British Journal of Mathematics & Computer Science
10(3): 1-9, 2015, Article no.BJMCS.18993
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Novel Chaff Generation for Fingerprint Fuzzy Vault

Rahul Hooda[1*] and Manavjeet Kaur[1]

[1]*Department of Computer Science and Engineering, PEC University of Technology, Chandigarh, India.*

Article Information

DOI: 10.9734/BJMCS/2015/18993
Editor(s):
(1) Victor Carvalho, Polytechnic Institute of Cávado and Ave, Portuguese Catholic University and Lusiada University, Portugal.
Reviewers:
(1) Anonymous, Al-Zaytoonah University of Jordan, Jordan.
(2) G. Y. Sheu, Accounting and Information Systems, Chang-Jung Christian University, Tainan, Taiwan.
Complete Peer review History: http://sciencedomain.org/review-history/10087

Original Research Article

Received: 20 May 2015
Accepted: 22 June 2015
Published: 08 July 2015

Abstract

Aims: To propose a new chaff generation method and to compare the results with the standard Clancy's Chaff Generation Method.
Place and Duration of Study: Department of Computer Science and Engineering, PEC University of Technology, Chandigarh during July 2012 and June 2013.
Methodology: Two databases are used to calculate the results. One is the FVC 2004-DB1 database which is approved by fingerprint recognition website. Other is the live database created using the Crossmatch's Verifier 300 LC scanner. In both the databases 100 images of 10 different persons were compared with each other and performances are computed and compared.
Results: Results show that proposed algorithm takes less time to generate different number of chaff points (from 50 to 500) than Clancy's algorithm. The performance metrics like Genuine Accept Ratio, False Accept Ratio and False Reject Ratio have same values of both the algorithms. Results are computed on both the databases.
Conclusion: Experiments results show that the proposed algorithm is faster than the Clancy's algorithm in generating equal number of chaff points.

Keywords: Biometrics; fuzzy vault system; fingerprint; chaff generation.

1 Introduction

Today a wide variety of systems require reliable personal authentication schemes to either confirm or determine the identity of individuals requesting their services. With hackers and electronic fraud, authentication has become a very crucial matter to ensure that the rendered services are accessed by a legitimate user. Establishing the identity of the person is a critical task in any authentication system [1]. This

**Corresponding author: r89hooda@gmail.com;*

problem is solved to an extent by the Biometric system which is the science of establishing the identity of a person using his/her anatomical and behavioral traits [2]. Biometric system uses a biometric trait to identify any person. Commonly used biometric traits include fingerprint, iris, face and palmprint.

Typically a biometric system consists of five main modules [3] as shown in Fig. 1:

i. Biometric Sensor Module: A biometric sensor is used for obtaining identifiable information from the users
ii. Feature extractor module: This module extracts a set of salient features from the acquired biometric data.
iii. Matching Module: This module compares the biometric sample, called a query or test, with the pre-stored template.
iv. Decision-making module: This module decides on the identity of the user based on the matching score.
v. Template database: The database is used for storing user templates captured during the enrolment stage.

The authentication to biometric system is granted only if same user biometric is given as input. Some methods have been developed to forge the identity to the system. So it becomes a challenge and of importance to guard the user template from the adversary attacks. For protecting the template, various template protection schemes have been used. A high promising approach of template protection is fuzzy vault scheme. In fuzzy vault scheme, unlike traditional systems, exact matching is not required and some fuzziness is allowed in terms of minutiae matching which make this approach quite popular in biometric field. Fuzzy vault scheme has been implemented using various traits like fingerprint [4], iris [5], face [6], palmprint [7]. The most compute-intensive block in the fuzzy vault scheme is the chaff generation module [8]. This module is used to generate noise points which hide the genuine points from attacker. In this paper, a new method for chaff generation is proposed.

