BMP file and how pixels are ordered into an figure of width w and height h. It is possible to observe some padding spaces in BMP format, however, these spaces are not considered in any further step. For encryption and decryption action figure information was obtained from BMP file and then it was reordered into a single dimension array as follow: v_k = I(i,j). Where v is single dimension array, i∈[0,h] and j∈[0,w]. Once figure is reordered, v is used as input for encryption and decryption libraries of DES step in open SSL, along with first 16 elements of K_u . Full denoted as: $d_{Ku}(e_{Ku}(v)) = v$. Where $eK_u \in E$ and $dK_u \in D$ are the encryption and decryption steps for every $K_u \in K$. E, D and K recurrent the encryption decryption and key spaces respectively.

5.3 SYSTEM INTEGRATION IN THE EMBEDDED PLATFORM

Hidden implementation was done through two open source libraries: Open CV and Open SSL. Open CV stands for Open source Computer Vision. It is an artificial vision library that has C++, C, Python and Java interfaces and supports Windows, Linux, Mac OS, ions and Android. It was designed for computational efficiency and with strong focus on real time function. Open SSL is an open source library that implements Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols as well as a full-strength general purpose cryptography library. Figure acquisition, figure presets, figure steps, encryption and decryption steps were implemented on a Humming board which is a low cost ARM based platform featuring 1GHz i.MX6 dual core Cortex-A9 and 1 GB of RAM memory. For this document was necessary to create with YOCTO a custom Linux stack, including Open CV and Open SSL libraries keeping Linux figure as small as possible.

6. RESULTS

6.1. IMAGE ACQUISITION DEVICE

The used web camera is a" Perfect Choice PC-320432" and has a result of 1:3Mp. In order to prevent ambient light interference there was built a small chamber using a 3D printer following the structure showed in Fig. 1. Fig. 5 illustrates the complete acquisition device used to get vein figures.

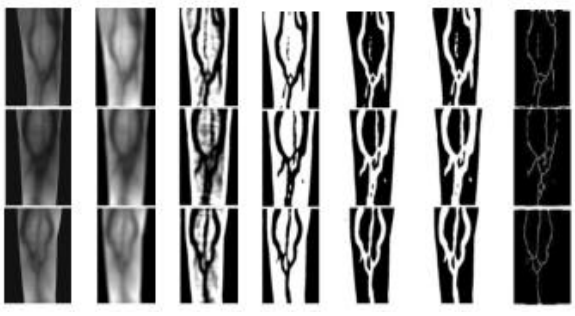
6.2. IMAGE PROCESSING STAGES

The described figure presets and steps stages can be resumed in Fig. 6.

6.2.1 PARAMETERS SELECTION FOR IMAGE PREPROCESSING STAGE:

The input figure taken with the described device above, acquires figures of size 1024x2048 pixels. Then an separated ROI of 710x1024 pixels is resized to generate a gray scale figure of 240x380 pixels. To smooth the figure and remove acquisition noise a Gaussian filter with a kernel of size15x15 and standard deviation of 15 was implemented. Fig. 6 illustrates the presteps stage where the background is removed from figure after Gaussian filtering is applied

Fig. 5: *Finger vein figure acquisition scheme*



(a) (b) (c) (d) (e) (f) (g)

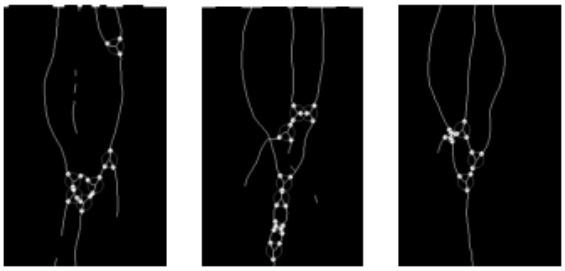
Fig. 6: *Figure steps for 3 respective. (a) Gray Scale Figures. (b) Figure presets. (c) Guided filtering. (d) Multichannel Gabor filtering. (e) Segmentation. (f) Morphological Functions. (g) Figure thinning*

6.2.2 PARAMETERS SELECTION FOR IMAGE PROCESSING STAGE

For finger vein enhancement, guided filtering followed by multichannel Gabor filtering is performed. Here a kernel of size 21x21 pixels is employed for guided filtering the presets figure so that veins are enhanced as showed in Fig. 6. Three channels Gabor filters are applied to enhance more the finger veins in order to make possible to binaries the figure with the specified global thresholding method. The Gabor filters were applied with the following parameters, kernel size of17x17, standard deviation of 16:3, central frequency f_k for every channel k is calculated as in [9], $\theta_k = 0, \frac{\pi}{8}, \frac{7\pi}{8}$), and bandwidth of B_k=(0.70,0.65,0.67). It should be noticed that only three Gabor filters were necessary. Applying more Gabor filter channels generates redundant information and also noise.

