An Efficient Biocrypto-system Using Least Square Polynomial Curve Fitting with Interpolation Based New Chaff-Points Generation Method

Neeraj TANTUBAY[1,2], Jyoti BHARTI[1]
[1]*Department of Computer Science & Engineering, Maulana Azad National Institute of Technology, Bhopal, 462003, India*
[2]*Rajkiya Engineering College, Banda UP, 210201, India*
neerajtantubay2007@gmail.com

***Abstract*—Large cryptographic-key ensures high security and robustness of asymmetric and symmetric cryptography. The conventional Fuzzy Vault Scheme (FVS) biocrypto-system is employed to shield private or secret-key using biometric features. The strength of FVS consists in its polynomial degree and chaff-points. In FVS, the system's performance is degraded with increment in the polynomial degree to make system robust against attacks. Similarly, valid chaff-point generation is also a crucial task that needs to be considered in the conventional FVS. Therefore, an efficient and more secure Modified FVS (MFVS) using Least Square Polynomial Curve Fitting (LSPC) is proposed in this paper to enhance the security of conventional FVS. Moreover, Newton's Divided Difference Interpolation (NDDI) based new chaff-points generation method is also proposed to minimize the number of required candidate points. The proposed system demonstrations average accuracy as 100%, Genuine Acceptance Rate (GAR) as 99%, False Rejection Rate (FRR) as 1%, and False Acceptance Rate (FAR) as 0%. Security of MFVS is analyzed against brute-force attack, it evident that 10-Million more combinations are required to break the generated Fuzzy Vault as compared to prior research. Consequently, proposed chaff-point generation reduces required candidate points by 13-times than existing methods.**

***Index Terms*—cryptography, curve fitting, information security, interpolation, least squares.**

I. INTRODUCTION

Nowadays, digital technology is a vital mechanism that is prominently using by billions of users. Thus, the users are continuously creating secret information and sharing it through the Internet as well as electronic media. To share the secret information, the requirement of information confidentiality is essential, which is provided by the cryptosystem. The Biosystem (Biometric system) provides its security features to make the cryptosystem more robust and secure [1]. Biocrypto-System uses the security of the biosystem to secure the encryption key of cryptosystem and eliminate the utilization of the public key infrastructure (PKI) model.

The Biocrypto-System is most notably used in two Sub-Biocrypto-Systems (1) Biometric Key-Binding (BKB) and (2) Biometric Key-Generation (BKG). The BKB provides security for the user defined crypto-key by binding it with the user's biometric and BKG is used to generate a secure user dependent cryptographic-key by using user's biometric. Fig.1 shows the sub-systems of biocrypto-system with corresponding algorithm [2]. A Fuzzy extractor and secure sketch are some crucial algorithms that are efficiently and frequently used for biometric key-generation from biometric traits [3]. The Biometric key binding scheme employs the two essential algorithms i.e. fuzzy commitment (FC) and fuzzy vault (FV) for securely binding cryptographic private or secret-key with extracted features of biometric [4].

The original principle of FVS is given by A. Juels and M. Sudan [5] in 2002, with the core concept of polynomial evaluation. The FVS is the widely used biometric key-binding scheme, many authors have proposed different frameworks in their researches to make it more secure and efficient. Chaff-point (noise point) generation is the most important part of the FVS. The complete security of the generated Fuzzy Vault (FV) or simple Vault (V) is primarily dependent on the polynomial re-construction and the chaff-points generation method [6]. The Large encryption key is one of the main requirements of any cryptographic algorithm to be more secure against attacks; therefore large key binding is another challenge of biocrypto-systems. The original FVS is performed well for the low polynomial degree but when the polynomial degree is increased for improving system's security against attack, the entire performance of the system goes reduced. In this research work, an efficient and secure Modified FVS (MFVS) is proposed using least square polynomial curve fitting (LSPC) to increase the polynomial degree as well as security of cryptographic-key. The MFVS is also incorporated with the new chaff point generation method based on NDDI.

In this paper, the rest of the sections are organized as, the brief literature review of the authors' previously approaches of different authors, in section II. In Section III, the biocrypto-system and FVS are explained in detail. Sections IV and V demonstrate the proposed work, experiment and result analysis respectively. The conclusion of the proposed work is shown in section VI.

II. LITERATURE REVIEW

Many authors have proposed several methods to enhance the performance of FVS and the security of vault template.

Digital Object Identifier 10.4316/AECE.2021.03003

A. Juels and M. Sudan [5] in 2002 introduced the concept of FVS which is the most popularly used biocrypto-system for securely hiding a secret into fingerprint features. In the original FVS, the secret-key is denoted as the polynomial coefficients. The FV construction locks secret-key by using some particular locking features, extracted from fingerprint. In the unlocking process, unlocking features are extracted from the query fingerprint template, and the same key is retrieved from the vault. The security of FV depends on the impossibility of the polynomial re-construct. The major issue with the original FVS is its lack of error tolerance, hence, a robust error-correcting technique (ECT) is required.

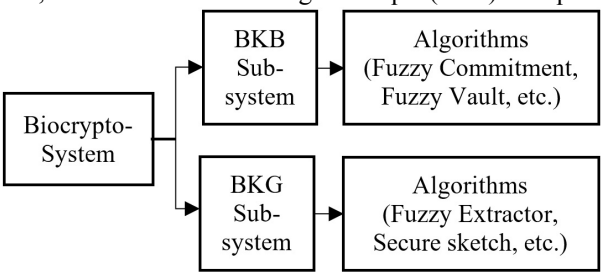

Figure 1. Sub-Biocrypto-Systems

V. A. Aquino et al. [7], proposed Keystroke based biocrypto-system to improve the security of the authentication system. D. Chang et al. [8] in 2021, proposed a BIOFUSE model as multimodal fusion framework to fuse FC and FV biocrypto-systems with possible combinations to overcome the security issues associated with FCS and FVS. F. Benhammadi et al. [9] in 2014, proposed fingerprint-based FVS for the authentication process and to overcome cross-matching attacks on fingerprint fuzzy vault by using a combination of transformed minutiae pairwise and user password. In [10], T. K. Dang et al. in 2016, proposed a fuzzy vault with a cancellable scheme to protect biometric templates using periodic transformation to resolve the issue of accurate rate and security problems.

T.C. Clancy et al. [11] in 2003, proposed a fingerprint-based fuzzy vault system with chaff generation method using minutiae point's location of fingerprint to randomly generate chaff point with assumption that input, and query templates are pre-aligned, which cannot be a faithful assumption in the actual system. M. Khalil-Hani et al. [12] in 2010 and M. Khalil-Hani et al. [13] in 2013, proposed chaff-point generation algorithms, which is 140-times better than Clancy's chaff generation method. G. Amirthalingam et al. [14] in 2016, proposed FV based multimodal bio-cryptosystem using face and ear as biometric features to generate fuzzy vault with new chaff-point, they explored the limitations of fuzzy vault i.e. the biometric information easily conspicuous, and the randomly generated chaff-points easily detected by the attackers, they employed particle swarm optimization (PSO) technique to calculate best locations to generate chaff-point.

