Enhanced Template Protection Algorithms Based on Fuzzy Vault and Cuckoo Hashing for Fingerprint Biometrics

Mulikat B. Akanbi[1*], Rasheed G. Jimoh[2], Agbotiname L. Imoize[3,4] , Joseph B. Awotunde[2], Olatunji S. Isiaka[1], Shade B. Abdulrahaman[1]

[1] Computer Science Department, Institute of Information and Communication Technology, Kwara State Polytechnic, Ilorin, Nigeria
[2] Department of Computer Science, Faculty of Information and Communication Sciences, University of Ilorin, Ilorin 240003, Nigeria
[3] Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria
[4] Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801 Bochum, Germany
Emails: akanbiforu@gmail.com; jimoh_rasheed@unilorin.edu.ng; aimoize@unilag.edu.ng; awotunde.jb@unilorin.edu.ng; isiakaosalman2@gmail.com; billy4us@gmail.com

Abstract

Biometrics provides better authentication. Unprotected biometrics is open to attacks from intruders as stolen biometrics may not be revocable. Although there are several points where attacks can be launched on biometric systems, template databases are said to be the most frequently attacked. When a template database is attacked, attackers can add fresh templates, modify the existing ones, copy or steal templates and later construct a spoof from it or replay it back into the biometric system to impersonate a genuine user. Several template security systems have been presented in the literature to secure biometric templates. Fuzzy vault, as proposed by many researchers is, to some extent, one of the best algorithms to achieve template protection as it has good security. Fuzzy vault, however, lacks irreversibility, revocability, and diversity. To address these disadvantages and strengthen fuzzy vault, this study combines a noninvertible feature transformation template protection algorithm known as cuckoo hashing that possesses irreversibility, revocability, and diversity properties with a fuzzy vault for privacy. The study used fingerprint biometrics as it is widely used. The proposed algorithm was implemented in the MATLAB 2016a environment using FVC 2004 DB1 fingerprint public database. The proposed algorithm recorded a FAR of 0.01% and an FRR value of 0.09% with an EER of 0.05%.

Keywords: Fingerprint; Template protection; Biocryptosystems; Fuzzy vault; Feature Transformation; Biometric system; Authentication; Template protection Revocability.

1. Introduction

Authenticating users before granting them access to use certain resources has been in use for many years [1]. Human authentication can be classified as What you know, for example, passwords, usernames, and individual check numbers; and What you have, for example, a token, smart card and What you are, biometrics [2-3]. In recent times, the earlier forms of personal identification or verification are not sufficiently effective in handling Internet crimes, frauds and security threats [4]. Due to the need for authentication in applications where security is very important, the use of biometric characteristics to recognize people has received more attention [5-6]. Biometrics refers to non-comparable physical or behavioural features of an Individual [2], [7]. Biometric systems employ physical (fingerprint, face, palm print, iris, or vein) or behavioural (voice, stride, handwriting, or typing rhythm) traits to determine a person's identity or validate that they are who they claim to be [8]. A biometric system is a pattern recognition system that obtains biometric patterns from a person, extracts biometric feature sets from them,

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

and then stores them in a database as biometric templates [9]. A template is a condensed depiction of a biometric feature that contains critical discriminatory information for identifying an authorized person [10]. To authenticate users, biometric template matching compares previously saved biometric templates to newly obtained biometric data. For a successful template match to be termed a positive match, a particular threshold must be met [11]. Even though biometric qualities are one-of-a-kind and difficult to counterfeit, research demonstrates that biometric systems are vulnerable to attacks. Stolen biometric templates are one of the most significant threats since they cannot be readily cancelled and can be exploited by an adversary in other apps that use the same biometric feature [12]. According to authors in [13], an adversary can attack point 1 (sensor module) by destroying the recognition sensor, causing a denial of service (DOS) attack, or by presenting bogus biometrics (spoof) to overcome the recognition systems. As shown in Figure 1, at the communication channels (points 2, 4, 5, 7 and 9), biometric traits can be stolen and stored somewhere for a replay back and substitution attacks.

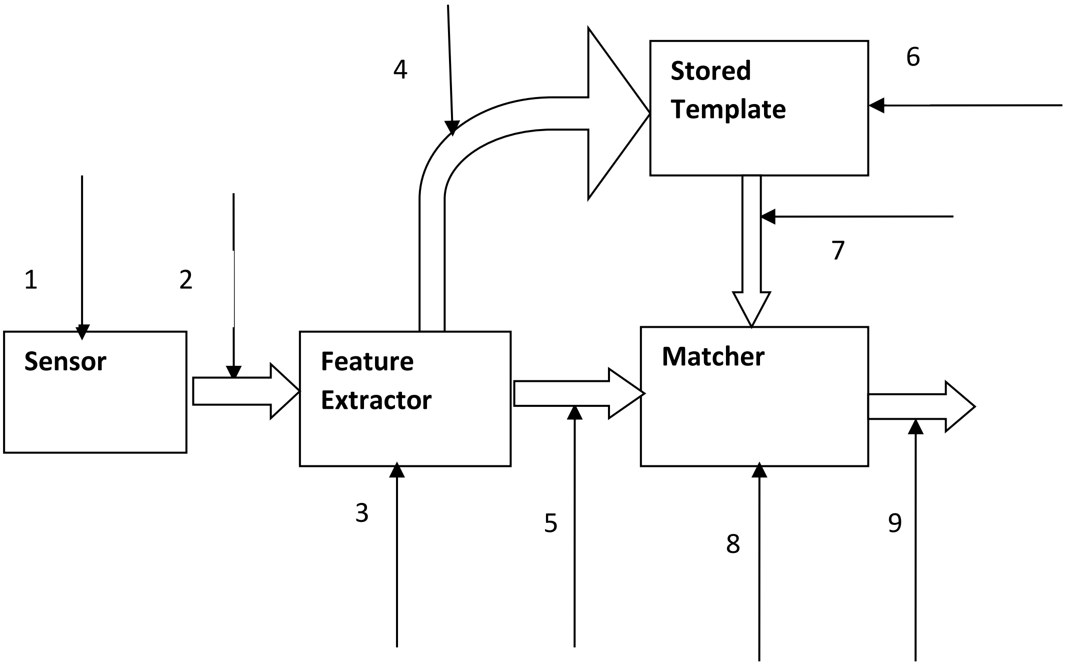


Figure 1: Vulnerable Points of Attack on Fingerprint Biometric Systems

At point 3, a substitution attack and a denial-of-service assault are both feasible. An intruder could force the feature extractor module to generate sample values he chooses instead of feature values generated from the sensor's original biometric data. An intruder can also deploy a Trojan horse to replace the feature extractor device, harvesting the user's biometrics samples and sending them to the intruder [14]. Invasion attacks at point 6 occur when an intruder steals a template, adds new templates, and modifies the present templates stored to gain unauthorized access. Attacks such as substitution and hill climbing are feasible. Fake matching scores may be substituted for real ones at point 8 (matching module). An intruder replaces the matcher with a Trojan horse and then instructs the Trojan horse to produce high matching scores and deliver a "Match" to the application, bypassing the biometric authentication method [15]. The two main approaches to safeguarding biometric templates from hackers are biocryptosystems and feature transformation methods [16]. A biocryptosystem combines biometrics with a cryptographic key to provide security that combines the benefits of both biometrics and cryptosystems [17]. A biometric cryptosystem can generate a key by binding it to biometric features (key binding) or directly generating it from biometric features (Key Generation). A feature transformation scheme transforms a biometric template from one form to another using a transformation function and then stores the transformed template in a database [18]. A non-invertible transform modifies the biometric picture by applying a one-way function making the changed template impossible to invert [19]. With the use of a key, invertible transforms apply the invertible transformation function to the template. This approach is only safe as long as the key's secrecy is maintained, as the original template could be regenerated if the key is compromised [20]. A biometric template protection scheme should meet several properties such as non-invertibility, revocability, non-linkability and performance to assure the biometric template's security [21].