6.2.3 RESPECTIVE ENROLLMENT AND AUTHENTICATION:

For fast testing the biometric cryptosystem, just six respective enrollments were achieved. In Fig. 6 and 7 are only displayed the results of 3 respective. The pattern extraction from the subjects is illustrated in Fig. 7, where the circles surround the detected crossing points and the small white circles recurrent the circle-vein's branches points required to measure the angles as specified in Fig. 3. To trigger encryption/decryption step, confirmation must be executed so that possessor's key can be used. Confusion tables and ROC (Receiver Operating Characteristic) space are used to evaluate the confirmation stage performance.



(a) (b) (c)

Fig.7: *Feature extraction from 3 respective (a). Respective (b).Individua2 (c) Individua3*

TABLE 1: *Confusion table for respective identity 1*

RESPECTIVE 1 IDENTITY

		Real values		
		P´	N´	total
Prediction outcome	P´	TP5	FP0	5
	N´	FN0	TN25	25
	total	5	25	30

To achieve this, an experiment involving the six respective was done. In this test, every respective pattern registered is compared against new acquired patterns from all possessors having five attempts, per respective, to achieve

confirmation. With this, a total of 30 confirmation actions were executed per possessor identity. Table I shows the confusion table for the experiment where all possessors had 5 attempts to authenticate as respective 1. In this experiment (p,n) are the real values and (p',n') are the prediction outcomes. The results exhibit a perfect confirmation for respective 1 identity. The rest of the experiments for subjects identities 2 6 appear almost a perfect confirmation due to 1 false opposite outcome for respective 2 identity, a perfect confirmation for respective 3 identity, 2 false absolute outcomes detected for respective 4 and 5 identities, and 2 false opposite outcomes for respective 6 identity.

6.3. SYSTEM PERFORMANCE

Figure acquisition and steps to extract finger vein pattern was completely implemented on the hidden platform, these steps take around 1400ms to 1800ms per iteration to be completed. In other words, as confirmation step is an iterative routine, it could take a variable number of iterations to identify a person. Number of iterations count on several role as: camera result, ambient light conditions, and feature matching step among others. The tests performed on the hidden platform show that the iterations needed to identify a person vary between 5 to 12. Once feature extraction is done, encryption or decryption are performed, both of them take around 250ms to 260ms (for a grayscale figure of 890x890 bytes).

Fig.8: *Experiment of encryption and for 2 different possessor (full description in text)*

In order to show the effectiveness of the suggested scheme two encryption models are compared. For this experiment 2possessors encrypted the input figure I. In the middle column we can see the encrypted result $I_e = e_{kn}(I)$. The final column shows the decrypted figure $I_d = d_{Ku}(I_e)$. In order to illustrate two encryption/decryption step, in Fig. 8 is appear a comparison between two different possessors. A CRC32 step is performed over the encrypted figure and the difference in checksum, shows that scheme is not just able to identify an specific possessor, but also is capable of generating different encrypted information depending on vein pattern used as input key Ku

7. FUTURE WORK

To prevent that, some extra work should be applied to get a specific threshold value per respective identity. Some of the future work has to be focused on solving problems when subjects whose vein pattern current few vein crossing points, the confirmation step can lead to false absolute results, we are currently working on a larger model to fully test the whole scheme.

8. CONCLUSION

This document has suggested a cryptosystem based on finger vein confirmation. First an acquisition device was built in order to get infrared figures where the finger veins appear as a dark network. An figure steps procedure consisting of background removal and finger vein enhancement was implemented so that veins could be easily segmented and a thinned vein pattern could be obtained. Vein crossing points and angles between the branches at those points were calculated to get the pattern from an respective. After respective enrollment, confirmation must be executed so that a possessor can trigger encryption/decryption functions. Even when DES step was used for this document, encryption step is totally independent of the scheme and a complete different step can be used, using the identical inputs: information to encrypt/decrypt and a key. By changing encryption step also times reported must change accordingly. An experiment involving six respective showed almost perfect confirmations for the subject's identities. It should be noticed than using a global threshold value for distance A of equation (8) to determine if possessor is authenticated or not can lead to false absolute and false opposite outcomes.

