Biometric Key Generation In Digital Signature Of Asymmetric Key Cryptographic To Enhance Security Of Digital Data

Kamini H Solanki[1] ,Chandni Patel[2]

Abstract— Associating an identity with an individual is called personal identification. A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual. The problem of resolving the identity of a person can be categorized into two fundamentally distinct types of problems with different inherent complexities: (i) Verification (authentication) and (ii) Recognition (identification). The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. In the absence of robust personal recognition schemes, these systems are exposed to the tricks of a fraud. Biometric recognition or, simply, biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. With the increasing reliance on electronic information, which needs to be exchanged across the internet or stored on open networks, cryptography is becoming an increasingly important feature of computer security. A biometric key dependent cryptosystem is proposed, to ensure the security of the whole system by using fingerprint features as a key in a cryptosystem. In this paper, extract the features of the fingerprint and use cryptography for related privacy concerns. Key generates from fingerprint and uses that key in digital signature to convert plain text into digital signature in asymmetric cryptography.

Index Terms—Biometrics, Fingerprint, Minutiae points, Cryptography, Key generation, asymmetric key, digital signature of cryptography.

1. INTRODUCTION

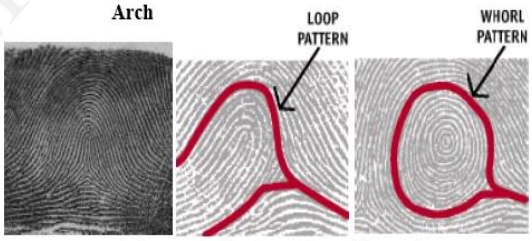
Fingerprint identification is one of the most important biometric technologies. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. Each individual has unique fingerprints. The uniqueness of a fingerprint is exclusively determined by the local ridge characteristics and their relationships.

Fingerprint Acquisition

The first challenge facing a finger scan system is to acquire a high quality image of the fingerprint. Image quality is measured by dots per inch (DPI)- more DPI means a high resolution image. The lowest DPI generally found is the 300 to 350 DPI range.

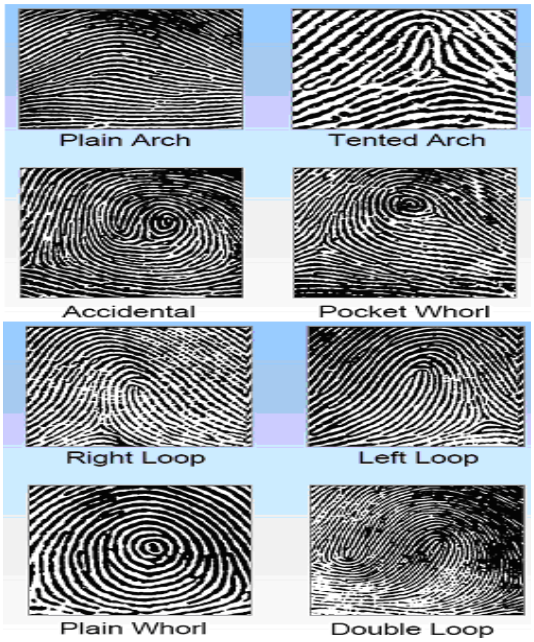
Fingerprint Representation

There is seven patterns of papillary ridge i.e. *Loop, Arch, Whorl, Tented Arch, Double Loop, Central Pocked Loop* and *Accidental.* From seven patterns of papillary ridge there are three patterns which most common like depicted below:



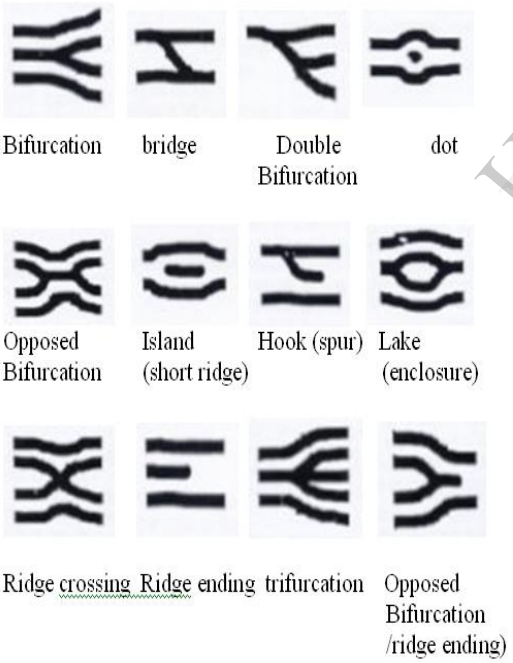
Fig(1) ridge pattern examples

- The human population has fingerprints in the following percentages:
  - Loop – 65%
  - Whorl -- 30%
  - Arch -- 5%



Fig(2) Some Fingerprint Patterns

Fingerprint Basics (minutiae)



Fig(3) Different minutiae

Feature Detection for Matching

Fig(4) Finger – scan minutiae

2. Methodology of image enhancement

- Segmentation
- Normalization
- Orientation estimation
- Ridge frequency estimation
- Gabor filtering

2.1 Segmentation

Image segmentation is the first step in the in the enhancement algorithm. Image segmentation is used to locate objects and boundaries like lines, curves in images. In a fingerprint image there are foreground regions and the background regions .The foreground regions show the ridges and valleys while the background regions are to be left out. The foreground regions have a high variance value while the background regions have low values. Segmentation separates the foreground regions from the background image for reliable extraction of minutiae.

The image is divided into blocks. For each block the gray scale variance is calculated. If the value is lower than the global threshold it is assigned to the background else it is assigned to the foreground.

Let V(k) be the variance for a block of size W×W. Then

$$V(k) = 1/W^2 \sum_{i=0}^{W-1} \sum_{j=0}^{W-1} (I(i,j) - M(k))^2$$

Where I(i.j) is the grey scale value at pixel(i,j) and M(k) is the mean gray value.

The variance threshold separates the foreground regions from the background regions. The foreground regions that are segmented are the

areas having the ridge structures. The remaining regions are untouched. However the threshold must be given properly. If the threshold value is too large, foreground regions may be incorrectly assigned as background regions. Conversely, if the threshold value is too small, background regions may be assigned as part of the fingerprint foreground area. A variance threshold of around 100 has been found to give optimal results in terms of differentiating the foreground and background regions.

2.2 Normalization

It is the next step in the enhancement algorithm. Normalization is done so that the gray level values lies within a given set of values. The fingerprint image is normalized to have a predefined mean and variance. This is required as the image usually has distorted levels of gray values among the ridges and the valleys. Normalization allows to standardize the distorted levels of variation in the gray scale values. Normalization involves pixel-wise operations and does not change the ridge and valley structures.

Normalization is a linear process. Suppose the intensity range of the image is 50 to 180 and the desired range is 0 to 255 the process entails subtracting 50 from each of pixel intensity, making the range 0 to 130. Each pixel intensity is multiplied by 255/130, making the range 0 to 255.

The normalized image is given by

$$N(i,j) = M_0 + \sqrt{V_0(I(i,j) - M)^2/V} \quad \text{if } I(i,j) > M$$

$$M_0 - \sqrt{V_0(I(i,j) - M)^2/V} \quad \text{otherwise}$$

Where for a pixel I(i,j) the estimated mean and variances are M and V respectively. M0 and V0 denote the desired mean and variance values.

Histogram equalization, as normalization method, is a process to enhance the contrast of images by transforming its intensity values. Usually a fingerprint image has different gray values for every pixel. It is desirable to have the gray value around a mean value. This is achieved by histogram equalization. It increases the local contrast of images. Thus the intensities can be distributed on the histogram. This allows for areas of lower local contrast to gain a higher contrast without affecting the global contrast. Histogram equalization accomplishes this by effectively spreading out the intensity values.