III. BIOCRYPTO-SYSTEMS

The biocrypto-system works in two phases enrollment and verification. In Enrollment phase of BKB, the user defined cryptographic-key and used dependent biometric are taken as the input to securely lock the cryptographic-key into the extracted features of biometric, it creates a fused data known as helper data, is stored in the database. In the enrollment phase of BKG, system takes only the user's dependent biometric as the input, and processes it to extract robust biometric features. These features are quantized to generate a unique pattern as a secret binary key. These extracted features are transformed and stored as helper data in the database for further use. In the verification phase, both the systems i.e. BKB and BKG take the query biometric from the user and stored helper data as the input to retrieve or re-generate the secret-key, successfully [4].

A. Helper-Data

In both BKB and BKG, the biometric dependent data is needed to be stored in the database for retrieving and re-generation of cryptographic-key. This data is known as the helper data (*HD*). As per the biocrypto-system security concerns, the *HD* must not entail substantial data of the original biometric. In BKB, the *HD* is created using the fusion of biometric feature and secret-key in key-binding phase and stored in the database. In key-retrieval phase, the same keys is generated again using stored *HD* and input biometric. In BKG, the *HD* is created using the biometric template only, and the key is re-generated directly by using stored *HD* and input biometric [15].

B. Fingerprint-based Fuzzy Vault Biocrypto-system

As FVS is a popularly used key-binding biocrytpo-system, the purpose of this system is to protect a crypto-key. The original fingerprint based FVS protects secret information by binding in biometric features in the encoding phase, thus the same secret information can only be retrieved when a legitimate person provides their biometric in the decoding phase. The Encoding phase of FVS is shown by Fig. 2, in which, a fingerprint image is used as input then pre-processing to find fingerprint minutiae points [16]. In encoding phase, polynomial construct is used with secret-key as the coefficients, whereas the x-coordinates of minutiae points are used to evaluate the polynomial for calculating the genuine points. To protect these genuine points, extra noise points i.e. chaff-points are merged. The combined set of genuine-points and chaff-points is known as vault (V), which does not reveal information about secret-key and biometric features. The generated vault can be stored in the database at a remote location or shared over the internet to be used in the decoding phase. The original FVS also uses the Error Correcting technique (ECT) because of the variability property of biometric. The ECT is applied over the secret-key to calculate error-correcting code (ECC), used at decoding phase to retrieve the secret-key [17].

The chaff-points (C) are generated randomly and combine with genuine points [18]. The chaff-points should have the following conditions with respect to coordinate values of other minutiae and genuine points: (i) The x-coordinate of the newly generated chaff point should not be equal to the genuine point's x-coordinates and the existing chaff point's x-coordinates. (ii) The y-coordinate of the newly generated points should be different from P(x) points. These chaff points are then merged with the genuine points and create vault (V). The chaff points provide security to the genuine points in the generated vault so that the genuine point cannot be extracted easily by the attackers, therefore, no. of chaff points should not be less than ten times of genuine point.

The decoding phase of the original FVS to retrieve the

same secret-key is shown in Fig. 3. In this phase, the query fingerprint image is used as the input, and pre-processed to enhance the image before extracting the minutiae points by applying the feature extraction method, same as in the encoding phase.

These extracted points are mapped over the fuzzy vault, stored in database during encoding phase, to find the genuine points. The polynomial is re-constructed using these genuine points to find its coefficients that represent the secret-key [19].

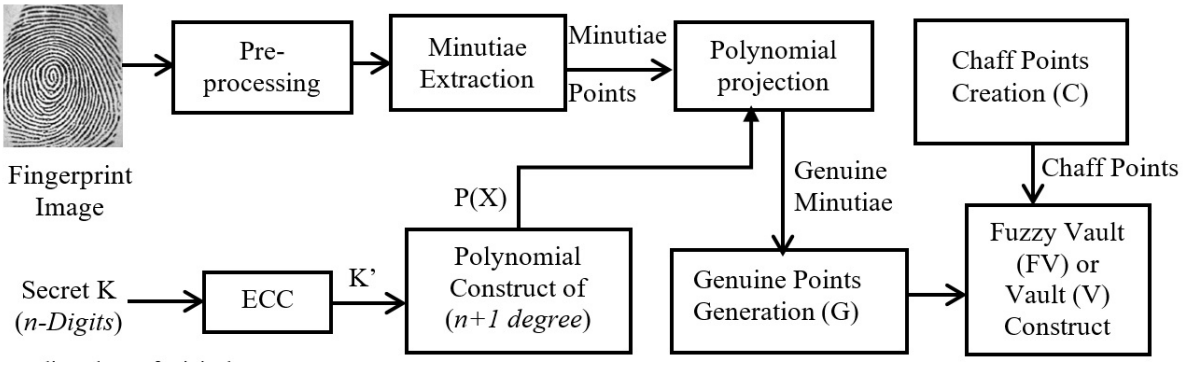

Figure 2. Encoding Phase of original *FVS*

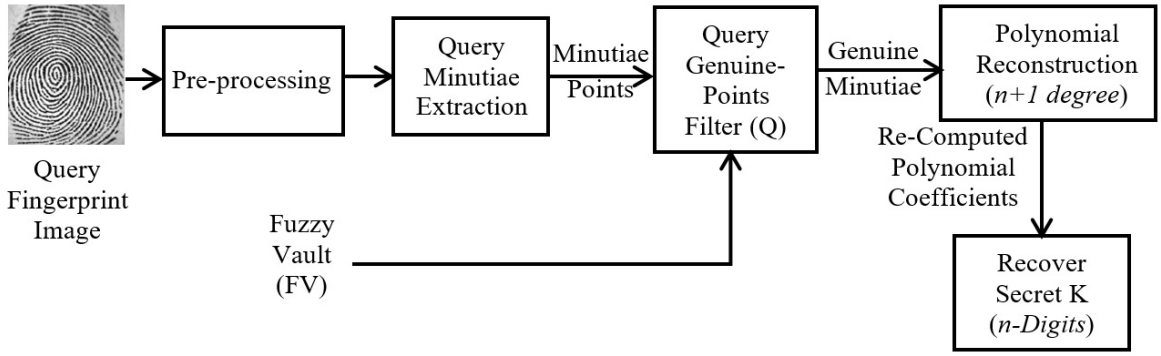

Figure 3. Decoding Phase of original *FVS*

IV. Proposed Work

The Modified FVS is proposed to enhance the original FVS using LSPC with mean and standard deviation instead of polynomial evaluation in the encoding phase. The NDDI based new chaff-points generation method is also proposed to implement with the modified FVS. The curve fitting based LSPC is employed in this research work instead of polynomial evolution at encoding phase. The LSPC is a statistical method, it is able to control the polynomial regression in higher degree polynomial equation. Hence, the proposed MFVS is implemented with higher polynomial degree using LSPC, and enhances the security of conventional FVS. The NDDI is a forward interpolation method, used to estimate the set of values using some sets of known values. Therefore, the NDDI is implemented to generate the chaff-points in MFVS. The NDDI ensure that the new estimated value will be unique among the input values. The NDDI fulfils the requirement of the chaff-points, hence it is suitable to generate the chaff-points in the MFVS. Moreover, MFVS also overcomes the limitation of conventional FVS by eliminating the use of ECT.