The non-invertibility or irreversibility quality makes obtaining the original biometric template from a protected biometric reference computationally difficult. Making it computationally difficult for attackers to recover the

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

original biometric template from many instances of protected biometric reference obtained from the same biometric trait of an individual is referred to as revocability (renewability). Protected templates should also be made Unlinkable (Unlinkability) by making determining whether two or more instances of protected biometric reference were derived from the same biometric trait of a person computationally difficult. Finally, any template protection strategy used on a biometric system should not compromise the system's overall performance. Biometric features for personal identification include fingerprints, iris, voice, gait, and signatures; however, fingerprint biometrics was employed in this study since it is the most feasible and extensively used biometric feature [1, 9].

A fuzzy vault is a key-binding biocryptosystem approach used to bind a key with the biometric template for security. To address the problem of template hacking, several studies have proposed fuzzy vault [25]. However, the fuzzy vault is prone to correlation attacks and therefore lacks cancelability [26]. Thus, for the enhancement of the security of the fuzzy vault and to overcome the limitation of correlation attack on the vault, techniques like a hybrid model that combine the fuzzy vault with another template protection scheme can be employed [20]. This study, therefore, proposes a dual-level algorithm for enhanced fingerprint template protection by combining fuzzy vault bio-cryptosystem and noninvertible Cuckoo hashing feature transformation method for better security, privacy and performance.

The paper contributions are as follows:

(i) proposes a dual-level template protection model using fuzzy vault and cuckoo hashing to prevent template hacking and a dual-template protection that is revocable and irreversible.

(ii) the proposed model was used for biometric authentication to prevent unauthorized access.

(iii) the proposed model was compared with a recent state-of-the-art model in biometrics using various performance metrics.

2. Related Work

Fuzzy vault and Fuzzy Commitment are the two key binding approaches in biocrytosystem. Key generation approaches include a Fuzzy extractor and Secure sketch. Biocrytosystems protect templates with good security; they however lack irreversibility, revocability and diversity [22]. From the drawbacks of biocryptosystems highlighted above, biocryptosystems can be combined with another template protection scheme to eradicate these drawbacks [23]. The proposed hybrid template protection approaches by authors in [20], a hybridized fuzzy commitment and fuzzy vault on multi-biometric templates and in [24], the authors hybridized fuzzy extractor and fuzzy vault for authentication in the internet of medical things to secure patients' details may lack irreversibility and revocability as the researchers hybridized two biocryptosystem algorithms. The authors in [26], developed a single template protection approach using the fuzzy vault. Apart from lacking irreversibility and revocability, the vault is vulnerable to correlation attacks. Where more than one vault is derived from the same biometric data, an intruder can correlate the values in those different vaults and thus identify the genuine points to reconstruct the original fingerprint [27]. Other single biocrytosystems proposed by authors in [28] also lack irreversibility and revocability.

Feature transformation template protection approaches apply transformation functions to biometric templates for template protection. Non-invertible or one-way feature transformation schemes apply non-invertible transformation functions to the biometric template to make it cancelable. The cancelable biometrics generated has the advantages of irreversibility, revocability and diversity. Several authors have proposed template protection based on the feature transformation approach. The authors in [30] used cuckoo hash and MinHash on palmprint templates while the authors in [36] used a double bloom filter to protect Iris templates. Authors in [37] developed an improved bio-hashing algorithm on finger knuckle prints. They enhanced the security of the BioHashing algorithm by limiting the impact of attacks based on the stolen token. In [37], the authors proposed a cancelable fingerprint template using spiral curves by contiguous right-angled triangles construction using the invariant distances between reference minutia and every other minutia in the fingerprint image.

The fingerprint image is then projected onto a 4D space before transforming the image. Another feature transformation approach based on a one-factor cancellable biometric authentication scheme that is empowered by Indexing First Order hashing, a tailor-made locality-sensitive hashing function for template protection was proposed by the authors in [38]. As fuzzy vault is good in template security but vulnerable to correlation attack

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

and like other biocryptosystems lacks irreversibility, revocability and diversity, the feature transformation approach on the other hand possesses irreversibility, revocability and diversity properties but cannot meet the security requirement in template protection [29]. For improved security and privacy of fingerprint templates stored in the database, the two template protection approaches can be combined to complement the drawbacks of the other. This research, therefore, proposes a dual-level template protection algorithm that combined a fuzzy vault biocryptosystem algorithm with a cuckoo hashing noninvertible feature transformation algorithm for better privacy and security in biometric applications.

3. Methodology

The study developed a fingerprint template protection algorithm by combining two template protection algorithms, fuzzy vault and cuckoo hashing algorithms, for enhanced security and privacy. A Gabor filter was applied on the grayscale for fingerprint image enhancement as shown in figure 2. Binarization and Thinning processes were applied to the image before the minutia features were extracted (see figure 2). FVC2004 DB1 (Fingerprint Verification Competition public dataset) was used for this study. The algorithm was implemented in MATLAB 2016a environment.

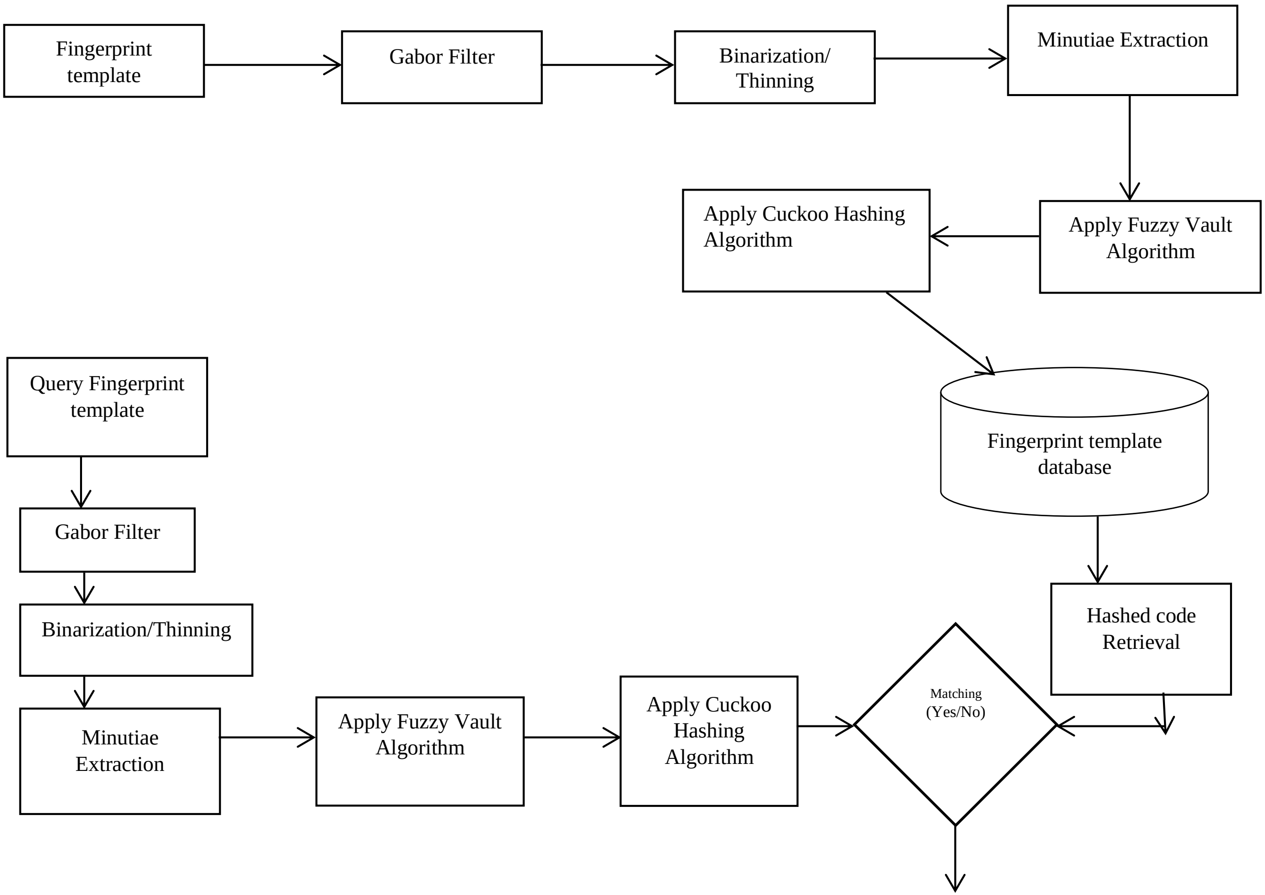

Fingerprint template
Gabor Filter
Binarization/ Thinning
Minutiae Extraction
Apply Fuzzy Vault Algorithm
Apply Cuckoo Hashing Algorithm
Fingerprint template database
Query Fingerprint template
Gabor Filter
Binarization/Thinning
Minutiae Extraction
Apply Fuzzy Vault Algorithm
Apply Cuckoo Hashing Algorithm
Matching (Yes/No)
Hashed code Retrieval

