Finger Knuckle Print Recognition using MMDA with Fuzzy Vault

MuthuKumar Arunachalamand and Kavipriya Amuthan
Department of Electronics and Communication Engineering, Kalasalingam Academy of Research Education, India

Abstract: *Currently frequent biometric scientific research such as with biometric applications like face, iris, voice, hand-based biometrics traits like palm print and fingerprint technique are utilized for spotting out the persons. These specific biometrics habits have their own improvement and weakness so that no particular biometrics can adequately opt for all terms like the accuracy and cost of all applications. In recent times, in addition, to distinct with the hand-based biometrics technique, Finger Knuckle Print (FKP) has been appealed to boom the attention among biometric researchers. The image template pattern formation of FKP embraces the report that is suitable for spotting the uniqueness of individuality. This FKP trait observes a person based on the knuckle print and the framework in the outer finger surface. This FKP feature determines the line anatomy and finger structures which are well established and persistent throughout the life of an individual. In this paper, a novel method for personal identification will be introduced, along with that data to be stored in a secure way has also been proposed. The authentication process includes the transformation of features using 2D Log Gabor filter and Eigen value representation of Multi-Manifold Discriminant Analysis (MMDA) of FKP. Finally, these features are grouped using k-means clustering for both identification and verification process. This proposed system is initialized based on the FKP framework without a template based on the fuzzy vault. The key idea of fuzzy vault storing is utilized to safeguard the secret key in the existence of random numbers as chaff pints.*

Keywords: *Finger Knuckle Print (FKP),2D Gabor filter, Multi-Manifold Discriminant analysis (MMDA),Fuzzy Vault*

Received January 5, 2018; accepted December 17, 2019
https://doi.org/10.34028/iajit/17/4/14

1. Introduction

At present, all are periodically asking for the authentication of individual identity, that is happens well through the adoption of pass code when enabling activities in public security, access control, application log on, etc., The enigma of classic protection evokes the shield of system elements. Hence, these securities can be easily breached, when a pass code is exhibited or any cards are hijacked. Furthermore, many of the people employ similar key over different applications e.g.,: A faker upon definite on a single pass code could ingress numerous applications. Fascicle pass code can be efficiently suggested, whereas crucial pass code may be firm to recollect and therefore pass codes are shattered by naive reference strikes. The urge for a stable user with authentication techniques has seasonable development for the use of several about security and prompts progression in networks, communication, and mobility. This kind of constraint associated with the benefit of pass code can be reformed by the incorporation of superior methods for user verification. This Biometrics proceeds with several fields of research in the present world scenario and it has been dedicated to the identification of individuals using one or several intrinsic physical or behavioural attributes. In the midst of these biometric technologies, hand-based biometrics including fingerprint, hand geometry, vein, etc are considering most prevalent and will have a heavy share in the particular biometrics market. This will happen because of the auspicious happenings of these biometric traits such as minimum cost, low-resolution imaging, and other firm features. In the above biometrics technologies, Finger Knuckle Print (FKP) has fascinated much concern in the biometrics research community. Meanwhile, FKP [1] is also highly peculiar so that it can be treated as a unique one when compared with traditional biometrics techniques like faces, fingerprints, and voices. There is no smear of illegal acceptance rate associated with FKP so that FKP has an eminent user acceptance rate. Hence this paper reveals that FKP is examined to be one of the assuring biometric techniques for personnel identification in the present& future.

It is noteworthy that Kumar and Ravikanth [7] developed a new approach for the finger knuckle surface that is normalized to minimizing the effect of scale, translation, and rotation. This system introduces peg free imaging for every knuckle image for calculating the time with Linear Discriminant Analysis (LDA), Principal Component Analysis (PCA) Techniques Matching scores are mainly calculated for the identification purposes. Feizollah *et al.* [4] develops in evaluating the achievement of two or more clustering

