paper

By joni

WORD COUNT 5767

TIME SUBMITTED 25-JAN-2019 05:09PM

PAPER ID 43847303

Improving The Accuracy of Fuzzy Vault Scheme in Fingerprint Biometric

*Note: Sub-titles are not captured in Xplore and should not be used

1st Given Name Snrname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

2nd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address

***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 this research, called the fuzzy vault scheme. Although the fingerprint data in the form of minutiae can he proteeted with a fuzzy vault schcme compared to traditional anthentication systems can rednce user convenience. Thc previous study, Yadav et al., proposed a distance-based mcthod in the fuzzy vault schcme. The distance-based method is proposed because there is no need to pre-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 this research, the distance-based method is propased with several modifications, which are the minutiae filter and candidate points identification techniques. From the experimental results using the based method obtained for the rate of mistaking templates from the same finger to be from two different fingers (false rejection rate) and the rate of mistaking templates from two different fingers to be from the same fingers (false acceptance rate) in the authentication process has decreased. The previous method produced FRR 13.4375% and FAR 0.4515% and the proposed method produced FRR 8.9475% and FAR 0.3520%.**

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

I. Introduction

In present, many technologies have been developed to identify and authenticate a person from his unique biological character, known as biometrics. Biometrics is a way of identifying and authenticating individuals based on their anatomical (e.g., fingerprints, iris, hand geometry) and behavioral (e.g., speech, handwritten signature) [1]. The advantages of using biometrics (called "something user is") are user convenience: user do not need to remember passwords or personal identification number/PIN (called "something user know"), carry a card/id card and it reduce the amount of cost for make a card/id card (called "something user has"). Fingerprint is the most popular biometric due to its permanence and distinctiveness. Fingerprints may change temporarily due to finger wounds or scratched, but over time the fingerprints will be back as usual. Then one person's fingerprint with others cannot be identical. Therefore, fingerprint widely used as a tool to identify and authenticate a person. A lot of studies have been conducted to design an authentication process that is safe and accurate using biometrics, especially fingerprints. However, to the unique nature of the fingerprint, it has a disadvantage that if the genuine template of a person's fingerprint stored in clear on the database system is stolen by the impostor, then to recreate it would be very difficult and almost impossible, unlike passwords and id card. Several ways are done to secure fingerprint data, one of them is by using a common security method using encryption techniques. However, this technique is still considered very vulnerable to security problems, because during the matching process, fingerprint data on the database will be firstly decrypted so that it returns to its original form. Therefore, to protect the genuine template of fingerprint from theft or duplication it is essential to guarantee the genuine template remains secure.

Biometric cryptosystem technique was introduced to guarantee the genuine template secure. 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 study focused 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 biometric because this scheme does not require the biometric features to be ordered set of elements [2], unlike fuzzy commitment scheme [3]. Fuzzy vault scheme uses features fingerprints called minutiae and is very depend on the location, orientation and type of the minutiae. Accuracy of location, orientation and type of minutiae are strongly influenced by the quality of image, the scale of image and behavior of user (e.g. displacement and rotation). Inaccuracies in the detection of minutiae on fingerprint can cause the matching process to be inaccurate

Identify applicable funding agency here. If none, delete this.

too. Therefore to overcome the inaccuracies in fingerprint biometric, an alignment and translation technique is applied [4]–[11]. The drawback of alignment and translation technique is that the process of matching between enrollment and query template requires a 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 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]. In this research used the distance based method with singular point (core point) detection as reference point, then Euclidean distance between core point and minutiae are used to do the matching process on a fuzzy vault scheme without using alignment and translation process [14]. The security of the fuzzy vault scheme is based on the infeasibility of the polynomial reconstruction problem, which is a special case of the Reed-Solomon list decoding problem, therefore CRC and Lagrange 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 construct the fuzzy vault hence an alignment and translation. The paper showed promising results using the distance based method. Experimental results from the paper obtained the rate of false rejection (FRR) and false acceptance (FAR) at 13.4375% and 0.4515%. The experiment result showed that the level of convenience is low because of high FRR. In this paper, our purpose is to decrease the FRR and maintain the FAR of fuzzy vault scheme from the previous method [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 organized as follows. We introducing the background and problem in this research on section 1 and explain the previous related work of this research on section 2. We present research method on section 3. On section 4, we present about experiment result. The last we make conclusion and recommendation in section 5.