A. Least Square Polynomial Curve Fitting

The conventional FVS works with polynomial evaluation and ECT. The existing proposed systems work well for a low polynomial degree i.e. small secret-key size, but when the secret-key is being increased the performance of FVS is reduced, and the need for stronger ECT is also increased. To overcome such limitations and eliminate ECT utilization, the LSPC with mean and standard deviation is used in MFVS to handle polynomial regression for higher-order polynomial [20]. The LSPC can be formulated as,

$$\Upsilon = LSPC\ (x, y, q)$$

where Υ is a vector of q+1 coefficients, x and y are data sets used to find coefficients and q is the polynomial degree.

Suppose the polynomial p(x) of degree q for the data in y [21]. The coefficients in p are in descending powers, and the length of p is *q+1*, which can be denoted by Equation (1),

$$y_i = p(x_i) = \alpha_1 x_i^{\,q} + \alpha_2 x_i^{\,q-1} + \ldots + \alpha_q x_i + \alpha_{q+1} \quad (1)$$

where, $i = \{1, 2 \ldots q+1\}$.

The arithmetic mean (AM), for a set of $x_1, x_2, ..., x_q$ samples, is denoted by $\overline{x}$,

$$\overline{x} = \frac{1}{q}\left(\sum_{i=1}^{q} x_i\right) \quad (2)$$

The standard deviation (s) and the variance (v), for a random vector x made up of q scalar observations can be formulated as

$$v = \frac{1}{q-1}\sum_{i=1}^{q} \left|x_i - \overline{x}\right|^2 \quad (3)$$

Then standard deviation can be defined using (3),

$$s = \sqrt{v} = \sqrt{\frac{1}{q-1}\sum_{i=1}^{q} \left| x_i - \bar{x} \right|^2} \quad (4)$$

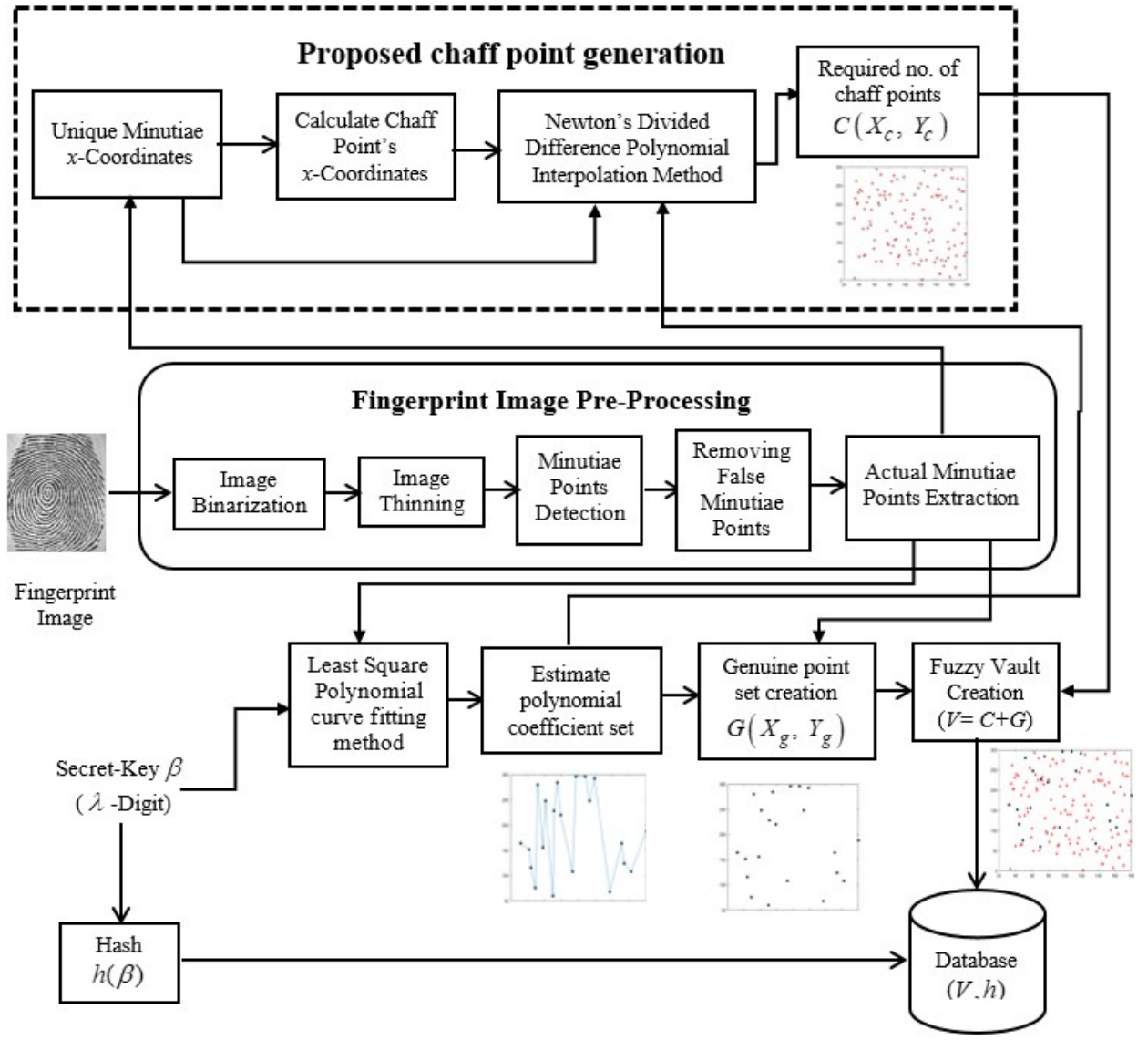

Figure 4. Encoding phase of Proposed Modified Fuzzy Vault Scheme with new chaff-points generation method

Then, the set of coefficients can be calculated by using equations (1), (2) and (4);

$$\Upsilon = (\alpha_1, \alpha_2, ...\alpha_q, \alpha_{q+1})$$

where, $\alpha_w \mid w = \{1, 2, ..., q+1\}$ represents the value of w^{th} coefficient.

