Improving The Accuracy of Fuzzy Vault Scheme in Fingerprint Biometric

Joni Saputra
School of Computing
Telkom University
Bandung, Indonesia
jonisaputra@student.telkomuniversity.ac.id

Parman Sukarno
School of Computing
Telkom University
Bandung, Indonesia
psukarno@telkomuniversity.ac.id

***Abstract*—At present, authentication techniques using fingerprint biometrics have been widely used in various fields. This is because the authentication techniques using biometrics are safer and more comfortable than using traditional passwords. In order to realize this, a technique in the biometric cryptosystem is proposed in the research, called the fuzzy vault scheme. Although the fingerprint data in the form of minutiae can be protected with a fuzzy vault scheme compared to traditional authentication systems, it can reduce user convenience. Previous studies proposed a distance-based method in the fuzzy vault scheme. The distance-based method is proposed because it is no need to align and rotate the fingerprint image during registration or authentication. Then with the distance-based method also does not produce a helper data that can lead to information leakage that can be exploited by impostor. In the research, the distance-based method is proposed with several modifications, which are the minutiae filter and candidate points identification techniques. The previous method produces FRR 13.4375% and FAR 0.4515% and the proposed method produced FRR 8.9475% and FAR 0.3520%.**

***Index Terms*—biometric cryptosystem, fuzzy vault scheme, minutiae filter, chaff point generation, candidate point identification**

I. Introduction

Nowadays many technologies have been developed to identify and authenticate a person from his unique biological character, known as biometrics. Biometrics is a method to identify and authenticate individuals based on their anatomical (e.g., fingerprints, iris, hand geometry) and behaviours (e.g., speech, handwritten signature) [1]. The advantages of using biometrics (called "something user is") are for users convenience: users do not need to remember passwords or personal identification number/PIN (called "something user know"), carry a card/id card and it reduces the amount of cost for making cards/ID cards (called "something user has"). Fingerprint is the most popular biometrics due to its permanence and distinctiveness.

Biometric cryptosystem has been introduced to secure genuine template. Biometric cryptosystem technique is used to bind a cryptographic key (i.e., key-binding biometric cryptosystem) and to generate a cryptographic key directly (i.e., key-generation biometric cryptosystem) from biometric feature. This research focuses on one method in key-binding biometric cryptosystem, called fuzzy vault. Fuzzy vault scheme is one of the key-binding biometric cryptosystem variants besides fuzzy commitment scheme. Fuzzy vault scheme is used in fingerprint biometrics because it can handle unordered set of elements in the biometric features [2], unlike fuzzy commitment scheme [3]. Fuzzy vault scheme uses features on fingerprints called minutiae and depends on the location, direction and type of the minutiae. Accuracy of location, direction and type of minutiae are strongly influenced by the quality of image, the scale of image and behaviour of the users (e.g. displacement and rotation). Inaccuracies in the detection of minutiae on fingerprint can cause the matching process to be inaccurate too. Therefore, to overcome the inaccuracies in fingerprint biometrics, an alignment and translation technique are applied [4]–[11]. The drawback of alignment and translation technique is that the process of matching between enrolment and query template requires helper data. The helper data can provide information leaks to impostor. To avoid forming the helper data from alignment and translation technique, the fuzzy vault scheme which does not use helper data is a better choice.

The distance based method is used in this research. The distance based method is the distance between minutiae point [12] or the distance between reference point (e.g., core point) and minutiae point as well as the orientation between them [13], [14]. This research uses the distance based method with singular point (core point) detection as the reference point, then Euclidean distance between core point and minutiae are used to run the matching process on a fuzzy vault scheme, without using alignment and translation process [14]. The security of the fuzzy vault scheme depends on the inability to rebuild polynomial, which is a special case of the Reed-Solomon decoding, therefore CRC and Lagrange's interpolation is used to decoding process [11]. Furthermore, in the fuzzy vault scheme, the addition of chaff point (noise) with certain criteria is used to make fingerprint templates more secure [4]. In 2016 [14], Yadav et al., proposed the distance based method to build the fuzzy vault without an alignment and translation process. The paper shows promising results using the distance based method. Experimental results indicated the false rejection rate (FRR) and false acceptance rate (FAR) at 13.4375% and 0.4515%, respectively. The experiment result showed that the level of convenience was low because of high FRR. Our purpose is to decrease the FRR and maintain the FAR of fuzzy vault scheme from the previous method

978-1-7281-0264-1/19/$31.00 ©2019 IEEE

[14] using the FVC2002 sets B database [15]. After that, we implement the proposed method in different degree of polynomial to find out and measure the effects of the degree of polynomial against the FRR and FAR.

This paper is arranged as follows. We conveying the background and issues in this research in section I and describe the related work of this research in section II. Section III describes the research method. We discuss about experimental result in section IV. Finally, we make conclusion in section V.

II. Related Work

This section discusses the references related to the general review of fingerprint biometrics and template protection techniques along with the related works that have been conducted. This section starts from the basic concept of fingerprint biometrics and then the design techniques used to protect fingerprint template, especially fuzzy vault scheme.