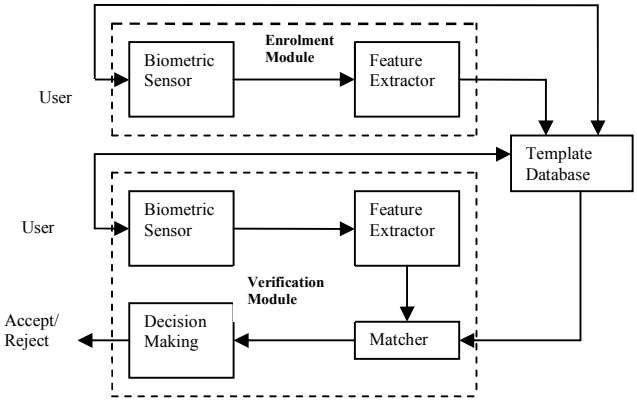

Fig. 1. Biometric system module

2 Fuzzy Vault Scheme

Originally the fuzzy vault was proposed by Juels & Sudan [9]. They used example of Alice and Bob where Alice encloses secret S in fuzzy vault and lock it using an unordered set A. Bob also having an unordered set B can unlock the vault only if set B substantially overlaps with set A. Based on secret key chosen by Alice, a polynomial P is formed. Set A constitute the points which lie on that polynomial and then some chaff points are added which do not lie on the chosen polynomial. Next, Bob tries to authenticate himself by using an

unordered set B. If this set B overlaps with unordered set A then Bob is authenticated and secret S is provided.

2.1 Fuzzy Vault Encoding

In this biometric data is used to hide the cryptographic secret key. Secret key is used to plot genuine points with Cartesian coordinates in a two dimensional plane. Lot of other non-genuine points is also added to protect the template with genuine points. The overall algorithm of fuzzy vault encoding is described below [10]:

i) Checksum Calculation: A random 128-bit secret key s is selected and is provided as input to the checksum calculation module. CRC-16-CCITT, which is a standard algorithm, is used for checksum calculation. This algorithm will produce 16 bit data string. The algorithm is described below:

$$x^{16}+x^{12}+x^{5}+1=0 \quad (1)$$

A number is chosen from 0x0000 or 0xFFFF which works as initial remainder. Then 0x1021 is chosen to form the CRC polynomial shown in (1). The secret key and the initial remainder are both righted shifted 1 bit. Then initial remainder value is XORed with CRC polynomial value that is 0x1021 and the result becomes the new initial remainder value. The rightmost bit of both the secret key and new initial remainder is compared with each other. If they are equal both are right shifted 1 bit. Otherwise, secret key is right shifted whereas remainder value is right shifted and XORed with polynomial value. This process is repeated for all the bits of the secret key. The remainder value at the end is considered as the checksum value of the secret key.

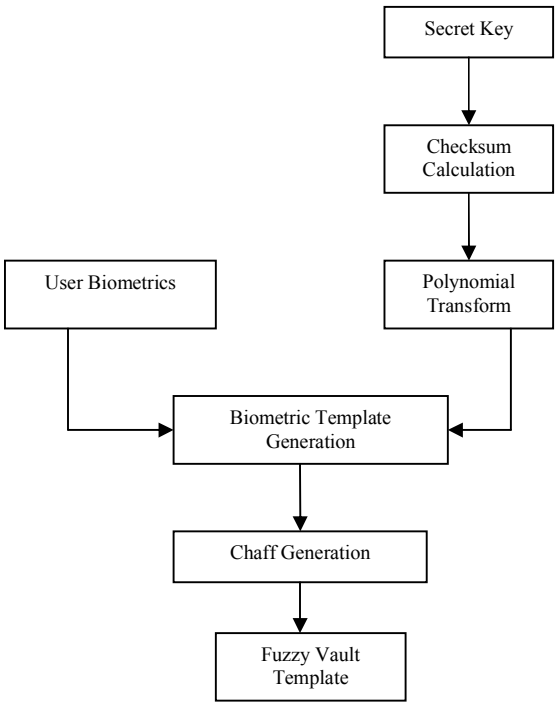

Fig. 2. Fuzzy vault encoding

ii) Polynomial Transform: 16 bit checksum value is concatenated at the end of secret key to form 144 bit modified secret key s'. This 144 bit key is divided into 8 equal parts to form the coefficients of polynomial with degree 7. Let s' be divided into s_1, s_2,…..s_8 and therefore polynomial p(x) can be represented as following:

$$p(x) = s_1x^7+s_2x^6+s_3x^5+s_4x^4+s_5x^3+s_6x^2+s_7x+s_8$$

iii) Biometric Template Generation: For each input fingerprint a template is generated which highlights the minutiae in the image. For template generation, raw data goes through various pre-processing stages followed by feature extraction. Type, location and orientation of the minutiae are considered to form 16 bit input to the polynomial. The 16-bit values which are formed using biometric feature, are taken as X-coordinate values which are then plotted onto the polynomial. Corresponding Y-coordinate values are calculated using polynomial equation and the set of X and Y coordinate values become genuine points which are also added to the fuzzy vault template.

iv) Chaff Generation: In this module, chaff points which are also known as noise points are generated to hide the genuine points in the template. The chaff generation procedure is repeated until a desired number of points are added to the fuzzy vault template. The greater number of chaff points ensures enhanced security but it also increases the execution time. So the number of points added is decided so that neither security nor execution time is compromised.

v) The combination of chaff points and genuine points is considered as a fuzzy vault template.

2.2 Fuzzy Vault Decoding

The overall algorithm of fuzzy vault decoding is described below [10]:

i) Biometric Template Generation: This module extracts the biometric features of the user.

ii) Biometric Data Mapping: The biometric features of test image which are in 16-bit format are then compared with the X-coordinate values of fuzzy vault members. The members with X-values equal to biometric features are stored along with their equivalent Y-coordinate values. This set of X and Y values are used for polynomial reconstruction.

iii) Polynomial Construction: The set formed in the previous step may contain some chaff points rather than the genuine points. So Lagrange interpolation is used to construct all the polynomials possible using the above set. Lagrange Interpolation will require one point extra than the degree of polynomial to construct the polynomial.

iv) Checksum Calculation: The coefficients of polynomial are concatenated to form a string of bits. Then the string is divided into two parts where end part has 16 bits and rest of the bits is in the first part. Checksum of the first part all the polynomial is calculated.

v) If the checksum calculated is equal to the last part of any polynomial then that polynomial is the required one and secret key is released to the user.

3 Chaff Generation Method

During the encoding phase of fuzzy vault chaff generation method is used to generate random points. These chaff points are used to hide the genuine minutiae points and therefore also secure the secret crypto-key. Any generated chaff points must satisfy few conditions. Firstly they should not lie on the polynomial on which genuine points lie because if they lie, they will work as genuine points. Secondly, all chaff points should be distributed randomly without any pattern otherwise attacker can find pattern and discard random points. Thirdly, each chaff points must be δ distance away from each other member of fuzzy vault member to avoid the possibility of clustering.

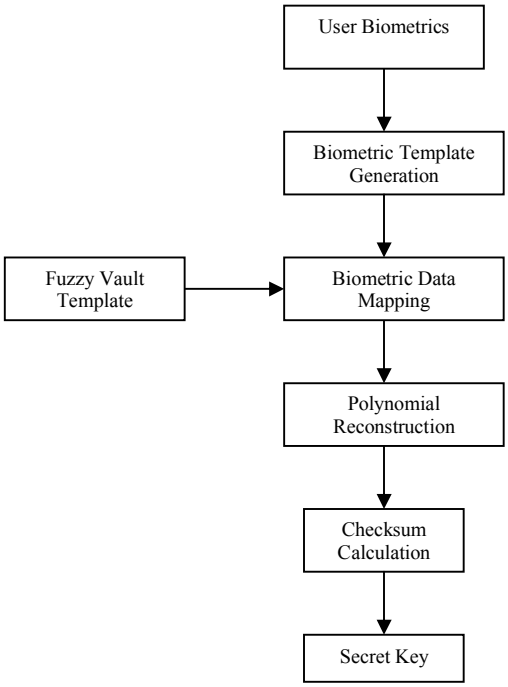

Fig. 3. Fuzzy vault decoding

3.1 Clancy's Chaff Generation Algorithm

Clancy [11] gave an algorithm of chaff generation for the fuzzy vault scheme originally proposed by Juels and Sudan. Clancy et al were first to propose that chaff points should be at a minimum distance δ from genuine points. In the algorithm Euclidean distance is used to compute distance between chaff points and genuine points. Computed distance is compared with δ and based on comparison of distance random point is either added to the fuzzy vault or not.