B. Newton's Divided Difference Interpolation

Interpolation is applied to estimate the unknown values by using a given set of observations. It is the technique to calculate the value of a function for any intermediate values of the independent variables [22]. There are many interpolation methods developed for the equal and unequal intervals between a given set of values. NDDI is used with unequal interval values [23].

Assume a set of values $x_0, x_1, ...x_m$, which has $m+1$ total argument values and corresponding function values, as $y = f(x)$, which can be shown as $y_0, y_1, ... y_m$, then according to the definition of divided difference (DD), the first order DD for two arguments x_0 and x_1 is given as [24],

$$f(x_0, x_1) = [x_0, x_1] = \frac{y_1 - y_0}{x_1 - x_0}, \quad (5)$$

and second order *DD* for x_0, x_1, x_2 is given as,

$$f(x_0, x_1, x_2) = [x_0, x_1, x_2] = \frac{[x_1, x_2] - [x_0, x_1]}{x_2 - x_1} \quad (6)$$

Such that the m^{th} *DD* is given as,

$$f(x_0, x_1, x_2, \ldots, x_m) = [x_0, x_1, x_2, \ldots, x_m] = \frac{[x_1, x_2, \ldots, x_m] - [x_0, x_1, x_2, \ldots, x_{m-1}]}{x_m - x_0} \quad (7)$$

The NDDI uses the concept of DD to estimate the function value *f(x)* at any given value of argument x. If the set of argument values are $x_0, x_1, ...x_m$, with its function values $y_0, y_1, ... y_m$, then the generalized formula to calculate *f(x)* at x is given by equation (8),

$$f(x) = \sum_{j=0}^{m} \left\{ f[x_0, x_1, ..., x_m] g \prod_{k}^{j} (x - x_{k-1}) \right\} \quad (8)$$

In the proposed MFVS, all minutiae points of fingerprint and genuine points are used as input arguments in NDDI to generate chaff-points, in such a way that no new chaff-point overlaps existing minutiae-points, genuine-points and other chaff-points.

ALGORITHM-1: ENCODING PHASE

Input: The fingerprint image of the user, cryptographic secret-key (β) of λ -digit defined by the user and polynomial degree- q .

Output: Hash value of secret-key as $h(\beta_s)$, set of coefficients (Υ) of $q+1$ values and fuzzy vault (V),

1. **Begin**
2. Extract the fingerprint minutiae and then sort with respect to *x-coordinate*,
   $X_t \mid x_i < x_{i+1}$ // where, i= {1,2,….,t} and X_t = Total no. of x-coordinates of extracted minutiae points
3. Find the unique minutiae using step-2 based on *x-coordinates*, as two value of *x-coordinates* must not be same, such that,
   $X_u \mid x_i \neq x_j$ // where, $x_i, x_j \in X_u$, i, j= {1,2,…,u}, and
   // $u \leq t$ and u = Total no. of unique minutiae
4. Input the user's defined cryptographic secret-key (β) of λ -digit,
   $\beta_s \mid \forall \beta_s =$ Integer no. // where, s = {1,2,….,λ }
5. Select set of x-coordinates from X_u using step-3
   $X_r \mid x_{r-1} \leq x_r - 4, \in X_u$, // where, r = {1,2,…, λ }
6. Calculate the hash value of the given key (β_s), as
   $h(\beta_s)$ // to store in database to be used at decoding phase
7. Using *LSPC* with values from step-4 and step-5 and polynomial degree- q as input,
   $\Upsilon = LSPC\ (x, y, q)$ // where $\Upsilon_w = (\alpha_1, \alpha_2, \ldots \alpha_q, \alpha_{q+1})$ and $w = \{1,2,\ldots,q+1\}$
8. Calculate genuine minutiae (G) using step-5 and step-7.
   $G_l = (X_r, \Upsilon_w)$, // where, l, r, & $w = \{1,2,\ldots,\lambda\}$
9. Calculate chaff points using Algorithm-2
   $C_b = (X_c, Y_c)$ // C_b is the set of generated chaff points
10. Generates the fuzzy vault (V) template by merging the values step-8 and step-9
    $Vault' = [X_t + X_c, \Upsilon_s + Y_c]$
    $Vault' = \left[X'_{vault}, Y'_{vault} \right]$ // Scramble values of Vault' to create final fuzzy vault (V)
    $V = Vault = \left[X_{vault}, Y_{vault} \right]$ // To store in Database to be shared in the decoding phase
11. **End**

C. Proposed Modified Fuzzy Vault Scheme (MFVS)

The MFVS also works in two phases, the encoding phase for key-binding, and decoding phase for key-retrieving.

1) Working of Encoding Phase

In the encoding phase of MFVS, the user-defined cryptographic secret-key is bound with the user's fingerprint minutiae points. The LSPC is implemented to perform polynomial arithmetic, which defines the polynomial arithmetic over $GF(2^n)$ in the proposed work.

The working of the encoding phase of MFVS is shown in Fig. 4 and the whole working of the proposed encoding phase is defined in Algorithm-1. In this, the fingerprint image and secret-key are taken as input, and find the minutiae points by applying the minutiae point extraction technique. The hash value of the given secret-key is calculated and stored in the database for further use in decoding phase.

The LPSC is applied using the secret-key as the set of polynomial coefficients and the extracted fingerprint minutiae points to calculate a set of genuine points. Now chaff-points generation method is applied as shown in Algorithm-2 to find the locations of new chaff-points. The genuine points are mixed with chaff-points to form helper data, known as fuzzy vault and stored in the database for further usage in decoding phase to retrieve the secret-key.

2) Proposed Chaff-points Generation

A new chaff-points generation method is proposed using NDDI. The x-coordinates of all extracted minutiae points, y-coordinates of genuine points, and calculated new x-coordinate values are used as the input in NDDI to estimate the new pair of x-y coordinates for new chaff-points. The proposed method ensures that newly estimated x-y coordinates does not equal to the x-y coordinates existing minutiae, genuine points, and generated chaff-points (C). The required no. of chaff-points in FV are,

C_b , *where, b=10*no. of genuine Points*

The proposed new chaff-points generation method reduces redundant candidate points, required to find valid chaff-points by generating only the actual number of required chaff-points.

The working of new chaff-points generation method is shown in Fig.4 and described in Algorithm-2. The higher no. of redundant candidate points increase the workload of the chaff-points generation method.

3) Working of Decoding Phase

In decoding phase of the proposed MFVS, the user's

secret-key is extracted by means of the public data, i.e., fuzzy vault, which is stored in the database and user's query fingerprint image. The chaff-points are removed from the fuzzy vault using the query fingerprint image, and the genuine points are retrieved.

Now, the polynomial evaluation is applied to recreate the secret-key. Calculate the hash value of this recreated secret-key and match it with the hash value stored in the database. If both the hash values are equal that means the query fingerprint image is from a legitimate person otherwise from an illegitimate user. The working of the decoding phase is shown in Fig. 5 and described in Algorithm-3.