The fuzzy vault scheme is one of the schemes found in key-binding biometric cryptosystems which was first introduced by Juels and Sudan [2]. This fuzzy vault scheme is another variant of the fuzzy commitment scheme which was previously proposed by Juels and Wattenberg [3]. The fuzzy vault scheme is proposed to handle unordered sets of biometric features. The fuzzy vault scheme is basically combining secret keys, unordered features of biometric and some noise into a single unit called vault. Juels and Sudan [2], in designing a fuzzy vault scheme not followed with the implementation. In the development of the fuzzy vault scheme, there are several studies that have implemented the scheme to protect biometric templates, especially on fingerprints.

In [4], Clancy, T. C., et al. implemented a fuzzy vault scheme using the location of the minutiae in the form of a cartesian coordinate (x, y) without the direction and type of the minutiae. The decoding process used is Reed-Solomon error correcting code with the Berlekamp-Massey algorithm [16], [17]. Authors assumed that fingerprints are used during enrolment and authentication is aligned. In reality, this is not realistic for the authentication process on fingerprint biometrics. From the results of the experiments, the average value of FRR is still high, i.e. 20-30% (without showing the results of FAR). Chung, Y., et al. [5] implemented fuzzy vault schemes by performing automatic alignment with geometric hashing techniques on feature minutiae [18]. Authors modified the geometric hashing technique from identification $1 : N$ to verification $1 : 1$. From the experimental results using the hash table can align the fingerprint feature accurately in the fuzzy vault scheme. However, this study has not presented experimental results in the form of FRR and FAR. Moreover Yang, S. and Verbauwhede, I. [6], also implemented using the fingerprint minutiae feature in the fuzzy vault scheme. They represented minutiae feature in the form of polar coordinates by finding the minutiae used as a reference point. For the decoding process, the authors used the Reed-Solomon error correcting code with the Berlekamp-Massey algorithm. From the experimental results obtained successful unlocking rate 83%, but the error rate obtained is still quite high compared to some of the other fingerprint verification algorithms. In the same year, Uludag, U., et al. [7] implemented a fuzzy vault scheme using the minutiae feature too. Different from Clancy's method, the minutiae feature is used by looking at the type of ridge on the fingerprint, in the form of a ridge ending and ridge bifurcation. Representation of feature extraction in the form of minutiae consists of 3 (triplets), i.e. location and orientation (x, y, θ). The decoding process used in the fuzzy vault scheme does not use Reed-Solomon error correcting code, but rather a error detection code, namely cyclic redundancy check (CRC). The tessellation process on fingerprint images is done to overcome the problems of translation and rotation on fingerprint images. From the experimental results obtained the average value of FRR and FAR are 21% and 0%, and has limitations in terms of the complexity of decoding processing time which is still high.

Uludag, U., et al. [8] implemented the fuzzy vault scheme in fingerprint biometrics by automatically creating field-based auxiliary data from fingerprints. The helper or auxiliary data in a fuzzy vault scheme can create opportunities for impostor to carry out attacks on the system. Experiments were conducted on the FVC2002 DB2 dataset and the authors only used two impressions of eight impressions for each fingerprint, i.e. impressions one and two. This experiment resulted in an average of GAR and FAR are 72.6% and 0%. After that the authors used impressions of two and seven and they produce an average value of GAR and FAR are 84.5% and 0%. Nagar and Chaudhury [9] merged the Fuzzy Vault scheme with the asymmetric RSA cryptosystem and apply the security level hierarchy in the cryptosystem by using properties invariant. The authors claimed the weaknesses in fuzzy vault schemes that do not exploit the order of biometric template, i.e. when the results of a polynomial evaluation of two or more feature elements have similar or adjacent value in the locking (encode) process, it will be considered the same element, thereby reducing the level of security system. The experiment was conducted with 29 fingerprint images of 9 people with a size of 256 x 256. From the experimental results, the FRR value is already low, but the FAR value is still high, depending on the fuzzy vault tolerance used. Moreover, Jeffers, J., et al. [10] proposed a translation and rotation method on fingerprint templates to make lock and unlock set. The authors conducted a study of three matching techniques in the translation structure and rotation invariant, i.e. five nearest neighbor based structures [19], triangle based structures [20] and Voronoi neighbor based structures [21]. From the experimental results obtained Voronoi neighbor based structures technique provides better performance than others techniques. The average value of FRR and FAR of the scheme are not shown in details and clearly.

In 2007, Nandakumar, K., et al. [11] proposed fuzzy vault method by using characteristics of local ridge type (terminations and bifurcations) in fingerprint biometrics. Authors used the location and orientation of minutiae points as three-tuple representations (u, v, θ). Authors also used the alignment method using iterative close point (ICP) and helper data extraction for matching between enrolment and query template.

Yadav, D. H. S., et al. [14] proposed the distance based method to build the fuzzy vault without an alignment and translation process. The distance base method used singular point (core point) detection as reference point. Euclidean distance between core point and each minutiae is used to do the matching process on a fuzzy vault scheme, without using alignment and translation process. The authors concatenated the distance and the angle to represent fingerprint template as abscissa of the polynomial. From the experimental results using the FVC2002 set B (DB1, DB2, DB3, DB4) and FVC2004 set B (DB1, DB2, DB3, DB4) dataset, the GAR and FAR with the fuzzy vault scheme were 86.0312% and 0.3944%. From the results of the experiment, it can be shown that the average value for the GAR is still low.

