Estimators in Cryptography

Nicolae Constantinescu
Faculty of Mathematics and Informatics,
Department of Informatics, University of Craiova

ABSTRACT. Cryptography is a field that relies on accurate data, but combining cryptography with biometry we will discuss an entirely different concept – estimators in cryptography. Human users have a tough time remembering long cryptographic keys. Hence, researchers, for so long, have been examining ways to utilize biometric features of the user instead of a memorable password or passphrase, in an effort to generate strong and repeatable cryptographic keys. Our objective is to incorporate the volatility of the user's biometric features into the generated key, so as to make the key unguessable to an attacker lacking significant knowledge of the user's biometrics.

Introduction

The necessity for reliable user authentication techniques has risen amidst of heightened issues about security and rapid progress in networking, communication and mobility [RJ04]. The generally utilized authentication systems that regulate the entry to computer systems or secured locations are password, but it can be cracked or stolen. For that reason, biometrics has turned out to be a practicable option to traditional identification methods in several application areas [RBM07]. Biometrics, expressed as the science of identifying an individual on the basis of her physiological or behavioral traits, seems to achieve acceptance as a rightful method for obtaining an individual's identity [RJ04]. Biometric technologies have established their importance in a variety of security, access control and monitoring applications. The technologies are still novel and momentarily evolving [WB06]. Biometric systems possess numerous advantages over traditional authentication methods, that is: 1). Biometric information cannot be obtained by direct covert observation; 2). It is difficult to share and reproduce; 3). It improves user easiness by lessening the necessity to memorize long and random passwords; 4). It safeguards against

repudiation by the user. Besides, biometrics imparts the same security level to all users unlike passwords and is tolerant to brute force attacks [Was05]. A number of biometric characteristics are being employed today, which comprises: fingerprint, DNA, iris pattern, retina, ear, thermogram, face, gait, hand geometry, palm-vein pattern, smell, keystroke dynamics, signature, and voice [S+09, LS09a].

Biometric systems that generally employ a single attribute for recognition (that is., unimodal biometric systems) are influenced by some practical issues like noisy sensor data, non-universality and/or lack of distinctiveness of the biometric trait, unacceptable error rates, and spoof attacks [JR04]. A probable improvement, multimodal biometric systems prevail over some of these issues by strengthening the proof acquired from several sources [JNR05, HWJ98]. Lately, the improved performance of cryptographic key generated from biometrics in accordance to security has acquired massive reputation amongst the researchers and experimenters [LS09b] and recently, researchers have made an effort towards combing biometrics with cryptography so as to enhance the security, by removing the requirement for key storage using passwords [GKD00, AS09]. Although it is highly impractical to break cryptographic keys generated from biometrics, the attackers have a good possibility of stealing by cryptographic attacks. One effectual solution with additional security will be the integration of multimodal biometrics into cryptographic key generation; in order to attain incredible security against cryptographic attacks.

1 Estimators

At this juncture, we introduce an efficient approach for the secure cryptographic key generation on the basis of multiple modalities like the Iris. The fingerprint features (minutiae points) are obtained from the fingerprint image using segmentation, Orientation field estimation and morphological operators.

Minutiae Points Extraction from Fingerprints

This sub-section describes the process of extracting the minutiae points from the fingerprint image. We chose fingerprint biometrics chiefly because of its two significant characteristics: uniqueness and permanence (ability to remain unchanged over the lifetime). A fingerprint can be described as a pattern of ridges and valleys found on the surface of a fingertip. The ridges of the finger form the so-called minutiae points: ridge endings (terminals of ridge lines) and ridge bifurcations (fork-like structures) [HJP99]. These minutiae points serve as an important means of fingerprint recognition. The steps involved in the proposed approach for minutiae extraction are as follows,

1) *Preprocessing*: The fingerprint image is first preprocessed by using the following methods,

- Histogram Equalization
- Wiener Filtering

Histogram Equalization: Histogram equalization (HE) is a very common technique for enhancing the contrast of an image. Here, the basic idea is to map the gray levels based on the probability distribution of the input gray levels. HE flattens and stretches the dynamic range of the image's histogram resulting in overall contrast improvement of the image [BB00]. HE transforms the intensity values of the image as given by the equation,

$$S_k = T(r_k) = \sum_{j=1}^{k} P_r(r_j) = \sum_{j=1}^{k} \frac{n_j}{n}$$

Where S_k is the intensity value in the processed image corresponding to intensity r_k in the input image, and $P_r(r_j)$ = 1,2,3…L is the input fingerprint image intensity level [KZ08].