Figure 2: Conceptual framework of the proposed Dual-Level algorithm

3.1 Overall Architecture of the Proposed Algorithm

The overall architecture of the hybrid template protection system is shown in Algorithm 1.

Algorithm 1: Algorithm for the overall architecture of the system

```
1.   Input Fingerprint
2.   Fingerprint image enhancement
3.   Perform  Binarization on the enhanced fingerprint image
4.   Thinning of the binarized image
5.   Minutiae points extraction
5.1  Extract the minutiae points using crossing number CN:
          $CN(P) = \frac{1}{2}\sum_{i=1}^{8}|p_i - p_i - 1|$
```

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

$$where\ p\ is\ pixel\ belonging\ to\ the\ streak\ of\ value\ 1$$

5.2 *Orientation and the coordinates (x, y, θ) of the extracted minutiae point is fed into the fuzzy vault as input.*

6. Apply fuzzy vault algorithm.

6. Harden the fuzzy vault's output by applying Cuckoo hashing.

3.1.1 Image Enhancement

The grayscale image of the fingerprint is enhanced to remove noise and increase the accuracy of the system. Algorithm 2 shows the step-by-step procedure for image enhancement.

Algorithm 2: Algorithm for the image enhancement using Gabor Filter

```
1. Start
2. Input images
3. Convert images into grayscale format (0-255)
4. Set the Wavelength to 1, the Orientation(s) (deg.) to 0, the Phase offset(s) (deg.) to 90,
The Aspect Ratio to 0.5, the Bandwidth to 1 and the Number of orientations to 1
5. Split the source image into 16 by 16 squares
6. Compute features for four distinct scales from eight distinct angles yielding eight alternative angles for each scale
7. Calculate the Mean (Average) of the various angles m = sum of the angles/number of angles
8. Determine the standard deviation of the different angles s = SQRT ( (SUM ($x_i$ - m)$^2$) / N)
9. Compute the Gabor filter characteristics vector$f_{Gabor}$ = (f – m) / s
10. End
11 m = Mean
12 s = Standard Deviation
13 $x_i$ = Each from the angles
14 N = Size of the angles
15 f = Feature vector
```

3.1.2 Binarization of the Enhanced Image

The process of transforming a grayscale image to binary form is known as binarization. In a grayscale image, a pixel can have 256 different intensity levels. To convert a grayscale image to binary, use a specific threshold value to get zero (0) and one (1) binary values by setting pixel values below the threshold to zero and intensity values over the threshold to one [28]. The pixel values 0 and 1 are allocated to black and white, respectively, in a binary image.

Algorithm 3 shows the procedure for the binarization of the enhanced fingerprint image.

Algorithm 3: Algorithm for Binarization

```
1.    Start
2.    Input filtered image
3.    Convert images into gray scale format
4.    Initialize processing (sum of a column of inverted gray image)
5.    Compute Vertical and Horizontal edge detection
6.    Calculate and check for the threshold
7.    Obtain Binarized template
8.    End.
```

3.1.3 Thinning of the Binarized Image

The thinning procedure is applied to the binarized image to make locating the minutiae details easier [43]. Thinning is the technique of applying a block filter to lower the width of each of the ridge's pixels such that their thickness is reduced to a single pixel width. Algorithm 4 shows the procedure involved in thinning the binarized fingerprint image.

Algorithm 4: Algorithm for Thinning

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

```
1.      Start
2.      Input Binarized image
3.      Repeat:
    3.1   Collect the entire removable pixel as S
    3.2   If S is empty, break
    3.3   Set all pixels in S to be background in I
4.      Set I as thinned image
5.      End
```

3.1.4 Minutiae Extraction

The thinned fingerprint image is used to extract features. The x and y coordinates of tiny points, as well as their orientation angle, are retrieved. The crossing number can be used to obtain the fourth component, which is the minutiae type.

In a 3x3 block, the crossing number (CN) is half of the sum of the differences between two consecutive pixels. The following is the CN equation [44]:

$$CN(P) = \frac{1}{2}\sum_{i=1}^{8} |p_{i-}p_{i-1}| \qquad (1)$$

If CN (P) = 1, then type is termination

If CN (P) = 2, then type is normal ridge

If CN (P) = 3, then type is bifurcation.

The extracted data (x, y, and minutiae type) is saved in the following matrix format: The number of rows corresponds to the number of minutiae points (a total of four columns).

Column 1: Each minutia point's row index (x coordinate)

Column 2: Each minutia point's column index (y coordinate)

Column 3: Each minutia point's inclination angle (Minutiae angle of the particular minutia point to be paired i.e input image and template image).

Column 4: Type minutiae (CN=1 indicates termination, while CN=3 indicates bifurcation).

3.1.5 Fuzzy vault encoding process

The steps for encoding a fuzzy vault are as follows [33]:

1. Let S = $\{s\}_{i=1}^{n-1}$ be the secret key. The polynomial P of order n is found using the symbol s.

2. The vault is built using minutiae's x and y coordinates $(v = x/y)$.

3. Genuine points (G) and chaff points (C) are created.

4. To obtain P, evaluate the polynomial P at all points in the specified region (v).

$$FV = G \cup C \qquad (2)$$

where $G = [(v1, P(v1)), (v2, P(v2)), \ldots. (vm, P(vm))]$

$$C = [(r1, s1), (r2, s2), \ldots. (rl, sl)]$$

$$rk \cdot vj$$

$$sk \cdot P(vj)$$

$$[k = 1, 2, \ldots l, j = 1, 2, \ldots. m]$$

Where v stands for genuine points, P (v) stands for projection of genuine points, r stands for chaff point, m stands for a number of genuine points, l stands for a number of chaff points, and s stands for dummy value.

The proposed dual-level algorithm only used the encoding process and not the decoding process as the matching is done in the hash domain after applying Cuckoo hashing.

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

3.1.6 Cuckoo Hashing Concept

Cuckoo hashing follows the algorithm below [41]:

Extraction of features is the first step.

The fingerprint image's region of interest (ROI) is extracted. The fingerprint image's orthogonal features are then encoded to create binary template F.

Perform an XOR operation.

Adopt a user-specific secret T to implement XOR operation with the received template F to ensure non-leakage at the template level and enforce noninverifability.

The third step is to divide the templates.

The orthogonal characteristics are broken down into sub-blocks that don't overlap. The column of each block is made up of nBits bits. The unprotected template size is nBits x nWords x nBlocks, and the block size is nBits x nWords.

Use the Cuckoo hashing method.

Orthogonal feature blocks are mapped into two sub-blocks using a random filter before hashing. Based on two hash functions, an item to be inserted is mapped to two possible buckets. Each block has the same dimensions as the original.

n = 2nBits + 1 is the length of the cuckoo hash.

For all points, the cuckoo hash starts at zero. The transform is implemented by assigning decimal value indexes to columns of the 2D fingerprint template in each block.

3.2 The proposed Dual-level Algorithm

Algorithm 5 shows the step-by-step procedure the proposed dual-level Algorithm.

