Generate a key for MAC Algorithm using Biometric Fingerprint

Dr.R.Seshadri[1] and T.Raghu Trivedi[2]
[1]Director, University Computer Center, S.V. University, Tirupathi, Andhra Pradesh,India.
ravalaseshadri@gmail.com
[2]Research Scholar, University Computer Center, S.V. University, Tirupathi, Andhra Pradesh,India.
tamirisa_t1@yahoo.com

Abstract

One of Authentication technique involves the use of a secret key to generate a small fixed size block of data known as cryptographic checksum or MAC that is appended to the message.

The unauthorized thefts in our society have made the requirement for reliable information security mechanisms. Information security can be accomplished with the help of a prevailing tool like cryptography, protecting the cryptographic keys is one of the significant issues to be deal with. Here we proposed a biometric-crypto system which generates a cryptographic key from the Finger prints for calculating the MAC value of the information we considered fingerprint because it is unique and permanent through out a person's life.

Key words *MAC, Fingerprint, Encryption, Decryption, Minutiae point, ROI.*

1. Introduction

Message authentication code is a public function of the message and a secret key that produces a fixed length value that serves as the authenticator. Protecting the secret key is major issue.we are going to use the biometrics for generating /protecting the secret key. A fingerprint is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutia points: ridge endings and ridge bifurcations. Many types of minutiae exist, including dots. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. There are five basic fingerprint patterns: arch, tented arch, left loop, right loop and whorl. Loops make up 60% of all fingerprints, whorls account for 30%, and arches for 10%.Fingerprints are usually considered to be unique, with no two fingers having the exact same dermal ridge characteristics. Here we use Novel method of biometrics based key generation technique. Biometric crypto systems can operate in one of the following three modes 1.Key Release 2.Key binding 3.Key generation. Here we use the key generation mode in which the key is derived directly from the biometric data and is not stored in the data base.

2. MAC

This is one of the message authentication techniques. This technique assumes that two communicating parties, say A,B share a common secret key k when A has a message to send to B, it calculates the MAC as a function of the message and the key MAC=$C_{k(}$(M). The message plus MAC are transmitted to the intended recipient. The recipient performs the same calculation on the

received message, using the same secret key, to generate a new MAC. The received MAC is compared to the calculated MAC.

If we assume that the receiver and the sender know the identity of the secret key. If received MAC matches the calculated MAC then receiver is assured that message has not been altered and the message is from alleged sender. MAC functions similar to encryption one difference is MAC algorithm need not be reversible , as it must for decryption .To provide confidentiality message is encrypted before the MAC algorithm .Here we need two separate keys, each of which shared by sender and receiver [1] .

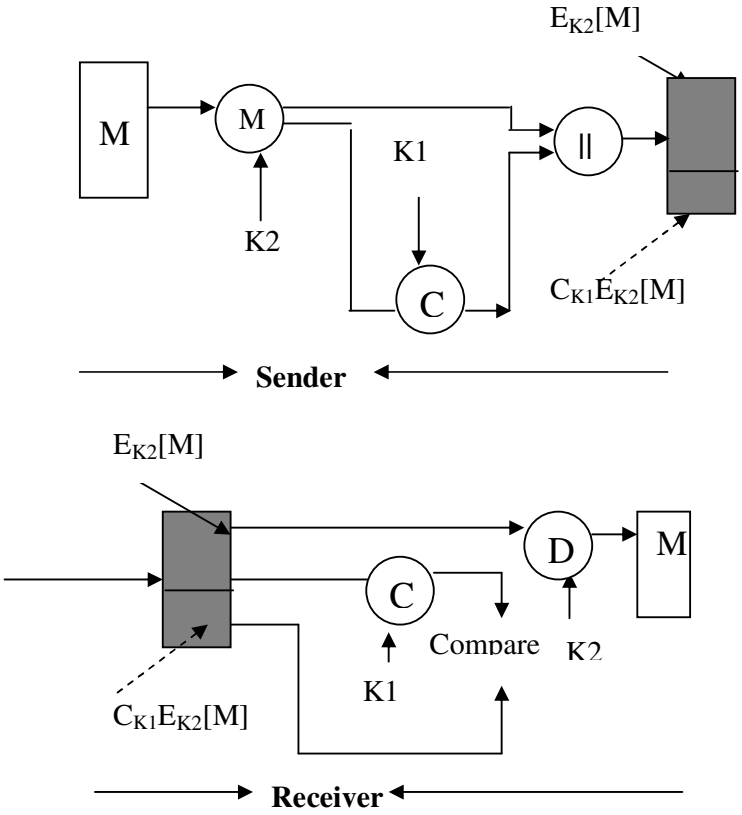

Figure1.Encryption and Decryption

3. How does fingerprint biometrics work

Maintaing and sharing the lengthy keys is critical problem. This can be overcome with the help of biometric system [2].Here we will use finger print.

