Journal of Computational Algorithms and Information Technology

*Article*

# A Novel Multimodal Key-Binding Biocrypto-System with Least-Square Polynomial Curve-Fitting for Feature-Level Fusion

**Avik Ho Han*** **and Dae Kyung Sohn**

Sogang University, South Korea.

* Correspondence: avik.de96@yahoo.com

Received: 12 September 2024; Accepted: 25 October 2024; Published: 5 November 2024.

**Abstract:** In last few years, many works has been proposed using multimodal biometric system because of its high performance as compare to unimodal biometric systems. Most of the Multimodal Biocrypto-System (MBS) have been previously proposed to securely share secret-key over the network, but these systems uses complex signal processing techniques like DFT, SVM, neural network etc. based fusion techniques and relatively low performance. Therefore, we propose simple and effective but mathematically irreversible statistically based new feature level fusion technique using Least-Square Polynomial Curve-Fitting (LPC) for the proposed efficient Multimodal Key-Binding Biocrypto-System (MKBB). We validate the effectiveness of proposed technique over the fuzzy vault scheme using biometrics fingerprint and iris datasets. This proposed system is implemented to protect the user's cryptographic secret-key and effectively remove the use of public key infrastructure (PKI) system because of its complex certification issuing and distributing management costs, and centralized structure which uses convention network system and shows single point of failure. We also evaluate the overall performance system to successfully retrieval of key with the help of AES-256 algorithm to perform encryption and decryption. The experimentations is done using fingerprint FVC2002DB_1 and Iris CASIA-IrisV1 datasets. The system gives the 99.96% of accuracy, with 99.98% of GAR and 0% FMR.

**Keywords:** Multimodal Key-Binding Biocrypto-System, fuzzy vaul

---

## 1. Introduction

Most of the organization, who need data privacy are fighting against the security and authentication vulnerabilities of the existing confidentiality and authentication systems due to cryptographic secret-key compromising because end users need to share keys over the internet and have to recorded for remember somewhere in offline line mode or written in diary. One efficient approach to protect cryptographic key is PKI system, which also has many difficulties such as failure of PKI system due network attacks like men-in-the-middle and Denial of service, its complex implementation of certification issuing and distributing management system, and centralized structure with single point of failure [1].

The original basic PKI model consists some specific software modules, hardware components, security and privacy related policies with the experts to implement this model. A trusted third party Certificate Authority (CA) provide a digitally signed certificate for each user for its public-private key pair, which are independent from user's identity [2]. The PKI model is the client-server based distributed model, so the certificates formation, delivering and cancellation very high complex and time taking, network related issues such as network congestion, attacks over the network. Therefore management of deploying the traditional PKI model is very difficult in exercise. Another problem with the tradition PKI model that must be considered seriously is that, some other vulnerabilities e.g. the malware systems can compromise certificate issuing software and create duplicitous certificate demand or appear as authentic access to core certificate issuing systems to issue certificate. All of these consequences demands a system that can overcome this influence on security systems and determine a trust and protected system for key management [3]. Several work already done by different authors to improve performance and security of traditional PKI [4].

The biocrypto-system (BCS) is the recent technique to protect the cryptographic secret-key and eliminate the use of PKI by merging it with the individual's biometric information i.e. the BCS actually applied the concept of biometric-system with the cryptography-system, it work in two way first to protect key by binding it with biometric and second to generate a key using biometric features [5].

The BCS further classified based on number of biometric data used in the system from different sources like biometric-systems i.e. i) Unimodal biocrypto-system (UBS) and ii) multimodal biocrypto-system (MBS). . UBS usage a single biometric trait for both key-binding and/or key generation whereas MBS usages at least two or more biometric trails for the same. The usage of biometrics in UBSs also faces some security challenges because of the noisy sensor data, spoof attacks and intra-class variations error due to the usage of altered secret-keys which requires the additional use of Error Correcting Codes to improve system's performance and overcome errors due to biometric variations. Many studies has been proposed to prove that MBS has a better performance in terms of accuracy and security than UBS, which also restricts the several error and limitations of UBS [6].

