International Journal of Engineering & Technology, 7 (3.27) (2018) 129-131

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Proposed Method to Generated Strong Keys by Fuzzy Extractor And Biometric

Huda Saleem[1]*, Salah Albermany[2], Husein Hadi[3]

[1]*Faculty of Computer Science and Mathematics, Mathematics Department, Iraq.*
[2]*Faculty of Computer Science and Mathematics, Mathematics Department, Iraq.*
[3]*Faculty of Computer Science and Mathematics, Mathematics Department, Iraq.*

Abstract

The typical scheme used to generated cryptographic key is a fuzzy extractor. The fuzzy extractor is the extraction of a stable data from biometric data or noisy data based on the error correction code (ECC) method. Forward error correction includes two ways are blocked and convolutional coding used for error control coding. "Bose_Chaudhuri_Hocquenghem" (BCH) is one of the error correcting codes employ to correct errors in noise data. In this paper use fuzzy extractor scheme to find strong key based on BCH coding, face recognition data used SVD method and hash function. Hash_512 converted a string with variable length into a string of fixed length, it aims to protect information against the threat of repudiation.

Keywords: *Fuzzy extractor, hashfunction, error correcting codes, BCH code, hamming distance, and biometric.*

1. Introduction

Cryptographic aims to defined and understanding of security [1]. Cryptographic require uniformly random strings [2]. In encryption need to the secrecy of the key whether public or private key to Encryption data and its keep from attack [٣], this key generated from fuzzy extractor and Biometric. Biometric Encryption, other names for Biometric Encryption are Biometric Cryptosystem, Secure Sketch, fuzzy extractor, helper data System. Biometric encryption is a set of technologies that binda key to a biometric or extract string key from the biometric [4, 5, 6]. Biometric is hard to be modified and the accuracy of the recognition effect on the decision of biometric systems [7]. Bio-cryptography methods base on biometric and cryptography, biometric is noisy data but cryptography includes correctness and exactness in keys [8].

Why Used Fuzzy Extractor

Sources random bits are important for cryptography applications. In many cases, these bits are not original form stored for future use but it is found by restoration the same procedure that generated the previous, this bit obtained from this way its contain noise [9,10,11,12]. To utilize from this the sources, from necessary remove noise, to obtain the same string in subsequent readings. Bennett, Brassard, and Robert [9] classification into two tasks are information reconciliation to removes the noise without losing information and privacy amplification to converts the high entropy to a uniform random value[13].

Fuzzy Extractor

Extracts strong key string R from input w, if the w change to input w', then the string R can be reproduced exactly [5], the method that used to estimation noise on input is hamming distance. First, the Secure sketch is a sketch (SS) and recover (Rec) as show figure 1(A), the following steps of secure sketch [8, 14, 15]:

1. Secure sketch (SS) apply on w and produced string S.
2. Recovery (Rec) apply on w' and S and produced w.

Granted correctness of secure sketch (SS) if $H\_dis(w,w') \leq t$, then $Rec\,(w', SS(w)) = w$, but no return output of Rec If $H\_dis(w,w') > t$, where t is represent different between (w,w').

Second, fuzzy extractor performance based on two stepsas show figure 1(B) [١٦,١٧,2]:

1. Generation procedure (Gen) apply on w and give string R and$P$.
2. Reproduction procedure (Rep) apply onw' and P and give string R. The Granted correctness of fuzzy extractor if $H\_dis(w,w')$ ≤t then R, S were created by (R, S) ← Gen (w) and Rep (w', S) = R [18].

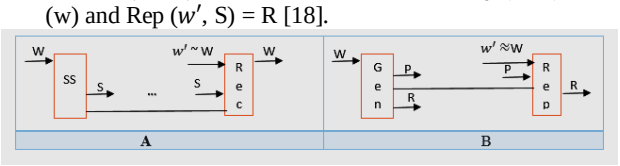

Figure 1: (A) secure sketch; (B) fuzzy extractor

Biometric

Some application need to merge between cryptography and noisy data is biometrics, biometrics aim to recognition Individuals by physiological or behavioral properties [5].

