IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Cryptographic Key Generation from Finger Vein

Dr. Algimantas Venckauskas[*1], Povilas Nanevicius[2]

[*1,2] Department of Computer Science, Kaunas University of Technology, Kaunas, Lithuania

algimantas.venckauskas@ktu.lt

Abstract

Bio-cryptography is a progressive technology that combines biometrics with cryptography. The use of biometric data for security purposes has become increasingly popular, but the use of biometric data in cryptography is a new, growing and promising area of research. One of the most important problems of bio-cryptography is generation of a stable encryption key. This paper proposes the method of cryptographic key generation from finger vein pattern. The approach is based on the established finger vein image pre-processing methods and authors' proposed Contour-tracing algorithm.

Keywords: Information security, cryptographic key generation, biometrics.

Introduction

Information security today is becoming more and more important. Cryptography is one of the most effective ways to solve the problem of information security. In the cryptographic algorithms information is encrypted and decrypted using cipher keys, which can cause some problems [1]. Simple users keys are easy to be remember, but they can also easily be cracked. Complex keys are difficult to crack, but they are difficult to remember as well and may have to be stored in a medium that could get lost or stolen. In addition, the cipher keys may be illegally shared and cannot provide non repudiation. In order to solve these problems, the biometric features which cannot be forgotten, stolen or cracked, have been combined with the cryptography to form biometric cryptography. One of the most important problems of biometric cryptography is generation of stable encryption key [2].The encryption keys must be generated truly randomly, to contain sufficient entropy and be of a sufficient length [3].

Biometrics employs a number of physiological and behavioural characteristics: face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice.

One of the newest biometric methods is finger vein recognition [4, 5]. The finger vein pattern based authentication method is highly reliable; veins are hidden underneath the skin surface so forgery is extremely difficult; it is non-invasive and easy to use, offering a balance of advantages. Unique aspects of finger vein pattern recognition set this method apart from other forms of biometrics. Experiments indicate that equal error rate (EER) of Miura "Repeated Line Tracking" finger vein method is 0.145%. To compare, ERR in fingerprint based systems ranges from 0.2% to 4%. This indicates, that finger vein based authentication is very effective [6].

Riley et al. study [7] suggests that vein technology is more suitable for use by the older population compared to fingerprint technology. The use of fingerprint based technologies is problematic for the following reasons: it is more susceptible to the environmental conditions (dust, dirt, temperature fluctuation), fingerprint image quality is lower, fingerprints can be forged and the process of enrolment and scanning may be more complicated.

Finger vein recognition is a relatively embryonic field, new methods are developed and existing ones are examined. In this paper we explore the possibilities of key generation from finger vein patterns.

Further parts of this paper are organized as follows: section II summarizes conventional methods used to retrieve cryptographic keys from biometric characteristics. A proposed method of cryptographic key generation directly from finger vein pattern is presented in section III. Investigation and discussion of the proposed method is presented in section IV. Conclusions are provided in the last section.

Related Work

Many cryptographic algorithms are available for securing information, but all of them are dependent on the security of the encryption or decryption key. To overcome this dependency, biometric techniques can be applied to ensure the security of keys and documents. Different methods

can be used to securely store and retrieve cipher keys from biometric characteristics.

The first method involves stored template matching to unlock a cipher key storage. If the user is authenticated, the key is released. The main problem here is using an insecure storage media [8].

The second method hides the cipher key within the enrolment template itself via a secret bit-replacement algorithm. If the user is successfully authenticated, this algorithm extracts the key bits from the appropriate place and releases the key [9].

Another method is to use data derived directly from a biometric image. In this method biometric data are used to generate a cryptographic key [10]. Quality of biometric data depends on the person's physiological characteristics and is strongly influenced by the environment; it is characterized by inaccuracy. Therefore, generation of cryptographic keys directly from biometric data is challenging. There are many works, aiming to fill the gap between the fuzziness of biometrics and achieving cryptographic accuracy. This would enable keys to be generated directly from biometric images. The main problem is that biometric data is noisy and only an approximate comparison is possible with the template. But cryptography requires that the cipher keys are absolutely correct.