Algorithm 5: The proposed Dual-level Algorithm

```
1. Define the Number of Fields
2. Define the degree of the polynomial
3. Define the number of chaffs
4. Define Tolerance
5. Enter the Key
6. Codeword and message word lengths
7. Create a Galois field array
8. Mix up the projected points with chaff points
9. Initialize a set of chaff points to zeros
10. Keep generating random points until  'numChaffs' is generated
11. Generate a random point (a,b) in the field
        12. Remove zeros from the chaff point set
13. Sort points and merge chaffs with points
        14. Express Galois output with cuckoo hashing
14.1    Start
14.2    Input Galois output
14.3    14.3 Maintain two tables, each of m rows and columns.
14.4    From U to [m], choose two hash functions, h1 and h2.
14.5    In the first table, U will be at position h1(x), while in the second table, U will be at position h2(x).
14.6    Lookup x in the hash table
14.7    IF Lookup(x) then
14.7.1  Loop MaxLoop times
14.7.2  Apply random rotation (R)
14.7.3  Hash minutiae point
14.7.4  If $h_1(x)$ is not occupied, put x there
14.7.5  If it is occupied, place x there, move the old element y, and place y into the second table
14.8    End IF
```

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023   Accepted: March 15, 2023

```
14.9    End
14.10   Continue bouncing between tables until all elements have stabilized.
14.11   If table insertion fails, repeat the process by selecting a new h1 and h2 and re-inserting all components into the tables.
14.12   Obtain Hashed Vault.
14.13   End
15. Return Secured Template
```

The fuzzy vault generated which returns an array of polynomials was converted to a Galois field array which serves as input for the cuckoo hash. The Cuckoo hashing works are based on the idea of resolving collisions by employing two hash functions instead of just one. This provides two possible locations in the hash table for each key. The cuckoo hashing was able to work on the Galois field array of the fuzzy vault. The fingerprint database setup is shown in Table 1 while the parameters used for the fuzzy vault are listed in Table 2.

Table 1: Fingerprint Database setup

Parameters	Value
Total Number of images	80
Total number of Training sets	20
Number of Testing Sets	60
Total number of impressions per finger	8
Total number of people per class	10
False Fingerprint impression Class	10

Table 2: Fuzzy Vault Parameters

Parameters	Value
Field	16
Degree	35
Number of chaffs	30
Tolerance	2

Finding the optimal production plan that makes the company's profit from the producers A, B as large as possible. We symbolize the quantities produced from the product A with the symbol x_1, and from the product B with the symbol x_2 , after building the appropriate mathematical model and solving it, we conclude that $x_1 = 5, x_2 = 3$, and hence the maximum profit $Z^* = 50$ of monetary unit.

4. Results and Discussion

4.1 Fingerprint Image Enhancement

After loading the fingerprint images, the images were run through a bank of Gabor filters. The number and direction of ridges and valleys fluctuate slowly over a limited, generally constant ridge orientation. Unwanted noise was filtered out and adjusted to the correct frequency and orientation, keeping the correct ridges and valleys in that direction. Figure 3 displayed the Gabor filter bank.

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

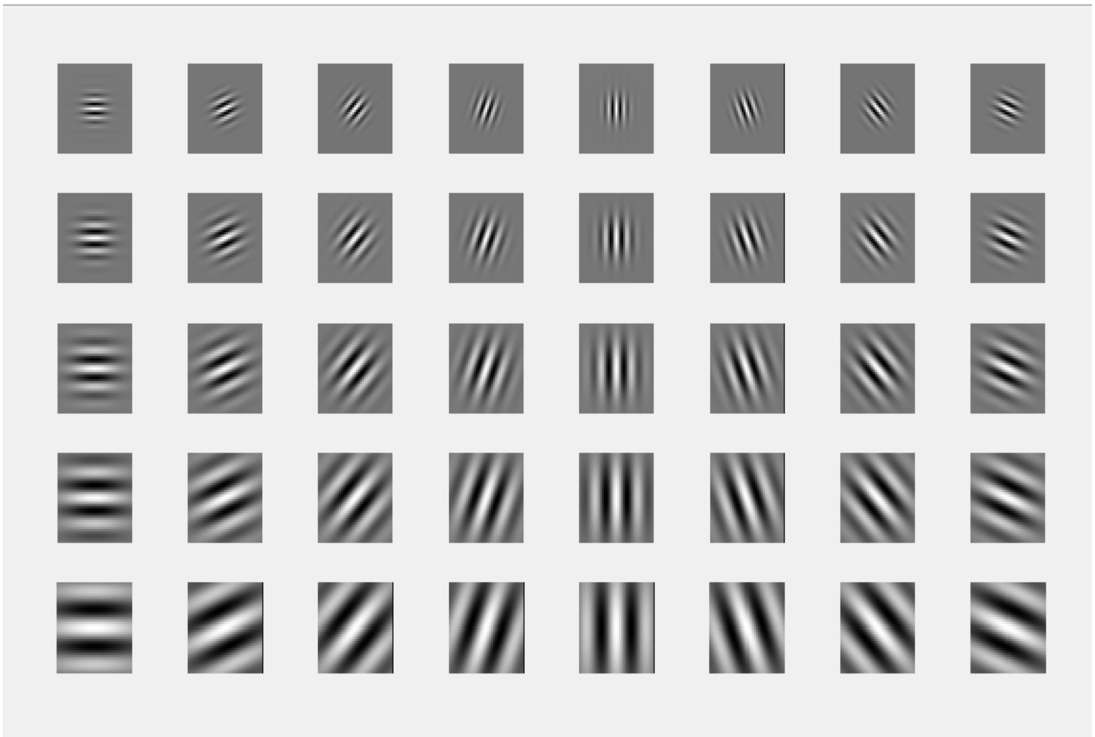


Figure 3: Gabor Filter Bank Binarization

The Fingerprint Image Binarization function converts an 8-bit Gray fingerprint image to a 1-bit image with 0-value ridges and 1-value furrows. The ridges in the fingerprint were emphasized in black after the procedure, while the furrows were highlighted in white. Figure 4 shows the fingerprint binarization.

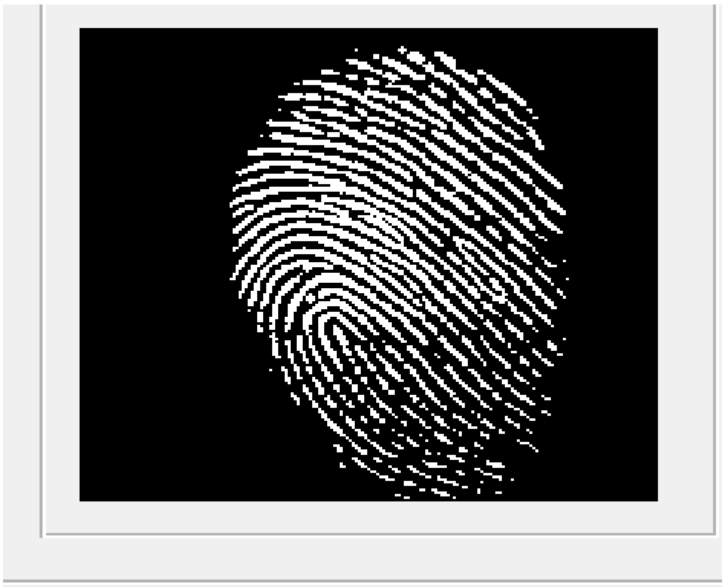


Figure 4: Binarized image

4.2 Thinning

Ridge Thinning reduces the size of ridges to one pixel wide by removing unneeded pixels. The thinning algorithm is iterative and parallel. The system flags down unnecessary pixels in each small picture window during each scan of the larger fingerprint image (3x3). After many scans, it ultimately removes all the flagged pixels. Figure 5 displayed the ridge thinning for the fingerprint.