algorithm that is k-mean and Minibatch k-means for the process of detecting the normal and malicious result from the Malgenome data sample. Badrinath *et al.* [2] presents a new combination of local information that is subjected to scales, rotation, and features of FKP are extracted based on Scale Invariant Feature Transform (SIFT) and Speeded Up Robust Features (SURF) transforms mainly done by nearest neighbour -ratio method and fused with a weighted sum-rule system which performs Crossover Rate (CRR) of 100% with Equal Error Rate (EER) as 0.215%.Similarly, Li *et al.* [9] gives a novel solution for the encrypted generation of keys. Based on the limitation of entropy-based security, this system assigns a new security analysis framework as a multi-biometric cryptosystem. It improves eminent authentication accuracy associated with a cryptosystem on unique biometric. Numerous schemes have been suggested in the literature for enforcing the cryptosystem framework as Fuzzy Vault. Jules and Sudan [5] developed a novel cryptographic construction named the fuzzy vault. It mainly deals with features of order invariance that is against an unbounded attacker with security. Koptyra and Ogiela [6] presents a unique idea of hiding the secrets using the fuzzy vault. It is mainly hidden the noisy data based on multi-biometric cryptosystem. It proposes a choice of authentication accuracy relevant with a cryptosystem on single biometric. Bae *et al.* [3] shows the encoding of iris code that helps in the performance of EER that gives the magnitude performance for iris size along with processing time. Uludag and Jain [11] aims in the security and privacy of biometric systems with the transformed version of a template that is stored as a cryptographic framework. So they introduce the orientation field of helper data for the extraction of fingerprints.

Yang *et al.* [13] proposed the dimensionality reduction method for pattern recognition purposes that is based on graph embedded learning. This technique mainly based on the construction of low dimensional data. Basically, it cannot be applied for small size problems. To overcome this, MMDA is calculated for Eigenvectors and Eigenvalue representations. Yang *et al.* [12] has attracted interest against the Gabor feature with MMDA. Certain Fuzzy vault system [5] is generally on the basis of local iris features from the exact values of the unordered set with basis if shift matching technique

The rest of the paper is organized as follows .Section 2and3 introduces the overview of proposed work and it describes the Fuzzy Vault which includes extraction of FKP with Gabor feature and grouped according to k-Means clustering algorithm in a detailed manner and Section 4 gives the details regarding the basic Fuzzy Vault construction with enrolment and verification phase. Experimental results are basically explained in Section 5and in Section 6 fully compile the basic work that provides points for future research.

2. Proposed Work

This paper also devises a distinct strategy for polynomial construction in generating the chaff points in both locking and the unlocking set for the pursuit of a fuzzy vault system. Figure 1 deliberates the proposed block diagram of the overall process in Fuzzy Vault generation with FKP. This block diagram illustrates the cryptographic fuzzy vault technique as two phases: The enrolment phase and the verification phase. In the enrolment phase, Gabor feature extraction is carried with five scales and eight orientations. The extracted features are high dimensional data values. To minimize this, MMDA is generated from LDA to calculate Eigen values and Eigen vectors feature and MMDA which is explained below in this block diagram with performance analysis.

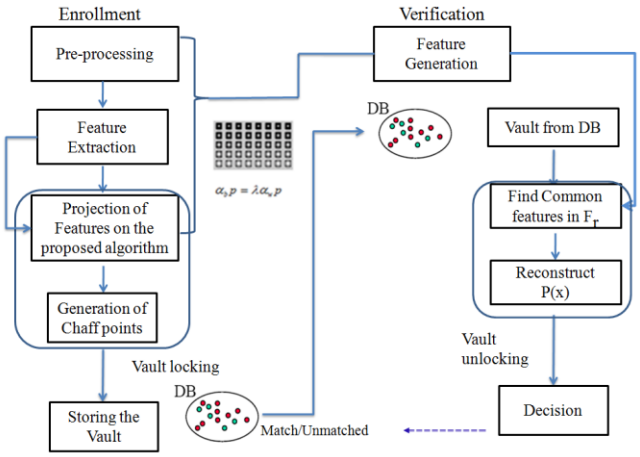

Figure 1. Proposed block diagram of Gabor feature generation with MMDA using fuzzy vault.

These features are clustered based on the points that are based on the manifold learning process. Further, this leads to the generation of chaff points of secret key for the vault locking process i.e., they are stored as the collapsed form in the vault. The locking process involves the polynomial generation of chaff points as the key that is entered. Similarly in the Verification phase, the same feature process is repeated as in the enrolment process to find out the common features and matching is done for revealing the secret key along with the biometrics.