The main technologies used to capture the fingerprint image with sufficient detail are optical, silicon, and ultrasound. There are two main algorithm families to recognize fingerprints:

Minutia matching compares specific details within the fingerprint ridges. At registration (also called enrollment), the minutia points are located, together with their relative positions to each other and their directions. At the matching stage, the fingerprint image is processed to extract its minutia points, which are then compared with the registered template.

Pattern matching compares the overall characteristics of the fingerprints, not only individual points. Fingerprint characteristics can include sub-areas of certain interest including ridge thickness, curvature, or density. During enrollment, small sections of the fingerprint and their relative distances are extracted from the fingerprint. Areas of interest are the area around a minutia point, areas with low curvature radius, and areas with unusual combinations of ridges.

Key vector Is formed based on minutiae points (ridge ending and ridge bifurcation)

4. Generating key vector from finger print

Step1: Capture finger print image

Step2: Minutiae points' extraction.

Step3: Key vector generation.

For key generation we need following concepts

4.1 Minutiae Points Extraction from Fingerprints

It is supposed that fingerprints are distinct across individuals and across the fingers of a particular individual [3]. Minutiae points are feature points extracted from a raw fingerprint image

A fingerprint can be defined as a pattern of ridges and valleys on the tip of the finger. A fingerprint is therefore described by the distinctiveness of the local ridge features and their relationships. Minutiae points denote these local ridge characteristics that appear either at a ridge ending or a ridge bifurcation. The point where the ridge comes to an abrupt end is known as ridge ending and the ridge bifurcation is denoted as the point where the ridge divides into two or more branches [3]. Minutiae points' extraction involves

- Segmentation
- Image Enhancement
- Minutiae Extraction

4.1.1Segmentation

The first step in the minutiae points' extraction is segmentation. The input fingerprint image is segmented from the background to actually extract the region comprising the fingerprint. Segmentation of an image represents the division or separation of the image into regions that have similar attributes. At first, the image is pre-processed. The pre-processing phase includes histogram equalization and Median filter. The pre-processed image is divided into blocks and segmentation is carried out.

4.1.1. a Histogram Equalization

Histogram equalization amplifies the local contrast of the images, particularly when they are represented with very close contrast values. Intensity is distributed through the histogram with the aid of this regulation. Histogram equalization converts the input image so that out put image comprises a uniform distribution of intensities The histogram, after the histogram equalization transforms all the range from 0 to 255 which results if enhanced visualization effect [4].

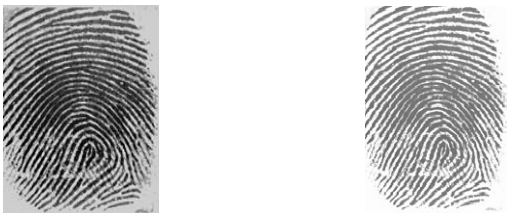

Figure2. Fingerprint image before and after Histogram Equalization

Median filter is a non-linear digital filtering methodology frequently employed to eliminate noise from images or other signals.

Preprocessed fingerprint image is divided into non-overlapping blocks of size 16x16 followed by the calculation of gradient of each block. The standard deviation of gradients in X and Y direction is computed and summed. Eventually, the resultant value is compared against a threshold value. If it is greater than the threshold value the block is filled with ones, otherwise the block is filled with zeros.

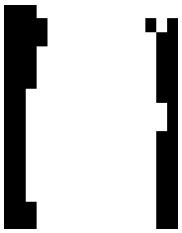

Fig3.Segmentation

4.1.2Minutiae Points Extraction

Minutiae points are extracted as follows:

• Binarization

• Morphological Operations

• Minutiae points' extraction

Initially, the enhanced image is binarized. After binarization, morphological operations are performed on the image to remove the obstacles and noise from it. Finally, the minutiae points are extracted using the approach discussed.

4.1.2.1Binarization

The binary images with only two levels of interest: The black pixels that denote ridges and the white pixels that denote valleys are employed by almost all minutiae extraction algorithms. A grey level image is translated into a binary image in the process of binarization, by which the contrast between the ridges and valleys in a fingerprint image is improved. The grey-level value of every pixel in the enhanced image is analyzed in the binarization process. Then, the pixel value is set to a binary value one when the value is greater than the global threshold, or else a zero is set as the pixel value.

Fig4. Finger print before and after binarization

4.1.2.2 Morphological Operation

This eliminates any obstacles and noise from image, later it removes unnecessary spurs, bridges and line breaks

Then thinning process is performed to reduce the thickness of the lines so that the lines are only represented except the other regions of the image. Clean operator, Hbreak operator, Spur operator and Thinning are the morphological operators applied.