The histogram of the original image illustrates that all the intensity values lie on the right hand side of the 0–255 scale, with no pixels in the left hand side. The histogram of the normalised image shows that the range of intensity values has been adjusted such that there is a more balanced distribution between the dark and light pixels. Normalizing the image improves the contrast between the ridges and valleys. It does not alter the shape of the original histogram plot. The relative position of the values along the *x* axis is shifted.

2.3 Ridge Orientation estimation

The next step is calculation of orientation image. Orientation calculation is critical for fingerprint image enhancement and restoration in both frequency and spatial domain. The orientation image represents the local orientation of the ridges and is a matrix of direction vectors. It is important as Gabor filtering depends on the proper orientation.

Most of the fingerprint classification and identification processes calculate the local ridge orientation of the fixed-size block instead of each pixel. The simplest and most natural approach for extracting local ridge orientation is based on computation of gradients in the fingerprint image. The gradient based approach is used to find the gradient. The gradient is perpendicular to the orientation vector.

Suppose the image is divided in square blocks of 15×15. In each block, frequencies F[i], i = 0...7 for eight directions are calculated. The average frequency is computed. Then the difference between the frequency for each direction and average frequency is calculated. For very pixel the gradient is calculated and standard deviation for the eight directions is calculated. If standard deviation is larger than a threshold, then the direction with the maximum frequency is regarded as the dominant direction. Otherwise, weighted average direction is computed as the dominant direction. The orientation vector for each block can be found out.

For this a block of W×W is chosen. The gradient in the horizontal and vertical directions are found and given by $\partial x(i,j)$ and $\partial y(i,j)$.

The local orientation is given by

$$V_x(i,j) = \sum_{p=i-W/2}^{i+W/2} \sum_{q=j-W/2}^{j+W/2} 2\partial_x(p,q)\partial_y(p,q)$$

$$V_y(i,j) = \sum_{p=i-W/2}^{i+W/2} \sum_{q=j-W/2}^{j+W/2} \partial^2_y(p,q)\partial^2_x(p,q)$$

$$\Phi(i,j) = 0.5 \tan^{-1}(V_y/V_x)$$

$\Phi(i,j)$ is the orientation estimation.

The ridges are oriented in a local direction for proper Gabor Filtering. It can produce accurate orientation estimates in the presence of minimal amounts of noise, but its perform deteriorates under high levels of noise.

2.4 Ridge frequency estimation

Local ridge frequency is another important parameter used in the construction of the Gabor filter. The local ridge frequency fxy at point [x, y] is the number of ridges per unit length along a hypothetical segment centered at [x, y] and orthogonal to the local ridge orientation θxy. A frequency image F, analogous to the orientation image D, can be defined if the frequency is estimated at discrete positions and arranged into a matrix.

The first step in the frequency estimation stage is to divide the image into blocks of size W×W. The next step is to project the gray-level values of all the pixels located inside each block along a direction orthogonal to the local ridge orientation. It forms an almost sinusoidal-shape wave with the local minimum points corresponding to the ridges in the fingerprint. The ridge spacing is calculated by counting the number of pixels between consecutive minima points in the projected waveform.

Let R(i,j) be the ridge spacing. For a block of size W×W, it is calculated by counting number of pixels between minutiae points. Then the ridge frequency F(i,j) is given by

$$F(i,j) = 1/R(i,j)$$

The ridge frequency values are presented in terms of ridge wavelength. The presence of noise leads to the creation of false local minima, which mask out the location of the true minimum points. These false minima can then lead to an inaccurate estimation of the ridge wavelength. Thus the noise needs to be filtered out for proper ridge frequency estimation. The image can now be applied to a Gabor filter. All fingerprints do not exhibit the same average ridge wavelength . Different ridge wavelength values may result from different fingerprints.

2.5 Gabor Filtering

Gabor filter is a linear filter used for edge detection. A Gabor filter is a linear filter whose impulse response is defined by a harmonic function multiplied by a Gaussian function .Gabor filter can be viewed as a sinusoidal plane of particular frequency and orientation, modulated by a Gaussian envelope.