3. Feature Extraction using Gabor Feature and MMDA

Gabor feature extraction with spatial locality and orientation selectivity is done with FKP images. Gabor wavelet formation is developed where kernels are identical to the field of several profiles that exhibit desirable, traits of spatial locality and orientation selectivity. By Yang *et al.* [13] Gabor wavelet determination is to be defined as

$$\Psi_{u.v}(z)=\frac{\left\|k_{u,v}\right\|^2}{\sigma^2}e^{\left(-\left\|k_{u,v}\right\|^2\|z\|^2/2\sigma^2\right)}\left(e^{ik_{u,v}z}-e^{-\sigma^{2}/2}\right) \quad (1)$$

Where u,v delineate the orientation and scale of Gabor kernels $\|.\|$ defines the norm operator. It is defined as

$$k_{u,v}=k_v e^{i\psi u} \quad (2)$$

$$\text{Where } k_v=k\max/2^{v/2} \quad (3)$$

$$\text{and } \phi_u=u\left(\frac{\Pi}{8}\right) \quad (4)$$

Which defines that where k max represents the highest frequency and f depict the spacing vector that is based on five different scales as?

v= {0,1....4}u={0,1....8}and it is represented based on the convolution factor as

$$G_{u,v}(z)=I(Z)*\psi_{u,v}(Z) \quad (5)$$

Convolution of Gabor function is defined as

Z= (*x*,*y*) represents the ultimate image position and * illustrates the convolution operator and $G_{u,v}$=(*Z*) declares the convolution result denotation

$$G_{u,v}(z)=A_{u,v}(z)\exp\left(i\theta_{u,v}(z)\right) \quad (6)$$

That shows the $A_{u,v}(z)$ single magnitude method $\left(i\theta u_{u,v}(z)\right)$as a phase method. Therefore the set represents in the form as

$$S=\left\{A_{u,v}(Z):U\xi\{0,1..7\},v\xi\{0,1...4\}\right\} \quad (7)$$

That helps in the Gabor feature representation. For encompassing different spatial frequencies, this paper concatenates the results with the augmented feature vector X. To solve this down sampling, the denotation $A_{u,v}$=(*Z*) by ρ for reducing the space dimension and form the normalization to zero mean and unit variance. Construction of vector $A_{u,v}$=(*Z*) by concatenating the rows and column-like $A_{u,v}(z)(\rho)$denotes the normalized vault construct. Gabor feature extraction as

$$A^{(\rho)}=\left(A_{0.0}^{\rho(t)},A_{0,1}^{(\rho)t}.....A_{4,7}^{(\rho)t}\right) \quad (8)$$

Where 't' represents the operation based on transpose for the Gabor feature extraction process.

The second idea deals with the projection of linear dimensional space. The motivation of this Discriminant analysis is to keep the class labeling after the process of graph embedding algorithm. In other words, considering the points that are close or far from each other from various classes to be named as within-class graph G_W and between-class graph G_B,

- **MMDA**

Collect the Sample Data Set with the class label

$$A^{(\rho)}=\left[A^{(\rho)}{}_1,A^{(\rho)}{}_2.....A^{(\rho)}{}_n\right]A_i\sum R^m \quad (9)$$

as A1,A2 introducesthe label with several datasets

Linear projection of low dimensional space

$$B=P^T A^{(\rho)} \quad (10)$$

$$B=\left[B_1B_2,.....B_n\right]B_i,\sum R^d$$

$$d<<m \quad (11)$$

Considering the points with a similar class label where this edge construction normally happens between the nodes Y_i and y_j from the identical class. Therefore the similarity can be defined as

Edge construction

$$cij=\left\{\exp\left(\left\|-y_i-y_j{}^2\right\|/t\right)\right\} \quad (12)$$

It is broadly utilized in manifold learning such as Yi and yj and its parameter

$$o\le c_{ij}\le 1$$

The weight function is strict with monotonically decreasing function *Yi* and *yj*

Obviously, it is noted that α_W and α_b are non-negative symmetrical matrices that are represented by the matrices for maximizing the between-class and between-class scatter in MMDA subspace whose main objective function is defined as

$$J(P)=Arg_p\max\equiv\frac{J_B(P)}{J_W(P)} \quad (13)$$

$$\frac{P^T\alpha_b P}{P^T\alpha_W P}$$

The projection matrix is generally represented by

$$\alpha_b p=\lambda\alpha_w p \quad (14)$$

This projection matrix is generally a graph embedded learning method MMDA and it can be based on Fisher Discriminant Analysis which is denoted by Eigenvalue. This value is clustered by k-means clustering by calculating the Centroid points and assigns the points to clusters