II. Related Work

This section discusses references related to the general review of fingerprint biometric with related work that has been done before. This section start with basic concept of fingerprint biometric and the de[24]n techniques used to protect fingerprint template, especially fuzzy vault scheme.

The fuzzy vault scheme is one of [27] 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 [71]ch was previously proposed by Juels and [64]tenberg [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. The general scheme of fuzzy vault is divided into two main parts, namely lock/encode (Fig. 1) and unlock/decode (Fig. 2).

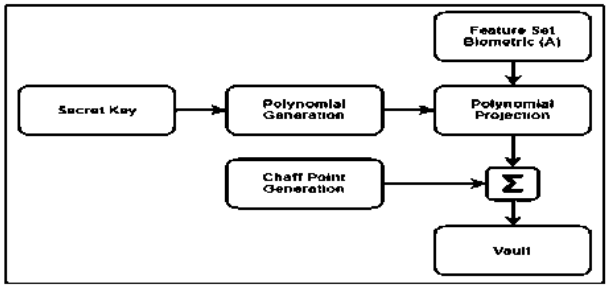

Fig. 1. Lock/encode design of fuzzy vault scheme.

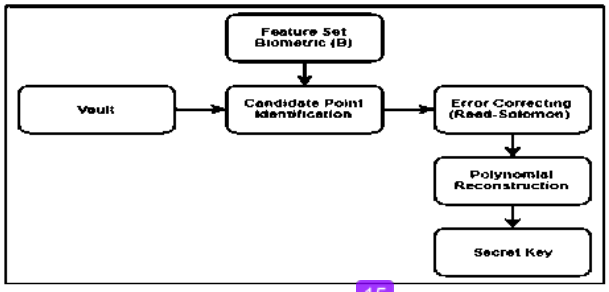

Fig. 2. Unlock/decode design of fuzzy vault scheme.

Juels and Sudan [2], in designing a fuzzy vault scheme [62] 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. [6]

In 2003, Clancy, T. C., et al. [4] implemented a fuzzy vault scheme using the loc[24]n of the minutiae in the form of a cartesian coordinate (x, y) without the orientation and type of the minutiae. The decoding process used is Reed-Solomon error correcting code with the Berlekamp-Massey algorithm [16], [17]. Author assumes that fingerprints are used during enrollment and authentication is aligned. In reality, this is not realistic for the authentication process on fingerprint biometric. From the results of the experiments, the average value of FRR is still high, i.e. 20-30% (without showing the results of FAR). In 2005, Chung, Y., et al. [5] implemented fuzzy vault schemes by performing automatic alignment with g[22]metric hashing techniques on feature minutiae [18]. Author modified the geometric hashing technique from identification [22] N to verification $1:1$. From the experimental results using the hash table can align the fingerprint feature accurately in the fuzzy vault scheme. Furthermore, Yang, S. and Verhauwhede, 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 author uses the Reed-Solomon error correcting code with the Berlekamp-Massey algorithm. From the experimental results obtained successful unlocking rate 83%. In the same year, Uludag, U., et al. [7] implemented a fuzzy vault scheme using the minutiae feature too. The decoding process used in the fuzzy vault scheme does not use Reed-Solomon error correcting code, but rather a detection code error, 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.

In 2006, Uludag, U., et al. [8] implemented the fuzzy vault scheme in fingerprint biometric based on orientation field based helper data that is automatically extracted from the fingerprints. The helper data in a fuzzy vault scheme can create opportunities for impostor to carry out attacks on the system. Experiments were carried out on the public FVC2002 DB2 dataset and the author only used two impressions of eight impressions for each fingerprint, i.e. impressions one and two. This experiment resulted in an average genuine acceptance rate (GAR) and false acceptance rate (FAR) are 72.6% and 0%. Furthermore, Nagar and Chaudhury [9] merged the asymmetric RSA cryptosystem into the Fuzzy Vault scheme and apply the security level hierarchy in the cryptosystem by using properties invariant. The author said the weaknesses in fuzzy vault schemes that do not utilize the order of feature elements, 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. Moreover, Jeffers, J., et al. [10] proposed a translation and rotation method on fingerprint templates to make lock and unlock set. The author conducted a study of three matching techniques in the translation structure and rotation invariant, i.e. five nearest neighbour based structures [19], triangle based structures [20] and Voronoi neighbour based structures [21].

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

Yadav, D. H. S., et al. [14] proposed distance based method to construct the fuzzy vault hence an alignment and translation. 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 concatenate 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 experimental results it can be seen that the average value for the GAR is still low.