Error Correcting Codes (BCH Coding)

Error correcting codes used in communication and digital technology [19]. BCH codes are a type from multiple error-correcting codes. The binary BCH codes were discovered in 1959 by Hocquenghem and independently in 1960 by Bose and Ray-Chaudhuri. BCH codes are developed in Galois Field (GF). GFhas

a finite number of elements in it. Galois field, also known as the finite fields, over set $GF(p)$ for each prime number p. The extended field, denoted as $GF(p^m)$, are the content of the polynomials of degree $m-1$ over the fieldZ_p. These a polynomials are $a_{m-1}\,x^{m-1}+\ldots+a_1x^1+a_0x^0$where the coefficients a_i in set$\{0,1,\ldots,p-1\}$. BCH codes use field theory as well as a polynomial over a finite filed [20,21]. BCH codes are a subset of the Block codes. A coded sequence, obtained by adding redundant bits to information, is known as code word [22]. BCH ac ode is dividing the message by generator a polynomial and then give the remainder to produce the code word a polynomial. The generator polynomial is created by taking the Least-Common Multiple (LCM) of each minimal a polynomials corresponding to the roots [20].
Code length $n=2^m-1$, Number of parity bits$n-k\le mt$, Minimum hamming distance $d\ge 2t+1$ and Error-correction capability t_{error}.BCH decoding are Calculate the syndrome from the received word, determine the error-locator polynomial, find the roots of error-locator-a polynomial and correct error [٢٣, ٢٤, ٢٥ ٢١].

Hamming Distance

The number of bits positions that different between $w$and w', it is the most natural method used in constructing sketches and fuzzy extractor [26].[32]

Hash_512

One the type of cryptographic algorithms used in digital signature to product the integrity and authentication security services [27]. The hash algorithm includes integrity to verify the modulation of messages, and it is widely used for digital signatures, message authentication codes, and etc. [28]. The SHA_512 generates a 512 hash value [29][31]

2. Implementation of the Proposed Approach

First, biometric consists of four stages: preprocessing, features extraction, classification, and matching, as show figure 2.

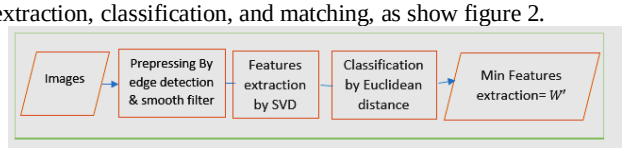

Figure 2: Show the main steps of biometric

Algorithm: Face Recognition
Input: face images, N represents a number of persons and M represent the number training sample or testing sample for each person.
Output: features extraction(W, W')

A) Training or testing images:
1- For I=1 to N
2- For J=1 to M
3- Compute Convolution between image and edge detection filter.
4- Compute Convolution between edge detection image and smooth filters.
5- Merge between edge detection and original.
6- Divided image into parts and compute the SVD for each part.
7- End for I.
8- End for J.
B) classification images:
1- For I=1 to M
2- $D(I)=\sqrt{testing(I)^2-traning^2}$
3- End for I.
4- Find smallest of Euclidean distance
5- W=features of training image
6- W'= features of the testing image with smallest of Euclidean distance

Second, apply fuzzy extractor to the optioned strong key used in encryption message, in figure 3showa fuzzy extractor scheme [23].

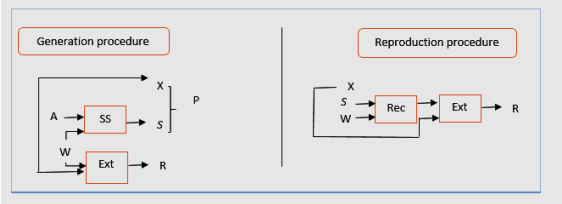

Figure 3: A system for a fuzzy extractor

To generate the key in fuzzy extractor used noise or biometric data, random data, BCH coding, BCH decoding and hash function. Obtain helper data and strong key. As show in figure 4.