3.1. k-means clustering

Clustering is mainly used to classify based on the performance of unsupervised classification of several patterns into groups. Considering based on the size of input and classification in larger quantity, k- Means focus on the execution that migrates the process on the

basis of finger knuckle points on the priority of k groups. Further, it is done based on the Centroid calculation and assigning objects to the group. Hencek-means basically target to partition observations to k-clusters (Nearest mean) prototype of the cluster as k<n. Basically, it is similar to the expectation-maximization algorithm for mixtures of gaussian and that deals with the process finding clusters in data based on object attributes from a vector space

$$J = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i^{(j)} - c_j \right\|^2 \qquad (15)$$

Where J Represents the Objective function that is to defined based on the number of cases and centroid for the cluster points that is based on the Euclidean distance based on the distance measure as classification of objects

Procedure: k-Means classification

- *Input:* kand $c_1.c_2.....c_k$; Clustering the data into several k groups where k is predefined
- *Cluster Update* :Selecting k points at random cluster centres
- *Centres Update*: Assigning objects to the closest cluster centre to determine according to the Euclidean distance function
- *Stopping Update* :Calculate the centroid points or mean of several FKP key points' objects in each cluster.
- *Output* :Repeating the steps 2, 3 until similar points that are assigned to each cluster

4. Fuzzy Vault for Securing and Revealing:

Biometrics-based authentication helps to enhance the security of a user's identity and applied to a variety of fields until now. Since the compromises of data are permanent, the security of data is important. Taking this into account, storing of data is a non-invertible version for the blockage of unauthorized access. Fuzzy vault is basically a cryptographic construction proposed by Jules and Sudan [5] to secure the critical information with biometric data.

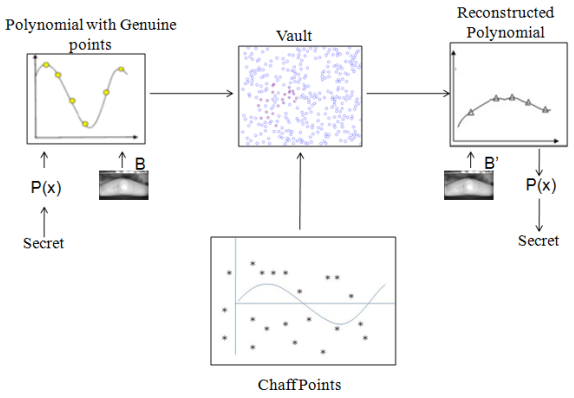

Figure 2. Block diagram of Fuzzy Vault Construct.

Figure 2 shows the polynomial with genuine points that stores the secret key as "B". This secret information is distributed in the vault as unordered sets with the polynomial construction of chaff points. These chaff points show the content of secure information to be reconstructed and reveals the secret code. This idea is generally based on the standard cryptographic technique that is developed by Jules and Sudan [5] and helps in securing important secret information.

The locking algorithm denotes the parameters used for sharing the secret key based on the set of points. This shows the locking algorithm steps for securing the key for the case of polynomial construction as chaff points and to secure the key in the vault.

Algorithm 1: LOCKING THE VAULT

Input: # *Parameters n, t, r so that* $n \le t \le r \le q$

 # Secret key $k \sum F^K$

For $B = \{bi\}_{i=1}^{t}$

{

#values $bi \sum F$ *are distinct.*

}

Output: The set 'B' contains the points 'S' of fuzzy vault (F) Points

For

{

$F = \{s(m, r, q)\}$

}

Algorithmic STEPS:

#Input parameters X, S, $F \leftarrow \phi$

$P \leftarrow K$ *K blocks are encoded into a polynomial of degree function n in fq as its coefficients*

For i= (1 to t)

{

$(x_i, y_i) \leftarrow (b_i\, p(b_i))$

$X \leftarrow X \cup \{x_i\}$

$S \leftarrow S \cup \{(x_i, y_i)\}$

For i= (t+1 to r)

$\sum_u F_q / x$

For each $X \leftarrow X \cup \{x_i\}$

For each $y_i \sum_u F_q \{p(x_i)\}$

$S \leftarrow S \cup \{(x_i, y_i)\}$

}

}

Output: Return $FV = \{s(m, r, q)\}$

Information about the order x_i is safely chosen. The set S is in a predetermined order as output. The points in the sets are developed to be arranged in x-coordinates as random manner. Chaff point in the locking algorithm is selected to intersect either B or P. Generally FV Combining S and (m, r, q) is named as Fuzzy vault.

