Bio-Crypto based Product Registration and Authentication using PDPA

B.Srinivas
CSE Department, MVGR College of Engineering, Vizianagaram, India

Koduganti Venkata Rao
School of Computing,Vignan University, Guntur

P. Suresh Varma
Adikavi Nannaya University, Rajahmundry, India

K.V.Ram Rohit
CSE Department, MVGR College of Engineering, Vizianagaram, India

Abstract:
Software Piracy is the most alarming issue in the day-to-day life. This refers to several practices which involve the unauthorized copying of commercial computer software. It is all, but difficult to stop, although software industries are launching more and more lawsuits against major infractors.In 2010, economists indicated that software piracy cost the industry $51.4 billion.When technology such as biometrics is used, this can be reduced to maximum extent.We propose a Bio-Crypto system which uses PDPA,which not only generates a activation key from the fingerprint but also identifies the user, for the legitimate use of the software.

Keywords:
Piracy Detection and Prevention Algorithm (PDPA), Manufacturer's Licensing Server(MLS),Biometric, Bio-Crypto, authentication, encryption, decryption, Fingerprint, Activation key, software piracy.

1. Introduction

Authentication plays an important role in protecting resources against unauthorized use, which on text based keys has major drawbacks.PlainKeys can be easily lost, stolen,forgotten or guessed using social engineering and dictionary attacks. Limitations of plain key-based authentication can be alleviated by using stronger authentication schemes such as biometrics [2]. Biometric systems [4] establish the identity of a person based on his/her anatomical or behavioral traits such as face, fingerprint, iris, voice, etc. Biometric authentication is more reliable than password-based authentication because biometric traits cannot be lost or forgotten and it is difficult to share or forge these traits. Hence, biometric systems offer a natural and reliable solution to the problem of user authentication in cryptosystems. Hence, we proposed and developed a Bio-Cryptosystem which uses Piracy Detection and Prevention Algorithm(PDPA) for verification of personal identity. According to this, fingerprint [1] is collected, processed forfeature extraction.Aunique key[5]is generated from feature in combination with unique manufacturer's private identity(fingerprint, pivot, constant etc.,). This key is stored in the server database with license counter and machine configuration details maintainedthere by, avoiding softlifting, counterfeit corporate software piracy [1, 2, 3, 4, 5 and 6].

2. Proposed System

In This paper we propose Bio-Crypto based registration and authentication system, which takes the user fingerprint as metric and provides authentication. Customer's Fingerprint is collected,which is processed using image processing algorithms for feature extraction and stored in theserver at manufacturer's end. A unique activation key(U_k)which can be of varying length (256, 512, 1024, 2048 bits) is generated from the extracted featurefurther processed with manufacturer's unique private identity.This key is encrypted with a sub key(S_k) derived from the unique activation key(U_k).This

Manuscript received March 5, 2011
Manuscript revised March 20, 2011

cipher(encrypted key) is deliveredto the user. The below [Figure 1] depicts the architecture view.

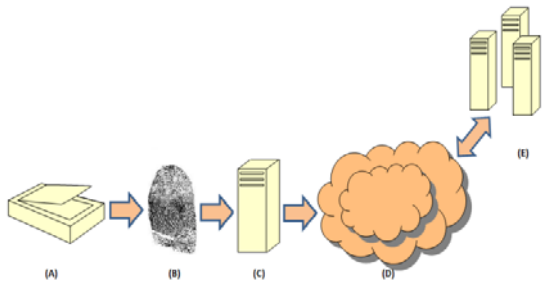

Figure 1 : Bio-Crypto Based Product Registration System Architecture View.

The whole process is carried out in two phases viz., fingerprint collection,key-gen process respectively.

2.1 Fingerprint Collection

User finger prints are collected through a well-equipped scanner [Figure 2]

Figure 2: Fingerprint Collection

The finger prints that are scanned are submittedto the manufacturer remotely. The manufacturer processes the images and delivers the key. The finger print collection can be centralized or decentralized accordingly.

2.2 Key-gen Process

The Manufacturer's Licensing Server MLS creates a new account and processes the finger prints collected, in various stages.

2.2.1 Pre-Processing

The raw image which has no clear view of ridges and bifurcations is processedby making use of featured algorithms like Histogram Equalization and Fast Fourier Transformfor increasing the quality of the image.