The Gabor filter is represented by

$$G(x, y, \Omega, f) = \exp\{0.5[x^2_\theta/\phi^2_x + y^2_\theta/\phi^2_y]\} \cos(2\pi f x_\theta)$$

$$x_\theta = x\cos\theta + y\sin\theta$$

$$y_\theta = -x\sin\theta + y\sin\theta$$

where θ is the orientation of the Gabor filter, f is the frequency of the wave, θx and θy are the standard deviations of the Gaussian function and xθ , yθ denote the x and y axes of the filter respectively.

Gabor filters have frequency-selective and orientation-selective properties which allow the filter to be tuned to give maximal response to ridges at a specific orientation and frequency in the fingerprint image. Once the ridge orientation and ridge frequency information has been determined, these parameters are used to construct the even-symmetric Gabor filter.

The Gabor filter is applied to the fingerprint image by convoluting the filter and image. For a pixel (i,j), the orientation value and ridge frequency value are required.

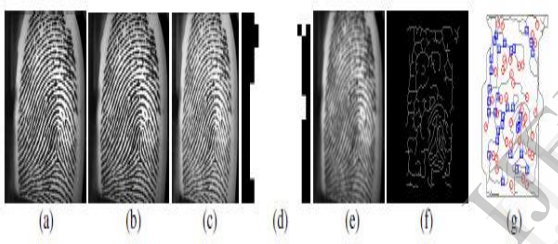
In fingerprint enhancement, Gabor filter can be tuned to specific frequency and orientation values. As the ridge orientation and frequency estimation has already been calculated, the Gabor filter can enhances the ridges in the direction of local orientation effectively preserving the ridge structures. The value of ∂x determines the degree of contrast enhancement and the value of ∂y determines the smoothing of the ridges. A large value will result in blurring of the images whereas a low value would not be effective in removing noise from the images. So a suitable value of ∂x and ∂y must be taken.

3. Minutiae extraction*:* The process of minutiae point extraction is carried out in the enhanced fingerprint image.

The steps involved in the extraction process are,

• **Binarization:** Binarization is the process of converting a grey level image into a binary image. It improves the contrast between the ridges and valleys in a fingerprint image, and thereby facilitates the extraction of minutiae. The grey level value of each pixel in the enhanced image is examined in the binarization process. If the grey value is greater than the global threshold, then the pixel value is set to a binary value one; or else, it is set to zero. The output of binarization process is a binary image containing two levels of information, the foreground ridges and the background valleys. The minutiae extraction algorithms are good operating on binary images where there are only two levels of interest: the black pixels that denote ridges, and the white pixels that denote valleys.

The input fingerprint image, the extracted minutiae points and the intermediate results of the proposed approach are shown in figure Finally, the generated 128-bit cryptographic key obtained from the proposed approach is shown in figure



Fig(5) Filtration of fingerprint images

(a) Input fingerprint image
(b) Histogram Equalized Image
(c) Wiener Filtered Image
(d) Segmented Image
(e) Enhanced image
(f) Morphological Processed Image (g) Fingerprint image with Minutiae points

4. Cryptography

Cryptography plays a very vital role in keeping the message safe as the data is in transit. It ensures that the message being sent at one end remains confidential and should be received only by the intended receiver at the other end. Cryptography converts the original message in to non readable format and sends the message over an insecure channel. The people who are unauthorized to read the message try to break the non readable message but it is hard to do it so. The authorized person has the capability to convert the non readable message to readable one. The original message or the actual message that the person wishes to communicate with the other is defined as Plain Text. The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. Encryption is the process of converting plaintext into cipher text with a key. A Key is a numeric or alpha numeric text or may be a special symbol. A decryption is a reverse process of encryption in which original message is retrieved from the cipher text. Encryption takes place at the sender end and Decryption takes place at the receiver end.