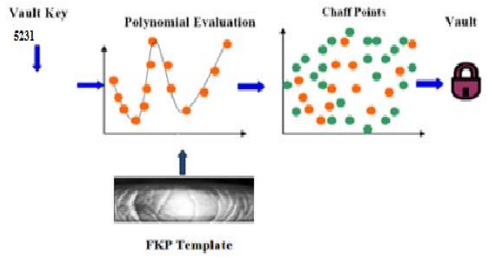

Figure 3. Block diagram of Fuzzy Enrolment construct.

This Figure 3 shows the enrolment phase of the fuzzy vault that shows the performance of construct which includes generation of chaff points on the construction of polynomial equation and the secret key is stored in the vault

The unlocking algorithm denotes the parameters used for revealing the secret key based on the set of points. This shows the decoding part for the set that includes the polynomial reconstruction that helps to show the secret information content and to classify the authorized or unauthorized person

Algorithm 2:UNLOCKING THE VAULT:

Input**:** #Parameters set (m, r, q)

Such that $m \le r \le q$ and the set of points S

#For Each Query set B'= $\{b'_i\}_{i=1}^{t}$ with following $b'_i \sum F_q$

Output: # $K' \sum F_q^n \cup ('null')$

Algorithmic Steps:

$Q \leftarrow \phi$

For i= (1 to t)

{

If there exists some $y_i \sum F_q$ *such that* $(b'_i, y_i) \sum S$ *)*

$Q \leftarrow Q \cup (b_i' y_i)$

For SET K' $\leftarrow Null$

{

else if

Q > n points.

Else

$K' \leftarrow RSDECODE(N, Q)$

}

}

Output K'

Assuming Fuzzy vault (V) is constructed by both Alice and Bob who tries to unlock V to recoup the key k. If bob using his set B' to resolve the secret word which is encoded with k for having the possible key k'. The set B discriminates the coordinates of genuine points on polynomial equation P. If B is close to B' it may help to identify the bulk of correct points However disparity between Alice and Bob will result in an error. This error is removed by the decoding algorithm if the majority of the keys overlap with each other

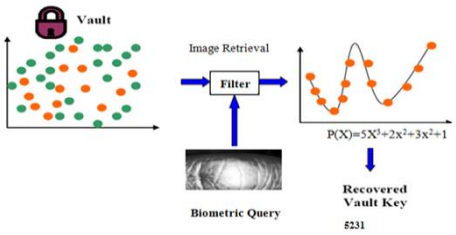

Figure 4. Block diagram of Fuzzy Verification Construct.

Figure 4 shows the Verification phase of the fuzzy vault that shows the performance of construct which includes regeneration of chaff points on the reconstruction of a polynomial equation and the secret key is retrieved which is stored in the vault based on the performance of biometric query and filter range.

5. Results and Discussion:

The performance of the FKP images is collected from the PolyU database and includes two phases; Enrolment and verification. The samples selected as the input image for the process of fuzzy vault implementation that includes enhancement process along with the feature extraction of Gabor and MMDA. These Samples are categorized on the basis of several FKP as left index, right index, right middle, left middle with the Performance analysis for the Eigen values, Eigenvector Based on the Figure 5 shows the FKP acquisition details of input image with Region of Interest of size 256*256 is used for enhancement process which helps for Gabor feature extraction and Figure 6 shows the real parts and magnitude of Gabor feature with five scales and eight orientation for feature extraction process that gives feature points for MMDA in case of Dimensionality Reduction, which helps for the further clustering process like k-means to calculate Eigen values, Eigenvectors, output of MMDA Analysis on the basis of performance.

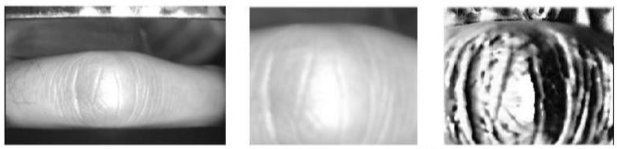

Figure 5. Results of FKP for ROI and Enhanced Image.