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

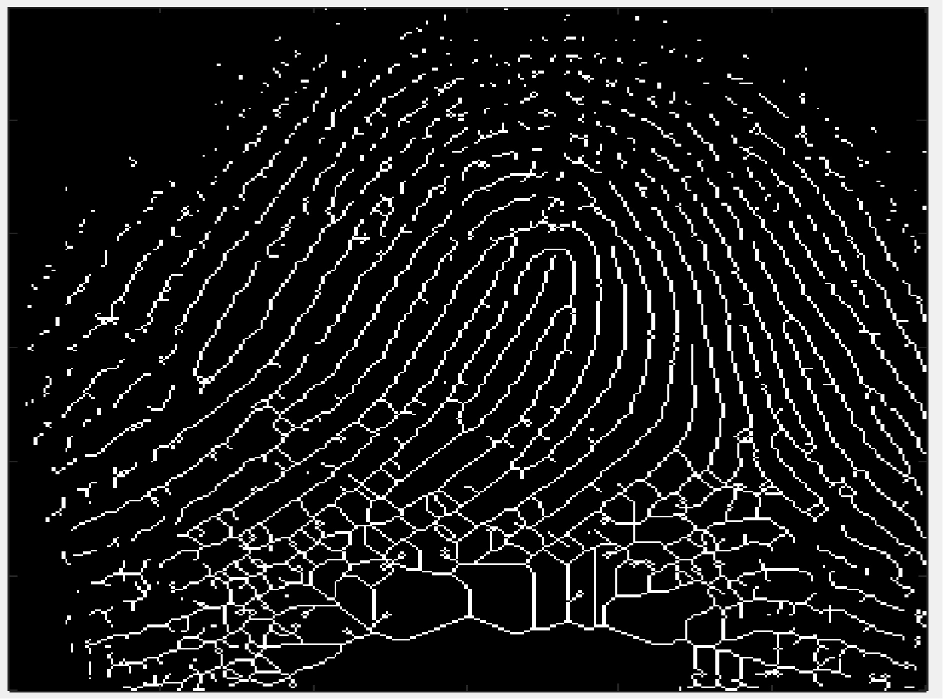
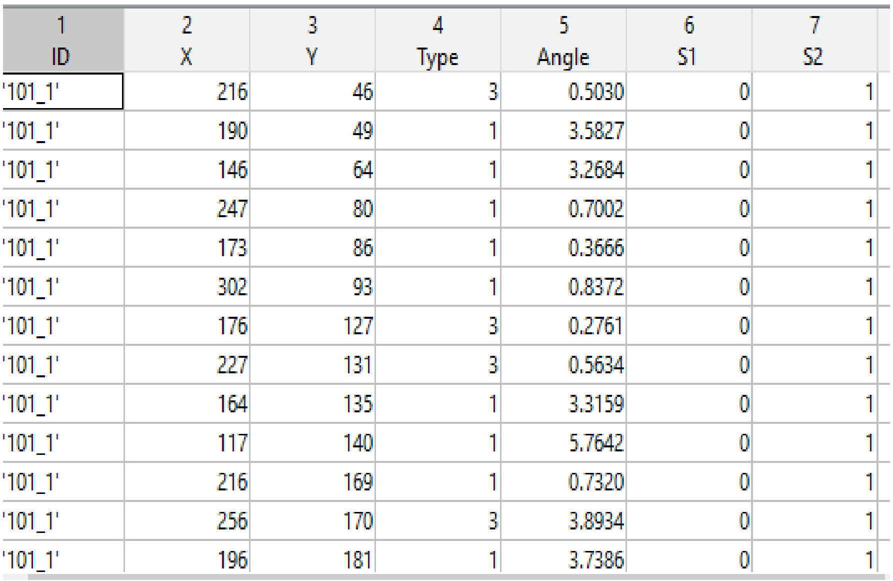


Figure 5: Ridge Thinning

4.3 Minutia Extraction

The minutia was marked and extracted using the concept of Crossing Number (CN). False minutia that lies at the image boundary was removed. The minutia X and Y vectors were outputted and concatenated as input to the fuzzy vault algorithm. Figure 6 shows the vector format and the corresponding components of the minutia extraction (X, Y, Type, Angle, and S1and S2).



1	2	3	4	5	6	7
ID	X	Y	Type	Angle	S1	S2
'101_1'	216	46	3	0.5030	0	1
'101_1'	190	49	1	3.5827	0	1
'101_1'	146	64	1	3.2684	0	1
'101_1'	247	80	1	0.7002	0	1
'101_1'	173	86	1	0.3666	0	1
'101_1'	302	93	1	0.8372	0	1
'101_1'	176	127	3	0.2761	0	1
'101_1'	227	131	3	0.5634	0	1
'101_1'	164	135	1	3.3159	0	1
'101_1'	117	140	1	5.7642	0	1
'101_1'	216	169	1	0.7320	0	1
'101_1'	256	170	3	3.8934	0	1
'101_1'	196	181	1	3.7386	0	1

Figure 6: Minutia Components extraction

A fuzzy vault was then applied to the minutia extracted using a polynomial in a degree order of 35.

4.4 Performance Evaluation

The system's evaluation is presented in this section. The system tested with the entire probe or testing images. The results were given in various performance metrics.

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

Table 3: Evaluation Parameters for the Test (Probe Fingerprint images)

Technique	True Positive	False Positive	True Negative	False Negative
Proposed Model	78	1	2	9

The evaluation parameters are presented in table 3. These parameters were used to calculate the FAR, the FRR and the proposed algorithm's Accuracy.

True Positive: The number of times the result of the system is positive for the enrolled fingerprint image and input image of the same user.

False Positive: The number of times the result of the system is positive for the enrolled fingerprint image and input image of different users.

True Negative: The number of times the result of the system is negative for the enrolled fingerprint image and input image of the same user.

False Negative: The number of times the result of the system is negative for the enrolled different users' fingerprints and input images. From the values generated in table 3, other performance metrics were also obtained.

False Rejection Rate (FRR) - Chances of failing to find a match between the input pattern and a database template. It calculates the percentage of legitimate inputs that are rejected wrongly.

$$FRR = \frac{FN}{TP + FN} \tag{3}$$

False Acceptance Rate (FAR) - Chances of mistakenly matching an input pattern to a database template that doesn't match. It calculates the percentage of mistakenly accepted invalid inputs.

$$FAR = \frac{FP}{FP + TP} \tag{4}$$

Equal Error Rate or Crossover Error Rate (EER or CER) - Both acceptance and rejection errors occur at the same rate. The ROC (Receiver Operating Characteristics) curve can readily be used to calculate EER. The lowest EER indicates good accuracy.

$$EER = \frac{FAR + FRR}{2} \tag{5}$$

Accuracy - True detection (TAR+TRR) and total detection (TAR+TRR+FAR+FRR) ratio in per cent.

$$ACCURACY = \frac{TAR + TRR}{TAR + TRR + FAR + FRR}\ X\ 100 \tag{6}$$

True Acceptance Rate (TAR) – The likelihood of matching an input pattern to a matching template accurately. It calculates the percentage of acceptable inputs that are accepted appropriately.

$$\text{TAR} = 1 - \text{FRR} \tag{7}$$

True Rejection Rate (TRR) - True Rejection Rate (TRR) - The probability of accurately detecting a non-matching input pattern against any database template. It calculates the percentage of correctly rejected invalid inputs.

$$\text{TRR} = 1 - \text{FAR} \tag{8}$$

The results generated from the evaluation of the equations above are listed in Table 4.