5. Goals of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today.
Following are the various goals of cryptography.

Confidentiality
Information in computer is transmitted and has to be accessed only by the authorized party.
Authentication
The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.
Integrity
Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.
Non Repudiation
Ensures neither the sender, nor the receiver of message can deny the transmission.
Access Control
Only the authorized parties are able to access the given information.

6. Types of Cryptography Key

• **Symmetric Key Cryptography**
In symmetric Cryptography the key used for encryption is similar to the key used in decryption. Thus the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6, BLOWFISH.

- **Asymmetric Key Cryptography**

In Asymmetric Cryptography, two different keys are used for encryption and decryption- Public and Private. The public key is meant for general use so it is available to anyone on the network. Anyone who wants to encrypt the plaintext should know the Public Key of receiver. Only the authorized person can be able to decrypt the cipher text through his own private key. Private Key is kept secret from the outside world. Symmetric Encryption Algorithm runs faster as compared to Asymmetric key algorithms. Also the memory requirement of Symmetric algorithm is lesser as compared to asymmetric.

7. Digital signature

The process of digitally signing starts by taking a mathematical summary (called a *hash code*) of the check. This hash code is a uniquely-identifying digital fingerprint of the check. If even a single bit of the check changes, the hash code will dramatically change. The next step in creating a digital signature is to sign the hash code with your private key. This signed hash code is then appended to the check. How is this a signature? Well, the recipient of your check can verify the hash code sent by you, using your public key. At the same time, a new hash code can be
created from the received check and compared with the original signed hash code. If the hash codes match, then the recipient has verified that the check has not been altered. The recipient also knows that only you could have sent the check because *only you have the private key that signed the original hash code.* Confidentiality and encryption Once the electronic check is digitally signed, it can be encrypted using a high-speed mathematical transformation with a key that will be used later to decrypt the document. This is often referred to as a *symmetric key* system because the same key is used at both ends of the process. As the check is sent over the network, it is unreadable without the key. The next challenge is to securely deliver the symmetric key to the bank. Public-key cryptography for delivering symmetric keys Public-key encryption is used to solve the problem of delivering the symmetric encryption key to the bank in a secure manner. To do so, you would encrypt the symmetric key using the bank's public key. Since only the bank has the corresponding private key, only the bank will be able to recover the symmetric key and decrypt the check. Why use this combination of public-key and symmetric cryptography? The reason is simple. Public-key cryptography is relatively slow and is only suitable for encrypting small amounts of information – such as symmetric keys. Symmetric cryptography is much faster and is suitable for encrypting large amounts of information.

The following illustration describes what Entrust does behind the scenes to deliver the secure electronic check.

The following procedure is outlined for providing a level of message integrity.

1. Encrypt the text with your private key to generate signature.
2. Send both the encrypted text and normal text to the recipient.
3. Recipient decrypt the encrypted text with your public key