Algorithm: a fuzzy extractor.
Input: random X, random Y, W, and W'.
Output: Cryptographic Strong key.

A) Generation procedure:
1- BCH encoding with block length=63, information bit=45 and error=3.
2- Select generator polynomial of six degrees.
3- Compute code word during find modular between generator and BCH block.
4- Compute XOR operation between W and result of step3 to give S.
5- Compute XOR operation between W and X.
6- Compute hash_512 to give the strong key.
B) Helper data (P): S and X.
C) Reproduction procedure:
1- Compute XOR operation between W' and S.
2- Compute S_i=V mod $\mu_i$where V is received code word and $\mu_i$minimal polynomial ofα^i.
3-Selecting the minimal polynomials for α.
4-Compute$S_i(\alpha^i)$.
5- BCH decoding during Newton's method.
6- Compute XOR operation between S and result of step5 to give W.
7- Compute XOR operation between W and X.
8- Compute hash_512 to give the strong key.

3. Conclusion

The general system is asymmetric biometric. Performance a system apply on face images as an example of the scheme. The main aim of this paper isgenerateda strong key used in cryptography application but unlike traditional keys and investigate the fuzzy extractor performance on based biometric used features extraction of the face. This work may be helpful to the understanding of system fuzzy extractor implementation.

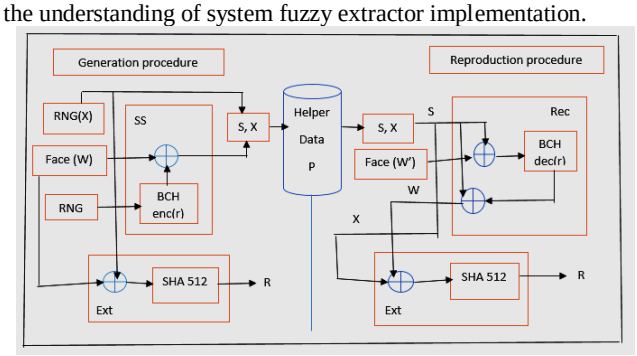

Figure 4: Implementation diagram of the fuzzy extractor

References

[1] Maes R, Tuyls P & Verbauwhede I, "Low-overhead implementation of a soft decision helper data algorithm for SRAM PUFs", *Cryptographic Hardware and Embedded Systems-CHES* (2009), pp.332-347.
[2] Yasunaga K & Yuzawa K, "On the Limitations of Computational Fuzzy Extractors", *work*, Vol.3, No.1,(2018), pp.7-9.
[3] Bösch C, Guajardo J, Sadeghi AR, Shokrollahi J & Tuyls P, "Efficient helper data key extractor on FPGAs", *International Workshop on Cryptographic Hardware and Embedded Systems*, (2008), pp.181-197.