III. Research Method

In order to obtain a better FRR and prevent the possibility of information leakage from alignment and rotation techniques in the form of helper data in the fuzzy vault scheme, the distance-based technique by Yadav et al. [14] is exploited in this research. In general, there are two main processes in fuzzy vault scheme, i.e., lock/encode and unlock/decode. However, the existing feature extraction technique was used to obtain set of minutiae and core point from fingerprint image that was used as one of the input to the fuzzy vault scheme. The techniques of feature extraction in the form of minutiae applied the implementation developed by Vahid K. Alilou [22]. After that, the techniques of feature extraction in the form of core point used the implementation developed by Luigi Rosa [23].

A. Lock/Encode Process

Lock/encode process is the process of encoding a fingerprint template representation into a polynomial with the secret key as its coefficient and adding some chaff point to a vault. The lock/encode design on the previous method [14] was modified by adding a shape, namely minutiae filter technique (the shapes in green color). The details of design for lock/encode process is shown in Figure 1.

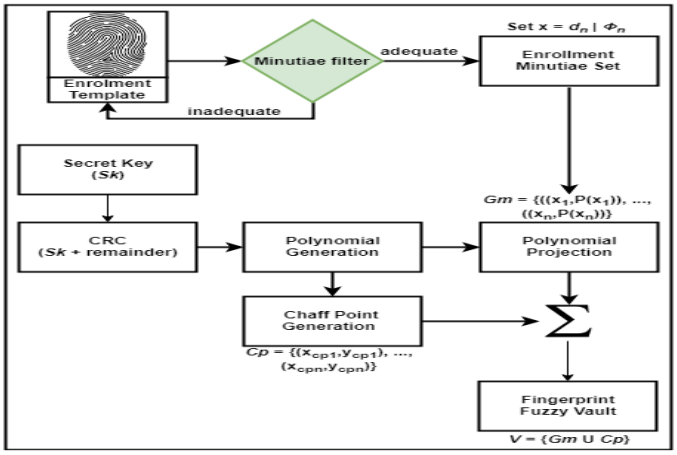

Fig. 1. Lock/encode design of proposed method.

The description of the lock/encode design process is as follows.

- First, the system generated a random secret key Sk of positive integer with the number n and the value of each positive integer was m bit. The random secret key Sk value was from 1 to 2^m–1.
- The n digits positive integer of secret key Sk were converted into binary to obtain $(m \times n)$ bit binary number. Furthermore, the $(m \times n)$ bit of secret key Sk was divided with generator polynomial of CRC (e.g., for $m = 16$ bit used CRC-16 $Gp_{CRC-16}(x) = x^{16} + x^{15} + x^2 + 1$) to obtain m' bit of remainder. The m' bit of remainder appended to the $(m \times n)$ bit of secret key Sk to obtain a new secret key Sk' bit (Sk+$remainder$). The secret key Sk' was separated into $(n + 1)$ with value of each part equal to m bit. Next, the separated number was converted again to positive integer number.
- The separated number $(n + 1)$ of secret key Sk' was encoded into polynomial with degree j as the coefficient, $P(x) = Sk'_1 x^j + Sk'_2 x^{j-1} + ... + Sk'_{n+1} x^{j-j}$.
- Next, in encoding technique of fuzzy vault scheme was proposed a new process, called minutiae filter. Details of the proposed minutiae filter technique will be discussed in subsection III-C. If the fingerprint image was declared to be adequate by minutiae filter process, then the feature extraction process was performed on the fingerprint image to obtain the enrolment template $Gm = \{Gm_1, Gm_2, ..., Gm_n\}$, where n was the total of minutiae, with location and orientation $\{(x_1, y_1, \theta_1), (x_2, y_2, \theta_2), ..., (x_n, y_n, \theta_n)\}$ and the core point C also obtained with location (x_c, y_c).
- Distance d and angle Φ were obtained from the calculation of Euclidean distance and angle between the core point C with set of minutiae Gm [14]. The size of each d and Φ was k bits. The value of distance d and angle Φ obtained would be concatenated into x, where $x = d \parallel \Phi$. The x size was m bits, where $m = k \times 2$. The formula were used to obtain distance d and angle Φ shown in equation 1 and 2.

$$d_n = \sqrt{(x_c - x_n)^2 + (y_c - y_n)^2} \tag{1}$$

$$\begin{aligned} \Phi_n &= \mid \theta_n - \theta_{Rn} \mid \\ \theta_{Rn} &= tan^{-1}((y_c - y_n)/(x_c - x_n)) \end{aligned} \tag{2}$$

- Each of x value obtained was projected into polynomial $P(x) = Sk'_1 x^j + Sk'_2 x^{j-1} + ... + Sk'_{n+1} x^{j-j}$. That was performed to obtain the coordinates of genuine point $Gp(x, y)$. After that, several chaff points Cp were generated by the system randomly to protect template. The criteria of the chaff point generation was not in the same polynomial equation to avoid chaff points being recognized as genuine minutiae by system and it was not form a certain pattern that was maked an impostor easy to know the position of genuine minutiae in the vault. The total number of chaff points were ten times the number of genuine point [11].

- Finally, when the number of chaff point was obtained according to the criteria, genuine points Gp and chaff points Cp were combined into vault V, $V = \{Gp \bigcup Cp\}$.

B. Unlock/Decode Process

Unlock/decode process was the process of reconstruct polynomial and decoding the secret key stored in vault using fingerprint template. The unlock/decode design was modified on the previous method [14] by making changes to the possible candidate point identification (a shape in green color). The details of design for unlock/decode process is shown in Figure 2.