This Figure 5 shows the basic pre-processing step that involves the enhanced image which undergoes the histogram equalization

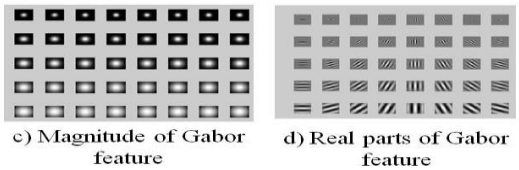

Figure 6. The magnitude and Real parts of Gabor feature.

This Figure 6 shows Gabor feature extraction that includes the real and magnitude of FKP image which helps in dimensionality reduction that is stored as a secret key.Table.1 shows the performance of MMDA for the process of several FKP as a left index, right index, right middle, right index and the values of Eigen values and Eigenvectors including the mean and output of MMDA with reference to the knuckle data and moreover dimensionality data is minimized for the better performance in MMDA.

Table 1.Feature points of Left Middle FKP using MMDA

Left Middle			
X1	**Y**	**Mean of MMDA**	**V**
13.6215	0.2001	3.584	8.7438
13.3551	0.2012	3.5744	9.8427
13.4897	0.2008	3.5813	8.1556
8.9231	0.2167	3.2357	8.6963
9.3106	0.217	3.2564	8.6228
9.6227	0.2196	3.2629	8.3669
10.8539	0.2208	3.2771	1.1342
16.096	0.2076	3.3019	1.2587
11.5215	0.0325	3.2326	1.2327
12.519	0.2137	3.2576	1.2959
16.226	0.2077	3.3009	1.1723
16.577	0.2071	3.3169	1.199

Table 2. Feature points of Right Middle FKP using MMDA

Right Middle			
X1	**Y**	**Mean of MMDA**	**V**
10.3751	0.182	3.1755	1.0679
11.6064	0.1844	3.159	1.0359
11.2311	0.2042	3.1947	9.2662
12.0204	0.2022	3.1385	8.982
11.2278	0.205	3.1478	8.9008
14.6373	0.2004	3.1397	1.0073
9.2064	0.2087	3.2387	9.0028
11.7934	0.207	3.298	1.0185
11.3776	0.2062	3.2716	9.4824
12.2899	0.2067	3.2915	1.0316
11.9873	0.0286	3.2337	8.9078
13.0249	0.2054	3.3095	9.7805

Table 3. Feature points of Left Index FKP using MMDA

Left Index			
X1	**Y**	**Mean of MMDA**	**V**
11.7946	0.2039	3.2886	7.9097
10.6153	0.2056	3.2635	9.4262
11.282	0.2033	3.2777	9.7116
12.764	0.2069	3.1816	1.2975
13.3815	0.2014	3.2385	1.2862
10.5839	0.204	3.2265	1.2402
10.5333	0.1963	3.3458	1.2862
14.021	0.2055	3.3622	1.2256
9.0504	0.2083	3.2819	1.1925
13.2864	0.2094	3.3575	1.238
13.3918	0.2071	3.348	1.2284
10.5333	0.1963	3.3458	1.1977

Table 4. Feature points of Right Index FKP using MMDA.

Right Index			
X1	**Y**	**Mean of MMDA**	**V**
9.3399	0.1875	3.2193	1.0457
11.4272	0.1765	3.2294	1.1807
10.864	0.177	3.2208	1.1426
10.8656	0.1894	3.2265	1.0812
11.5142	0.1798	3.1878	1.101
11.0206	0.1824	3.1996	1.1424
13.6526	0.2123	3.3085	9.5968
12.0837	0.205	3.2789	9.8795
12.0115	0.0505	3.2895	8.9986
11.9166	0.2123	3.2827	9.3657
13.4738	0.209	3.2974	9.7161
13.3624	0.2112	3.3012	9.2687

Table 5. Performance Metrics of FKP

	FAR	**FRR**	**EER**	**GAR**	**Avg Encoding Time (ms)**	**Avg Decoding Time (ms)**
Left index	0.0024	3.95	0.23	97.11	95	99
Left middle	0.0013	1.94	0.16	98.01	89	95
Right index	0.0016	2.82	0.2	96.14	92	98
Right middle	0.0059	4.3	0.28	94.1	94	93