Wiener filtering: Wiener filtering improves the legibility of the fingerprint without altering its ridge structures [U+04]. The filter is based on local statistics estimated from a local neighborhood η of size 3×3 of each pixel, and is given by the following equation:

$$w(n_1, n_2) = \mu + \frac{\sigma^2 - v^2}{\sigma^2}(I(n_1, n_2) - \mu)$$

where v^2 is the noise variance, μ and σ^2 are local mean and variance and I represents the gray level intensity in $n_1, n_2 \in \eta$ [GZ03].

2) *Segmentation*: The fingerprint image obtained after preprocessing is of high contrast and enhanced visibility. The next step is to segment the preprocessed fingerprint image. First, the fingerprint image is divided into non-overlapping blocks of size 16×16. Subsequently, the gradient of each block is calculated. The standard deviation of gradients in X and Y direction are then computed and summed. If the resultant value is greater than the threshold value the block is filled with ones, else the block is filled with zeros.

3) *Orientation Field Estimation*: A fingerprint orientation field is defined as the local orientation of the ridge-valley structures [Y+07]. To obtain reliable ridge orientations, the most common approach is to go through the gradients of gray intensity. In the gradient-based methods, gradient vectors $[g_x, g_y]^T$ are first calculated by taking the partial derivatives of each pixel intensity in Cartesian coordinates. Traditional gradient-based methods divide the input fingerprint image into equal-sized blocks of $N \times N$ pixels, and average over each block independently [4] [28]. The direction of orientation field in a block is given by,

$$\theta_B = \frac{1}{2} a\tan\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{N} 2g_x(i,j)g_y(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N} g_x^2(i,j) - g_x^2(i,j)}\right) + \frac{\pi}{2}$$

Note that function $a\tan(\cdot)$ gives an angle value ranges in $(-\pi, \pi)$ which corresponds to the squared gradients, while θ_B is the desired orientation angle within $[0, \pi]$.

4) *Image Enhancement*: It would be desirable to enhance the fingerprint image further prior to minutiae extraction. The fingerprint image enhancement is achieved by using,

- Gaussian Low-Pass Filter
- Gabor Filter

Gaussian Low-Pass Filter: The Gaussian low-pass filter is used as to blur an image. The Gaussian filter generates a 'weighted average' of each pixel's neighborhood, with, the average weighted more towards the value of the central pixels. Because of this, gentler smoothing and edge preserving can be achieved. The Gaussian filter uses the following 2-D distribution as a point-spread function, and is achieved by the convolution [HJP99].

$$G(x,y) = \left(\frac{1}{2\pi\sigma}\right)^2 \exp\left\{\frac{(x^2+y^2)}{2\sigma^2}\right\}$$

Where, σ is the standard deviation of the distribution.

Gabor Filter: Mostly used contextual filter [M+03] for fingerprint image enhancement is Gabor filter proposed by Hong, Wan, and Jain [LLS92]. Gabor filters have both frequency-selective and orientation-selective properties and they also have optimal joint resolution in both spatial and frequency domains. The following equation shows the 2-Dimensional (2D) Gabor filter form [M+03],

$$G(x,y,\theta,f_0) = \exp\left\{-\frac{1}{2}\left(\frac{x_{\theta^2}}{\sigma_x^2} + \frac{y_{\theta^2}}{\sigma_y^2}\right)\right\}\cos(2\pi f_0 x_\theta)$$

$$\begin{bmatrix} x_\theta \\ y_\theta \end{bmatrix} = \begin{bmatrix} \sin\theta & \cos\theta \\ -\cos\theta & \sin\theta \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}$$

where θ is the orientation of the filter, f_0 is the ridge frequency, $[x_\theta, y_\theta]$are the coordinates of $[x, y]$ after a clockwise rotation of the Cartesian axes by an angle of $(90° - \theta)$, and σ_x and σ_y are the standard deviations of the Gaussian envelope along the x -and y -axes, respectively.

5) *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
- Morphological Operators

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.