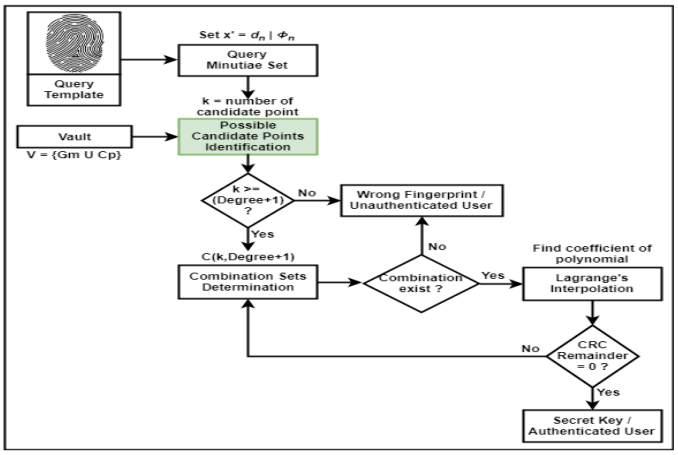

Fig. 2. Unlock/decode design of proposed method.

The description of the unlock/decode design process is as follows.

- First, the fingerprint image was captured to obtain query template, which was going to be matched with vault V. After that, same with encoding process, the feature extraction process was performed on the fingerprint image to obtain the query template $Gm' = \{Gm'_1, Gm'_2, ..., Gm'_n\}$, where n denoted the total of minutiae, with location and orientation $\{(x'_1, y'_1, \theta'_1), (x'_2, y'_2, \theta'_2), ..., (x'_n, y'_n, \theta'_n)\}$ and core point C' also obtained with location (x'_c, y'_c).
- Next, same process with encoding was performed to obtain x' value. distance d' and angle θ' were obtained from the calculation of Euclidean distance and angle between the core point C' with set of minutiae Gm'. The value of distance d' and angle θ' obtained was concatenated into x', where $x' = d' \parallel \theta'$. The x' value was m bit, with each of d' and θ' were $m/2$ bit.
- The next step was to find the candidate point of minutiae $Cd = \{Cd_1, Cd_2, ..., Cd_n\}$, where n was the number of candidate points. Details of the proposed candidate points identification technique will be discussed in subsection III-D. The minimum number of candidate points Cd obtained to rebuild the polynomial with degrees j is $(j+1)$. With all possible combinations of $(j+1)$ candidate points, the combination sets were identified as $C(Number\_of\_Cd, j+1)$.
- Reed-Solomon decoding in this research was not used because the inability to rebuild polynomial [11]. Instead, Lagrange interpolation was used to rebuild the polynomial for each candidate points Cd combination. The formula for Lagrange interpolation is shown in equation 3.

$$\begin{aligned} P(x) = &\frac{(x-x_2)(x-x_3)...(x-x_n)}{(x_1-x_2)(x_1-x_3)...(x_1-x_n)}y_1 \\ &+ \frac{(x-x_1)(x-x_3)...(x-x_n)}{(x_2-x_1)(x_2-x_3)...(x_2-x_n)}y_2 \\ &+ ...\frac{(x-x_1)(x-x_2)...(x-x_{n-1})}{(x_n-x_1)(x_n-x_3)...(x_n-x_{n-1})}y_n \end{aligned} \tag{3}$$

- Finally, when the polynomial $P(x)$ was obtained, the coefficients of the polynomial were separated. The coefficients were converted into binary bit string and divided with the same of generator polynomial CRC was used in enrolment process. If the quotient with the generator polynomial CRC produced remainder zero, then the coefficient was secret key Sk. Conversely, if the remainder was not zero, the Lagrange interpolation process was performed again for the next combinations of candidate points Cd until the remainder result was zero. If all combinations of candidate points Cd had been selected and the zero remainder was not achieve then the fingerprint template was concluded from the unauthenticated user.

C. Proposed Minutiae Filter Technique

Minutiae filter technique was used to check the fingerprint template to be adequate or inadequate as an enrolment template. The criteria used in minutiae filter process was calculated the minimum and maximum number of true minutiae contained in the fingerprint image. When it did meet the specified criteria, then the fingerprint image was captured again until the criteria was reached. The proposed minutiae filter algorithm can be shown in Algorithm 1. However, this proposed technique caused not all images in the database to be used as enrolment image on the system because not all fingerprint images on the database used meet the criteria specified in the experimental parameters.

Algorithm 1 Proposed Minutiae Filter

$blocks, min\_minutiae, max\_minutiae$;
$core\_point$ and $minutiae\_point \leftarrow$ **extract_finger**;
$true\_minutiae \leftarrow minutiae\_point$ (type of ridge 1 or 3);
$minutiae\_detected \leftarrow find(dist) < blocks$;
if (size($minutiae\_detected$) $\geq$ $min\_minutiae$) **and** (size($minutiae\_detected$) $\leq max\_minutiae$)
    output $\leftarrow$ accepted and continue to next process;
else
    output $\leftarrow$ rejected and return to capture image;
endif.