REFERENCES

[1] D. Bhattacharyya, R. Ranjan, F. Alisherov, and M. Choi, "Biometric authentication: A review," International Journal of u-and e Service, Science and Technology, vol. 2, no. 3, pp. 13–28, 2009.

[2] F. Hao, R. Anderson, and J. Daugman, "Combining cryptography with biometrics effectively," University of Cambridge Computer Laboratory, Tech. Rep, 2005.

[3] K. He, J. Sun, and X. Tang, "Guided image filtering," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 6, pp. 1397–1409, 2013.

[4] J. Hoffstein, J. C. Pipher, J. H. Silverman, and J. H. Silverman, An introduction to mathematical cryptography. Springer, 2008.

[5] T. Ignatenko and F. M. Willems, "Biometric systems: Privacy and secrecy aspects," IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, pp. 956–973, 2009.

[6] S. Joardar, A. Chatterjee, and A. Rakshit, "A real-time palm dorsa subcutaneous vein pattern recognition system using collaborative representation-based classification," IEEE Transactions on Instrumentation and Measurement, vol. 64, no. 4, pp. 959–966, 2015.

[7] A. Kumar and Y. Zhou, “Human identification using finger images,” IEEE Transactions on Image Processing, vol. 21, no. 4, pp. 2228–2244, 2012.

[8] L. Lam, S.-W. Lee, and C. Y. Suen, “Thinning methodologies-a comprehensive survey,” IEEE Transactions on pattern analysis and machine intelligence, vol. 14, no. 9, pp. 869–885, 1992.

[9] T. S. Lee, “Image representation using 2d gabor wavelets,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 18, no. 10, pp. 959–971, 1996.

[10] M. Mansoor, S. Sravani, S. Zahra Naqvi, I. Badshah, and M. Saleem, “Real-time low cost infrared vein imaging system,” in Signal Processing Image Processing & Pattern Recognition (ICSIPR), 2013 International Conference on. IEEE, 2013, pp. 117–121.

[11] M. Murillo-Escobar, C. Cruz-Hern´andez, F. Abundiz-P´erez, and R. L´opez-Guti´errez, “A robust embedded biometric authentication system based on fingerprint and chaotic encryption,” Expert Systems with Applications, 2015.

[12] N. Otsu, “A threshold selection method from gray-level histograms,” Automatica, vol. 11, no. 285-296, pp. 23–27, 1975.

[13] K. Parthiban, A. Wahi, S. Sundaramurthy, and C. Palanisamy, “Finger vein extraction and authentication based on gradient feature selection algorithm,” in 2014 Fifth International Conference on the Applications of Digital Information and Web Technologies (ICADIWT). IEEE, 2014, pp. 143–147.

[14] R. Raghavendra, K. B. Raja, J. Surbiryala, and C. Busch, “A low-cost multimodal biometric sensor to capture finger vein and fingerprint,” in 2014 IEEE International Joint Conference on Biometrics (IJCB). IEEE, 2014, pp. 17.

[15] C. Rathgeb and A. Uhl, “A survey on biometric cryptosystems and cancelable biometrics,” EURASIP Journal on Information Security, vol. 2011, no. 1, pp. 1–25, 2011.

[16] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, “Biometric cryptosystems: issues and challenges,” Proceedings of the IEEE, vol. 92, no. 6, pp. 948–960, 2004.

[17] S. J. Xie, J. Yang, S. Yoon, L. Yu, and D. S. Park, “Guided gabor filter for finger vein pattern extraction,” in 2012 Eighth International Conference on Signal Image Technology and Internet Based Systems (SITIS). IEEE, 2012, pp. 118–123.

[18] J. Yang, J. Yang, and Y. Shi, “Finger-vein segmentation based on multichannel even-symmetric gabor filters,” in IEEE International Conference on Intelligent Computing and Intelligent Systems, 2009. ICIS 2009., vol. 4. IEEE, 2009, pp. 500–503.

[19] A. Yimit, M. Takagi, Y. Hagihara, T. Miyoshi, and Y. Hagihara, “Visual vein segmentation for an intravenous injection support system,” in SICE Annual Conference (SICE), 2013 Proceedings of. IEEE, 2013, pp. 2290–2295.

[20] Yuksel, L. Akarun, and B. Sankur, “Hand vein biometry based on geometry and appearance methods,” IET computer vision, vol. 5, no. 6, pp. 398–406, 2011.