Morphological Operations: Following the binarization process, morphological operators are applied to the binarized fingerprint image. The objective of the morphological operations is to eliminate obstacles and noise from the image. Furthermore, the unnecessary spurs, bridges and line breaks are removed by these operators. The process of removal of redundant pixels till the ridges become one pixel wide is facilitated by ridge thinning. The Ridge thinning algorithm utilized for Minutiae points' extraction in the proposed approach has been employed by the authors of [U+04]. The image is first divided into two dissimilar subfields that resemble a checkerboard pattern. In the first sub iteration, the pixel p from the initial subfield is erased only when all three conditions, G1, G2, and G3 are satisfied. While, in the second sub iteration, the pixel p from the foremost subfield is erased when all three conditions, G1, G2, and G3' are satisfied.

Condition G1: $X_H(P) = 1$

Where

$$X_H(P) = \sum_{i=1}^{4} b_i$$

$$b_i = \begin{cases} 1 \text{if } x_{2i-1} = 0 \text{ and } (X_{2i} = 1 \text{ or } X_{2i+1} = 1) \\ 0 \text{ otherwise} \end{cases}$$

$x_1 x_2, \ldots, x_8$ are the values of the eight neighbors of *p*, starting with the east neighbor and numbered in counterclockwise order.

Condition G2: $2 \leq \min\{n_1(p), n_2(p)\} \leq 3$

where

$$n_1(p) = \sum_{k=1}^{4} x_{2k-1} \vee x_{2k} \quad \text{and} \quad n_2(p) = \sum_{k=1}^{4} x_{2k} \vee x_{2k+1}$$

Condition G3: $(x_2 \vee x_3 \vee \overline{x}_8) \wedge x_1 = 0$

Condition G3': $(x_6 \vee x_7 \vee \overline{x}) \wedge x_5 = 0$

The resultant fingerprint image produced by the morphological thinning algorithm composes of ridges each one pixel wide. This improves the visibility of the ridges and enables effective and effortless of minutiae points.

Conclusion

In this paper, we have attempted to generate a secure cryptographic key by incorporating multiple biometrics modalities of human being, so as to provide better security. An efficient approach for generation of secure cryptographic key based on multimodal biometrics (fingerprint) has been presented in this paper. Biometrics and cryptography have been seen as competing technologies and identified as two of the most important aspects of digital security environment. Working separately, the two technologies develop activities in isolation, sometime in competition with each other. For various types of security problems the merging between these aspects has led to the development of new bio crypt technology. Based on merging technique, the bio crypt categorized into: (i) loosely-coupled mode, the biometric matching is decoupled from the cryptographic part. Biometric matching operates on the traditional biometric template: if they match, the cryptographic key is released from its secure location, e.g. a server or smart card. (ii) tightly-coupled mode, biometric and cryptography are merged together at a much deeper level, where matching can effectively take place within cryptographic domain, hence there is no separate matching operation that can be attacked; key extracted from a collected heterogeneous mass (key/bio template) as a result of positive matching. Bio crypt is giving hope to an ideal technology combination and security integration. The bio crypt process can be carried out in three different modes: key generation, binding and construction.

References

[Amb05] **Parvathi Ambalakat**, "Security of Biometric Authentication Systems", in proceedings of 21st Computer Science Seminar, 2005.

[AS09] **P. Arul, Dr. A. Shanmugam**, "Generate a Key for AES Using Biometric for VOIP Network Security", Journal of Theoretical and Applied Information Technology, vol. 5, no.2, 2009.

[BB00] **K. Balasubramanian, P. Babu**, "Extracting Minutiae from Fingerprint Images using Image Inversion and Bi-Histogram Equalization", Proceedings of SPIT-IEEE Colloquium and International Conference, Mumbai, India

[BG02] **A.M. Bazen, S.H. Gerez**, "Systematic methods for the computation of the directional fields and singular points of fingerprints", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 24, no.7, pp.905-919, 2002.

[BR05] **M. Baca, K. Rabuzin**, "Biometrics in Network Security", in Proceedings of the XXVIII International Convention MIPRO 2005, pp. 205-210 , Rijeka,2005.

[CCG07] **Sharat Chikkerur, Alexander N. Cartwright, Venu Govindaraju**, "Fingerprint enhancement using STFT analysis", Pattern Recognition, vol. 40, no.1, pp. 198-211, 2007.