ALGORITHM-2: CHAFF-POINTS GENERATION

Input: Total no. of x-coordinates of extracted minutiae points (X_t), calculated coefficients using proposed MFVS [$\Upsilon_w = (\alpha_1, \alpha_2, ...\alpha_q, \alpha_{q+1})$],

Output: Set of chaff-points (C_b)

1. **Begin**
2. Calculate the *x-coordinates* using step-2 of *Algorithm-1* to generate chaff-point,
   $X_{chaff\_points} \notin X_{minutiae\_points}$
   $X_c \notin X_t$ such that $x_c(i) \neq x_t(j) \quad \forall i = \{1,2,...,b\}, \& j = \{1,2,...,t\}$
3. To calculate chaff-point ($X_{c,}$)
   $X_{temp}(i) = X_t(j)$,
   if $X_{temp}(i) + 3 \neq X_t(j+1)$, *then*
   $X_c(i) = X_{temp}(i) + 3$, // $\forall i = \{1,2,...,b\}, \& j = \{1,2,...,t\}$
   if i=b *then,*
   stop
   else
   $X_c(i+1) = X_c(i) + RAND[3..9]$
   End if
   End if
4. Apply *NDDI* using Equation (8), with three sets of data as input i.e., two set X_t , Υ_w and X_c as argument:
   if w < t , *then*
   $$\Upsilon_{w+1} = \Upsilon_w + \left(\frac{\Upsilon_w}{4}\right)$$
   Now calculate,
   $$Y_c = NDDI(X_t, \Upsilon_w, X_c)$$
5. This method generates Y_c and ensure that,
   $Y_c(i) \neq \Upsilon_w(j)$, where i={1,2,…,b} and $w = \{1,2,\ldots,q+1\}$
6. Then the set of chaff points is generated by scrambling the value of X_c and Y_c that can be represented as,
   $C_b = (X_c, Y_c)$ // *where,* values of b and c are equal to *ten-time* of total no. of genuine points.
7. **End**

V. EXPERIMENT AND RESULT ANALYSIS

The proposed MFVS is implemented using the LSPC method and NDDI based new chaff-points generation method. For fingerprint feature points mining, a method proposed by J. Abraham et al. [25] and freely available, is implemented in this research work.

The proposed system is analyzed using performance evaluation parameters. Moreover, the MFVS is evaluated against the brute-force attack for analyzing security. The MFVS is also analyzed against the number required redundant candidate points [17].

A. Performance Evaluation Parameters

1) False Acceptance Rate (FAR)

The FAR shows the rate of recognition of non-authorized persons who are recognized incorrectly, which can be formulated as:

$$FAR = \frac{No.\ of\ illegitimate\ input\ falsely\ recognized}{Total\ no.\ of\ inputs} \times 100$$

2) False Rejection Rate (FRR)

The FRR shows the rate of not recognition of authorized persons who are not recognized incorrectly, which can be formulated as:

$$FRR = \frac{No.\ of\ legitimate\ inputs\ falsely\ not\ recognized}{Total\ no.\ of\ inputs} \times 100$$

3) Genuine Acceptance Rate (GAR)

The GAR shows the rate of a true recognition of the persons who are matched by the system, it can be calculated as:

$$GAR = (1 - FRR) \times 100$$

4) Accuracy

The accuracy shows the robustness of the systems in terms of successful attempts against the total number of attempts. The accuracy of the system is formulated as follows,

$$Accuracy = \frac{Total\ no.\ of\ successful\ outputs\ of\ the\ system}{Total\ no.\ of\ outputs\ of\ the\ system} \times 100$$

The Modified FVS is evaluated using the FVC2002

DB1_A fingerprint dataset. A total of 800 images of 100 fingers of the persons (Per finger 8 impressions) are stored in the dataset with the size of 388×374 and resolution of 500 dpi. The MATLAB tool is used to implement the proposed system. The evaluation parameters with their values are shown in Table I.

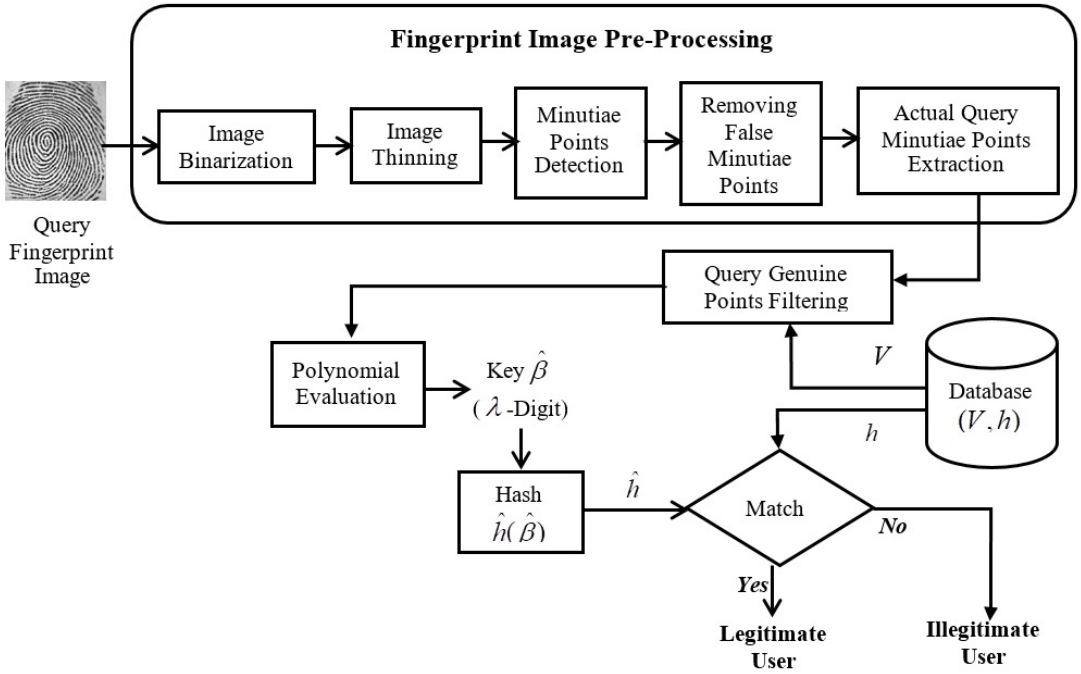

Figure 5. Decoding phase of Proposed Modified Fuzzy Vault Scheme

ALGORITHM-3: DECODING PHASE

Input: Take the query fingerprint image, Hash value of secret-key as $h(\beta_s)$ and Fuzzy Vault (V) stored in Database.

Output: Retrieval of cryptographic secret-key ($\hat{\beta}_{\hat{s}}$) and Retrieved-key matching result.

