www.iosrjen.org ISSN : 2250-3021
Vol. 2 Issue 2, Feb.2012, pp. 325-330

Design of Secured Key Generation Algorithm using Fingerprint Based Biometric Modality

***A. Jaya Lakshmi, #I. Ramesh Babu**
** DevineniVenkataRamana&Dr.Himasekhar MIC College ofTechnology*
#Professor, AcharyaNagarjuna University

ABSTRACT

Many high-secure applications are using biometrics for natural, user-friendly and quick authentication. Cryptography is meant to make sure the secrecy and authenticity of message and protecting the confidentiality of the cryptographic keys is one among the numerous problems to be dealt with. Researchers are examining suggests that to utilize biometric options of the user to get sturdy and repeatable cryptographic keys rather than a memorable password. This may be efficiently solved by the combination of biometrics with cryptography. This paper presents ways for generating the strong bio-crypt key based mostly on fingerprint. Fingerprint biometric modality is predominantly thought of due to its two vital characteristics uniqueness and permanence that's ability to stay unchanged over the lifetime.

I. INTRODUCTION

Among all the biometric modalities, fingerprint-based identification is the oldest methodology, that has been successfully employed in numerous applications. Most are known to possess distinctive, immutable fingerprints. The individuality of a fingerprint will be determined by the pattern of ridges and furrows as well as the trivialities points. Trivialities points are native ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

Fingerprints are one in all the foremost mature biometric technologies and also are thought-about legitimate proofs of proof in courts of law everywhere the planet. Fingerprints are, therefore, employed in forensic divisions worldwide for criminal investigations. Massive volumes of fingerprints are collected and stored everyday in an exceedingly wide selection of applications together with access management, and driver license registration. A lot of recently, an increasing variety of civilian and business applications are either using or actively considering using finger print primarily based identification attributable to a higher understanding of fingerprints also as demonstrated matching performance than the other existing biometric technology [1]. The analysis of fingerprints for matching functions usually needs the comparison of many options of the print pattern. These embrace patterns, that are combination characteristics of ridges, and minutia points, that are distinctive options found inside the patterns [2]. The figure-1 depicts numerous electronic access applications in widespread use that need automatic recognition.

If the fingerprint recognition may be aa part of a security concept, one needs to expect specialised attacks. The appliance determines quality and amount of the safety demand. Every application state of affairs the expected attacks and their likelihood needs to be determined to be ready to determine that is that the expense for countermeasures against each reasonably attack. Attacks like Brute force, Latent print attacks, Replay attacks, worm attacks, faux feature attacks, Dead feature attacks, Hill climbing attacks, Software leaks and Use of force attacks are most typical and vital to biometric security parts. It depends on the particular application, against that attacks security measures are necessary.

This paper is organized as follows. The first two sections of this paper introduces and summarizes the state of art in terms of technological developments for finger print based biometric modality. Section 3 presents design of the fingerprint based Key Generation Algorithm[FPKGA] and Section 4 presents BioCrypt Key Generation Algorithm.In section 5 presents results analysis followed by conclusion in section 5.

II.STATE OF THE ART IN FINGERPRINT BASED BIOMETRICS

We were motivated by variety of earlier researchers with their work existing within the literature regarding fingerprint biometrics, cryptography and cryptographic key generation. This section provides a quick clarification of a number of the noteworthy contributions.

C. Nandini et.al [3] presented a unique technique for generating Cryptographic key by hashing the fingerprint trivia and using completely different set of symmetric hash functions[4] for various users, that is safe andquick. k-plets are extracted [5] from every fingerprint image and calculate the hash values primarily based on the closest neighbors of a minutia purpose within the k-plet. A mix of those hash values are used to come up with a key.

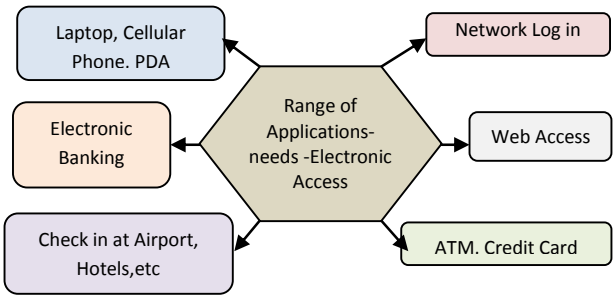

Figure-1 : A range of electronic access applications that require automatic recognition

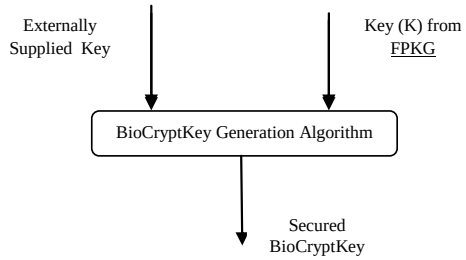

Figure 2: Abstract view of generation of secured Biometric based encrypted key.