Further a few works describing various methods for generating cryptographic keys directly from biometric data are analysed.

Topological fingerprint pattern minutiae point neighbourhood descriptors based approach has been proposed by Ushmaev et al. [11]. It has the following advantages: Topological descriptors are very stable fingerprint features. They don’t depend on finger alignment and elastic deformations. The approach allows varying decryption rates and key lengths.

The core of bio-cryptography lies in the stability of cryptographic keys generated from uncertain biometrics. Hu et al. [12] investigated the effect on the generated keys when an original fingerprint image is rotated. Analysis indicates that information integrity of the original fingerprint image can be significantly compromised by image rotation transformation process. It was discovered that the quantization and interpolation process can change the fingerprint features significantly without affecting the visual image.

Costanzo [13] proposed an approach that eliminates the need for template storage and demonstrates how a cryptographic key can be constructed through the use of biometric feature and parametric aggregation along with certain mathematical combinatorial and permutation constructs.

Zheng et al. [14] paper presents a lattice mapping based fuzzy commitment method for cryptographic key generation from biometric data. The proposed method not only outputs high entropy keys, but also conceals the original biometric data such that it is impossible to recover the biometric data even when the stored information in the system is opened to an attacker.

Wu et al [15] proposed a novel biometric cryptosystem based on the most accurate biometric feature - iris. In this system, a 256-dimension textural feature vector is extracted from the pre-processed iris image by using a set of 2-D Gabor filters. And then a modified fuzzy vault algorithm is employed to encrypt and decrypt the data.

Unimodal biometric systems, which utilize a single trait for recognition, have certain problems like noisy sensor data, non-universality, unacceptable error rates, insufficient length and entropy of generated key. Jagadeesan et al. [16] proposed an efficient approach based on multimodal biometrics (iris and fingerprint) for generating a secure cryptographic key, where the security is further enhanced with the difficulty of factoring large numbers. At first, the features, minutiae points and texture properties are extracted from the fingerprint and iris images respectively. Then, the extracted features are fused at the feature level to obtain the multi-biometric template. Finally, a multi-biometric template is used to generate a 256-bit cryptographic key.

As seen, mainly researches were performed for generating keys using fingerprints. We propose the method of cryptographic key generation from finger vein pattern.

Key Generation from Finger Vein

This paper proposes a method for cryptographic key generation from finger vein pattern images.

A schematic representation or proposed cryptographic key generation method from finger vein patterns is shown in Fig. 1.

The essence of this method is:

1. The key is generated using multiple finger vein patterns. It's a certain implementation of pseudo-multimodality, where a biometric method is combined with a password. The password is 'entered' by providing different finger sequences for the system. A total of 10 different finger vein patterns and combinations of enrolling these images to the system allows for virtually endless number of keys to be generated. Also longer keys and keys with higher entropy can be generated.
2. Initial vein pattern image is processed using established methods: *Miura “Repeated Line Tracking”*, *Miura “Maximum Curvature”*, *Huang*

"Wide Line Tracking" and additional sets of mathematical Morphology functions [17, 18, 19].

3. The processed vein pattern is used as an input to *Contour Tracing Algorithm* to generate a partial cryptographic key.

4. *Error Correcting Code* (ECC) [20] method is used to reduce the variability of biometric data.

5. Partial cryptographic keys are concatenated to combine a final cryptographic key.

Generated variable length cryptographic key is normalized using *Key Derivation Functions* [21].