Therefore, MBS bind the user's cryptographic keys with its biometric identities and successfully replace the PKI system and efficiently protect the cryptographic secret-key. The MBS system uses at least two or more biometric data to protect the secret-key in case of key-binding system. The features from biometric images, after pre-processing, are extracted and merged using suitable fusion technique and generates a transformed fused feature template. These fused features are used to successfully bind the secret-key at the encoding phase using fuzzy commitment, fuzzy vault, and etc. key-binding schemes. The secret-key again will only be retrieved successfully if the same biometric images will be input at decoding phase with same fusion technique [7].

The MSB also has a problem of feature fusion of more than one feature of biometric modalities. Most of the existing MSB uses digital signal processing and machine learning based complex fusion techniques at different level, for example Discrete Fourier Transform [8], Gaussian mixture mode , Convolutional Neural Network, Pulse-Coupled Neural Network, Discrete wavelets transform, Discrete Cosine Transformation, log-Gabor filter and Haar wavelet. The following levels of fusion techniques based on different principles are implemented in MBSs i.e. rank level, decision-level, feature-level and score-level fusion. The fusion must improve the performance and security of the MBS efficient and must leave behind unimodal biocrypto system. In this proposed work, we propose an MKBB using on new proposed feature-level fusion technique based Least-Square Polynomial Curve-Fitting (LPC) and perform AES encryption as well to show the whole working of the system [9].

The main purpose of the proposed work is to implement an effective and robust new feature-level fusion method for the MKBB to protect the user define secret-key and overcome the use of PKI based secret-key protection.

This research paper is organized as follows, literature review is given in section-2 which has the brief discussion about previous works, section-3 gives the detail of proposed methodology, the experiment implementation and result discussion is shown in section-4, finally section-5 gives the conclusion of the proposed work.

## 2. Literature Review

In [10], the authors propose a score-level fusion technique based quality of features to enhance recognition rate of iris colour image based authentication system. The match score of correlation information of the red, green, and blue channels is applied to Redundant Discrete Wavelet Transform for information association at image level. In score-level fusion technique, the consequential image with the remaining channel is used to enhance recognition rate.

The authors in [11], propose a qualified analysis of iris based recognition system using based on Haar wavelet, log-Gabor filter, Fast Fourier Transform, and Discrete Cosine Transform techniques. The CASIA v1, CASIA v3, and IITD Iris databases are used to perform all experimental analysis. The weighted-sum rule are used in both log-Gabor filter and Haar wavelet based on score level. The Haar wavelet is a computationally efficient approach which requires minimum computation time and its combination with log-Gabor filters is create an efficient model. The authors also evaluate the comparative performance of various descriptors with singular training images. The performance of the system is evaluated using one training image on the CASIA and IITD In propose a feature level fusion technique to implement fuzzy commitment. The purpose of the suggested feature level fusion technique is to fuse two biometric templates with its binary feature descriptors into a single template of the same size. The presented feature level fusion technique is proposed to stability average reliability through all the biometric templates based on small training set. The proposed technique is more efficient to successfully reduce the use of error correction schemes. The CASIA v3 dataset is used to perform all the experiments and to demonstrate that the performance of proposed fusion technique to overcome the limitations of traditional fuzzy commitment schemes based multimodal-biometric systems. Authors in [12] present the working of multi-unit iris recognition based on Relevance Vector Machines (RVM) to implement score-level fusion technique using diverse classifiers with its applications. The performance analysis is made using the CASIA v4 database and demonstrate the improved performance of RVM with enhanced accuracy as compared to single iris recognition. The presented score-level fusion technique overall enhanced the recognition rate 4%. The computational required time of RVM based fusion techniques is comparatively less than fusion techniques using SVM, with equivalent recognition rate. In combined the working of Bayes rule based score level fusion and distance based indexing to present an identification technique. The proposed scheme chooses the template of the user based on its posterior probability of being identical. The proposed work is done using two datasets Biosecure DS2 and CASIA v5 Fingerprint dataset to analyse the performance of the proposed work and shows the reduction in identification error rates as compare to unimodal biometrics system.