III. Research Method

In order to obtain a better false rejection rate and prevent the process of fingerprint image alignment and rotation in the fuzzy vault scheme, the distance-based technique by Yadav et al. [14] is exploited in this research. The fuzzy vault scheme is divided into two main processes, namely lock/encode and unlock/decode. However, the feature extraction process is done first to obtain set of minutiae and core point from fingerprint image that is used as one of the input to the fuzzy vault scheme.

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 design for lock/encode process can be seen in Figure 3.

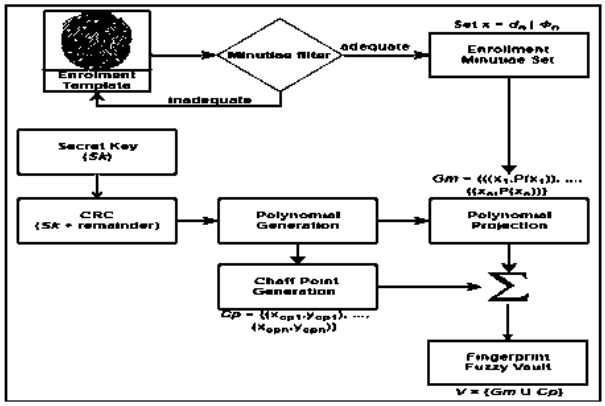

Fig. 3. Lock/encode design of proposed method.

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

- First, the system will generate a random secret key Sk of positive integer with the number n and the value of each positive integer is m bit (1 to 2^m–1).
- The n digits positive integer of secret key Sk are converted into binary to obtain $(m \times n)$ bit binary number. Furthermore, the $(m \times n)$ bit of secret key Sk will be divided with generator polynomial of CRC 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' is separated into $(n+1)$ with value of each part is equal to m bit.
- The separated number $(n + 1)$ of secret key Sk' is 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 is 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 is declared adequate by minutiae filter process, then the feature extraction process is performed on the fingerprint image to obtain the enrolment template $Gm = \{Gm_1, Gm_2, ..., Gm_n\}$, where n is number 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 will be obtained from the calculation of Euclidean distance and angle between the core point C with set of minutiae Gm [i4]. The size of each d and Φ is k bits. The value of distance d and angle Φ obtained will be concatenated into x, where $x = d \parallel \Phi$. The x size is m bits, where $m = k \times 2$. The formula used to obtain distance d and angle Φ are shown in equation 1 and 2.

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

$$\Phi_n = \mid \theta_n - \theta_{Rn} \mid$$
$$\theta_{Rn} = tan^{-1}((y_c - y_n)/(x_c - x_n)) \quad (2)$$

- Each of x value obtained is 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 Gp are generated by the system randomly to protect template. The criteria of the chaff point generation are not to be in the same polynomial equation to avoid chaff points being recognized as genuine minutiae by system and may not form a certain pattern that will make an impostor easy to know the position of genuine minutiae in the vault. The total number of chaff points to be generated is ten times the number of genuine point [1
- Finally, when the number of chaff point is obtained according to the criteria, genuine points Gp and chaff points Cp are combined into vault V, $V = \{Gp \bigcup Cp\}$.

B. Unlock/Decode Process

Unlock/decode process is the process of reconstruct polynomial and decoding the secret key that was stored in vault ng fingerprint template. The design for lock/encode process can be seen in Figure 4.

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

- First, the fingerprint image is captured to obtain query template, which will be matched with vault V. After that, same with encoding process, the feature extraction is performed on the fingerprint image to obtain the query template $Gm' = \{Gm'_1, Gm'_2, ..., Gm'_n\}$, where n is the number 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 with encoding process is performed to obtain x' value. distance d' and angle θ' will be 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 will be concatenated into x', where $x' = d' \parallel \theta'$. The x' value is m bit, with each of d' and θ' are $m/2$ bit.
- The next step is to find the candidate point of minutiae $Cd = \{Cd_1, Cd_2, ..., Cd_n\}$, where n is 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 reconstruct the polynomial with degrees j is $(j + 1)$. With all these probable combinations of $(j + 1)$ candidate points, the combination sets are identified $C(Number\_of\_Candidate\_Point, j + 1)$.
- We not use Reed-Solomon decoding in this research because the infeasibility of the polynomial reconstruction problem [25]. Instead, we use Lagrange interpolation to reconstruct the polynomial for each candidate points Cd combination.
- Finally, when the polynomial $P(x)$ is obtained, the coefficients of the polynomial will be separated. The coefficients will be converted into binary bit string and will be divided with the same of generator polynomial CRC was used in enrolment process. If the quotient with the generator polynomial CRC produces remainder zero, then the coefficient is secret key Sk. Conversely, if the remainder is not zero, the Lagrange interpolation process is performed again for the next combinations of candidate points Cd until the remainder result is zero. If zero remainder is not obtained for all combinations of candidate points Cd then the fingerprint template can be concluded from the unauthenticated user.