2.2.1.1 Histogram Equalization

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information. The histogram after the equalization occupies all the range from 0 to 255 and the visualization effect is enhanced. The original image and equivalent histogram equalized enhanced image can be seen in below diagram[Figure 3].

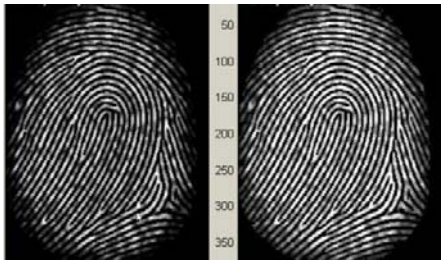

Figure 3 : Histogram Enhancement.
Original Image (Left). Enhanced image (Right)

2.2.1.2 Fingerprint Enhancement by Fourier Transform

We divide the image into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to:

$$F(U,V)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)e^{\left\{-j^2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\}} \quad (1)$$

for u = 0, 1, 2, ..., 31 and v = 0, 1, 2, ..., 31.

In order to enhance a specific block by its dominant frequencies, we multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original

FFT = abs(F(u,v)) = |F(u,v)|.

Get the enhanced block according to

$$g(x,y) = F^{-1}\{F(u,v)|F(u,v)|^k\} \quad (2)$$

where F-1(F(u,v)) is done by:

$$f(x,y) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(u,v)e^{\left\{j^2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\}} \quad (3)$$

for x = 0, 1, 2, ..., 31 and y = 0, 1, 2, ..., 31.

The k in formula (2) is an experimentally determined constant, where k=0.45.Figure 4 presents the image after FFT enhancement.

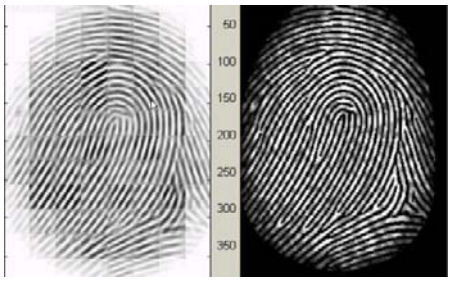

Figure 4 : Fingerprint enhancement by FFT
Enhanced image (left), Original image (right)

And then the fingerprint image is binarized using the locally adaptive threshold method[7].Figure 5 depicts the binarized fingerprint image.

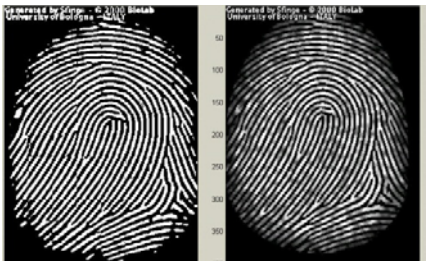

Figure 5:Fingerprint image after adaptive binarization
Binarized image(left), Enhanced gray image(right)

The image segmentation task is fulfilled by a three-step approach:

1)Block direction estimation

2)Segmentation by direction intensity[8]

3)Region of Interest extraction by Morphological operations.

After the image passes this section it is very much refined.

2.2.2 Minutia Extraction

Feature extraction is the process of thinning. For this purpose a Morphological thinning operation is applied which have high efficiency and pretty good thinning quality.The input given is the above processed image.Recognition mostly depends on the quality of the image this section generates. The output of this section Figure 12, is almost purified and a high quality image with each line of only 1 pixel wide.

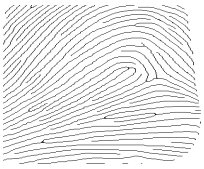

Figure 6: High Quality Image(feature)

2.2.3 Generating a unique activation key

The feature extracted is further processed with any one of the manufacturer's private identitylike fingerprint, pivot value, constant, threshold etc., and a unique activation key is generated.This key can be of any size depending upon the level of security needed.This can be visualized in diagram[Figure 7] below.

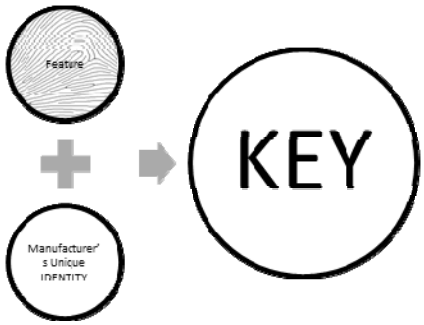

Figure 7

2.2.4 Generating a Sub-key and encrypting

The activation key is permutated and a sub-key is generated[Figure 8]. The activation key is encrypted using symmetric key cryptographic algorithm RC4and delivered to the user.The sub-key is preserved in the server.