In, present a feature-level fusion technique for multi-biometric cryptosystems to successfully secure the multi-biometric templates using secure-sketch of an individual. The proposed feature-level fusion framework is implemented using the fuzzy vault and fuzzy commitment biocrypto-systems to improve recognition accuracy rate and security of the proposed multibiometric cryptosystems based on real and virtual multi-biometric database, each containing the three most popular biometric modalities, namely, fingerprint, iris, and face. A synthetic multimodal database is assembled using the FVC2002 database for fingerprints, the CASIA v1 database for irises, and the XM2VTS database for faces. The proposed fusion scheme combines a set of biometric features and generates a fused multi-biometric feature template. The proposed system achieve average GAR 99% and 71.5% of both FC and FV scheme using virtual multimodal dataset and real multimodal dataset, respectively. The proposed multibiometric cryptosystem shows overall higher security and recognition rate as compare with unimodal biocrypto-systems.

In [15] propose multimodal biometric system based on deep learning for both the image of right and left irises of a person, and uses ranking-level fusion technique for fusing the features. They propose a system IrisConvNet based on a combination of Convolutional Neural Network (CNN) and Softmax classifier. All the experiments are analysed using the three datasets SDUMLA-HMT, CASIA-Iris-V3 and IITD iris. The experimental results shows the 100% recognition rate using highest rank identification for all three used databases. The authors in, present a new framework to generate chaff points using PSO for fuzzy vault based multimodal biometric cryptosystem. In this approach using particle swarm optimization (PSO) algorithm is used to find optimal and best locations to place chaff points. The experimentations are done using two dataset i.e. Yale face and IIT Delhi ear to evaluate and using different performance parameters. The proposed MBS demonstrates 90% of Genuine Acceptance Rate (GAR) as well as recognition rate of person with PSO.

In, author proposes a score-level fusion technique, GPSO, using the hybrid of GA and PSO. In this work, the features of every biometric modality is used as the score weights for optimization. The system uses four CASIA Image Databases i.e. CASIA-Iris, face, palm, finger to evaluate its performance and achieve 0.42% of FAR, 0.79% FRR and 95% of accuracy using the Naive Bayes (NB) classifier based decision rule for authentication.

The propose CNN and Q-Gaussian multi support vector machine (QG MSVM) based multimodal biometric authentication system, in which features of each biometric traits are extracted using CNN, with two different level fusion algorithms: a feature level fusion and a decision level fusion to enhance the performance and security of unimodal biometric system. The proposed system is evaluated using two datasets PTB and CYBHi database for ECG and two datasets LivDet2015 and FVC2004 database for fingerprint which are openly accessible for experiment usage. The calculated accuracy of proposed multimodal systems are 98.66% for PTB database, 98.97% for CYBHi database, 98.81% for LivDet2015 and 98.20 for FVC2004 database respectively.

## 3. Proposed Multimodal Key-Binding Biocrypto-System

In this research work, we propose a new efficient Multimodal Key-Binding Biocrypto-System (MKBB) using statistically based new feature-level fusion technique. The proposed system is being implemented using traditional fuzzy vault scheme of key-binding. As the key binding biocrypto-system work in two phases encoding phase and decoding phase. In encoding phase, a user dependent one or more biometric traits, and user defined cryptographic secret-key are taken as input, then the key-binding system hide this secret-key in the biometric features and create a public data known as helper data which stores in database and shared over the Internet. This helper data is very secure and not revealed the important information about the biometric features of the user as well as the secret key and it very difficult for the attackers to break this helper data. In decoding phase, the user's same biometric traits again taken as input and helper data stored in database are used as the input and retrieve the same secret-key as the output. The same secret-key will be retrieved successfully if the biometric input from the legitimate user and not retrieved otherwise.