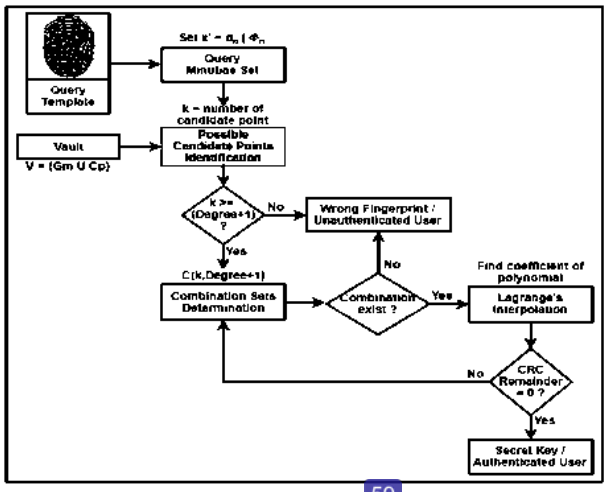

Fig. 4. Unlock/decode design of proposed method.

C. Proposed Minutiae Filter Technique

Minutiae filter technique is used to check the fingerprint template is adequate or inadequate as an enrolment template.

The criteria used in minutiae filter process is calculate the minimum and maximum number of true minutiae contained in the fingerprint image. If it does meet the specified criteria, then the fingerprint image will be capture again until the criteria are reached. The proposed minutiae filter algorithm can be shown in Algorithm 1. However, this proposed technique causes not all images in the database to be used as enrolment image on the system. This is 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 ← extract_finger;
true_minutiae ← minutiae_point (type of ridge 1 or 3);
minutiae_detected ← find(dist) < blocks;
if (size(minutiae_detected) ≥ min_minutiae) and
(size(minutiae_detected) ≤ max_minutiae)
    output ← accepted and continue to next proccss;
else
    output ← rejected and return to capture image;
endif;
```

D. Proposed Identification of Candidate Points

Identification of candidate points is the process of matching points in vault V with query template Gm' to obtain points that will be used to reconstruct polynomial. The candidate point of minutiae Cd is obtained by calculating the difference between abscissa x in vault V with abscissa x' at query template Gm'. Each abscissa x and x' is split 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 is $m/2$ bits and the first k bits represents distance and the second k bits represents angle). If the difference between distance and angle of abscissa x and distance and angle of abscissa x' is less than equal the specified threshold value (i.e., distance and angle threshold), the abscissa x and ordinate y at vault V will be mapped back as candidate points = $\{(x_{Cd1}, y_{Cd1}), (x_{Cd2}, y_{Cd2}), ..., (x_{Cdn}, y_{Cdn})\}$, where n is the number 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 is the result of candidate points obtained not more than one or in other words, x' may not produce more than one candidate point at x in the vault V.

IV. Experimental Result

In this section, the experiment was divided into three parts: databases, experimental scenario 1 and 2. The first experiment scenario was conducted to compare the false rejection rate and false acceptance rate between proposed method and previous method [14] using FVC2002 databases. The second experiment scenario was conducted to measure and determine the effect of giving different degree of polynomial on the proposed method to produce FRR and FAR.

Algorithm 2 Proposed Candidate Points Identification