This key is used for any sort of cryptography. The generated key was tested using existing AES algorithm with 128 bits key size and increase within the security was theoretically proved.

H. A. Garcia-Baleon et al. [6] proposed an approach for cryptographic key generation that is on the idea of keystroke dynamics and therefore the k-medoids algorithm. The approach checks the identity of people off-line by not employing a centralized database. From the simulation results, a false acceptance rate (FAR) of five.26% and a false rejection rate (FRR) of 100 percent were obtained.

B. Chen et al. [7] have presented a method that uses the entropy oriented feature extraction procedure and Reed-Solomon error correcting codes that are able to generate deterministic bit-sequences from the output of an iterative one-way rework. The assessment of the methodology was done with the 3D face information. The methodology was additionally established to be competent of generating keys of correct length for 128-bit Advanced Encryption normal (AES) during a dependable approach.

Advanced Encryption normal (AES), is one amongst the foremost widespread algorithms utilized in symmetric key cryptography. AES [9][10] is a symmetric block cipher which will encipher and decipher data. It has been analyzed extensively and is widely used to shield crucial data.

III. Design of Fingerprint based Bio-Crypto System

Cryptography provides the secure manner of data transmission over the insecure channel. It authenticates messages primarily based on the key however not on the user. It needs a lengthy key to encrypt and decrypt the sending and

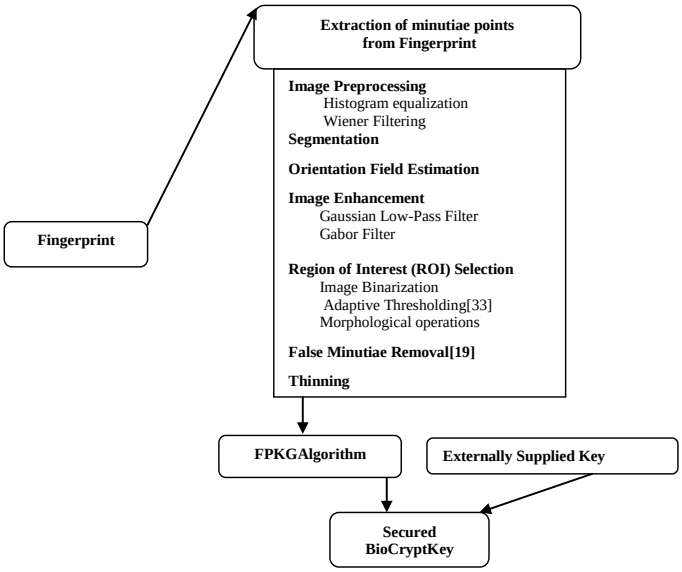

Figure 3: Detailed view of generation of fingerprint based Biometric encrypted key

receiving the messages, respectively. However these keys may be guessed or cracked. Moreover, Maintaining and sharing lengthy, random keys in enciphering and deciphering method is that the crucial drawback within the cryptography system. The higher than mentioned drawback is solved by a Biometric cryptosystems.
Biometric cryptosystems [8] integrate cryptography and biometrics to learn from the strengths of each fields. In such systems, whereas cryptography provides high and adjustable security levels, biometrics brings in non-repudiation and eliminates the requirement to recollect passwords or to hold tokens etc. In biometric cryptosystems, a cryptographic key's generated from the biometric template of a user stored within the database in such the simplest way that the key cannot be revealed while not a successful biometric authentication. The applying of biometric keys cannot solely hide the knowledge of the users' biometric options, however can even securely notice secret key production, key recovery and authentication.The secured fingerprint biometric based cryptographic key generation includes the following components.

- **Finger Print Key Generation Algorithm (FPKGA):** FPKG is an algorithm that returns a key K by using the minutiae points of fingerprint image, denoted by k ← FPKG, such that k €K.
- **Externally Supplied Key: It** is externally supplied for BioCryptKey Generation Algorithm
- **BioCryptKey Generation Algorithm:** This algorithm will take output of FPKG algorithm and an externally supplied key and fuse them to generate the combined finger print based biometric cryptographic key.

Figure - 2 depicts the abstract view of generation of secured Biometric based encrypted key and Figure 3 depicts detailed view of generation of secured Biometric based encrypted key.

3.1 Finger Print based Key Generation Algorithm (FPKGA):

This section proposes an efficient algorithm to generate irrevocable cryptographic key using a minutiae points extracted from fingerprint biometrics. The quality of minutiae influences the key generation as shown in the Figure 3. This section elaborates the various methodologies used in the process of generating the encrypted key.The algorithm comprises of two major phases namely

- Extraction of minutiae points from Fingerprint
- Key generation from minutiae.