Clancy chaff generation method is described as follows:

1. Minutiae points are extracted and stored in an array, Min.

   $Min = [(mx_1,my_1), (mx_2,my_2)\ldots\ldots\ldots(mx_n,my_n)]$.

2. Coordinate values of the minutiae x and y are concatenated along with the orientation θ form 16 bit variables.

   $X_i = (mx_i \mid my_i \mid \theta)$

3. Values in X_i are considered as x values for polynomial p and Y_i values are computed by putting x values in polynomial. The set of values are considered as valid points and are added to the fuzzy vault Fv.

   $Fv = [(X_1,Y_1), (X_2,Y_2)\ldots\ldots\ldots..(X_n,Y_n)]$

4. A random point is generated in minutiae domain

   R = (R_x, R_y)

5. Euclidean distance of the random point is calculated with all the members of Min

$$d_1=\sqrt{(mx_1 - R\_x)^2 + (my_1 - R\_y)^2}$$

$$\ldots..$$

$$d_n=\sqrt{(mx_n - R\_x)^2 + (my_n - R\_y)^2}$$

If the conditions $d_i > \delta$ (i = 1 to N) are satisfied, the random point (R_x, R_y) is added to the fuzzy vault Fv and otherwise not. This process is repeated until required number of chaff points is generated. As can be seen, for finding Euclidean distance multiple squares and square-root operations to be performed which takes time. So this process is very intensive in terms of calculations and therefore not suitable for implementation in real systems.

3.2 Proposed Chaff Generation Algorithm

The proposed method of chaff generation is based on reducing the number of calculations of square and square-root operation to reduce the computation time. In this method instead of finding Euclidean distance between two points, we find axis difference between two points, the formula for which is given below:

$$D= |(x_1-x_2)| + |(y_1-y_2)|$$

As can be seen, in this formula, only addition, subtraction and mod operations are used and square and square-root operations are avoided. To make the effect of both the x-value and y-value these calculations are done in the Galois field. Other conditions for selecting a random point as chaff point are same as that in Clancy's method.

Proposed chaff generation method is described as follows:

1. Minutiae points are extracted and stored in an array, Min.

   $Min = [(mx_1,my_1), (mx_2,my_2)\ldots\ldots\ldots(mx_n,my_n)]$.

2. Coordinate values of the minutiae x and y are concatenated along with the orientation θ form 16 bit variables.

   $X_i = (mx_i \mid my_i \mid \theta)$

3. Values in X_i are considered as x values for polynomial p and y values are computed by putting x values in polynomial. The set of values are considered as valid points and are added to the fuzzy vault Fv.

   $Fv = [(X_1, Y_1), (X_2, Y_2)\ldots\ldots\ldots..(X_n, Y_n)]$

4. A random point is generated in Galois domain. In Galois field, a point can lie in the range of 0 to 65536(2^{16}). Therefore random point is generated between 0 and 1 and it is multiplied by 65536 so that it will be within range.

   R = (R_x, R_y)

5. Axis distance of the random point is calculated with all the members of Fv

$$D_1 = |(mx_1 - R\_x)| + |(my_1 - R\_y)|$$
$$\ldots\ldots$$
$$D_n = |(mx_n - R\_x)| + |(my_n - R\_y)|$$

If the conditions $D_i > \delta$ (i = 1 to N) are satisfied, the random point (R_x, R_y) is added to the fuzzy vault Fv and otherwise not. Value of δ is taken as 20 after experimentation. This process is repeated until required number of chaff points is generated. As the chaff generation formula does not include computation-intensive mathematical operations so the proposed method will take less effort for calculation then Clancy's. This can contribute to a significant reduction in the overall execution time.