```
x, x', th_dist, th_angle;
Cd ← ∅;
for i ← 1 to size (x')
    for j ← 1 to size (x)
        if not empty (find(Cd = j))
            continue;
        endif;
        dist ←| dist_x(j) − dist_x'(i) |;
        angle ←| angle_x(j) − angle_x'(i) |;
        if (dist ≤ th_dist) and (angle ≤ th_angle)
            Cd ← [Cd j];
            break;
        endif;
    endfor;
endfor;
output ← Cd;
```

A. Databases

The databases were used for the experiments in this research is taken from FVC2002 [15]. In this research, only databases DB1, DB2, DB3 and DB4 sets B are used for evaluation purposes, just like the studies conducted by Yadav et al. [14]. However, in the experiment, we use only four impressions (impressions 1, 2, 7 and 8) because impressions 3, 4, 5 and 6 were obtained by requesting volunteers to present fingerprint with exaggerated 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
No. of Finger	10	10	10	10
No. of Impressions	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 - 29			
Chaff point count	130 - 290			
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 aims to compare the results of false rejection rate and false acceptance rate 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.

To determine the FRR, the authentication attempts between enrolment and query template from the same finger is 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 ($j = 1, 2, 7, 8$) will be used to build the vault with the parameters in Table II. However, the fingerprint image that will be built will be checked for eligibility as an enrolment template by the minutiae filter technique. Furthermore, to determine the FAR, the authentication attempts between enrolment and query template from the different finger is 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 ($j = 1, 2, 7, 8$) will be used to open the vault with the parameters in Table II. The fingerprint image used as an enrolment template in each database is the same as that used in the previous process. In the first experiment scenario, we used two impressions as query from a total of four impressions on each different finger.

From the results of the experimental scenario 1 obtained for FRR and FAR with degree of polynomial 8 are 8.9475% and 0.3520%, respectively. The details can be seen in Table III. The FRR and FAR results show that using the proposed method is lower than the previous method [14] with a difference of 4.49% and 0.0995%. This is because the previous method [14] did not use minutiae filter technique to filter the number of minutiae in a particular area in the enrollment process which cause the authentication process for the same finger (intra-class) to be reduced. This arises because the minutiae is extracted from the same finger at different times of enrollment and authentication resulting different locations and orientations of minutiae. In the method proposed to minimize this impact, a number of minutiae is filtered with a particular block area using minutiae filter technique.

The proposed method also use 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] combines distance and angle to identify minutiae points. Combining between distance and angle results in accuracy of the comparative process between the minutiae points in the enrollment and query template to be reduced compared to separating them. Therefore, the candidate point identification technique in proposed method requires two thresholds, i.e., the threshold for the distance and threshold for the angle. However, the threshold for the distance and angle must be set correctly, because if the two threshold values are not set correctly, the accuracy will decrease. For example, if the threshold for distance and angle is set higher it can cause high of FAR and low of FRR. Whereas if the threshold for distance and angle is set lower can result in high of FRR and low of FAR.