1. **Begin**
2. Extract all minutiae points and then sort these with respect to $\hat{x}-coordinates$,
   $\hat{X}_{\hat{i}} \mid \hat{x}_i < \hat{x}_{i+1}$ // *Where i= {1, 2, $\hat{t}$} and $\hat{X}_{\hat{t}}$ = total no. of extracted minutiae from query image*
3. Find the unique minutiae ($\hat{X}_{\hat{u}}$) using step-2 based on $\hat{x}-coordinates$ of minutiae points as two values of $\hat{X}$ must not be same, such that,
   $\hat{X}_{\hat{u}} \mid \hat{x}_i \neq \hat{x}_j$ // *Where* $\hat{x}_i, \hat{x}_j \in \hat{X}_{\hat{u}}$ *and i= {1, 2, $\hat{u}$},* $\hat{u} \leq \hat{t}$ *and* $\hat{u}$ *= Total no. of unique minutiae*
4. Take the *Vault = [X_{vault}, Y_{vault}],* which was generated in enrolment phase, sort with respect to X_{vault} coordinates and separate all X_{vault} -coordinates.
5. Calculate the intersection of $\hat{X}_{\hat{u}}$ and X_{vault}, and separate the common values with corresponding Y_{vault} values, such as $(\hat{X}_{\hat{q}}, \hat{\Upsilon}_{\hat{q}}) \mid \hat{q} = \{1, 2, \ldots, \lambda\}$
6. Calculate the mean and standard deviation using Equations (2) and (4) as,
   $mu_1 = mean(\hat{X}_{\hat{q}})$ and $mu_2 = s(\hat{X}_{\hat{q}})$
   Then calculate, $\overline{X}_{\overline{q}} = \dfrac{\left(\hat{X}_{\hat{q}} - mu_1\right)}{mu_2}$
7. Evaluate the polynomial of q-degree by using input values $\overline{X}_{\overline{q}}$ and $\hat{\Upsilon}_{\hat{q}}$ from Step-5 and Step-6, it provides the set of values, as retrieved secret-key, as $\hat{\beta}_{\hat{s}}$, // *where* $\hat{s} = \{1, 2, \ldots, \lambda\}$
8. Calculate the hash value of $\hat{\beta}_{\hat{s}}$, as $\hat{h}(\hat{\beta}_{\hat{s}})$ and compare with $h(\beta_s)$ stored in Database.
9. At the time of key matching
   if (Query_Fingerprint_Image == legitimate user) {
   $\hat{\beta} = \beta$ // *Retrieved Key will be same as original key*
   } else
   $\hat{\beta} \neq \beta$ // *Retrieved Key will not be same as original key*
10. **End**

B. Performance Analysis of the Proposed MFVS

The performance of the proposed MFVS is measured using two circumstances:

a) The 500-randomly generated secret-keys are taken to test the proposed MFVS system's accuracy;

b) GAR and FAR are calculated to examine the performance of the proposed MFVS.

Firstly, 500 different secret-keys are generated randomly. The identical fingerprint images are taken arbitrarily from

the FVC2002 DB1_A dataset in both encoding and decoding of the secret-keys, to analyse the accuracy of the proposed MFVS system for different secret-keys with different digits in key.

TABLE I. LIST OF PARAMETERS WITH VALUES

Parameters	Values
Secret-Key β (λ -Digit)	16
Degree of polynomial (q)	15
No. of genuine points (G)	16
No. of chaff-points (C)	160
Total points in vault (£)	176

The purpose of this experiment is to investigate the robustness of the proposed MFVS for different key sizes, because the key size is a significant factor in the performance of FVS. In order to analyze the performance of the proposed MFVS, twenty different fingerprint images are selected arbitrarily from FVC2002 DB1_A. The following analyzing cases are formed for all images:

Case-1: Randomly generated 500 secret-keys of 16-Digits and each digit is single-digit.

Case-2: Randomly generated 500 secret-keys of 16-Digits and each digit is double-digit.

Case-3: Randomly generated 500 secret-keys of 16-Digits and each digit is triple-digit.

In each analysis, 10000-times encoding and 10000-times decoding are performed, that means total 20000 experiments are performed. In all 3-cases total of 60000 experiments are performed to calculate the accuracy of the proposed MFVS using LSPC and NDDI based new chaff-points generation method.

The result in Table II shows the average accuracy of the proposed MFVS, which is calculated as the total no. of successful key retrieval divided by the total no. of attempts. For all cases, it is unchanged as it is 100% that means the proposed system is robust for 16-digit secret-key of any number of digit (i.e. single, double and triple).

TABLE II. ACCURACY ANALYSIS OF PROPOSED MFVS

	Accuracy (%)		
Proposed MFVS	***Case-1***	***Case-2***	***Case-3***
	100	100	100

In second condition, an experiment scenario is formed to calculate GAR and FAR. To calculate GAR, twenty 16-Digits secret-keys are generated randomly, and first fingerprint impressions of all 100-persons are used from the FVC2002 DB1_A dataset to encode and decode the secret-keys. A total of 4000 experiments, 2000 for each encoding and decoding for all 100 fingerprint impressions, are performed.

TABLE III. GAR AND FAR OF PROPOSED MFVS

Authors	Polynomial Degree	GAR (%)	FAR (%)
T. H. Nguyen et al. [26], 2015	10	89	0
T. K. Dang et al. [27], 2016	11	69	0
D. Chitra et al. [28], 2019	12	82	0.01
Proposed MFVS	15	99	0

Again, to calculate FAR, twenty 16-Digits secret-keys are encoded with the first fingerprint impression, and the first fingerprint impression of each 100-persons is used to decode the secret-key.

Table III shows the values of GAR and FAR which are 99% and 0% respectively. The GAR is 99% because in our experiment identical fingerprint impression is used for both encoding and decoding. FRR is 1%, due to inadequate no. of minutiae points with less distance between each other.

C. Security Analysis

In fuzzy vault key-binding scheme, brute-force is a common attack against FV. In brute-force attack, all possible combinations of the values in the FV are applied to reconstruct the polynomial. As mentioned earlier, the fuzzy vault is shared publicly. Suppose the attacker has achieved the information about the FV, then all possible subsets of points in vault are tried to find genuine points and regenerate polynomial by the attacker, so that, the secret-key can be retrieved from the FV. The security of a FV is directly proportional to its polynomial degree; if the polynomial degree increases, the strength of the FV against brute-force attack will be higher, as it will be very tough to regenerate the polynomial. In the brute-force attack, for a FV with polynomial degree (q) and total points £, the attacker has to apply a total of $C(£, q+1)$ combinations. To decode the FV, a total of $C(G, q+1)$ combinations are required. The brute-force attacker has to perform a total numbers of $C(£, q+1)/C(G, q+1)$ combinations to reconstruct the polynomial of q-degree. The polynomial curve fitting is used in the proposed Modified FVS; therefore, the no. of Genuine points (G) are equal to Polynomial degree (q)+1. Thus, as per the mathematical rules of combination theory the value of $(G, q+1)$ combinations is 1 for all values of polynomial degree [29]. Thus, the total combinations required to break the vault in proposed MFVS is equal to total combinations applied to decode fuzzy vault i.e. $C(£, q+1)$. The security analysis against brute-force attack is shown in Table IV. The Proposed MFVS shows the highest value of total evaluation performed in brute-force attack for all polynomial degrees.