3.1.1 Extraction of minutiae points from Fingerprint:

Various methods are used forextracting minutiae points from fingerprint are shown in figure 3

Scenario-1

Step 1. First we apply histogram equalization [11] to increase the perceptional information of the image. Wiener filtering [12][13] is used to improves the legibility of the fingerprint without altering its ridge structures. The fingerprint image obtained after pre processing is of high contrast and enhanced visibility.

Step 2. Segmentation is applied on the pre processed fingerprint image. First, the fingerprint image is divided into non-overlapping blocks of size 16x16. Subsequently, a fingerprint orientation field is defined as the local orientation of the ridge-valley structures. Further fingerprint image is enhanced with Gaussian Low-Pass Filter[15]

Step 3. The Ridge Thinning algorithm [14] is used in the proposed approach for Minutiae points' extraction.

Scenario-2

Step 1. First we apply histogram equalization to increase the perceptional information of the image. Wiener filtering is used toimprove the legibility of the fingerprint without altering its ridge structures. The fingerprint image obtained after pre processing is of high contrast and enhanced visibility.

Step 2. Segmentation is applied on the pre processed fingerprint image. First, the fingerprint image is divided into non-overlapping blocks of size 16x16. Subsequently, a fingerprint orientation field is defined as the local orientation of the ridge-valley structures. Further fingerprint image is enhanced with Gabor Filter[16]

Step 3. The Ridge Thinning algorithm [14] is used in the proposed approach for minutiae points' extraction.

Scenario-3

Step 1. First we apply histogram equalization to increase the perceptional information of the image. Wiener filtering is used toimprove the legibility of the fingerprint without altering its ridge structures. The fingerprint image obtained after pre processing is of high contrast and enhanced visibility.

Step 2. Binarizationprocess is used to select the region of interest with adaptive thresholding. Morphological operators used to get the tightly bounded region just containing the bound and inner area.

Step 3. The Ridge Thinning algorithm [14] is used in the proposed approach for minutiae points' extraction.

3.1.2 Finger Print based Key Generation Algorithm(FPKGA)

In this Section we provide the procedure for key generationby using the minutiae extracted from fingerprint after through initial pre processing.

IV. SECURED BIOCRYPT KEY GENERATION ALGORITHM

Algorithm BioCryptKey( )
{
Step1: FPKG algorithm produces a key vector which is supplied as one of the two inputs to the Secured Bio cryptographic key generation (Secured BioCryptKey) algorithm. The key K_v is divided into n parts and then converts each into an integer K_i, Where n is some property pre-chosen integer.
Step 2: The system randomly chooses a large prime p. Generates the user A's secret key *key*and splits it into t ($\leq$ n) sub-keys
Key = (key_0, key_1, ... , key_{t-1})
Here each $key_i \leq p$
Step3: Generate test-degree polynomial in $F_p[x]$
$f(x) = key_{t-1}\, x^{t-1} + key_{t-2}\, x^{t-2} + ... + key_1\, x + key_0$
Step 4: For each i = 1,2,3,....n , the system computes
$k_i = f(x_i \bmod p) \bmod p$
And later, completely delete or throw away the *key*, each key_i and f(x)
Step 5: The system selects an error-correct Hamming encoding function Encoder( ) and compute
Encoder (K_i) = Ck_i i = 1,2,3,...n
Step 6: The system computes
$\delta_i = K_i \oplus X_i$
For i = 1,2,3,...,n , where $\oplus$ indicates the bitwise XOR operation.
Step 7: Store n parts of δ_i or concatenate them into the binary number $\delta_1 \| \delta_2 \| \cdots \| \delta_n$ as the Fingerprint based biometric cryptographic key (BioCryptKey). (that is, Bio-key =$U_{i=1}^{n} \delta_i$ *or* $\delta_1 \| \delta_2 \| \cdots \| \delta_n$) and store it.
}

IKV = { K_i : m(K_i) } where i=1,…. K_l and m(K_i) = | IKV|
IKV_{ij} is a sub matrix formed from the key matrix where -1 <i,j< $K_{l/2}$

Step 5 : The final key vector is formed from IKV as shown below.
K_v = {1, if IKV [i] >mean(IKV) ,
0 otherwise }
}

The whole procedure of the algorithm doesn't directly store the user's any fingerprint options. The real users will offer their own biometric data will acquire their key data.
However illegitimate users will get the key data after they offer abundant high similarity of the fingerprint options to the registered fingerprint's options. Such cases conjointly effectively prevented within the proposed FPBKG algorithm by thorough thinning and removal of false trivialities. Hence, our algorithm can't solely forestall the user's biometric feature data from being exposed, however can also safely defend the user's key.

V. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the experimental analysis of the proposed fingerprint primarily based biometric cryptographic approach. The proposed approach is programmed in Matlab. The proposed approach was tested with completely different fingerprint pictures obtained from publicized databases. Minutiae points are extracted by using three scenarios. The experimental results as well as the input image, the intermediate results obtained for three completely different scenarios are depicted in figure-4.

a) Original Image b) Image after Step 1 c) Image after Step 2

1. Resultant Images for Scenario -1

a) Original Image b) Image after Step 1 c) Image after Step 2

2. Resultant Images for Scenario 2

a) Original Image b) Image after Step 1 c) Image after Step 2

3. Resultant Images for Scenario 3

Figure 4: Evaluation of Three Scenario

Eventually, a strong cryptographic key is generated from the minutiae points. The sequence of the operations discussed in three scenarios to generate bio-crypto keys are giving good results. However the scenario-3 is generating more complex keys with minimum amount of time complexity, which is aptly suited for any real time use. The final cryptographic key generated is stable throughout person's lifetime.

VI. CONCLUSION

In this paper we presented the basics of fingerprint biometric modality, its applications.Various methods for extracting minutiae points from input fingerprint images are presented in detail. Fingerprint based key generation algorithm was presented by extracting the minutiae points from three different scenarios.The final cryptographic key generated is complex and stable throughout person's lifetime.

REFERENCES

[1] C. J. Hill. Risk of masquerade arising from the storage of biometrics.Available at http://chris.fornax.net/biometrics.html, 2001.

[2] Jain A.K, Bolle. R, and Pankanti .S, eds., Biometrics: PersonalIdentification in Networked Society. Kluwer Academic Publishers, 1999.

[3] C. Nandini and B. Shylaja., "Efficient Cryptographic key Generation from Fingerprint using Symmetric Hash Functions" International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 4, ISSN: 2079-2557, August 2011.
[4] Sergey Tulyakov, Faisal Farooq, PraveerMansukhani, VenuGovindaraju, "Symmetric hash functions for secure fingerprint biometric systems", Pattern Recognition Letters 28 (2007) 2427–2436
[5] Gaurav Kumar, Sergey Tulyakov, VenuGovindaraju, "Combination of Symmetric Hash Functions for Secure Fingerprint Matching", IEEE, 2010.
[6] H. A. Garcia-Baleon, V. Alarcon-Aquino ,O. Starostenko, "K-Medoids-Based Random Biometric Pattern for Cryptographic KeyGeneration", Proceedings of the 14th Iberoamerican Conference on Pattern Recognition: Progress in Pattern Recognition, ImageAnalysis, Computer Vision, and Applications, Vol. 5856, pp: 85 - 94, 2009.
[7] B. Chen, V. Chandran, "Biometric Based Cryptographic Key Generation from Faces", Proceedings of the 9th Biennial Conference ofthe Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp: 394-401, 2007.
[8] UmutUludag, SharathPankanti, SalilPrabhakar, Anil K.Jain "BiometricCryptosystems Issues and Challenges"Proceedings of the IEEE 2004.
[9] Announcing the "AdvancedEncryption Standard (AES)" –Federal Information, Processing StandardsPublication 197,November 26, 2001
[10] "Advanced Encryption Standard " fromhttp://en.wikipedia.org/wiki/Advanced_Encryption_ Standard
[11] Jain, A.K.; Prabhakar, S.; Hong, L.; Pankanti, S., "Filterbank-basedfingerprint matching",IEEE Transactions on Image Processing, vol. 9, no.5, pp: 846-859, May 2000, Doi:10.1109/83.841531.
[12] Amir Hussain, Stefano Squartini, and Francesco Piazza, "Novel Sub-band Adaptive systems incorporating Wiener filtering forBinaural Speech Enhancement", A ISCA tutorial research workshop on Non-Linear Speech processing, NOLISP, Barcelona, April 19-22, 2005.
[13] Saeed V. Vaseghi, "Advanced signal processing and digital noise reduction (Paperback)", John Wiley & Sons Inc, pp: 416, July 1996.
[14] Greenberg, S. Aladjem, M. Kogan, D and Dimitrov, I, "Fingerprintimage enhancement using filtering techniques" in Proceedings of the15th International Conference on Pattern Recognition, vol.32, pp. 322-325, Barcelona, Spain, 2000.
[15] KeokanlayaSihalath, SomsakChoomchuay, Shatoshi Wada andKazuhiko Hamamoto, " Performance Evaluation Of Field SmoothingFilters", in Proceedings of 2th International Conference on BiomedicalEngineering (BMEiCON-2009), Phuket, Thailand, August 2009.
[16] D. Maltoni, D. Maio, A. K. Jain, and s. Prabhakar, Handbook ofFingerprint Recognition, Springer-Verlag, 2003.