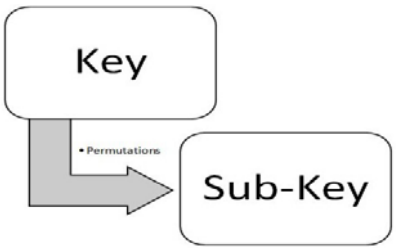

Figure 8

PDPA stated as follows.,

Piracy Detection and Prevention Algorithm(PDPA):

Step 1 : Start

Step 2: Collect fingerprint from user.

Step 3: Generate a Unique Activation Key Uk{} in combination with product manufacturer's confidential identity.

Step 4 : A key Sk is derived from Unique Activation Key Uk

Sk← Sub Key Generation Algorithm(Uk). Sk and Uk are stored in the server database.

Step 5 : Activation key is encrypted using derived key

Ck ← ESk[Uk] and is delivered.

Step 6 : Registration count C and license count N per Activation key is maintained
accordingly.

/* User Registers the software → Validation*/

Step 7: Upload ciphered Activation Key Ck .

Step 8: Decrypt the key and

if C <=N

Collect machine hardware details Mhc{} and store them as Mhs{} correspondingly.

/*nearly 10 hardware components */

if threshold(Mhc{}) not equals Mhs{}

/*Threshold gives the minimum number of configuration matches needed*/

C←C+1

else

goto step 9.

Step 9: Registration Failure

Step 10 : End

2.3Process at User End

The user will be prompted for online registration at the installation startup. User uploads the unique encrypted activation key provided.

3. Results

We have tested our Bio-Crypto based system. The table 1 shows the elapsed time for the whole process i.e. (key generation and encryption).In the aspect of time efficiency, each fingerprint can be processed and key can be generated and encrypted within 0.564 second using an ordinary PC(with a single Intel dual core with 1.6Ghz CPU,512M RAM).

No of Fingerprints	Elapsed time
50	28.21
100	57.66
150	85.89
200	113.21
250	141.126

Table 1

The above tabulated experimental results are plotted[Figure 9] with no of fingerprints processed against elapsed time for processing.

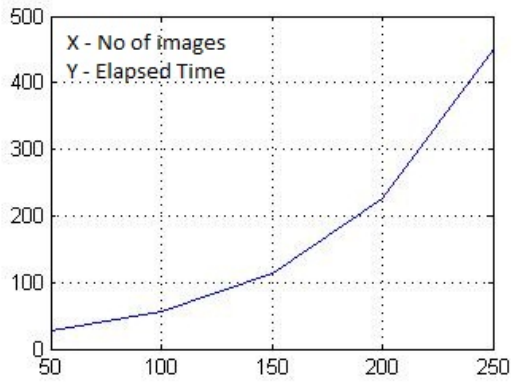

Figure 9 : Processed images against elapsed time

We have observed that there is a match percent of above 75 between some fingerprints, which might affect the uniqueness of the key.

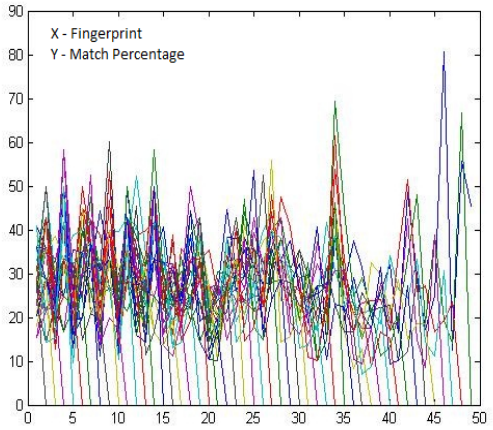

Figure 10 : Comparison Study

The above graph[Figure10]depicts a comparison study over 50 fingerprints. The highest peaks appeared among 30th-35th,45th-50thfingerprints.These fingerprints matched against others with a maximum percent of 80.This might limit the uniqueness of keys generated but not the user.Even 1% change in biometric key can identify the user.Experimentally a 128-bit key generated from the above most relevant fingerprints are nearly 30-40% in common. A change of 1% in fingerprint reflects a maximum change in the key derived.Henceby using PDPA,where we add manufacturer's private identity the similarity of key can be reduced to 8-10%.