4 Results and Analysis

The experiment setup for the fuzzy vault consists of 128-bit secret key. Cyclic Redundancy Check (CRC-16 CCITT) is used for checksum calculation with a value of 0x1021 to form the polynomial. In fuzzy vault encoding process the 128-bit secret key s is concatenated with 16 bit CRC to form 144 bit modified secret key s'. Then s' is divided into 9 equal parts to form the coefficients of 8-degree polynomial. The performance of the Clancy and proposed algorithm is compared for generating various number of chaff points. The common practise is to use around 20 minutiae and also setting the value of δ as 20. The results are collected using two databases. One is the standard one called FVC database and other is live database collected using CrossMatch's Verifier 300LC Scanner. The GAR of the system is 90%, FRR of the system is 10% and FAR of the system is 9% and is same for fuzzy vault system using Clancy's method as well as proposed method.

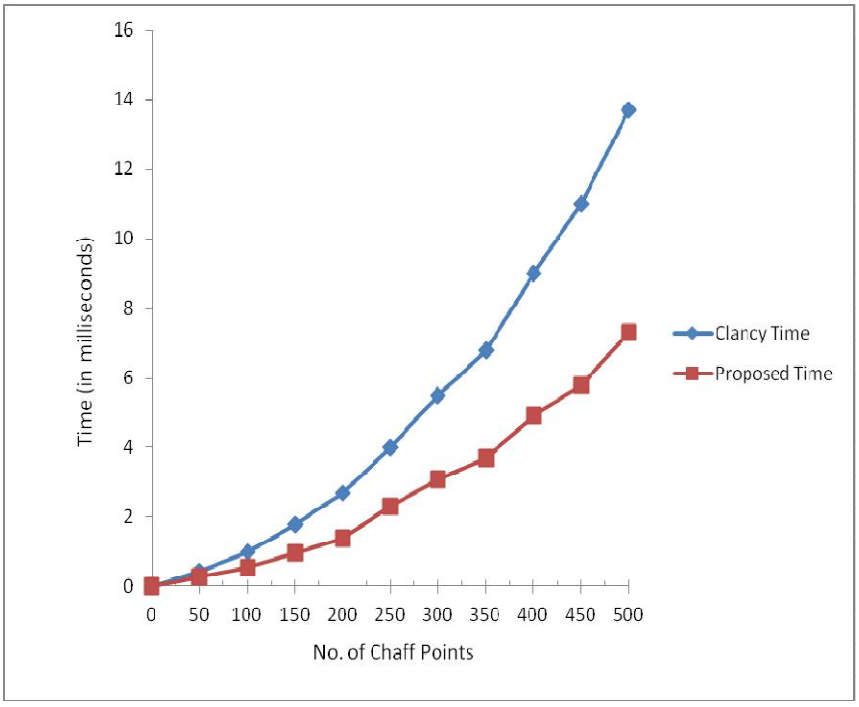

Fig. 4. Graph of chaff generation time vs no. of chaff points for Clancy's method and proposed method using FVC database

Table 1. Presents the performance of both Clancy's and proposed algorithm for generating different number of chaff points using FVC database

No. of chaff points	Clancy time (in milliseconds)	Proposed time (in milliseconds)
50	0.42	0.27
100	1.0	0.54
150	1.8	0.98
200	2.7	1.4
250	4.0	2.3
300	5.5	3.1
350	6.8	3.7
400	9.0	4.9
450	11.0	5.8
500	13.7	7.3

Table 2. Presents the performance of both Clancy's and proposed algorithm for generating different number of chaff points using live database

No. of chaff points	Clancy time (in milliseconds)	Proposed time (in milliseconds)
50	1.0	.58
100	1.9	1.1
150	3.6	2.4
200	6.7	3.5
250	8.8	5.6
300	10.5	7.2
350	13.9	10.1
400	18.7	12.8
450	21.0	15.4
500	24.2	17.9