Table 4: Evaluation Parameters for Test (Probe Fingerprint images)

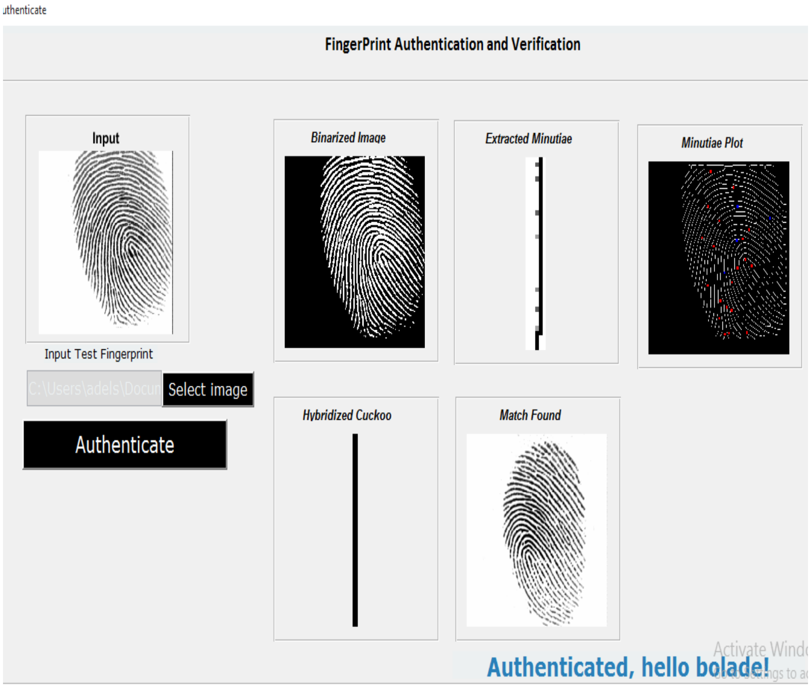
Metrics	Values
True Acceptance Rate (TAR)	0.91
True Rejection Rate (TRR)	0.99
False Rejection Rate (FRR)	0.09
False Acceptance Rate (FAR)	0.01

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

Equal Error Rate	0.05
Accuracy	95%

4.5 Authentication stage

Figure 6 below shows the authentication process when a fingerprint image is correctly recognized or matched. Figure 7 shows fingerprint output with the matched individual's name.

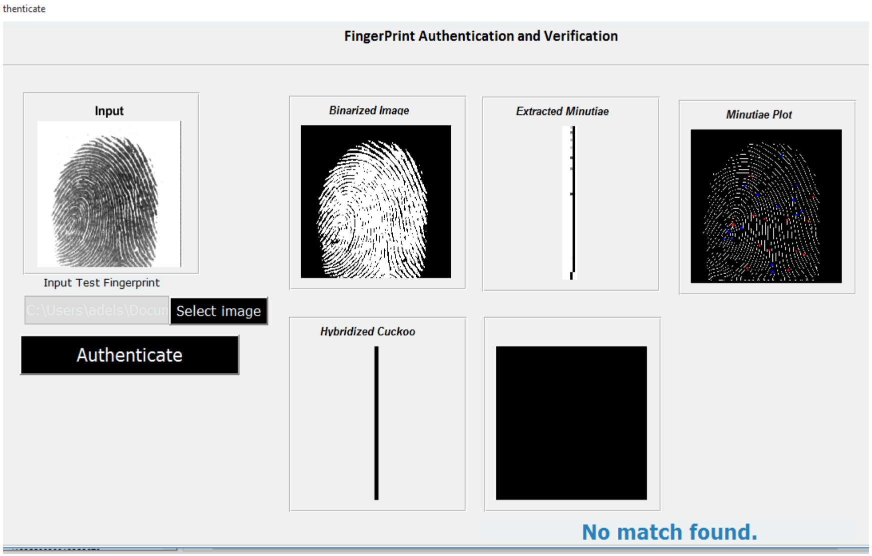


C:\Users\adels\Docu

Authenticated, hello bolade!

Figure 7: Correct Match Authentication

Figure 8 shows when a fingerprint image is not correctly classified; as no corresponding match was identified, the output axis stays dark and blank. This happens when the value of the protected template generated falls below the system's Threshold value of 0.48.



C:\Users\adels\Docu

No match found.

Figure 8: Match Not Found During Authentication.

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

Table 5 compares the results of the fingerprint recognition system obtained in this investigation with other results collected from other studies. False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER) were used to assess the proposed algorithm's performance.

Table 5: The study's findings in comparison with other studies.

S/No	Authors	Biometrics Used	Methods	FAR	FRR	EER
1	[34]	Fingerprint	Nil	0.1	0.18	0.19
2	[35]	Fingerprint	Fuzzy vault	0.35	0.09	0.22
3	[39]	Iris	Fuzzy vault and Fuzzy extractor	0.14	0.09	0.115
4	[40]	Fingerprint (Dual instances)	region code-based hashing	0.2	0.05	0.13
5	[41]	Face	random spaces	0.1179	0.0	0.059
6	Proposed Model	Fingerprint	Fuzzy vault and Cuckoo hashing	0.01	0.09	0.05

As depicted in Table 5, Figure 9 shows the diagrammatical presentation of the results using a bar plot with respect to the author's findings.

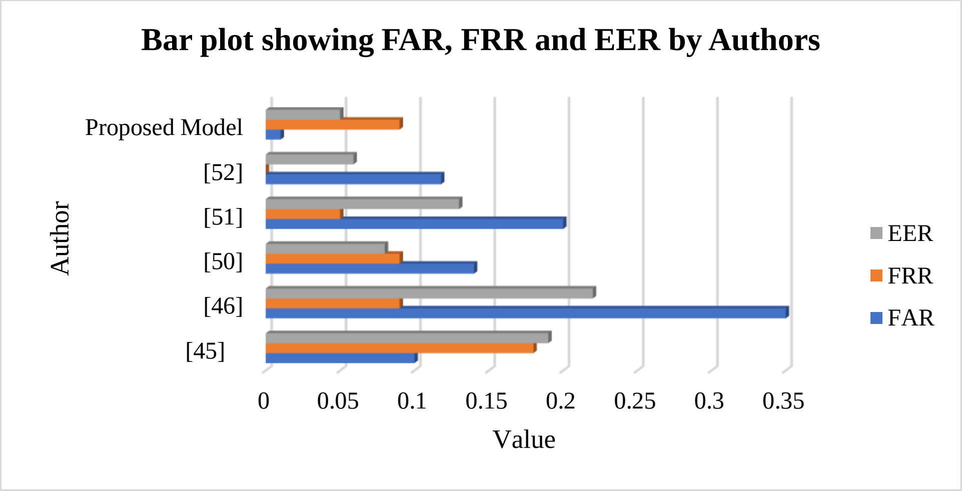


Figure 9: Distribution of the authors' findings relative to FAR, FRR and EER

Figure 9 shows the distribution of the authors' findings relative to FAR, FRR and EER results obtained from their studies. The individual results are explicitly discussed in the subsequent paragraphs. Figure 10 shows the FAR of each study as drawn from Table 5 and Figure 9.

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

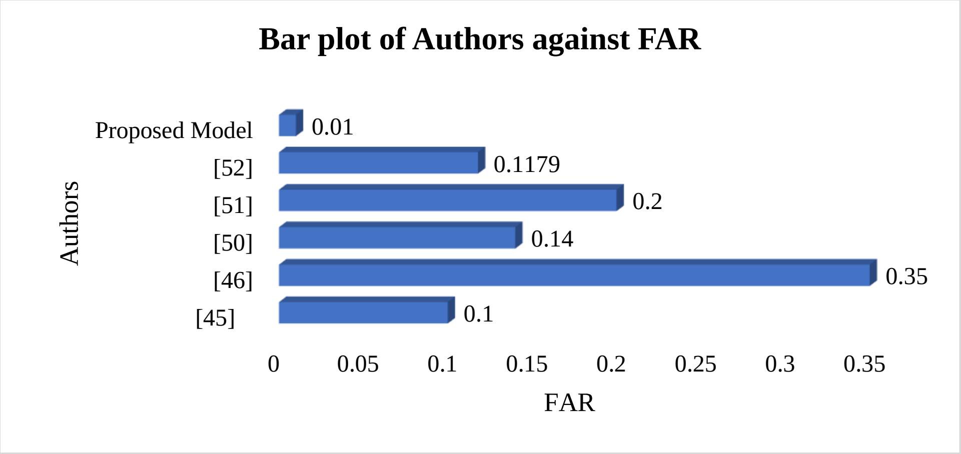


Figure 10: Graphical representation of average FAR by Author

As depicted in Table 5 and figure 10, [35], fuzzy vault biocryptosystem template protection recorded the highest FAR with FAR= 0.35%. This means [35] is the least performed study in terms of security closely followed by [51], which proposed cancellable biometrics for dual instances of the fingerprint using a new region code based hashing with FAR= 0.2%. [50], which combined fuzzy vault and fuzzy extractor biocrytosystem template protection to protect the iris template performed better next to [40] with FAR=0.14%. A smaller FAR means better security as the rate at which unauthorized users are granted access will be minimal. The proposed system using fuzzy vault and cuckoo hashing, a combination of biocryptosystem and cancellable biometric template protection for fingerprint, with the lowest FAR performs best with better security than other studies with FAR=0.01%. This is closely followed by [34] without any template protection on fingerprint with FAR=0.1% while a secure cancellable face biometric proposed in [41] using random spaces with FAR=0.1179% ranked third in terms of security.