In the proposed MKBB, two user's biometric i.e. iris and fingerprint are being used to efficiently protect the secret-key using least-Square Polynomial Curve-Fitting (LPC) based new feature-level fusion method. The fusion method plays very important role in biometric multimodal system as well as in biometric-cryptosystems. Efficient fusion method generates the more secure helper data in multimodal system.

### 3.1. Least-Square Polynomial Curve-Fitting

In this research work, we are proposing a new feature-level fusion method using statistical polynomial based curve fitting method known as Least-Square method in short, LPC, with mean and standard deviation [11]. It can be formulated as,

$$Y = \mathrm{LPC}(x, y, d)$$

where, $Y$ is a vector of $d+1$ coefficients, $x$ and $y$ are the data set at which coefficients are calculated, and $d$ is the polynomial degree.

Suppose the polynomial $p(x)$ of degree $d$, for the data in $y$ [8]. The coefficients in $p$ are in descending powers, and the length of $p$ is $d+1$, then,

$$y_i = p(x_i) = \alpha_1 x_i^d + \alpha_2 x_i^{d-1} + \cdots + \alpha_d x_i + \alpha_{d+1}, \quad \text{where,} \quad i \in \{1, 2, \ldots, d+1\} \tag{1}$$

The arithmetic mean for a set of $x_1, x_2, \ldots, x_d$ is denoted by $\bar{x}$:

$$\bar{x} = \frac{1}{d}\left(\sum_{i=1}^{d} x_i\right) \tag{2}$$

The standard deviation ($s$) can be defined as the square root of the variance ($v$). The variance uses a normalization factor of $d$ instead of $d-1$. For a random variable vector $x$ made up of $d$ scalar observations, the variance is defined as:

$$s = \sqrt{\frac{1}{d}\sum_{i=1}^{d}(x_i - \bar{x})^2}$$

$$v = \frac{1}{d-1}\sum_{i=1}^{d}|x_i - \bar{x}|^2 \tag{3}$$

$$s = \sqrt{v} = \sqrt{\frac{1}{d-1}\sum_{i=1}^{d}|x_i - \bar{x}|^2} \tag{4}$$

Then, the set of coefficients can be calculated using LPC as:

$$Y = (\gamma_1, \gamma_2, \ldots, \gamma_d, \gamma_{d+1}) \tag{5}$$

where $\gamma_m \mid m = \{1, 2, \ldots, d+1\}$ represents the value of the $m^{\text{th}}$ coefficient.

### 3.2. Encoding Phase of proposed MKBB

The working of complete encoding phase of proposed MKBB is demonstrated in Fig.1. In the proposed multimodal encoding phase, features from iris and fingerprints are extracted and applied as input to the proposed new feature-level fusion method which employs the polynomial curve fitting method to fuse these features and produce a set of fused template which further used in fuzzy vault encoding scheme. The polynomial is constructed using the cryptographic secret-key as its coefficients. The genuine points are now generated by polynomial projection over the set of fused value and create a fuzzy vault by merging the chaff points, which are randomly generated.

In this research work, a complete Advanced Encryption Standard (AES) cryptography is implemented to verify secret-key retrieval as well as the performance of the proposed MKBB system. The user-defined secret-key which is used in the encoding phase for binding is also applied in the encryption phase of the AES to produce the cipher text of the given plaintext.

The generated Vault and ciphertext are stored in the database or shared with the other user over the internet for further use in the decoding phase.

#### 3.2.1 Working of Proposed Encoding Phase

In most iris-based authentication systems, the iris template suffers from serious noise elements such as eyelid, eyelashes, etc., which may affect the genuine feature extraction from the iris template. Due to this reason, in the proposed work, some certain part of the iris, the side part of it, is selected as shown in Fig. 2. This selected part is then encoded in binary and then converted into a set of decimal values ($\eta_e$).

The detailed working of the proposed encoding phase is shown by the following steps:

**Step 1:** The iris image is taken as input, after pre-processing and normalization, the selected part, which is most probably noise-free, is displayed in Fig. 2.