D. Proposed Identification of Candidate Points

Identification of candidate points was the process of matching points in vault V with query template Gm' to obtain points

that was used to reconstruct polynomial. The candidate point of minutiae Cd was obtained by calculating the difference between abscissa x in vault V with abscissa x' at query template Gm'. Each abscissa x and x' was splited into two equal bits size (e.g., if the size of x or $x' = m$ bits, then split its into two binary numbers of the same size k bits, where k was $m/2$ bits and the first k bits represented distance and the second k bits represented angle). Furthermore, when the difference between distance and angle of abscissa x and distance and angle of abscissa x' was lessed than equal the specified threshold value (i.e., distance and angle threshold), the abscissa x and ordinate y at vault V were mapped back as candidate points = $\{(x_{Cd1}, y_{Cd1}), (x_{Cd2}, y_{Cd2}), ..., (x_{Cdn}, y_{Cdn})\}$, where n denoted the total of candidate points. The proposed candidate points identification algorithm can be shown in Algorithm 2. Furthermore, the criteria must be considered in candidate point identification technique i.e., the result of candidate points obtained not more than one or in other words, x' might not produced more than one candidate point at x in the vault V.

Algorithm 2 Proposed Candidate Points Identification

x, x', th_dist, th_angle;
$Cd \leftarrow \emptyset$;
for $i \leftarrow 1$ **to** size (x')
  for $j \leftarrow 1$ **to** size (x)
    if not empty $(find(Cd = j))$
      continue;
    endif;
    $dist \leftarrow \mid dist\_x(j) - dist\_x'(i) \mid$;
    $angle \leftarrow \mid angle\_x(j) - angle\_x'(i) \mid$;
    if $(dist \leq th\_dist)$ **and** $(angle \leq th\_angle)$
      $Cd \leftarrow [Cd\ j]$;
      break;
    endif;
  endfor;
endfor;
output $\leftarrow Cd$;

IV. Experimental Result

In this section, the experiment was divided into three parts: databases, experimental scenario 1 and 2. The first experimental scenario was conducted to compare the FRR and FAR between proposed method and previous method [14] using degree of polynomial 8. The second experimental scenario was conducted to measure and determine the effect of giving polynomial degrees 6, 7, 8, 9 and 10 on the proposed method to produce FRR and FAR.

A. Databases

The databases were used for the experiments in this research was taken from FVC2002. FVC2002 was the Second International Competition for Fingerprint Verification Algorithm [15]. This research only used databases DB1, DB2, DB3 and DB4 sets B for evaluation purposes, similar to the studies conducted by Yadav et al. [14]. However, in the experiment, only four different impressions of the same finger (impressions 1, 2, 7 and 8) were used because four other impressions (impressions 3, 4, 5 and 6) were obtained by asking volunteers to present fingerprints with excessive displacement and rotation [11]. The Table I shows the properties of the FVC2002 sets B.

TABLE I
The properties of the FVC2002 sets B

FVC2002	DB1	DB2	DB3	DB4
Fingers Amount	10	10	10	10
Impressions Amount	8	8	8	8
Sensor	Optical	Optical	Capacitive	SFinGe
Image Size	388x374	296x560	300x300	288x384

For evaluation of the vault implementation on the FVC2002 DB1, DB2, DB3 and DB4 sets B, the following parameters are applied (Table II).

TABLE II
The Parameters for fuzzy vault implementation

Parameters	DB1	DB2	DB3	DB4
Genuine point count	13 - 24	19 - 24	18 - 29	15 - 24
Chaff point count	130 - 240	190 - 240	180 - 290	150 - 240
Block size	80			
Threshold for distance	2			
Threshold for angle	10	6	7	14

B. Experimental Scenario 1

The first experiment scenario conducted on this subsection aimed to compare the results of FRR and FAR using the proposed method and the method of Yadav et al. [14] with degree of polynomial 8. Evaluation in this experiment is to see two types of errors in the authentication process i.e., FRR and FAR. The FRR is the rate of false reject from the same finger with different impression, and the FAR is the rate of false accept from two different fingers [1].

To determine the FRR, the authentication attempts between enrolment and query template from the same finger was done. The enrolment template in the form of minutiae and core point of each finger i-th $(i = 1, ..., 10)$ and each fingerprint impression j-th $(j = 1, 2, 7, 8)$ were used to build the vault with the parameters in Table II. However, the fingerprint image that was going to be built would be checked for eligibility as an enrolment template by the minutiae filter technique (e.g., for databases DB1 have the criteria for the minimum and maximum number of minutiae 13 and 24). Note, when all fingerprint images were declared to be adequate, then the total authentication attempted was $10 \times (3 \times 4) = 120$. The number was obtained from 10 fingers with each of the 4 impressions of each finger and each impression was authenticated with 3 other impressions from the same finger, except with itself. To determined the FAR, the authentication attempted between enrolment and query template from the different finger was conducted. The enrolment template in the form of minutiae and core point of each finger i-th $(i = 1, ..., 10)$ and each

fingerprint impression j-th ($j = 1, 2, 7, 8$) were used to open the vault with the parameters in Table II. The fingerprint image used as an enrolment template in each database was the same as that used in the previous process. The two impressions as query image from a total of four impressions on each different finger were used. Note, for this experimental scenario, when all fingerprint images were declared to be adequate, then the total authentication attempted was $(9 \times 4) \times (9 \times 2) = 648$ attempted. The number was obtained from 10 fingers with each of the 4 impressions of each finger and each impression was authenticated with 2 other impressions from the different finger.