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 measure 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, we calculated the number of points that were matched for each authentication attempts in the FVC2002 sets B database. The number of minutiae points that were matched was used to determine authentication attempts accepted or rejected. For example, if the system is set with the degree of polynomial k, the authentication attempts are accepted if the minimum number of minutiae points matched are $(k + 1)$.

In this second experiment scenario, we implemented it using the same parameters as the first experiment scenario. In this experiment scenario, we used four impressions as query from a total of four impressions on each different finger. The results of this second experiment scenario are shown in Fig 5, 6, 7 and 8.

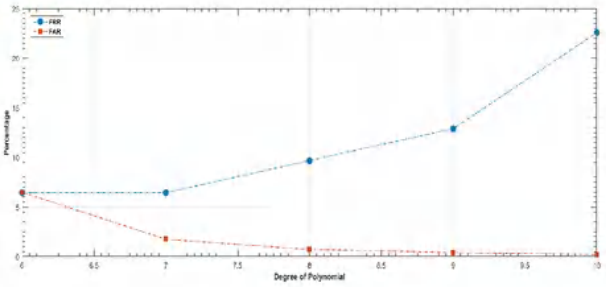

Fig. 5. FRR and FAR for DB1 with Degree of Polynomial 6,7,8,9 and 10

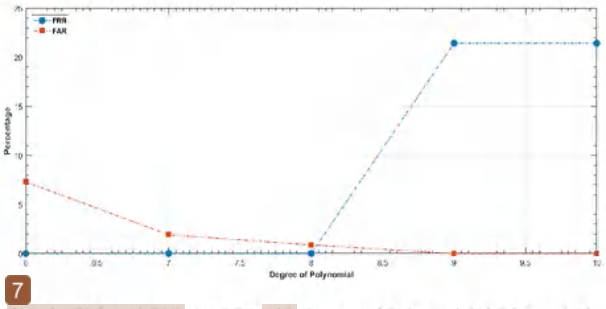

Fig. 6. FRR and FAR for DB2 with Degree of Polynomial 6,7,8,9 and 10

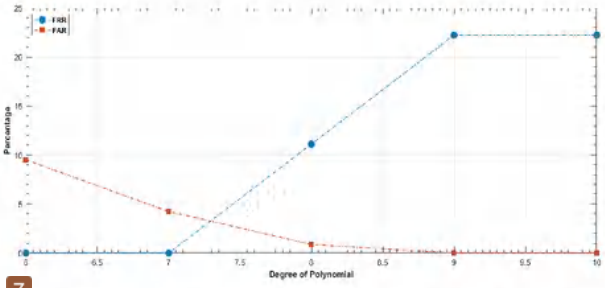

Fig. 7. FRR and FAR for DB3 with Degree of Polynomial 6,7,8,9 and 10

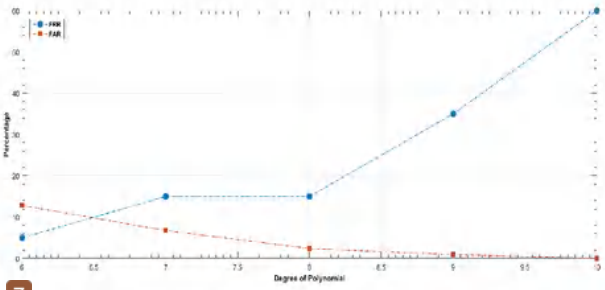

Fig. 8. FRR and FAR for DB4 with Degree of Polynomial 6,7,8,9 and 10

From the graph for each database (DB1, DB2, DB3 and DB4) in FVC2002 sets B (Figure 5, 6, 7 and 8), it is shown that the higher of polynomial degree implemented in the system result in FRR will be higher and FAR will be lower. Whereas if the degree of polynomial implemented lower will result in FRR getting lower and FAR will be higher. It proves that there are trade-off between the FRR and the FAR on fingerprint biometrics. It can be concluded that the length of the secret key or size of polynomial degree used ha[27]n effect on FRR and FAR. Therefore, the selection of the length of the secret key used or the degree of polynomial in the system must 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 must be safer or more comfortable.

V. Conclusion

In this paper shows that the proposed method is better than the previous method [68]. The previous method [14] produced FRR 13.4375% and FAR 0.4515% and the proposed method produced FRR 8.9475% and FAR 0.3520%. The proposed method adds and modifies distance-based method [14], namely minutiae filter and candidate point identification techniques.

Furthermore, determining the threshold and degree of polynomial used in the authenticatio[20]stem with the fuzzy vault scheme will affect the rate of false reject (FRR) and false accept (FAR). Setting a threshold that is too high will cause the FAR to be high, whereas if the threshold is set too low will cause the FRR to be high. Likewise, with the size of the degree of polynomial, the higher degree of polynomial used will result in a higher of FRR and the smaller degree of polynomial used will result in high of FAR.

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.

paper

ORIGINALITY REPORT

23%

SIMILARITY INDEX

PRIMARY SOURCES

1	D H Sharath Yadav, Maya V Karki, S M Sarala. "Fuzzy vault for fingerprint template security with error correcting codes", 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2016 Crossref	127 words — 2%
2	tel.archives-ouvertes.fr Internet	64 words — 1%
3	link.springer.com Internet	52 words — 1%
4	Jaka E. Sembodo, Erwin B. Setiawan, Z K Abdurahman Baizal. "The improvement of Indonesian news curator classification in Twitter", 2017 5th International Conference on Information and Communication Technology (ICoICT), 2017 Crossref	48 words — 1%
5	Anil K. Jain. "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, 2008 Crossref	38 words — 1%
6	M.S. AlTarawneh, W.L. Woo, S.S. Dlay. "Biometric Key Capsulation Technique Based on Fingerprint Vault: Anatomy and attack", 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications, 2008 Crossref	38 words — 1%
7	Lecture Notes in Computer Science, 2011. Crossref	38 words — 1%

8	Authentication in Insecure Environments, 2014. Crossref	37 words — 1%