D. Chaff-points and Candidate-points

As the total numbers of chaff-points in a fuzzy vault are ten times of the genuine points. The authors have previously proposed several chaff-points generation methods [6], [11-12], [14], [18].

In most of the methods, the chaff-points are generated randomly then find their appropriateness whether it is a valid chaff-point or not; some chaff points may overlap the locations of genuine points; these points cannot be considered as valid chaff-points.

Hence, in existing approaches, the generated no. of chaff-points are more than the actual required points because of invalid chaff-points. In the MFVS, NDDI based new chaff-points generation method is used, in which the location of all genuine points and minutiae points are used as the input to NDDI.

The GAR is 99% because in our experiment identical fingerprint impression is used for both encoding and decoding. FRR is 1%, due to inadequate no. of minutiae points with less distance between each other.

TABLE IV. PERFORMANCE COMPARISON OF PROPOSED MFVS AGAINST BRUTE FORCE ATTACK

Methods	**Polynomial Degree** (q)	**Total Genuine points** (G)	**Total points in Vault** (£) =G+C	**Total combinations applied to decode fuzzy vault** $C(£,\ q+1)$	**Total combinations required** $C(G,\ q+1)$	**Total evaluation performed** $\frac{C(£,q+1)}{C(G,q+1)}$
T. H. Nguyen et al. [26], 2015	10	24	262	8.0862×10^{18}	2.4961×10^{6}	3.2395×10^{12}
D. Chitra et al. [28], 2019	8	40	440	1.5687×10^{18}	2.7343×10^{8}	5.7371×10^{9}
	12	40	440	3.1110×10^{24}	1.2033×10^{10}	2.5853×10^{14}
H. Choi et al. [29], 2011	5	25	325 &305	$(1.56 \times 10^{12}) \times (4.44 \times 10^{4})$	$(1.77 \times 10^{5}) \times 10$	4.40×10^{10}
Proposed MFVS	8	9	99	7.0625×10^{11}	1	7.0625×10^{11}
	10	11	121	1.2767×10^{15}	1	1.2767×10^{15}
	12	13	143	2.6159×10^{17}	1	2.6159×10^{17}
	15	16	176	4.0599×10^{21}	1	4.0599×10^{21}

TABLE V. ALL GENERATED CANDIDATE POINTS TO FIND REQUIRED VALID CHAFF POINTS

Total Genuine Points used	**No. of valid Chaff-Points required**	**All generated candidate points to find required valid chaff points**		
		T.C. Clancy et al. [11], 2003	**T. H. Nguyen et al. [30], 2013**	**Proposed MFVS**
10	100	191	154	100
18	180	1123	981	180
20	200	2358	981	200
22	220	9084	1654	220
23	230	18615	2373	230
24	240	66609	3276	240

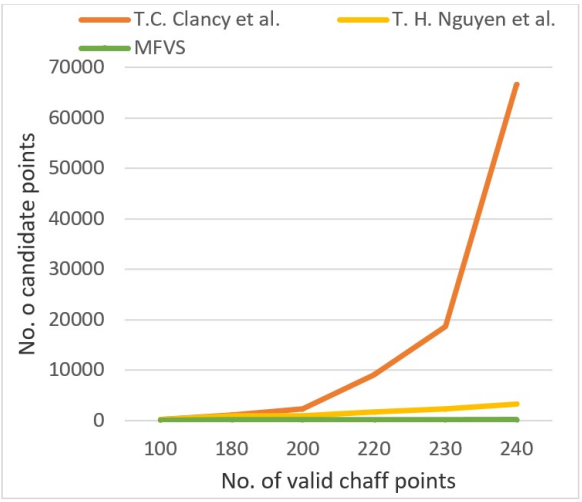

Figure 6. Graph between valid chaff points and required candidate points to generate valid chaff points

VI. CONCLUSION

In this paper, the MFVS is proposed using least square polynomial curve fitting, and Newton's divided difference interpolation-based new chaff-points generation method. The average accuracy of the proposed system is 100% for secret-key regeneration in all cases of secret-key with different sizes. Moreover, the MFVS using LSPC with proposed chaff-point method performs better than existing works and shows the results as GAR is 99% and FAR is 0%. The MFVS uses a comparatively high polynomial degree to make the fuzzy vault more robust against brute-force attack. To break the fuzzy vault and extract the genuine points, the attacker has to apply a total of 4.0599×10^{21} combinations, which are relatively 10-Million more as compared to existing research. The MFVS with the new chaff-point generation method generates only the valid chaff-points, in such a way that the generated points do not overlap the genuine points as well as other chaff-points. Thus, MFVS minimizes the number of candidate points about 13-times as compared to the method proposed by T. H. Nguyen et al. in 2013. In conclusion, all the investigated results demonstrate that the proposed MFVS system performs better in all experimental aspects.

As the key-biding biocrypto-systems are influenced by the variability and uncertainty in the biometric traits due to haphazard noise. The work can be explored further to design an algorithm that can modeled and handle variability in the different biometric traits. The proposed works are evaluated with small samples, the work can be further extend for the large biometric samples to demonstrate its performance.

REFERENCES

[1] D. Sadhya, S. K. Singh, and B. Chakraborty, "Review of key□binding□based biometric data protection schemes," IET biom., vol. 5, no. 4, pp. 263–275, Dec. 2016. doi:10.1049/iet-bmt.2015.0035

[2] Z. Jin, A. B. J. Teoh, B.-M. Goi, and Y.-H. Tay, "Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation," Pattern Recognition, vol. 56, pp. 50–62, Aug. 2016. doi:10.1016/j.patcog.2016.02.024

[3] Y.-L. Lai, J. Y. Hwang, Z. Jin, S. Kim, S. Cho, and A. B. J. Teoh, "Symmetric keyring encryption scheme for biometric cryptosystem," Information Sciences, vol. 502, pp. 492–509, Oct. 2019, doi:10.1016/j.ins.2019.05.064

[4] N. Tantubay and J. Bharti , "Multimodal key-binding biocrypto-system using leastsquare polynomial curvefitting based new feature level fusion method," INDJCSE, vol. 12, no. 1, pp. 10–20, Feb. 2021. doi:10.21817/indjcse/2021/v12i1/211201022