From the results of the experimental in the form of FRR and FAR for the FVC2002 sets B database with degree of polynomial 8 obtained were 8.9475% and 0.3520%. These results were lower on the FRR and the FAR when compared to the previous distance-based method by Yadav et al. [14]. The details can be seen in Table III. The FRR and FAR results showed that using the proposed method was lower than the previous method [14] with a difference of 4.49% and 0.0995%. This was caused by the previous method [14] which did not use minutiae filter technique to filter the number of minutiae in a particular area in the enrolment process which caused the authentication process for the same finger (intra-class) to be reduced. This arised because the minutiae was extracted from the same finger at different times of enrolment and authentication resulting different locations and orientations of minutiae. In the method proposed to minimize this impact, a number of minutiae was filtered with a particular block area using minutiae filter technique. The area block was made to reduce the number of minutiae which had different properties. In other words, the block area created aimed to minimize intra-class variation problems. Although by making certain area blocks on the fingerprint image to filter the number of minutiae, not all fingerprint images were used as enrolment template.

The proposed method also used the modified candidate point identification technique to identify minutiae points in the process of authentication (decoding) by separating the representation of minutiae into distance and angle in enrolment and query templates. Whereas the previous method [14] combined distance and angle to identify minutiae points. Combining between distance and angle resulted in accuracy of the comparative process between the minutiae points in the enrolment and query template to be reduced compared to separating them. Therefore, the candidate point identification technique in proposed method required two thresholds, i.e., the threshold for the distance and threshold for the angle. However, the threshold for the distance and angle might be set correctly because if the two threshold values were not set correctly, the accuracy would be decrease. For example, if the threshold for distance and angle was set higher that could caused high of FAR and low of FRR. Whereas, if the threshold for distance and angle was set lower that could resulted in high of FRR and low of FAR. Like the parameters used in experiment (Table II), the threshold for distance was set with a value of 2 for all FVC2002 sets B databases, while the threshold angle was set differently for each DB. From the results of experimental scenario 1, it was concluded that giving the right threshold distance and angle could increased the FRR and also maintained the FAR. If the threshold value was too high, it was caused the FAR to be high, on the contrary if the threshold value was too low it was caused the FRR to be high.

TABLE III
COMPARISON OF FRR AND FAR ON DATABASE FVC2002 SETS B

FVC2002	Yadav et al. [14]		Proposed Method	
	FRR	FAR	FRR	FAR
DB1	12.50%	0.6944%	9.68%	0.2000%
DB2	12.50%	0.4167%	0.00%	0.3704%
DB3	13.75%	0.4167%	11.11%	0.3086%
DB4	15.00%	0.2780%	15.00%	0.5291%
Average	13.4375%	0.4515%	8.9475%	0.3520%

C. Experimental Scenario 2

This second experiment scenario was conducted to find out and measured the effects of the use of the proposed method on the polynomial degrees 6, 7, 8, 9 and 10 against the FRR and FAR. To obtain the FRR and FAR from the degrees of polynomials 6, 7, 8, 9 and 10, the number of points that were matched for each authentication attempts in the FVC2002 sets B database were calculated. The number of minutiae points that were matched was used to determine authentication attempts accepted or rejected. For example, when the system was set with the degree of polynomial k, the authentication attempts were accepted if the minimum number of minutiae points matched were $(k + 1)$.

Same as experimental scenario 1, the authentication attempts between enrolment and query template from the same finger was conducted to determine the FRR. The enrolment template in the form of minutiae and core point of each finger i-th ($i = 1, ..., 10$) and each fingerprint impression j-th ($j = 1, 2, 7, 8$) was used to build the vault with the parameters in Table II. However, the fingerprint image that was built would be checked for eligibility as an enrolment template by the minutiae filter technique (e.g., for databases DB1 have the criteria for the minimum and maximum number of minutiae 13 and 24). Note, if all fingerprint images were declared to be adequate, then the total authentication attempts was $10 \times (3 \times 4) = 120$. The number was obtained from 10 fingers with each of the 4 impressions of each finger and each impression would be authenticated with 3 other impressions from the same finger, except with itself. To determine the FAR, the authentication attempts between enrolment and query template from the different finger was done. The enrolment template in the form of minutiae and core point of each finger i-th ($i = 1, ..., 10$) and each fingerprint impression j-th ($j = 1, 2, 7, 8$) would be used to open the vault with the parameters in Table II. The fingerprint image used as an enrolment template in each database was the same as that used in the previous process. All impressions (four impressions) as

query image on each different finger was conducted. Note, for this experimental scenario, if all fingerprint images were declared adequate, then the total authentication attempts was $(9 \times 4) \times (9 \times 4) = 1296$ attempts. The number was obtained from 10 fingers with each of the 4 impressions of each finger and each impression would be authenticated with 4 other impressions from the different finger.

The purpose of second experimental scenario was to determine the effect of adding and subtracting the length of the secret key used as the coefficient of polynomial to FRR and FAR (e.g., if the degree of polynomial = 9 with size of each secret key = 16 bits, we could secured the total size of secret key = 144 bits). To see the intended effect, the results of FRR and FAR for each DB with degree of polynomial 6, 7, 8, 9 and 10 were plotted as shown in Fig 3, 4, 5 and 6.