9	Karthik Nandakumar. "Fingerprint-Based Fuzzy Vault: Implementation and Performance", IEEE Transactions on Information Forensics and Security, 12/2007 Crossref	37 words — 1%
10	subs.emis.de Internet	32 words — 1%
11	Ferhaoui Chafia, Chitroub Salim, Benhammadi Farid. "A biometric crypto-system for authentication", 2010 International Conference on Machine and Web Intelligence, 2010 Crossref	29 words — < 1%
12	www.casprlab.com Internet	27 words — < 1%
13	www.compsys.ia.ac.cn Internet	26 words — < 1%
14	www.pubzone.org Internet	25 words — < 1%
15	pdfs.semanticscholar.org Internet	25 words — < 1%
16	adt.lib.rmit.edu.au Internet	23 words — < 1%
17	toc.proceedings.com Internet	22 words — < 1%
18	Chakraborty, Bodhi, Sanjay Singh, and Debanjan Sadhya. "A Review of Key Binding Based Biometric Data Protection Schemes", IET Biometrics, 2016. Crossref	22 words — < 1%
19	etd.lib.metu.edu.tr Internet	

20 words — < 1 %

20	www.dtic.mil Internet	20 words — < 1%
21	Karthik Nandakumar, Anil K. Jain. "Multibiometric Template Security Using Fuzzy Vault", 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems, 2008 Crossref	20 words — < 1%
22	Lecture Notes in Computer Science, 2005. Crossref	20 words — < 1%
23	Short, Nathaniel J., A. Lynn Abbott, Michael S. Hsiao, and Edward A. Fox. "Robust feature extraction in fingerprint images using ridge model tracking", 2012 IEEE Fifth International Conference on Biometrics Theory Applications and Systems (BTAS), 2012. Crossref	19 words — < 1%
24	Ha, Yajun, Thi Hanh Nguyen, Renfa Li, and Yi Wang. "Performance and security-enhanced fuzzy vault scheme based on ridge features for distorted fingerprints", IET Biometrics, 2015. Crossref	19 words — < 1%
25	jsrn.dk Internet	18 words — < 1%
26	logic.pdmi.ras.ru Internet	18 words — < 1%
27	Youn Joo Lee. "A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System", IEEE Transactions on Systems Man and Cybernetics Part B (Cybernetics), 2008 Crossref	18 words — < 1%

28	"Digital Forensics and Watermarking", Springer Nature, 2017 Crossref	18 words — < 1%
29	K. Kale, R. Manza, S. Gornale, P. Deshmukh, Vikas Humbe. "SWT based Composite Method for Fingerprint Image Enhancement", 2006 IEEE International Symposium on Signal Processing and Information Technology, 2006 Crossref	17 words — < 1%
30	Li, Renfa, Yi Wang, Yajun Ha, and Thi Hanh Nguyen. "Improved chaff point generation for vault scheme in bio-cryptosystems", IET Biometrics, 2013. Crossref	17 words — < 1%
31	A. Nagar, S. Chaudhury. "Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme", 18th International Conference on Pattern Recognition (ICPR'06), 2006 Crossref	16 words — < 1%
32	onlinelibrary.wiley.com Internet	15 words — < 1%
33	nvlpubs.nist.gov Internet	15 words — < 1%
34	Thi Hanh Nguyen, Yi Wang, Trung Nhan Nguyen, Renfa Li. "A fingerprint fuzzy vault scheme using a fast chaff point generation algorithm", 2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2013), 2013 Crossref	15 words — < 1%
35	"Biometric Security and Privacy", Springer Nature, 2017 Crossref	14 words — < 1%
36	biometrics.cse.msu.edu Internet	14 words — < 1%

37	wavelab.at Internet	14 words —	< 1%
38	hal.inria.fr Internet	13 words —	< 1%
39	Radha Narayanan, S. Karthikeyan. "Double encryption based secure fuzzy vault construction using fingerprint biometric features", International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012), 2012 Crossref	12 words —	< 1%
40	Vu Hiep Dao, Quang Duc Tran, Thi Hoang Lan Nguyen. "A Multibiometric Encryption Key Algorithm Using Fuzzy Vault to Protect Private Key in BioPKI Based Security System", 2010 IEEE RIVF International Conference on Computing & Communication Technologies, Research, Innovation, and Vision for the Future (RIVF), 2010 Crossref	12 words —	< 1%
41	Maltoni. "Securing Fingerprint Systems", Handbook of Fingerprint Recognition, 2009 Crossref	12 words —	< 1%
42	Encyclopedia of Biometrics, 2015. Crossref	12 words —	< 1%