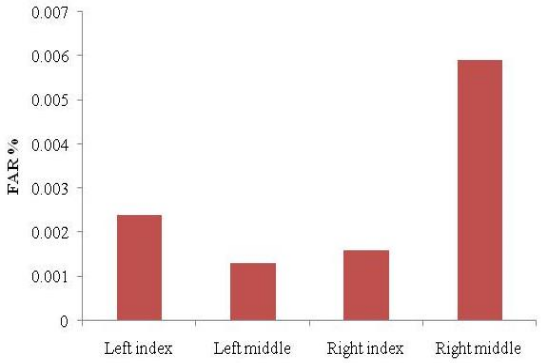

Figure 7. FAR Performance of Fuzzy Vault.

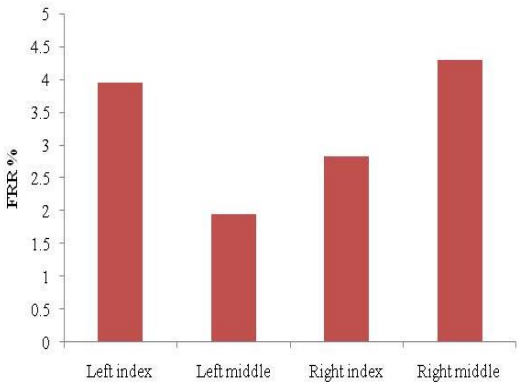

Figure 8. FRR Performance of Fuzzy Vault.

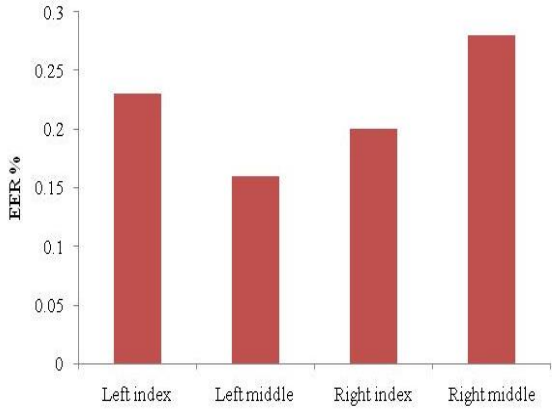

Figure 9. EER Performance of Fuzzy Vault.

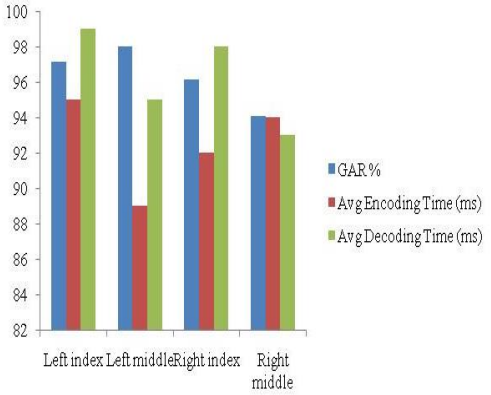

Figure 10. GAR Performance and authentication time Of Fuzzy Vault.

Figure 7 shows the performance of the various data sets, with 12 samples per various Finger Knuckle Print. Herewith it shows that the right middle FKP shows a high False Accept Rate (FAR) percentage (0.0059) compared to other datasets. Similarly, the graph Figure 8 shows the Rejection Rate (FRR) performance for left index and right middle of nearly (3.95-4.30)and the error rate also helps to identify the performance between FAR and FRR intersection performance has EER performance among the finger knuckle set in Figure 9 GAR shows the performance of genuine accept rate performance in the Figure 10 with (94.10-98.01) and the encoding and decoding time is calculated for every key retrieval steps as encoding time as min as 89 ms-95 and decoding time calculated as (93-1)

6. Conclusions

The schemed approach plan helps to boost the pattern template shield using the avail of fuzzy vault construction. Basically, inputs of the FKP Images are originally refined relevant for equating the image and frame it capable of the process of feature extraction. Moreover, feature extraction is borne to possess Eigen Vector and Eigenvalue representation with MMDA output values. This feature vector initializes the clustering process and undergoes the cluster centroid performance and the features together with the key that forms the fuzzy vault construction which is accumulated in the database as the enrolment phase. In the authentication phase, the features of the test image are perfected and equalled to vault in the database. If all the points in the test image feature pair, then the secure key are retrieved with minimum decoding time in the right middle FKP based on their performance. Henceforth this idea can be implemented in other biometric like Ear to improve their recognition accuracy based on the Secret key Performance with chaff points.