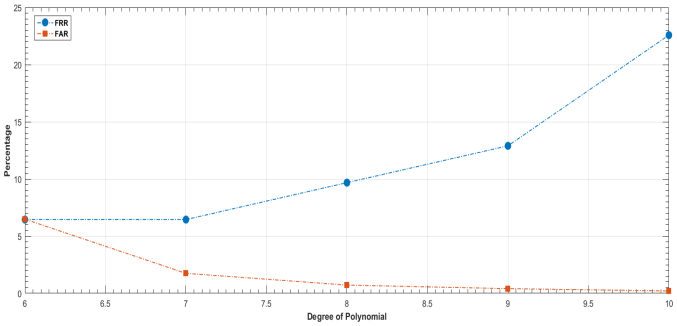

Fig. 3. FRR and FAR for DB1 with Degree of Polynomial 6,7,8,9 and 10

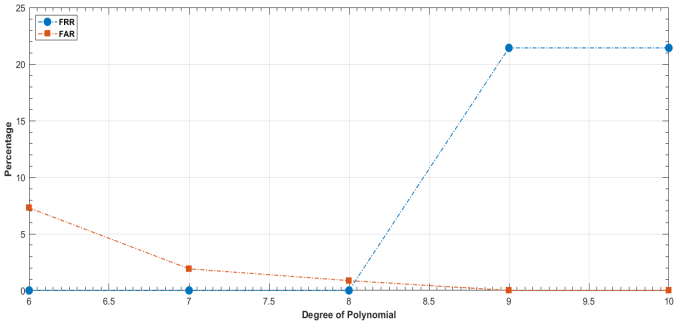

Fig. 4. FRR and FAR for DB2 with Degree of Polynomial 6,7,8,9 and 10

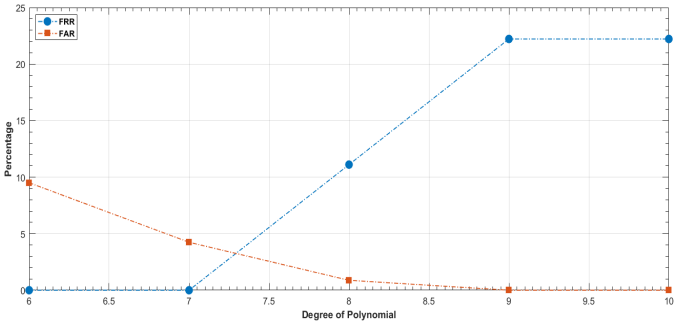

Fig. 5. FRR and FAR for DB3 with Degree of Polynomial 6,7,8,9 and 10

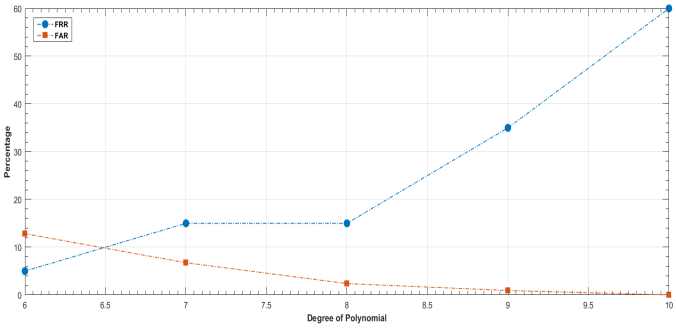

Fig. 6. FRR and FAR for DB4 with Degree of Polynomial 6,7,8,9 and 10

From the graph for each database (DB1, DB2, DB3 and DB4) in FVC2002 sets B (Figure 3, 4, 5 and 6) were showed that the higher of polynomial degree implemented in the system result in FRR would be higher and FAR would be lower. Whereas, when the degree of polynomial implemented lower would result in FRR would be lower and FAR would be higher. It proved that were trade-off between the FRR and the FAR on fingerprint biometrics. From that, it was concluded that the length of the secret key or size of polynomial degree used had an effect on FRR and FAR. Therefore, the selection of the length of the secret key used or the degree of polynomial in the system might be done correctly. In other words, the use of polynomial degree or the length of secret key depends on the application requirements, whether the application might be safer or more comfortable.

V. Conclusion

This paper shows that the proposed method is better than the Yadav et al. method [14]. The previous method [14] produced FRR 13.4375% and FAR 0.4515% while the proposed one produces FRR 8.9475% and FAR 0.3520%. The proposed method was divided into two parts, including the minutiae filter technique in encode side of fuzzy vault scheme and the candidate point identification technique in decode side of fuzzy vault scheme. By using the minutiae filter technique and identification of candidate points in the proposed method obtained the FRR and FAR which were better than the previous method [14]. This was as result of filtering the number of minutiae points during the enrolment process using the minutiae filter technique which would reduced the missing minutiae and spurious minutiae from the fingerprint image. Then in the authentication process, when making a comparison between the vault and the template query by using the threshold distance and angle to identify candidates the points would increase the accuracy of the matching process compared to only using the threshold distance or angle. Meanwhile, determining the threshold and degree of polynomial used in the authentication system with the fuzzy vault scheme would affected the rate of false reject (FRR) and false accept (FAR). Setting a threshold that was too high will cause the FAR to be high, whereas if the threshold was set too low, it caused the FRR to be high. Likewise, with the size of the degree of

polynomial, the higher degree of polynomial used resulted in a higher of FRR and the smaller degree of polynomial used resulted in high of FAR. The size of the polynomial degree used was the same as the length of the secret key used in the system.

Although the result shows that the proposed method has delivered a better accuracy than the previous method [14], there are some tasks which need to be conducted in the future to further justify and improve this research. Firstly, in real situation, the different value of thresholds are also needed because of more variation in fingerprints and the different properties of scanners used to obtain the features from finger. Therefore, it is recommended that the system can be more adaptive. Secondly, the pre-processing stage for extracting minutiae and core points needs to be improved, because if the image quality of the fingerprint is low and there are many variations of the fingerprint impressions on the same finger (e.g., displacement and rotation), its often results in the location and orientation of minutiae extraction and core points becomes much different which will cause the FRR and FAR increases.