[4] Jain AK, Nandakumar K & Nagar A, "Biometric template security", *EURASIP Journal on advances in signal processing*, (2008).
[5] Tuyls P, Škoric B & Kevenaar T. eds., *Security with noisy data: on private biometrics, secure key storage and anti-counterfeiting*, Springer Science & Business Media, (2007).
[6] Cavoukian A & Stoianov A, "Biometric encryption: The new breed of untraceable biometrics", *Biometrics: fundamentals, theory, and systems. Wiley, London*, (2009).
[7] Li N, Guo F, Mu Y, Susilo W & Nepal S, "Fuzzy Extractors for Biometric Identification", *IEEE 37th International Conference on Distributed Computing Systems*, (2017), pp.667-677.
[8] Yang W, Hu J & Wang S, "A delaunay triangle-based fuzzy extractor for fingerprint authentication", *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, (2012), pp.66-70.
[9] Bennett CH, Brassard G & Robert JM, "Privacy amplification by public discussion", *SIAM journal on Computing*, Vol.17, No.2, (1998), pp.210-229.
[10] Brostoff S & Sasse MA, "Are Passfaces more usable than passwords? A field trial investigation", *People and Computers XIV—Usability or Else!*, (2000), pp.405-424.
[11] Daugman, J, "How iris recognition works", *The essential guide to image processing*, (2009), pp.715-739.
[12] Ellison C, Hall C, Milbert R & Schneier B, "Protecting secret keys with personal entropy", *Future Generation Computer Systems*, Vol.16, No.4,(2000), pp.311-318.
[13] Fuller B, Reyzin L & Smith A, "When are fuzzy extractors possible?", *International Conference on the Theory and Application of Cryptology and Information Security*, (2016), pp.277-306.
[14] Li Q, Guo M & Chang EC, "Fuzzy extractors for asymmetric biometric representations", *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, (2008), pp.1-6.
[15] Khalil MS, "Generating Public Key from Fingerprint using Fuzzy Extractor" *International Journal of Scientific & Engineering Research*, (2017).
[16] Gupta NK & Kaur M, "A robust and secure multitrait based fuzzy extractor", *8th International Conference on Computing, Communication and Networking Technologies*, (2017), pp.1-6.
[17] Kaur T & Kaur M, "Cryptographic key generation from multimodal template using fuzzy extractor", *Tenth International Conference on Contemporary Computing (IC3)*, (2017), pp.1-6.
[18] Dodis Y, Ostrovsky R, Reyzin L & Smith A, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", *SIAM journal on computing*, Vol.38, No.1,(2008), pp.97-139.
[19] Chen H, "CRT-based high-speed parallel architecture for long BCH encoding", *IEEE Transactions on Circuits and Systems II: Express Briefs*, Vol.56, No.8,(2009), pp.684-686.
[20] Prashanthi M & Samundiswary P, "An Area Efficient (31, 16) BCH Decoder for Three Errors", *International Journal of Engineering Trends and Technology (IJETT)*, (2014).
[21] Shu L & Costello DJ, "Error control coding: fundamentals and applications", *Englewood Cliffs, New Jersey*, (1983).
[22] Kristian H, Wahyono H, Rizki K & Adiono T, "Ultra-fast-scalable BCH decoder with efficient-Extended Fast Chien Search", *3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)*, (2010), pp.338-343.
[23] Qamar RA, Maarof MA & Ibrahim S, "An efficient encoding algorithm for (n, k) binary cyclic codes", *Indian Journal of Science and Technology*, Vol.5, No.5,(2012), pp.2757-2761.
[24] Sahana C & Anandi V, "Error Detection Using Binary BCH (255, 215, 5) Codes", *IJESRT*, (2015).
[25] Edwards I, Newell P & Trufan C, "SRAM PUF Analysis and Fuzzy Extractors", (2010).
[26] Kodra S, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", 2015.
[27] Algredo-Badillo I, Morales-Sandoval M, Feregrino-Uribe C & Cumplido R, "Throughput and efficiency analysis of unrolled hardware architectures for the sha-512 hash algorithm", *IEEE Computer Society Annual Symposium on VLSI*, (2012), pp.63-68.
[28] Vishnu, S., Vignesh, S., & Surendar, A. (2017). Design and implementation of ZETA micro-inverter for solar PV application. International Journal of Mechanical and Production Engineering Research and Development, 7(4), 215–222.
[29] Kahri F, Mestiri H, Bouallegue B & Machhout M, "An efficient fault detection scheme for the secure hash algorithm SHA-512", *International Conference on Green Energy Conversion Systems (GECS)*, (2017), pp.1-5
[30] Nguyen TAT & Dang TK, "Combining fuzzy extractor in biometric-kerberos based authentication protocol", *International Conference on Advanced Computing and Applications (ACOMP)*, (2015), pp.1-6.
[31] G Ainabekova, Z Bayanbayeva, B Joldasbekova, A Zhaksylykov (2018). The author in esthetic activity and the functional text (on the basis of V. Mikhaylov's narrative ("The chronicle of the great jute"). Opción, Año 33. 63-80.
[32] D, Ibrayeva, Z Salkhanova, B Joldasbekova, Zh Bayanbayeva (2018). The specifics of the art autobiography genre. Opción, Año 33. 126-151.