An increase in the sensitivity of the biometrics system means a reduction in FAR value and this usually leads to an increase in FRR. As a low FAR denote good security, a large or high FRR is synonymous with better user convenience or ease of use since the percentage at which authorized users are granted access will be high and a genuine user will not be denied access unnecessarily. Based on Table 5, the percentage of each author’s work in terms of FRR is presented in figure 11.

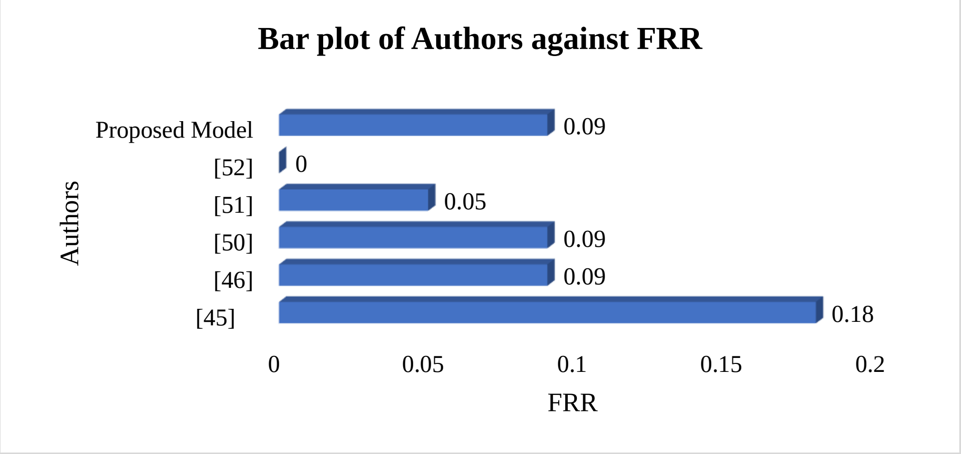


Figure 11: Graphical representation of average FRR by Author

In terms of user convenience, [34] with FRR=0.18% performs best as it has the highest FRR. Research implication of this is that an unprotected biometric system is likely to have better user convenience but lacks better system security as unprotected templates can be stolen. [35] is closely followed by [35], [39] and the proposed fuzzy vault and cuckoo hashing which recorded the same FRR with FRR=0.09% by ranking second as far as user convenience or user-friendliness is concerned. [40], with FRR=0.05% performs better than [41] with the least user convenience that has the lowest FRR=0.0%. The desire or decision for a lower FAR and a higher FRR and vice versa is a tradeoff between security and user convenience in a system.

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

From Table 5, the EER of all studies is also presented in Figure 12. EER is used to measure the overall performance of biometric systems. This is the average of the sum of FAR and FRR. Just like FAR, the lower or smaller the EER, the better the performance of the system.

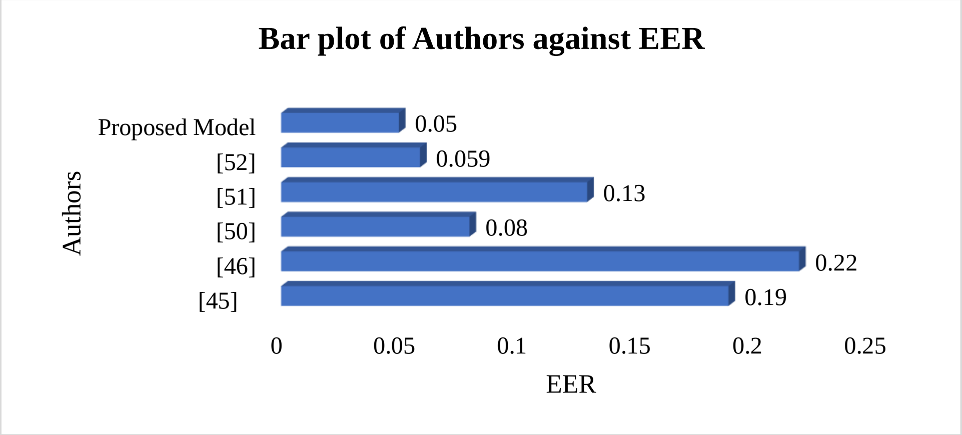


Figure 12: Graphical representation of average ERR by Authors

As seen in Figure 12, the proposed system outperformed the other studies presented as it recorded the lowest EER of 0.05%. [41], [39],[40],[34] and [35] outperform one another in that order with EER=0.059%, EER=0.115%, EER= 0.13%, 0.19% and EER=0.22% respectively. This study shows that the proposed system performs best in terms of security and performance with average user convenience.

5. Conclusion

This study combined fuzzy vault and Cuckoo hashing algorithms as dual-level algorithms to protect fingerprint templates in the database. The proposed algorithm was simulated in MATLAB 2016a environment. Performance evaluation was based on FAR, FRR and EER. From the results generated, the proposed study has a better FAR compared with others with the lowest FAR of 0.01 and a little higher FRR of 0.09 when compared with other studies. The proposed algorithm has the lowest EER of 0.05 as a lower EER denotes better performance. The study also shows that the overall system performance of the proposed Fuzzy vault and Cuckoo hashing outperformed other studies presented in terms of FAR and EER. Further studies can focus on the security analysis of the algorithm in terms of brute force attacks, correlation attacks and blended substitution attacks with different attack scenarios.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

Acknowledgements: The work of Agbotiname Lucky Imoize was supported in part by the Nigerian Petroleum Technology Development Fund (PTDF) and in part by the German Academic Exchange Service (DAAD) through the Nigerian-German Postgraduate Program under Grant 57473408.

References

[1] Ogundokun, R. O., Awotunde, J. B., Adeniyi, E. A., & Ayo, F. E. (2021). Crypto-Stegno based model for securing medical information on IOMT platform. Multimedia tools and applications, 80(21), 31705-31727.

[2] Abikoye, O. C., Ojo, U. A., Awotunde, J. B., & Ogundokun, R. O. (2020). A safe and secured iris template using steganography and cryptography. Multimedia Tools and Applications, 79(31), 23483-23506.

[3] Kavya, R., & George, A. (2018). Survey on encryption approaches for secure face biometrics. In IOP Conference Series: Materials Science and Engineering , 396(1), p. 012-028 . IOP Publishing.

[4] Iloanusi, O. N., & Osuagwu, C.C (2008). Biometric Recognition: Overview and Applications, Nigerian Journal of Technology, 27(2), 36-45.

[5] Boucetta, A., & Boussaad, L. (2022). Biometric authentication using finger-vein patterns with deep-learning and discriminant correlation analysis. International Journal of Image and Graphics, 22(01), 2250013.

Doi: https://doi.org/10.54216/FPA.100201
Received: January 10, 2023 Accepted: March 15, 2023

[6] Oo, A.K & Aung, Z.L (2019). A Robust Fingerprint Recognition Technique Applying Minutiae Extractors and Neural Network, International Journal of Engineering Research and Advanced Technology (IJERAT), 5(3), 78-87.