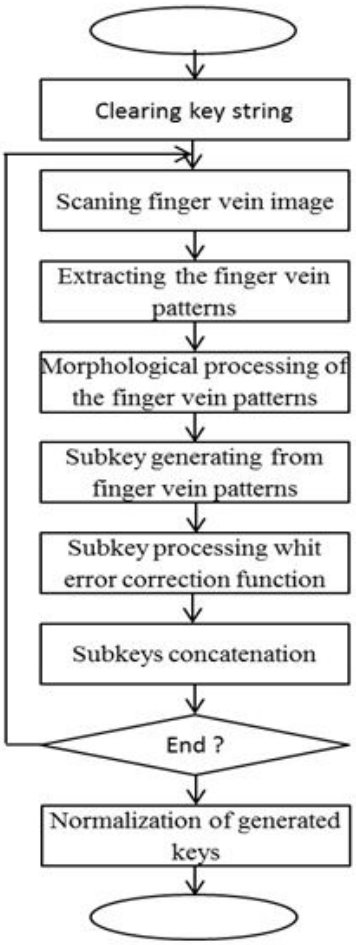

Fig. 1. Schematic representations of proposed cryptographic key generation method using finger vein patterns

A binary finger vein pattern *FVP(n×m)*, previously processed using initial and morphological functions is further processed by *Meaningful Coordinate Detection Algorithm* (Fig. 2).

The supplied vein network is a 1 pixel width line in the image. Algorithm is used to identify blood vessel beginning point *VBP(n×2)*, vessel end point *VEP(n×2)* and crossing vessel point coordinates *CVP(k×2)*. Finger vein pattern may be cropped depending on it's size to ensure, that vein beginning and end points reach edges of the image. Vein beginning and end points are found by scanning binary values along the edges of the image and coordinates of intersections in the network are identified using a morphological *branchpoints* function. *Meaningful coordinate Detection algorithm* is also used to visualise and allow user to select which VBP will be used as a starting point for contour tracing. Extracted coordinates will be later used by other algorithms.

```
% Input:
%  IMG – B/W [0,1] 1 pixel width vein image
%
%  Output:
%  IMG2 – reduced size image;
%  VBP   - Nx2 vessel beginning point matrix;
%  VEP   - Nx2  vessel end point matrix;
%  CVP   - N x 2  vessel intersection point matrix;
%  xy0     - initial tracing point;

%image measurement and resize
  {IMG > CROP > IMG2}
%detecting VBP
  for i = 1:IMG2_height
    if {vein starting point detected}
      {note VBP point coordinates and assigned
       entrance number}
    end
  end
%detecting VEP
  for i = 1:IMG2_height
    if {vein end point detected}
      {note VEP point coordinates and assigned
       exit number}
    end
  end
%detecting intersections
  CVP=bwmorph(IMG2,'branchpoints',1);
%selecting initial tracing point
  {Display pattern and prompt user to select
   initial tracing point}
  xy0={user selected starting point}
```

Fig. 1. Coordinate Detection Algorithm

Fig. 2.

Contour Tracing Algorithm (Fig. 3) is used to trace the contour and allows generating partial cryptographic key from the image processed by initial functions and with meaningful pattern points detected. The algorithm is used to identify which Vessel Beginning Points and which vessel end points are connected with a selected VBP or VEP. The contour is traced until a vessel intersection is detected. After an intersection is detected, all following branches are traced simultaneously. Fig. 4, shows a vascular pattern image with 100 initial contour points highlighted by *Contour Trace Algorithm.*

```
%  Input:
%  IMG – B/W [0,1] 1 pixel width vein image
%  xy0 – Trace starting point
%
% Output:
% CNTR - N x 2 contour coordinate matrix

%Trace directions: [x; y]
  superposition(1)=[0;-1];
  superposition(2)=[1;-1];
  superposition(3)=[1;0];
  superposition(4)=[1;1];
  superposition(5)=[0;1];
  superposition(6)=[-1;1];
  superposition(7)=[-1;0];
  superposition(8)=[-1;-1];
%Tracing the contour
  while(1)
    {check all contour directions (point
superpositions)
      starting from the xy0}
    if {contour point detected}
      {record contour point coordinate and
       algorithm iteration number}
      {invert traced point value to avoid
       repeated tracing}
    end
    if {no more points to trace}
      {exit from while(1) loop}
  end
```