**Step 2:** Encode the selected part in binary codes ($I_B$). In our case, the part is selected to generate 256-bits of code for each image of the dataset.

**Step 3:** Make 16 parts of $I_B$, where each part consists of a group of 16-bits. Then convert each group from binary code to a set of 16-decimal values ($\eta_e$) using the formula:

$$\eta_e = \text{BinToDec}(t_{1:16}) \quad \text{where, } e \in \{1,2,\ldots,16\}$$

**Step 4:** Now the other biometric image is taken, i.e., a fingerprint as input, and feature points are extracted (i.e., minutiae points), which give a set of coordinates $(x, y)$. Find the set of unique $x$-coordinates:

$$X_u \mid X_u \neq X_{u+1} \quad \forall u = \{1,2,\ldots,16\} \tag{5}$$

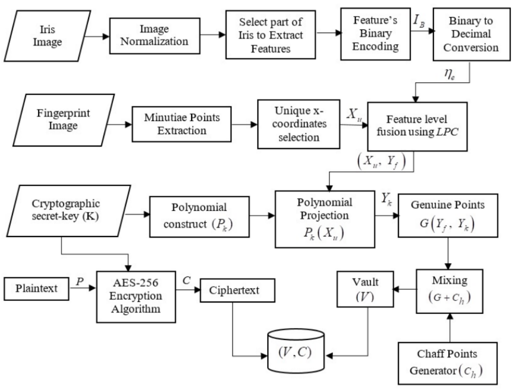


**Figure 1.** Encoding phase of proposed MKBB using New LPC Feature-level fusion method

**Step 5.** The proposed feature-level fusion method based on LPC from Eq. (1) and Eq. (4) is applied using feature sets minutiae points ($X_u$) from fingerprints and set of decimal values ($\eta_e$) from iris as input, and produce the set of values ($Y_f$) as output.

$$Y_f = \text{LPC}\,(X_u, \eta_e, d) = (\gamma_1, \gamma_2, \ldots, \gamma_d, \gamma_{d+1}) \tag{6}$$

Finally, the set of fused features is formed as $(X_u, Y_f)$ using Eq. (5) and Eq. (6).

**Step 6.** Now user-defined cryptographic secret-key ($K$) is taken and generates a polynomial ($P_k$) with coefficients as key-value. Calculate its projection over the $X_u$, as $P_k(X_u)$. The output of the polynomial projection is $Y_k$, then form the set of Genuine Points as $G(Y_f, Y_k)$.

**Step 7.** The random Chaff Points Generator is used to create the noise points ($C_h$) to protect the genuine points. The chaff points are mixed with genuine points then shuffled to create helper data known as Vault ($V$) and stored in the database.

**Step 8.** Now AES-256 encryption algorithm is implemented using the secret-key ($K$) and plaintext ($P$) as input then generates ciphertext ($C$) and shares over the Internet to end users or stores in the database for future use in decryption.

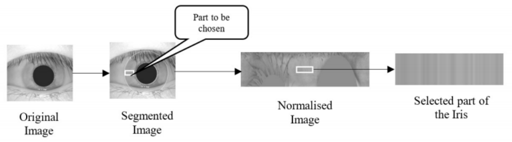


**Figure 2.** Selected Iris image in proposed system (CASIA-IrisV1 databases)

### 3.3. Decoding Phase of Proposed MKBB

The decoding phase is performed to retrieve the secret key which is bound in the encoding phase. The encoding phase of the proposed MKBB is shown in Fig. 3, which describes its complete working. In this phase, again the query biometrics are taken as input, the same as in the encoding phase, then extract features and fuse them as done in the encoding phase. These fused features are used to retrieve the set of genuine points from the vault, which is stored in the database. Now reconstruct the polynomial using the extracted genuine points and find the secret key as its coefficients, verify this retrieved secret key by applying AES-256 decryption.