By using PDPA the relevance between fingerprints can be reduced to below 40%[Figure 11] which in turn reduces the key similarity to 8-10%.

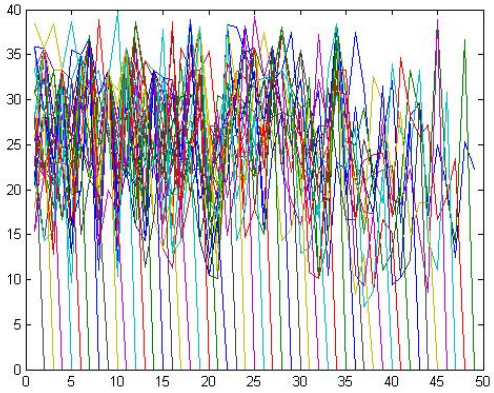

Figure 11:Relevance reduction between fingerprints

4. Conclusion

Our proposed system for Product Authentication using a Bio-Crypto System can be concluded as a sophisticated approach to the normal key based activation system, which greatly reduces the software piracy. The biometric not only provides the authentication but also useful for the identification of illegal users.

As customer is delivered with a cipher key it is highly difficult to decrypt. The registration count and hardware configuration helps to limit the user,installing the software on different machines. If any registration is unauthorised which might limit the legitimacy, then user can contact the manufacturer and block the unauthorised machines. If the key gets revealed, then there will be a possibility of multiple registration requests which can be controlled. As biometric identifies the person we can warn the owner of that key accordingly.

5. Future Work

The proposed system mainly concentrates on online registration and authentication using PDPA. This can be extended for offline registration process accordingly.

6. References

[1] "An identity-authentication system using fingerprints" Proceedings of the IEEE Volume 85, Issue 9, Sep 1997 Page(s):1365 – 1388, Jain A.K, Lin Hong; Pankanti S. Bolle.

[2] "Biometric Authentication", 05/04/2005, Computerworld, Russel Kay. http://www.csoonline.com.au/index.php/id;453581685

[3] "Hilditch Algorithm", "Hit-and-Miss Algorithm", Computer Based Learning Unit, University of Leeds and Ross Moore, Mathematics Department, Macquarie University, Sydney and DanielleAzar.

[4] "Technology for secure biometrics", Galton Biometrics Corporation. http://www.research.ibm.com/ecvg/pubs/ratha-notes.pdf

[5] "The Practical Subtleties of Biometric Key Generation" Lucas Ballard,Seny Kamara,Michael K. Reiterhttp://www.usenix.org/events/sec08/tech/full_papers/ballard/ballard.pdf

[6] "D. E. Denning, Cryptography andData SecurityAddison-Wesley, 1983."

[7] " L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui. Intelligent biometric techniques in fingerprint and face recognition. 1999, the CRC Press".

[8] N. Ratha, S. Chen and A.K. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, pp. 1657-1672, November 1995.

Srinivas Baggam received the M.Tech (Computer Science & Engineering) from R.V.R & J.C college of Engineering, Guntur, Affiliated to Acharya Nagarjuna University. Currently working as an Assistant Professor in M.V.G.R. College of Engineering. He got two and half years of Industrial and Three years in teaching Experience.

Koduganti Venkata Rao received the M.Sc (computer science) from Nagarjuna University, M.Tech in (Computer Science and Technology) from Andhra University and Ph.D in Computer Science and Engineering from Andhra University in 1994, 1999, 2008 respectively. Currently working as a Professor School of Computing,Vignan University,Guntur

P.Suresh Varma Ph.D. in Computer Science and Engineering with specialization in Communication Networks from Acharya Nagarjuna University.M.Tech (Computer Science and Technology from Andhra University in 1998.A.M.I.E (Computer Science and Engineering from Institute of Engineers. M.Sc (Nuclear Physics from Andhra University from 1993.

K.V.Ram Rohit received the B.Tech in (Computer Science & Engineering) from M.V.G.R College Of Engineering. His area of interest is Network security and cryptography.