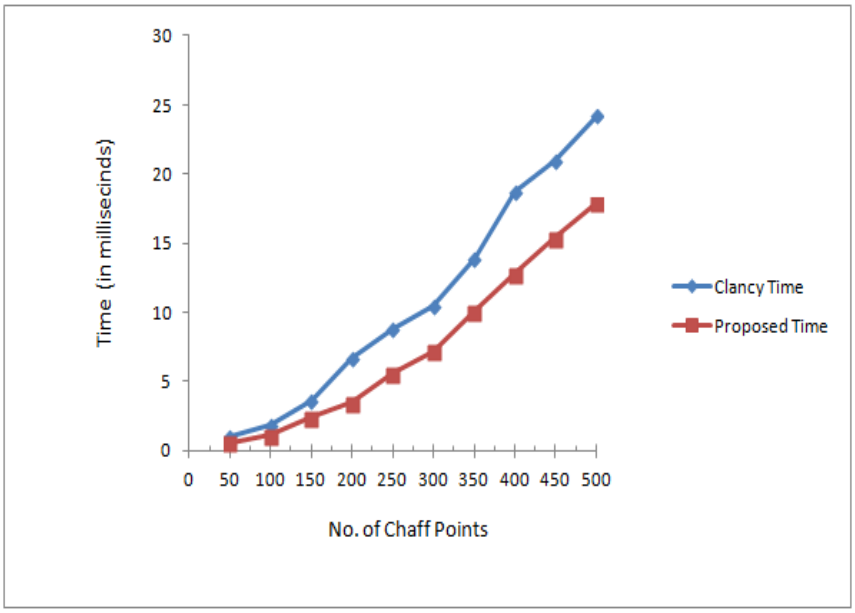

Fig. 5. Graph of chaff generation time vs. no. of chaff points for Clancy's method and proposed method using live database

5 Conclusion

In this paper a new chaff point generation technique for fuzzy vault has been proposed. Experiments results show that the new algorithm is faster than the existing algorithm. The results clearly show that the proposed algorithm is quicker than the Clancy's algorithm. This is due to the fact that simple arithmetic operators like addition and subtraction are used, whereas Clancy's method uses square and square-root operators.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Anil K Jain, Karthik Nandakumar, Abhishek Nagar. Biometric template security. In Journal on Advances in Signal Processing. Michigan State University. 2007;1-17.

[2] Cengiz Orencik. Fuzzy vault scheme for fingerprint verfication: Implementation, analysis and improvements. Sabanci University. 2008;1-50.

[3] Xi Kai, Ho Jiankun. Bio-cryptography. 2009;139-148.

[4] Umut Uludag, Sharath Pankanti, Anil K Jain. Fuzzy vault for fingerprints. In Proceedings of Audio- and Video- based Biometric Person Authentication, Rye Town. NY; 2005.

[5] X Wu, N Qi, K Wang, D Zhang. A novel cryptosystem based on Iris Key Generation. Fourth Int. Conf. on Natural Computation (ICNC 2008). 2008;53–56.

[6] Y Wang, Plataniotis KN. Fuzzy vault for face based cryptographic key generation. Biometrics Symposium; 2007.

[7] A Kumar, A Kumar. Dev. of a new cryptographic construct using palmprint based fuzzy vault. EURASIP Journal on Advances in Signal Processing; 2009.

[8] Mohammad Khalil-Hani, Rabia Bakhteri. Securing cryptographic key with fuzzy vault based on a new chaff generation method, in proceedings of IEEE. 2010;259-265.

[9] Ari Juels, Madhu Sudan. A Fuzzy Vault Scheme. IEEE International Symposium Information Theory, Lausanne, Switzerland. 2002; 408.

[10] Karthik Nandakumar, Anil K Jain, Sharath Pankanti. Fingerprint-Based Fuzzy Vault: Implementation and Performance. IEEE Transition for Information Forensics & Security. 2007;744-757.

[11] T Clancy, D Lin, N Kiyavash. Secure smartcard-based fingerprint authentication. In Proceedings of ACM SIGMM Workshop on Biometric Methods and Applications, Berkley, CA. 2003;45-52.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/10087