REFERENCES

[1] Davide Maltoni, Dario Maio, Anil Jain, and Salil Prabhakar, Handbook of Fingerprint Recognition. Springer London, 2009.

[2] Ari Juels and Madhu Sudan, "A fuzzy vault scheme," Designs, Codes and Cryp-tography, 38(2):237–257, Kluwer Academic Publishers Norwell, MA, USA, February 2006.

[3] Ari Juels and Martin Wattenberg, "A fuzzy commitment scheme," In Proceedings of the 6th ACM conference on Computer and communications security - CCS '99. ACM Press, New York, NY, USA, 1999.

[4] T. Charles Clancy, Negar Kiyavash, and Dennis J. Lin, "Secure smartcard-based fingerprint authentication," In Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications - WBMA '03. ACM Press, Berkley, California, 2003.

[5] Yongwha Chung, Daesung Moon, Sungju Lee, Seunghwan Jung, Taehae Kim and Dosung Ahn, "Automatic alignment of fingerprint features for fuzzy fingerprint vault," In Information Security and Cryptology, pages 358–369. Springer Berlin Heidelberg, 2005.

[6] Shenglin Yang and I. Verbauwhede, "Automatic secure fingerprint verification system based on fuzzy vault scheme," In Proceedings. (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005. IEEE, Philadelphia, PA, USA, March 2005.

[7] Umut Uludag, Sharath Pankanti, and Anil K. Jain, "Fuzzy vault for fingerprints," In Lecture Notes in Computer Science, pages 310–319. Springer Berlin Heidelberg, July 2005.

[8] U. Uludag and Anil Jain, "Securing fingerprint template: Fuzzy vault with helper data," In 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06). IEEE, New York, NY, USA, June 2006.

[9] A. Nagar and S. Chaudhury, "Biometrics based asymmetric cryptosystem design using modified fuzzy vault scheme," In 18th International Conference on Pattern Recognition (ICPR'06). IEEE, Hong Kong, China, August 2006.

[10] Jason Jeffers and Arathi Arakala, "Minutiae-based structures for a fuzzy vault," In 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference. IEEE, Baltimore, MD, USA, September 2006.

[11] Karthik Nandakumar, Anil K. Jain, and Sharath Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," IEEE Transactions on Information Forensics and Security, 2(4):744–757, December 2007.

[12] C.I. Watson, M.D. Garris, E. Tabassi, C.L. Wilson, R.M. McCabe, S. Janet, K. Ko, National Institute of Standards, and Technology (U.S.), "User's Guide to Export Controlled Distribution of NIST Biometric Image Software (NBIS-EC)," NIST Biometric Image Software (NBIS-EC), US, July 2007.

[13] S. M. Sarala, Maya V. Karki, and D. H. Sharath Yadav, "Blended substitution attack independent fuzzy vault for fingerprint template security," In 2016 International Conference on Circuits, Controls, Communications and Computing (I4C). IEEE, Bangalore, India, October 2016.

[14] D. H. Sharath Yadav, Maya V. Karki, and S. M. Sarala, "Fuzzy vault for fingerprint template security with error correcting codes," In 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). IEEE, Bangalore, India, May 2016.

[15] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Second fingerprint verification competition," In Object recognition supported by user interaction for service robots. IEEE Comput. Soc, Washington, DC, USA, August 2002.

[16] E. Berlekamp, "Nonbinary BCH decoding," IEEE Transactions on Information Theory, 14(2):242–242, Dublin, Ireland, March 1968.

[17] J. Massey, "Shift-register synthesis and BCH decoding," IEEE Transactions on Information Theory, 15(1):122–127, IEEE Press Piscataway, NJ, USA, January 1969.

[18] H. J. Wolfson and I. Rigoutsos, "Geometric hashing: an overview," IEEE Computational Science and Engineering, 4(4):10–21, IEEE Computer Society Press Los Alamitos, CA, USA, October 1997.

[19] D. P. Mital and Eam Khwang Teoh, "An automated matching technique for fingerprint identification," In Proceedings of 1st International Conference on Conventional and Knowledge Based Intelligent Electronic Systems. KES '97. IEEE, Taipei, Taiwan, August 1996.

[20] Xinjian Chen, Jie Tian, and Xin Yang, "A novel algorithm for distorted fingerprint matching based on fuzzy features match," In Lecture Notes in Computer Science, pages 665–673. Springer Berlin Heidelberg, 2005.

[21] Kyung Deok Yu, Sangsin Na, and Tae Young Choi, "A fingerprint matching algorithm based on radial structure and a structure-rewarding scoring strategy," In Lecture Notes in Computer Science, pages 656–664. Springer Berlin Heidelberg, 2005.

[22] Vahid K. Alilou, "Fingerprint matching: a simple approach," https://www.mathworks.com/matlabcentral/fileexchange/44369-fingerprint-matching-a-simple-approach/. Mathwork, accessed 03 May 2019.

[23] Luigi Rosa, "Core Point Detection Using Orthogonal Gradient Magnitudes of Fingerprint Orientation Field," http://www.advancedsourcecode.com/. Mathwork, accessed 03 May 2019.