#### 3.3.1. Working of Proposed Decoding Phase

In the proposed decoding phase of MKBB, again the part of the query iris image which is most probably noise-free, as discussed in the encoding phase and Fig. 2, is selected. The detailed working of the proposed decoding phase is shown by the following steps:

**Step 1.** The query iris image is taken as input and processed as in step 1 of the encoding phase. Then encode the selected part in binary codes ($\hat{I}_B$), resulting in 256-bits of code.

**Step 2.** Again make 16 groups of $\hat{I}_B$, and convert each group into decimal values ($\hat{\eta}_e$), which makes a set of 16 decimal values as:

$$\hat{I}_B = \{t_1, t_2, \ldots, t_{16}\}$$

$$\hat{\eta}_e = \text{BinToDec}(t_{1:16}), \quad \text{where } e \in \{1, 2, \ldots, 16\}$$

**Step 3.** Now extract the minutiae points of the query fingerprint, which again gives a set of coordinates $(\hat{x}, \hat{y})$. Find the set of unique $\hat{x}$-coordinates:

$$\hat{X}_u \mid \hat{X}_u \neq \hat{X}_{u+1}, \quad \forall u = \{1, 2, \ldots, 16\} \tag{7}$$

## 4. Experiment and Result Analysis

The proposed MKBB based on a new feature-level fusion method is evaluated using two biometric datasets:

1. **FVC2002_Db1_a** fingerprint dataset, which is provided by the Biometric System Lab of University of Bologna, Pattern Recognition and Image Processing Lab of Michigan State University, and U.S. National Biometric Test Center of San Jose State University. It consists of 800 images of 100 persons, 8 images for each person.
2. **CASIA-IrisV1** iris dataset, which is provided freely by the Institute of Automation (IA) and Chinese Academy of Sciences (CAS) for researchers. It includes 756 images from 108 eyes, 7 images for each eye, taken in two sessions.

In our experiment, the 1st fingerprint image of each of the 100 persons is considered with a pair of 1st iris images of the first session of only 100 persons to implement the proposed system and evaluate the performance. The proposed MKBB system based on fingerprint and iris images is evaluated using the following evaluation parameters:

### 4.1. False Matching Rate (FMR)

The FMR shows the rate of recognition of non-authorized persons who are recognized incorrectly. The FMR is formulated as follows:

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

### 4.2. False Non-Matching Rate (FNMR)

The FNMR shows the rate of recognition of authorized persons who are not recognized incorrectly. The FNMR is formulated as follows:

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

In the encoding phase of the proposed MKBB system, a pair of fingerprint and iris images is considered from a person and processed using the proposed LPC-based new feature-level fusion method. The parameters used in our proposed work are shown in Table 1.

**Table 1.** List of parameters with their values

| Parameters | Values |
|---|---|
| Iris binary codes ($I_B$) | 256-bits |
| Set of Decimal values ($\eta_e$) | 16 |
| Set of unique minutiae points ($X_u$) | 16 |
| Degree of Polynomial ($d$) | 15 |
| Set of fused features ($Y_f$) | 16 |
| Size of cryptographic secret-key ($K$) | 16-digits |
| No. of genuine points ($G$) | 16 |
| No. of chaff points ($C_h$) | 160 |

## 5. Conclusion

The results of proposed Least-Square Polynomial Curve-Fitting (LPC) based feature-level fusion method is has better performance than complex fusion techniques. The performance results shows that the proposed MKBB using LPC fusion is efficient and robust in terms of accuracy and recognition rate (GAR) which are 99.96% and 99.98% respectively. Thus, the proposed MKBB is efficient to protect cryptographic secret-key and can effectively overcome the use of third party based PKI system. The proposed work can be extended to enhance the security of Multimodal Biocrypto-systems in future.

**Author Contributions:** All authors contributed equally to the writing of this paper. All authors read and approved the final manuscript.

**Conflicts of Interest:** "The authors declare no conflict of interest."

### References

[1] Jiang, W., Li, H., Xu, G., Wen, M., Dong, G., Lin, X. (2019). PTAS: Privacy-preserving Thin-client Authentication Scheme in Blockchain-based PKI. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2019.01.026.