[5] A. Juels and M. Sudan, "A Fuzzy vault scheme," Des Codes Crypt, vol. 38, no. 2, pp. 237–257, Feb. 2006. doi:10.1007/s10623-005-6343-z

[6] B. Tams, P. Mihailescu, and A. Munk, "Security considerations in minutiae-based Fuzzy vaults," IEEE Trans. Inform. Forensic Secur., vol. 10, no. 5, pp. 985–998, May 2015. doi:10.1109/TIFS.2015.2392559

[7] V. Alarcon-Aquino, J. Ramirez-Cortes, O. Starostenko, H. Garcia-Baleon, and P. Gomez-Gil, "Biometric cryptosystem based on keystroke dynamics and K-medoids," IETE J Res, vol. 57, no. 4, p. 385, 2011. doi:10.4103/0377-2063.86341

[8] D. Chang, S. Garg, M. Ghosh, and M. Hasan, "BIOFUSE: A framework for multi-biometric fusion on biocryptosystem level," Information Sciences, vol. 546, pp. 481–511, Feb. 2021. doi:10.1016/j.ins.2020.08.065

[9] F. Benhammadi and K. Beghdad Bey, "Password hardened fuzzy vault for fingerprint authentication system," Image and Vision

Computing, vol. 32, no. 8, pp. 487–496, Aug. 2014. doi:10.1016/j.imavis.2014.04.014

[10] T. K. Dang, Q. C. Truong, T. T. B. Le, and H. Truong, "Cancellable fuzzy vault with periodic transformation for biometric template protection," IET biom., vol. 5, no. 3, pp. 229–235, Sep. 2016. doi:10.1049/iet-bmt.2015.0029

[11] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smartcardbased fingerprint authentication," in Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications - WBMA '03, Berkley, California, 2003, p. 45. doi:10.1145/982507.982516

[12] M. Khalil-Hani and R. Bakhteri, "Securing cryptographic key with fuzzy vault based on a new chaff generation method," in 2010 International Conference on High Performance Computing & Simulation, Caen, France, Jun. 2010, pp. 259–265. doi:10.1109/HPCS.2010.5547122

[13] M. Khalil-Hani, M. N. Marsono, and R. Bakhteri, "Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm," Future Generation Computer Systems, vol. 29, no. 3, pp. 800–810, Mar. 2013. doi:10.1016/j.future.2012.02.002

[14] G. Amirthalingam and G. Radhamani, "New chaff point based fuzzy vault for multimodal biometric cryptosystem using particle swarm optimization," Journal of King Saud University - Computer and Information Sciences, vol. 28, no. 4, pp. 381–394, Oct. 2016.. doi:10.1016/j.jksuci.2014.12.011

[15] G. S. Eskander, R. Sabourin, and E. Granger, "A bio-cryptographic system based on offline signature images," Information Sciences, vol. 259, pp. 170–191, Feb. 2014. doi:10.1016/j.ins.2013.09.004

[16] S. S. Ali, I. I. Ganapathi, S. Prakash, P. Consul, and S. Mahyo, "Securing biometric user template using modified minutiae attributes," Pattern Recognition Letters, vol. 129, pp. 263–270, Jan. 2020. doi:10.1016/j.patrec.2019.11.037

[17] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," EURASIP J. on Info. Security, vol. 2011, no. 1, p. 3, Dec. 2011. doi:10.1186/1687-417X-2011-3

[18] A. I. Arrahmah, Y. S. Gondokaryono, and K.-H. Rhee, "Fast non-random chaff point generator for fuzzy vault biometric cryptosystems," in 2016 6th International Conference on System Engineering and Technology (ICSET), Bandung, Indonesia, Oct. 2016, pp. 199–204. doi:10.1109/ICSEngT.2016.7849650

[19] L. You, L. Yang, W. Yu, and Z. Wu, "A cancelable Fuzzy vault algorithm based on transformed fingerprint features," Chin. j. electron, vol. 26, no. 2, pp. 236–243, Mar. 2017. doi:10.1049/cje.2017.01.009

[20] A. Kharab and R. Guenther, "The method of Least-Squares," in An Introduction to Numerical Methods: A MATLAB® Approach, Fourth Edition, Boca Raton, Florida : CRC Press, [2018] CRC Press, 2018, pp. 209–234. doi:10.1201/9781315107042

[21] A. K. Jaiswal and A. Khandelwal, "Curve fitting," in A textbook of computer based numerical and statistical techniques, New Delhi: New Age International Pvt. Ltd., 2009, pp. 387–424

[22] A. P. de Camargo, "On the numerical stability of Newton's formula for Lagrange interpolation," Journal of Computational and Applied Mathematics, vol. 365, p. 112369, Feb. 2020. doi:10.1016/j.cam.2019.112369

[23] R. Douaifia, S. Bendoukha, and S. Abdelmalek, "A Newton interpolation based predictor–corrector numerical method for fractional differential equations with an activator–inhibitor case study," Mathematics and Computers in Simulation, vol. 187, pp. 391–413, Sep. 2021. doi:10.1016/j.matcom.2021.03.009

[24] L. Gupta, L. Barash, and I. Hen, "Calculating the divided differences of the exponential function by addition and removal of inputs," Computer Physics Communications, vol. 254, p. 107385, Sep. 2020. doi:10.1016/j.cpc.2020.107385

[25] J. Abraham, P. Kwan, and J. Gao, "Fingerprint matching using a hybrid shape and orientation descriptor," in State of the art in Biometrics, J. Yang, Ed. InTech, 2011. doi:10.5772/19105

[26] T. H. Nguyen, Y. Wang, Y. Ha, and R. Li, "Performance and security□enhanced fuzzy vault scheme based on ridge features for distorted fingerprints," IET biom., vol. 4, no. 1, pp. 29–39, Mar. 2015. doi:10.1049/iet-bmt.2014.0026

[27] T. K. Dang, M. T. Nguyen, and Q. H. Truong, "Chaff point generation mechanism for improving fuzzy vault security," IET Biometrics, vol. 5, no. 2, pp. 147–153, Jun. 2016. doi:10.1049/iet-bmt.2015.0023

[28] D. Chitra and V. Sujitha, "Security analysis of prealigned fingerprint template using fuzzy vault scheme," Cluster Comput, vol. 22, no. S5, pp. 12817–12825, Sep. 2019. doi:10.1007/s10586-018-1762-6

[29] H. Choi, Y. Chung, W. Choi, S. Lee, H. Cho, and S. Pan, "Smartcard-based secret distribution for secure fingerprint verification," IETE J Res, vol. 57, no. 4, p. 299, 2011. doi:10.4103/0377-2063.86263

[30] T. H. Nguyen, Y. Wang, Y. Ha, and R. Li, "Improved chaff point generation for vault scheme in bio□cryptosystems," IET biom., vol. 2, no. 2, pp. 48–55, Jun. 2013. doi:10.1049/iet-bmt.2012.006