Fig3. Contour Trace Algorithm

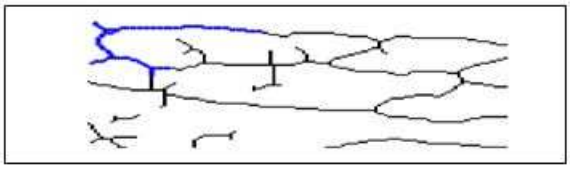

Fig. 4. Finger vein patter being tracked by Contour Trace Algorithm. The first 100 algorithm iteration points are highlighted.

Contour Trace Iteration Number Method (Fig. 5) combines the results of *Meaningful Coordinate Detection Algorithm* and *Contour Trace Algorithm*. The previously numbered vein beginning points (*VBP*) and vein end points (*VEP*) each have digital value assigned to them. When contour is traced starting from the initial point *xy0* different *VBP* and *VEP* points will be reached after a different number of *Contour Trace Algorithm* iterations.

Figure (Fig. 5) shows a vascular pattern image with values from 1 to 11 assigned in sequence to each VBP and VEP. An initial tracing point is set as point number 4 and contour is traced. Figure 5 illustrates contour tracing at a point when first 'exit' point (number 5) is reached after 826 iterations of the *Contour Trace Algorithm*.

After all accessible VBP and VEP points are reached, the values assigned to each of these points are concatenated into one partial key in order of when they were hit by the *Contour Trace Algorithm.*

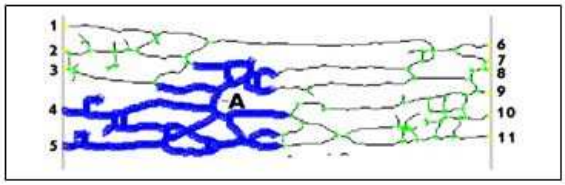

Fig. 5. Contour Trace Iteration Method used on an image starting from VBP number 4

Investigation and Discussion

Steps 1 to 3 of the proposed cryptographic key generation method using finger vascular pattern have been implemented and tested. For investigation of proposed method, a Matlab graphical testing model has been created using Bram Ton [22] implementations of *Miura "Repeated Line Tracking"*, *Miura "Maximum Curvature"* and *Huang "Wide Line Tracking"* and a set of mathematical Morphology functions. Additional functions, required for key generation were created in this research. Initial and morphological image processing and partial key generation interface are presented in Fig. 6. The model allows visualising intermediate stages of key generation. This allows to dynamically asses possible issues in steps of key generation and selects optimal settings in each step.

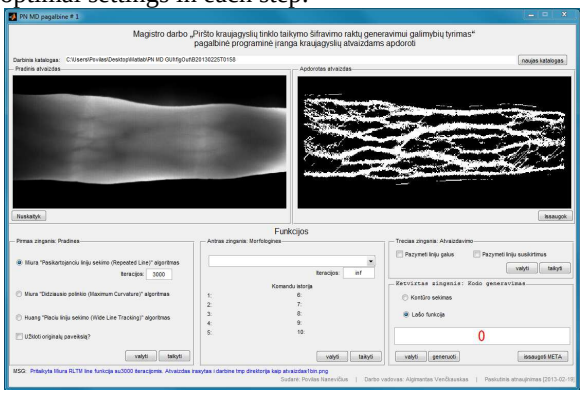

Fig. 3. Matlab graphical interface

Original vascular pattern (left) and binary vein image (right) created using Miura et al. *"Repeated Line Tracking Method"* after 3000 line tracking iterations are shown in Fig. 6. Initial vascular pattern image source is Bram Ton [22].