Acknowledgment

We thank the department of electronics and communication Engineering of (Kalasalingam Academy of Research and Education),Tamil Nadu, India for permitting to use the computational facilities available in the centre for research in signal processing and VLSI Design which was setup with the support of the Department.

References

[1] Arunachalam M. and Subramanian K., "AES Based Multimodal Biometric Authentication using Cryptographic Level Fusion with Fingerprint and Finger Knuckle Print," *The International Arab Journal of Information Technology*, *vol.* 12, no. 5, pp. 431-440, 2015.

[2] Badrinath G., Nigam A., and Gupta P., "An Efficient Finger Knuckle Print-Based Recognition Fusing SIFT and SURF Matching Scores," *in Proceedings of International Conference on Information and Communications Security*, Kanpur, pp. 274-484, 2011.

[3] Bae K., Noh S., and Kim J., "Iris Feature Extraction Using Independent Component Analysis," *International Conference on Audio- and Video-Based Biometric Person Authentication*, *Guildford*, pp. 838-844, 2003.

[4] Feizollah A., Anuar N., Salleh R., and Amalina F., "Comparative Study of K-Means and Mini Batch K-Means Clustering Algorithms in Android Malware Detection Using Network Traffic Analysis," *International Symposium on Biometrics and Security Technologies*, pp. 193-197, 2014.

[5] Jules A. and Sudan M, "A Fuzzy Vault Scheme," *in Proceedings IEEE International Symposium on Information Theory*, Lausanne, pp. 237-257, 2006.

[6] Koptyra K. and Ogiela M., "Fuzzy Vault Schemes in Multi-Secret Digital Steganography," *in Proceedings of 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, pp. 183-186, 2015.

[7] Kumar A. and Ravikanth C., "Personal Authentication Using Finger Knuckle Surface,"

IEEE Transactions on Information Forensics and Security, vol. 4, no.1, pp. 98-110, 2009.

[8] Lee Y., Park K., Lee S., Bae K., and Kim J., "A New Method for Generating An Invariant Iris Private Key Based on the Fuzzy Vault System," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 38, no. 5, 2008.

[9] Li C., Hu J., Pieprzyk J., and Susilo W., "A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multi-biometric Cryptosystems Based on Decision Level Fusion," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1193-1206, 2015.

[10] Nandakumar K., Jain A., and Pankanti S., "Fingerprint-Based Fuzzy Vault: Implementation and Performance," *IEEE Transactions on Information for Ensics and Security*, vol. 2, no. 4, pp. 744-757, 2007.

[11] Uludag U. and Jain A., "Securing Fingerprint Template: Fuzzy Vault with Helper Data," *in Proceedings of Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, New York, pp. 163-163, 2006.

[12] Yang W., Sun C., and Wang Z., "Finger Knuckle Print Recognition Using Gabor Feature and MMDA," *Frontiers of Electrical and Electronic Engineering*, vol. 7, no. 4, pp. 374-380, 2012.

[13] Yang W., Sun C., and Zhang L., "A Multi-Manifold Discriminant Analysis Method for Image Feature Extraction," *Pattern Recognition*, vol. 44, no. 8, pp. 1649-1657, 2011.

[14] Zhang L., https://www4.comp.polyu.edu.hk/~biometrics/FKP, Last Visited, 2018.

Muthukumar Arunachalam received BE (ECE), ME (Applied Electronics) degrees from Madurai Kamaraj University and Anna University in 2004 and 2006 respectively and PhD from Kalasalingam University, India. He is an Associate Professor Electronics and Communication Engineering, in Kalasalingam University, India, where he has been since 2007. His area of interest is Image processing, signal processing, biometrics, and wireless communication. He is a life member of ISTE.

Kavipriya Amuthan received BE (ECE) and ME (Digital Communication and Networking) degrees from Kalasalingam Academy of Research and Education, in 2013 and 2015 respectively. Currently, she is pursuing as PhD full-time scholar in ECE at Kalasalingam Academy of Research and Education, India. Her area of interest is Image processing, Biometrics, Cryptography and Network Security.