[2] Shamir, A. (1984). Identity-Based Cryptosystems and Signature Schemes. In: B GR, Chaum D., editors. *Work. Theory Appl. Cryptogr. Tech. CRYPTO 1984, Lect. Notes Comput. Sci.*, 196. Springer, pp. 47-53. https://doi.org/10.1007/3-540-39568-7_5.

[3] Daniel, R. M., Rajsingh, E. B., Silas, S. (2019). An efficient eCK secure certificateless authenticated key agreement scheme with security against public key replacement attacks. *Journal of Information Security and Applications*, 47, pp. 156-172. https://doi.org/10.1016/j.jisa.2019.05.003.

[4] Lozupone, V. (2018). Analyze encryption and public key infrastructure (PKI). *International Journal of Information Management*, 38, pp. 42-44. https://doi.org/10.1016/j.ijinfomgt.2017.08.004.

[5] Zhang, H., Wang, J., Ding, Y. (2019). Blockchain-based decentralized and secure keyless signature scheme for smart grid. *Elsevier Energy*, 180, pp. 955-967. https://doi.org/10.1016/j.energy.2019.05.127.

[6] Kubilay, M. Y., Kiraz, M. S., Mantar, H. A. (2019). CertLedger: A new PKI model with Certificate Transparency based on blockchain. *Computer & Security*, 85, pp. 333-352. https://doi.org/10.1016/j.cose.2019.05.013.

[7] Hiep, D., Tran, D., Nguyen, L. (2010). A Multibiometric Encryption Key Algorithm Using Fuzzy Vault to Protect Private Key in BioPKI Based Security System. *DOI: 10.1109/RIVF.2010.5632693*.

[8] Tantubay, N., Bharti, J. (2020). A Survey of Biometric Key-Binding Biocrypto-System using Different Techniques. *International Journal on Emerging Technologies*, 11(1), pp. 421-432.

[9] Balakumar, P., Venkatesan, R. (2012). A Survey on Biometrics Based Cryptographic Key Generation Schemes. *International Journal of Computer Science and Information Technology & Security*, 2(1), pp. 80-85.

[10] Dinca, L. M., Hancke, G. P. (2017). The Fall of One, the Rise of Many: A Survey on Multi-Biometric Fusion Methods. *IEEE Access*, 5, pp. 6247-6289. *DOI: 10.1109/ACCESS.2017.2694050*.

[11] Kumar, A., Kumar, A. (2015). A Cell-Array-Based Multibiometric Cryptosystem. *IEEE Access*, 4, pp. 15-25. *DOI: 10.1109/ACCESS.2015.2428277*.

[12] Ilankumaran, S., Deisy, C. (2018). Multi-Biometric Authentication System Using Finger Vein and Iris in Cloud Computing. *Cluster Computing*. *https://doi.org/10.1007/s10586-018-1824-9*.

[13] Alaa, S., Waisy, A., Qahwaji, R., Ipson, S., Al-Fahdawi, S., Nagem, T. A. M. (2017). A Multi-Biometric Iris Recognition System Based on a Deep Learning Approach. *Pattern Anal Applic, Springer*. *https://doi.org/10.1007/s10044-017-0656-1*.

[14] Balaka, R. N., Maddali, S. P. B. (2018). Biometric Authentication Data with Three Traits Using Compression Technique, HOG, GMM and Fusion Technique. *Data in Brief*, 18, pp. 1976-1986. *https://doi.org/10.1016/j.dib.2018.03.115*.

[15] Wang, Zhaobin, Wang, Shuai, Zhu, Ying, Ma, Yide. (2015). Review of Image Fusion Based on Pulse-Coupled Neural Network. *Archives of Computational Methods in Engineering*. *DOI: 10.1007/s11831-015-9154-z*.

[16] Vatsa, M., Singh, R., Ross, A., Noore, A. (2010). Quality-Based Fusion for Multichannel Iris Recognition. In: *20th International Conference on Pattern Recognition*, pp. 1314-1317. *DOI: 10.1109/ICPR.2010.327*.