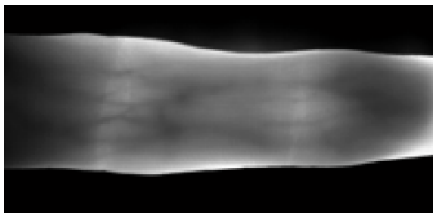

Fig. 4. Initial finger vascular pattern image

Resulting image after Miura "*Repeated line tracking*" and a set of mathematical morphology functions is a binary matrix (image), where 1 pixel wide lines represent finger veins. The processed image is shown in Fig. 8.

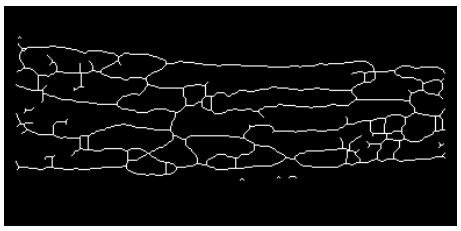

Fig. 5. Processed finger vascular pattern image

Fig. 5 illustrates *Contour Trace Iteration Number Method* when the first 'exit' point is reached after tracing 826 points in the vascular pattern. After a full processing cycle a result – secret key composed of numbers „532111910678" is obtained. The sequence of numbers (a sub-key) generated by this method depends on the values assigned to the *VBP* and *VEP* points and functionality of contour trace algorithm. A previously discussed *Contour Trace Algorithm* has been used in this example.

In *Contour Trace Algorithm* the contour is traced until a vessel intersection is detected. After an intersection is detected, all following branches are traced simultaneously. An alternative to such operation could be to trace one of the branches applying predetermined set of rules on how all following intersections should be crossed. These aspects of algorithm operation would have influence on the end result of the method, accuracy and key cardinality.

The advantage of using *Contour Trace Iteration Number Method* is a relatively small probability of error when the vein pattern image is altered insignificantly. The algorithm would not be affected by minor changes in the direction or position of certain veins in the pattern or any noise that is not directly connected to the main vein network. Algorithm is also able to manage additional loops, more complex junction structure and branches in the vein pattern. This algorithm is mostly misleading by incorrectly detected (or undetected) line connections in the main vein pattern and false *VBP*/*VEP* determination. Method generates incorrect code when when vein pattern changes significantly shortens or lengthens certain sections of the vein images. Further research will be carried out to analyse *Contour Trace Iteration Number Method* properties and possibilities for improvement.

This paper does not cover steps 4, 5 and 6 (Fig.1) of cryptographic key generation. Research of these key generation steps will be carried out in future work.

Conclusions

A method to generate cryptographic keys from finger vein patterns is proposed in this paper. The pseudo-multimodal key generation method could be used to generate a virtually limitless number of keys from finger vein characteristics of an individual. Proposed *Contour-tracing algorithm* generates cryptographic key directly from finger vein patterns without using any pre-captured samples or templates. In the future work all steps of proposed method of cryptographic key generation will be implemented and quality properties of the generated keys will be investigated.

References

[1] Venckauskas, N. Jusas, I. Mikuckiene, S. Maciulevicius, "Generation of the secret encryption key using the signature of the embedded system", Information technology and control, T. 41, nr. 4, pp. 368–375, 2012.

[2] Yao-Jen Chang, Wende Zhang, Tsuhan Chen, "Biometrics-based cryptographic key generation," Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on , vol.3, pp. 2203,2206 Vol.3, 27-30 June 2004.

[3] C. Tilborg (Ed). Encyclopedia of Cryptography and Security. Springer, 2005.

[4] J. Hashimoto, Finger "Vein Authentication Technology and Its Future", VLSI Circuits, Digest of Technical Papers. – pp. 5–8, 2006.

[5] A. Venckauskas, N. Morkevicius, K. Kulikauskas, "Study of Finger Vein Authentication Algorithms for Physical Access Control", Electronics and Electrical Engineering, No. 5(121). – pp. 101–104, 2012.