43	Grzybowski. "Appendix B: Matlab Code for the Minotaur (Example 4.1)", Chemistry in Motion, 04/17/2009 Crossref	11 words —	< 1%
44	www.win.tue.nl Internet	10 words —	< 1%
45	linknovate.com Internet	10 words —	< 1%
46	Jason Jeffers, Arathi Arakala. "Minutiae-Based Structures for A Fuzzy Vault", 2006 Biometrics	10 words —	< 1%

Symposium: Special Session on Research at the Biometric Consortium Conference, 2006
Crossref

47	www.waset.org Internet	10 words — < 1%
48	class.ece.iastate.edu Internet	9 words — < 1%
49	"Biometric Authentication", Springer Nature America, Inc, 2004 Crossref	9 words — < 1%
50	"Image Analysis and Recognition", Springer Nature America, Inc, 2010 Crossref	9 words — < 1%
51	epdf.tips Internet	9 words — < 1%
52	Laurence Cholvy. "Querying Contradictory Databases by Taking into Account Their Reliability and Their Number", Studies in Fuzziness and Soft Computing, 2006 Crossref	9 words — < 1%
53	Abdul Razaque, Prudhvi Sagar Sreeramoju, Fathi H. Amsaad, Chaitanya Kumar Nerella, Musbah Abdulgader, Harsha Saranu. "Multi-biometric system using Fuzzy Vault", 2016 IEEE International Conference on Electro Information Technology (EIT), 2016 Crossref	9 words — < 1%
54	"Proceedings of the 16th International Conference on Hybrid Intelligent Systems (HIS 2016)", Springer Nature, 2017 Crossref	9 words — < 1%
55	www.ijirset.com Internet	9 words — < 1%

Luis Di Martino, Alicia Fernandez, Rafael Grompone von Gioi,

56	Federico Lecumberry, Javier Preciozzi. "A Statistical Approach to Reliability Estimation for Fingerprint Recognition", 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), 2016 Crossref	8 words — < 1%
57	repository.lib.polyu.edu.hk Internet	8 words — < 1%
58	Lecture Notes in Computer Science, 2006. Crossref	8 words — < 1%
59	Khalil, Mohammed S. "Reference point detection for camera-based fingerprint image based on wavelet transformation", BioMedical Engineering OnLine, 2015. Crossref	8 words — < 1%
60	docplayer.net Internet	8 words — < 1%
61	Arathi Arakala. "Protection of minutiae-based templates using biocryptographic constructs in the set difference metric", Security and Communication Networks, 06/09/2010 Crossref	8 words — < 1%
62	Abhilasha Bhargav-Spantzel, Anna Squicciarini, Elisa Bertino, Xiangwei Kong, Weike Zhang. "Biometrics-based identifiers for digital identity management", Proceedings of the 9th Symposium on Identity and Trust on the Internet - IDTRUST '10, 2010 Crossref	8 words — < 1%
63	Thomas Frassen, Xuebing Zhou, Christoph Busch. "Fuzzy Vault for 3D Face Recognition Systems", 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008 Crossref	7 words — < 1%
64	Christian Rathgeb, Andreas Uhl, Peter Wild. "Iris Biometrics", Springer Nature America, Inc, 2013 Crossref	7 words — < 1%

65	Ahmad, Tohari, Jiankun Hu, and Song Wang. "String-based cancelable fingerprint templates", 2011 6th IEEE Conference on Industrial Electronics and Applications, 2011. Crossref	7 words — < 1%
66	Rumana Nazmul, Md. Rafiqul Islam, Ahsan Raja Chowdhury. "Chapter 32 Alignment-Free Fingerprint Template Protection Technique Based on Minutiae Neighbourhood Information", Springer Nature, 2018 Crossref	7 words — < 1%
67	Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar. "Handbook of Fingerprint Recognition", Springer Nature America, Inc, 2009 Crossref	7 words — < 1%
68	"Biometric Recognition", Springer Nature, 2016 Crossref	6 words — < 1%
69	Security and Privacy in Biometrics, 2013. Crossref	6 words — < 1%
70	U. Uludag, Anil Jain. "Securing Fingerprint Template: Fuzzy Vault with Helper Data", 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), 2006 Crossref	6 words — < 1%
71	Computation Cryptography and Network Security, 2015. Crossref	6 words — < 1%
72	Andreas Uhl, Christian Rathgeb. "Chapter 9 The State-of-the-Art in Iris Biometric Cryptosystems", InTech, 2011 Crossref	6 words — < 1%

EXCLUDE QUOTES OFF EXCLUDE MATCHES OFF

EXCLUDE BIBLIOGRAPHY OFF