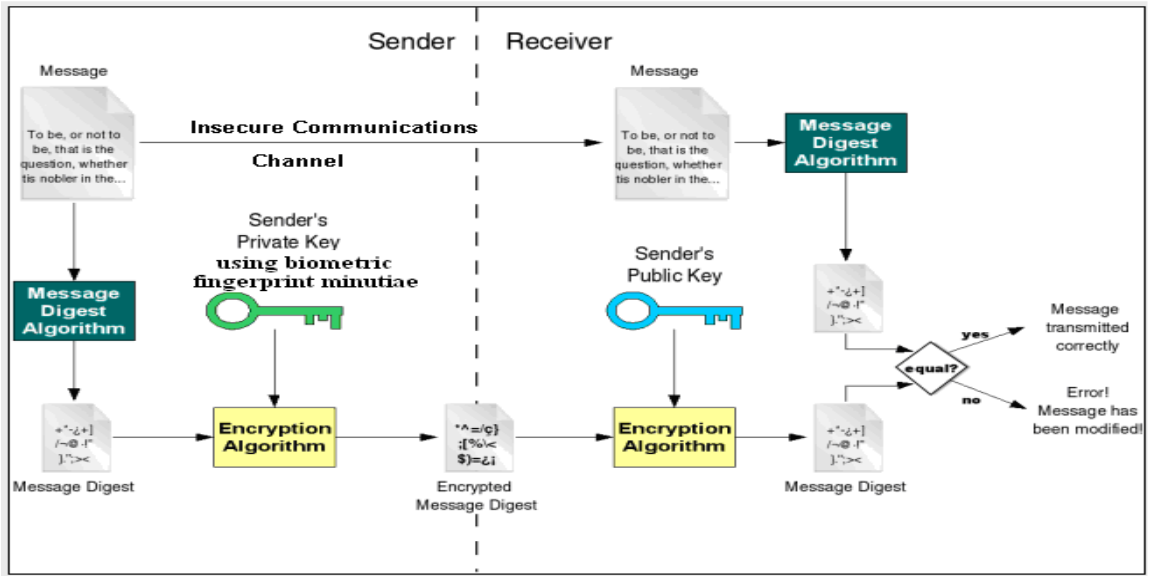


Figure 6. Digital Signature of asymmetric cryptography

8. CONCLUSION

Biometrics-based Key Generation has been found to outperform traditional cryptographic systems, chiefly because, it is impossible for a person to lose his/ her biometrics, and also the biometrics are intricate to falsify or steal. In this paper, we have presented an efficient approach for generation of irrevocable cryptographic keys from fingerprint biometrics using minutiae extraction from biometric image. The approach has been composed of two phases namely:

1) Minutiae points' extraction from the fingerprint image,

2) Cryptographic key generation from Secured finger print minutiae in digital signature.

The resultant Biometric key generated from fingerprint minutiae in asymmetric cryptography, has been irrevocable and unique to a specific identity, providing better protection and replacement features for lost or stolen biometrics. The Proposed work has represented the effectiveness and enhances security in generating an irrevocable cryptographic key.

9. REFERENCES

[1] C.E. Shannan, "Communication Theory of Security System", Bell, System Technical Journal , vol 28,pp.656-715,1949.

[2] Nalini. N and G. Raghavendra Rao," A New Encryption and Decryption Algorithm Combining the Features of Genetic Algorithms(GA) and Cryptography"

[3] H. Feistel ," Cryptography and Computer Privacy", Scientific American Vol. 228 ,no. 5,pp 15-23,1973.

[4] Uttam Kr. Mondal**,"** Frame Based Symmetric Key Cryptography **",** Int. J. Advanced Networking and Applications 762, Volume: 02, Issue: 04, Pages: 762-769 (2011)

[5] K. Hassanain1 ,M. Shaarawy, E. Hesham2," A Proposal for a Biometric Key Dependent Cryptosystem " , Global Journal of Computer Science and Technology , Vol. 10 Issue 11 (Ver. 1.0) October 2010.

[6] Dr.R.Seshadri , T.Raghu Trivedi,"Efficient Cryptographic Key Generation using Biometrics" , Int. J. Comp. Tech. Appl., Vol 2 (1), 183-187, ISSN: 2229-6093

[7] Sunil V. K. Gaddam 1 and Manohar Lal 2," Efficient Cancellable Biometric Key Generation Scheme for Cryptography ",International Journal of Network Security, Vol.11, No.2, PP.61{69, Sept. 2010

P.Arul, Dr.A.Shanmugam "Generate a Key For AES Using Biometric For VOIP Network Security" Journal of Theoretical and Applied Information Technology 2009.107-112.

[8]Principles of fingerprint (http://www.biometricnewsportal.com/fingerprint_biometrics.asp)

[9]. Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K.Jain "Biometric Cryptosystems Issues and Challenges"Proceedings of the IEEE 2004.

[10] Sunil V. K. Gaddam 1 and Manohar Lal 2,"Effecient Cancellable Biometric Key Generation Scheme for Cryptography" International Journal of Network Security, Vol.11, No.2, Sep. 2010.