[6] N. Miura, A. Nagasaka ir T. Miyatake, "Automatic Feature Extraction from non-uniform Finger Vein Image and its Application to Personal Identification" IAPR Workshop on Machine Vision Applications, Dec. 11 - 13.2002, Nara- ken New Public Hall, Nara, Japan, 2002.

[7] C. Riley, H. McCracken, K. Buckner, “Fingers, veins and the grey pound: accessibility of biometric technology”, Proceedings of the 14th European conference on Cognitive ergonomics (ECCE’07). – New York, NY, USA, 2007. – pp. 149–152, 2007

[8] Handbook of Information and Communication Security, P. Stavroulakis, M. Stamp (Eds.), Springer, 2010.

[9] U. Uludag, "Secure biometric systems," Ph.D. dissertation, Michigan State University, http://biometrics.cse.msu.edu/Publications/Thesis/ UmutUludag_SecureBSecureBio_PhD06.pdf, 2006.

[10] M. S. Al-Tarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, “Crypto key generation using contour graph algorithm”, in Proceedings of the 24th IASTED international conference on Signal processing, pattern recognition, and applications (SPPRA'06), M. H. Hamza (Ed.). ACTA Press, Anaheim, CA, USA, pp. 95-98, 2006.

[11] O. Ushmaev, V. Kuznetsov, V. Gudkov, "Extraction of Binary Features from Fingerprint Topology," Hand-Based Biometrics (ICHB), 2011 International Conference on , vol., no., pp.1,6, 17-18 Nov. 2011.

[12] Peng Zhang, Jiankun Hu, Cai Li, Mohammed Bennamoun, Vijayakumar Bhagavatula, “A pitfall in fingerprint bio-cryptographic key generation”, Computers & Security, Volume 30, Issue 5, July 2011, pp. 311–319, 2011.

[13] C. R. Costanzo, "Active Biometric Cryptography (ABC): Key Generation Using Feature and Parametric Aggregation," Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on , vol., no., pp.28,28, 1-5 July 2007.

[14] Gang Zheng, Wanqing Li, Ce Zhan, "Cryptographic Key Generation from Biometric Data Using Lattice Mapping," Pattern Recognition, 2006. ICPR 2006. 18th International Conference on , vol.4, pp.513–516, 2006.

[15] Xiangqian Wu, Ning Qi, Kuanquan Wang, Zhang D., "An Iris Cryptosystem for Information Security", Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on, pp. 1533–1536, 2008.

[16] J. Jagadeesan, T.Thillaikkarasi, K.Duraiswamy, “Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature”, International Journal of Computer Applications 2(6), pp. 16–26, June 2010.

[17] N. Miura, A. Nagasaka ir T. Miyatake, “Automatic Feature Extraction from non-uniform Finger Vein Image and its Application to Personal Identification” IAPR Workshop on Machine Vision Applications, Dec. 11 - 13.2002, Nara- ken New Public Hall, Nara, Japan, 2002.

[18] N. Miura, A. Nagasaka ir T. Miyatake “Feature extraction of finger vein patterns based on repeated line tracking and its application to personal identification“, Machine Vision and Applications, Volume 15, Number 4, pp. 194—203, 2004.

[19] P. Maragos, R. W. Schafer, M. Akmal Butt,”„Mathematical Morphology and its applications to image and sygnam processing“, Kluwer Academic Publishers, 1996.

[20] S. Kanade, D. Petrovska-Delacrétaz, B. Dorizzi, "Cancelable iris biometrics and using Error Correcting Codes to reduce variability in biometric data", Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on , vol., no., pp.120–127, 20-25 June 2009.

[21] International Organization for Standardization. ISO/IEC FCD 18033–2, IT Security techniques — Encryption Algorithms — Part 2: Asymmetric Ciphers, 2004.

[22] T. Bram, “Miura et al. vein extraction methods”,http://www. mathworks.com/matlabcentral/fileexchange/ 35716-miura-et-al-vein-extraction-methods.