[GN03] **Goh, D.C.L. Ngo**, "Computation of cryptographic keys from face biometrics", International Federation for Information Processing 2003, Springer-Verlag, LNCS 2828, pp. 1-13, 2003.

[GZ03] **Jinwei Gu, Jie Zhou**, "A Novel Model for Orientation Field of Fingerprints", in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, vol.2, 2003.

[GKD00] **S. Aladjem Greenberg, D. M. Kogan, I. Dimitrov**, "Fingerprint image enhancement using filtering techniques" in Proceedings of the 15th International Conference on Pattern Recognition, vol.32, pp. 322325, Barcelona, Spain, 2000.

[HJP99] **L. Hong, A.K. Jain, S. Pankanti**, "Can multibiometrics improve performance?", in Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies, pp. 59-64, NJ, USA, 1999.

[HWJ87] **L. Hong, Y. Wan, AI. Jain**, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 8, pp. 777-789, August 1998.

[JR05] **A.K. Jain, A. Ross**, "Multi-biometric systems: special issue on multimodal interfaces that flex, adapt, and persist", Communications of the ACM, vol. 47, no. 1, pp. 34-40, 2004.

[JNR05] **Anil Jain, Karthik Nandakumar, Arun Ross**, "Score normalization in multimodal biometric systems", Pattern Recognition, vol. 38, pp. 2270 -2285, 2005.

[KZ08] **Muhammad Khurram Khan, Jiashu Zhang**, "Multimodal face and fingerprint biometrics authentication on space-limited tokens", Neurocomputing, vol. 71, pp. 3026-3031, August 2008.

[LS09a] **N. Lalithamani, K.P. Soman**, "Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced

and Effective Scheme", European Journal of Scientific Research, vol.31, no.3, pp.372-387, 2009.

[LS09b] **N. Lalithamani, Dr. K.P. Soman**, "An Effective Scheme for Generating Irrevocable Cryptographic Key from Cancelable Fingerprint Templates", International Journal of Computer Science and Network Security, vol. 9, no.3, March 2009.

[LLS92] **L. Lam, S. W. Lee, C. Y. Suen,** "Thinning Methodologies-A Comprehensive Survey", IEEE Transactions on Pattern analysis and machine intelligence, vol. 14, no. 9, 1992.

[M+03] **D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar**, "Handbook of Fingerprint Recognition", Springer-Verlag, 2003.

[RJ04] **Arun Ross, Anil K. Jain**, "Multimodal Biometrics: An Overview", in proceedings of the 12th European Signal Processing Conference, pp. 1221-1224, 2004.

[RBM07] **Kornelije Rabuzin, Miroslav Baca, Mirko Malekovic**, "A Multimodal Biometric System Implemented within an Active Database Management System", Journal of software, vol. 2, no. 4, October 2007.

[SBM08] **M. Sepasian, W. Balachandran, C. Mares**, "Image Enhancement for Fingerprint Minutiae-Based Algorithms Using CLAHE, Standard Deviation Analysis and Sliding Neighborhood", in Proceedings of the World Congress on Engineering and Computer Science 2008, San Francisco, USA, October 2008.

[S+09] **Keokanlaya Sihalath, Somsak Choomchuay, Shatoshi Wada, Kazuhiko Hamamoto**, "Performance Evaluation Of Field Smoothing Filters", in Proceedings of 2th International Conference on Biomedical Engineering (BMEiCON-2009), Phuket, Thailand, August 2009.

[U+04] **Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K. Jain**, "Biometric Cryptosystems Issues and Challenges", in Proceedings of the IEEE, vol. 92, pp. 948-960, 2004.

[Was05] **Richard A. Wasniowski**, "Using Data Fusion for Biometric Verification", in Proceedings of World Academy of Science, Engineering and Technology, vol. 5, April 2005.

[WB06] **R. Wang, B. Bhanu**, "Performance prediction for multimodal biometrics", In Proceedings of the IEEE International Conference on Pattern Recognition, pp. 586-589, 2006.

[Y+07] **Jang-Hee Yoo, Jong-Gook Ko, Sung-Uk Jung, Yun-Su Chung, Ki-Hyun Kim, Ki-Young Moon, Kyoil Chung**, "Design of an Embedded Multimodal Biometric System", ETRI-Information Security Research Division, 2007.