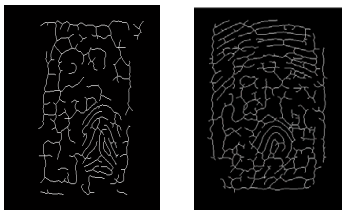

Figure5.Morphological operation

4.1.2.3 Minutiae points' extraction

Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. uses an iterative, parallel thinning algorithm. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3). And finally removes all those marked pixels after several scans. . Marking minutia point is relatively easy after thinning. For each 3X3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch. if the central pixel is 1 and has only 1 one –value neighbors , then the central pixel is ridge ending. Suppose both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbor outside the 3X3 window, so the two pixels will be marked as branches too. Actually only one branch is located in the small region. So a check routine requiring that none of the neighbors of a branch are branches is added.

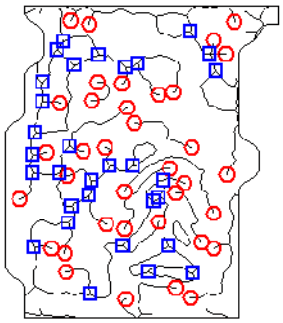

Figure6.Minutiae points

False Minutia Removal

False ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated. This false minutia will significantly affect the accuracy of matching if they are simply regarded as genuine minutia. So some mechanisms of removing false minutia are essential to keep the fingerprint verification system effective.

Key vector generation

Using above discussion the Key is generated in following process

The minutiae points extracted from the fingerprint image are represented as follows

Mp=Minutiae point set

N= number minutiae points

Mp_i (x_i , y_i) = ith minutiae point with x,y Co-ordinates

$$\begin{bmatrix} Mp_1 \\ . \\ . \\ . \\ Mp_1 \end{bmatrix} = \begin{bmatrix} (P_1,P_j) \\ (P_2 ,p_j) \\ . \\ (p_n,p_j). \end{bmatrix}$$

J=1….m $\quad P_i \neq P_j$

Distance between two points pi, pj are calculated as

$\sqrt{(x_i \_ x_j)^2 + (y_i - y_j)^2}$

After calculation of the distances the values are stored in vector as

$$\begin{bmatrix} D1 \\ D2 \\ \\ Dn \end{bmatrix} = \begin{bmatrix} d_{11} \ldots d_{1m} \\ d_{21} \ldots d_{2m} \\ \\ d_{n1} \ldots d_{nm} \end{bmatrix}$$

Sort the above vector name it as V

$$V = [\ v_1 , v_2 \ldots\ v_n\ ]$$

Now V is divided into two equal parts

$$Va = [\ v_1 , v_2 \ldots\ v_{n/2]}$$

$$Vb = [\ v_{n/2+1} , \ldots\ v_{n]}$$

Va and Vb are shuffled and stored in Sa and Sb

Sd = Sa U Sb

Convert the Sd into a matrix form of size $\sqrt{n/2} * \sqrt{n/2}$ and name it Md

$IK_V = \{Ki : P(K)\},\ i = 1,...., |Sd|$

Where

$$P(k) = | SMij | \bmod 2,$$

$$SMij = Md \qquad i, j : i + size, j + size, \ -1 < i, j < \sqrt{Sd}$$

5. Conclusion

Document transmission between systems that are in distributed environment is common task. System should ensure the security and authentication. There are number of cryptographic Techniques. MAC algorithm is used for authentication. Here we have proposed a method for generation of secured key for MAC algorithm using Novel approach for finger based cryptography system. The key has been generated using fingerprint patterns, which is stable through out person's lifetime. Password can be hacked by trial and error basis. But it is not possible to break the biometrics based security system.

REFERENCES

[1]. William Stallings, "*Cryptography and Network Security Principles and practice*", 2nd Edition,Prentice Hall,

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

[3]. N.Lalithamani, K.P.Soman "Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced and Effective Scheme". European Journal of Scientific Research ISSN 1450-216X Vol.31 No.3 (2009), pp.372-387

[4] Jain, A.K.; Prabhakar, S.; Hong, L.; Pankanti, S., "Filter bank-based fingerprint matching", IEEE Transactions on Image Processing, vol. 9, no. 5, pp: 846-859, May 2000, Doi:10.1109/83.841531.

[5] 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.

Authors

Dr.R.Seshadri was born in Andhra Pradesh, India, in 1959. He received his B.Tech degree from Nagarjuna University in 1981. He completed his Masters degree in Control System Engineering from PSG College of Technology, Coimbatore in 1984. He was awarded with PhD from Sri Venkateswara University, Tirupati in 1998. He is currently Director, Computer Center, S.V.University,Tirupati, India. He published number of papers in national and international journals.

Mr.T.RaghuTrivedi received MCA degree from Andhra University, Vizag He received his M.Tech in Computer Science from Nagarjuna University.He is a research scholor in S.V.University,Tirupathi, Andhra Pradesh.