[7] Gaddam, S. V., & Lal, M. (2011). Development of bio-crypto key from fingerprints using cancelable templates. International Journal on Computer Science and Engineering, 3(2), 775-783.

[8] Adeniyi, A. E., Abiodun, K. M., Awotunde, J. B., Olagunju, M., Ojo, O. S., & Edet, N. P. (2023). Implementation of a block cipher algorithm for medical information security on cloud environment: using modified advanced encryption standard approach. Multimedia Tools and Applications, 1-15.

[9] Khodadoust, J., Medina-Pérez, M. A., Monroy, R., Khodadoust, A. M., & Mirkamali, S. S. (2021). A multibiometric system based on the fusion of fingerprint, finger-vein, and finger-knuckle-print. Expert Systems with Applications, 176, 114687.

[10] Nandakumar, K., & Jain, A.K (2015). Biometric Template Protection: Bridging the performance Gap Between Theory and Practice, IEEE Signal Processing Magazine. 88-100. https://doi.org/10.1109/MSP.2015.2427849.

[11] Mwema, J., Kimwele, M., & Kimani, S. (2015). A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates, International Journal of Computer Trends and Technology (IJCTT), 20 (1) 12-18.

[12] Nandakumar, K., Nagar A., & Jain A.K. (2007). Hardening Fingerprint Fuzzy Vault Using Password. In: Lee SW., Li S.Z. (eds) Advances in Biometrics. ICB 2007. Lecture Notes in Computer Science, 4642. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74549-5_97.

[13] Habibu, T., & Sam, A. E. (2018). Assessment of vulnerabilities of the biometric template protection mechanism. International Journal of Advanced Technology and Engineering Exploration, 5(45), 243-254.

[14] Awotunde, J. B., Abiodun, K. M., Adeniyi, E. A., Folorunso, S. O., & Jimoh, R. G. (2021, November). A Deep Learning-Based Intrusion Detection Technique for a Secured IoMT System. Communications in Computer and Information Science, 2022, 1547 CCIS, pp. 50–62.

[15] Awotunde, J. B., Chakraborty, C., & Adeniyi, A. E. (2021). Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection. Wireless Communications and Mobile Computing, 2021, 2021, 7154587.

[16] Gavrilova, M., Luchak, I., Sudhakar, T., & Tumpa, S. N. (2022). Artificial Intelligence in Biometrics: Uncovering Intricacies of Human Body and Mind. In Advances in Selected Artificial Intelligence Areas (pp. 123-169). Springer, Cham.

[17] Dong, X., Jin, Z., Zhao, L., & Guo, Z. (2021, August). BioCanCrypto: An LDPC coded bio-cryptosystem on fingerprint cancellable template. In 2021 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-8). IEEE.

[18] Awotunde, J. B., Jimoh, R. G., Folorunso, S. O., Adeniyi, E. A., Abiodun, K. M., & Banjo, O. O. (2021). Privacy and security concerns in IoT-based healthcare systems. Internet of Things, 2021, pp. 105–134.

[19] Ashiba, H.I, & Abd El-Samie, F.E (2020). Implementation face based cancelable multi-biometric system, Multimedia Tools and Applications, 79, 30813–30838.

[20] Panwar, A., Singla, P., & Kaur, M. (2018). Techniques for enhancing the security of fuzzy vault: a review Progress in Intelligent Computing Techniques: Theory, Practice, and Applications (205-213): Springer.

[21] Awotunde, J. B., Fatai, O. W., Akanbi, M. B., Abdulkadir, S. I., & Idepefo, O. F. (2014). A Hybrid Fingerprint Identification System for Immigration Control Using the Minutiae and Correlation Methods. The Journal of Computer Science and its Applications, 21(2), 97-108.

[22] Bedari, A., Wang, S., & Yang, W. (2021). Design of cancelable MCC-based fingerprint templates using Dyno-key model. Pattern Recognition, 119, 108074.

[23] Xi, K., Ahmad, T., Han, F., & Hu, J. (2011). A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment. Security and communication networks, 4(5), 487-499.

[24] Mahendran, R. K., & Velusamy, P. (2020). A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things. Computer Communications, 153, 545-552.

Received: January 10, 2023 Accepted: March 15, 2023

[25] Ponce-Hernandez, W., Blanco-Gonzalo,R., Liu-Jimenez,J. & Sanchez-Reillo, R. (2020). Fuzzy Vault Scheme Based on Fixed-Length Templates Applied to Dynamic Signature Verification, IEEE Access, 8, 11152-11164.

[26] Machado, S., D'silva, P., D'mello, S., Solaskar, S., & Chaudhari, P. (2018). Securing ATM Pins and Passwords Using Fingerprint Based Fuzzy Vault System. Paper presented at the 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA).

[27] Morampudi, M. K., Prasad, M. V., & Raju, U. S. N. (2020). Privacy-preserving iris authentication using fully homomorphic encryption. Multimedia Tools and Applications, 79(27), 19215-19237.

[28] Loukhaoukha, K., Refaey, A., Zebbiche, K., & Shami, A. (2018). Efficient and secure cryptosystem for fingerprint images in wavelet domain. Multimedia Tools and Applications, 77(8), 9325-9339.

[29] Kaur, M., & Sofat, S. (2016). Secure fingerprint fuzzy vault using hadamard transformation to defy correlation attack. In 2016 Sixth International Symposium on Embedded Computing and System Design (ISED) (pp. 122-126). IEEE.

[30] Li, H., Qiu, J., & Teoh, A.B.J (2020) Palmprint template protection scheme based on randomized Cuckoo hashing and MinHash, Multimedia Tools and Applications,79(17-18) 11947-11971.

[31] Ghammam, L., Barbier, M., & Rosenberger, C. (2018). Enhancing the security of transformation based biometric template protection schemes. In 2018 International Conference on Cyberworlds (CW) (pp. 316-323). IEEE.

[32] Joshi, M., Mazumdar, B., & Dey, S. (2020). A Comprehensive Security Analysis of Match-in-Database Fingerprint Biometric System, Pattern Recognition Letters, 138,247-264.

[33] Chitra, D., & Sujitha, V. (2018). Security analysis of prealigned fingerprint template using fuzzy vault scheme. Cluster Computing, 22(5), 12817-12825.

[34] Debnath, R., Nandi, S., & Majumder, S. (2021). Fingerprint Authentication System for BaaS Protocol. In Applications of Internet of Things (pp. 39-48). Springer, Singapore.

[35] Saputra, J., & Sukarno, P. (2019). Improving The Accuracy of Fuzzy Vault Scheme in Fingerprint Biometric. In 2019 7th International Conference on Information and Communication Technology (ICoICT) (pp. 1-8). IEEE.

[36] S. A & AnilKumar, K.S. (2020) Iris Template Protection using Double Bloom Filter Based Feature Transformation, Computers & Security 97, 1-15.

[37] Prasad, M. V., Anugu, J. R., & Rao, C. (2016). Fingerprint template protection using multiple spiral curves. Paper presented at the Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics.

[38] Kim, J., & Teoh, A. B. J. (2018). One-factor cancellable biometrics based on indexing-first-order hashing for fingerprint authentication. Paper presented at the 2018 24th International Conference on Pattern Recognition (ICPR).

[39] Wang, N., Li, Q., Han, Q., Abd El-Latif, A. A., & Niu, X. (2011, October). A novel multi-division template protection (mdtp) scheme for iris recognition based on fuzzy vault. In 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (pp. 101-104). IEEE. doi: 10.1109/IIHMSP.2011.66.

[40] Sharma, D., & Selwal, A. (2020, May). A Novel Transformation Based Security Scheme for Multi-instance Fingerprint Biometric System. In International Conference on Information, Communication and Computing Technology (pp. 147-159). Springer, Singapore.

[41] Dabbah, M. A., Dlay, S. S., & Woo, W. L. (2008, April). PCA authentication of facial biometric in the secure randomized mapping domain. In 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications (pp. 1-5). IEEE.

Doi: https://doi.org/10.54216/FPA.100201

Received: January 10, 2023 Accepted: March 15, 2023