J. Integr. Sci. Technol.2024, 12(3), 763

Article

Journal of Integrated
SCIENCE& TECHNOLOGY

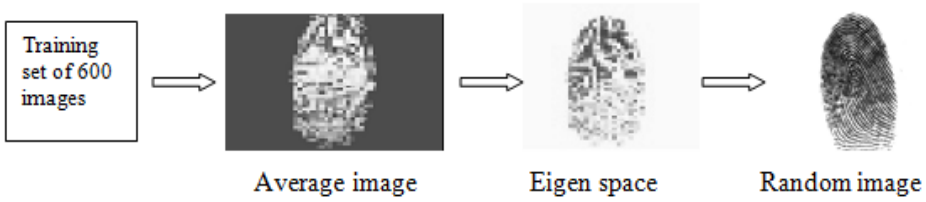
Finger print recognition based on biometric cryptosystem

V. Jalaja,[1] Anjaneyulu G.S.G.N.,[2] L. Narendra Mohan[3]

[1]Mathematics, Mohan Babu University (Erstwhile Sree Vidyanikethan Engineering College), Tirupathi, India. [2]Mathematics, School of Advanced Sciences, Vellore Institute of Technology, Vellore, Tamilnadu, India. [3]Mathematics, Sri Venkateswara College of Engineering, Tirupathi, India.

Received on: 12-Aug-2023, Accepted and Published on: 02-Dec-2023

ABSTRACT



In this article, we design a new Biometric Cryptosystem based on finger print recognition. In this Cryptosystem the algorithm is based on Eigen space approach. This approach has been compared with the conventional approaches which are based on exercise object geometry. The execution described uses the arrangement of Eigen space, and by calculating Eigen values and Eigen vectors of the image set. The image set is defined by taking different positions of images of finger prints. For an anonymous input image, the identification algorithm projects this image to the Eigen space and calculates Euclidean distance between the unknown image and the Eigen space. If this distance is minimum then the person is known. Otherwise it is unknown. Experimental results for different number of persons are shown to verify the viability of the designed method.

Keywords: Biometric Cryptosystem, Eigen Spaces Method, Finger Print recognition.

INTRODUCTION

Generally Biometric innovation is utilized for ID (or) verification purposes. Biometric[1] is the study of setting up the personality of an individual dependent on the physical, chemical (or) conduct attributes of the individual. It is an establishment of a character dependent on your identity, instead of by what you have, for example, an ID card, (or) what you recollect, such as a password.[2]

In the mode of the identification, the biometric scheme recognizes an individual from the whole selected clients in the scheme via hunting a database down a match. This type of identification is known as one-to-many correspondence. A framework can likewise be utilized in confirmation mode, where the biometric framework validates an individual's guaranteed character from their recently put away example. This is called coordinated correspondence.

*Corresponding Author: V. Jalaja
Tel:9492460994
Email: valisireddyjalaja0@gmail.com

Cite as: *J. Integr. Sci. Technol., 2024, 12(3), 763.*

We can protect biometric templates by combining biometrics & cryptography. This combination is also called as untraceable Biometrics, Biometric Encryption, Fuzzy Extractor, Biometric Key Generation etc. Biometric cryptosystems are like secret word based key age frameworks as they are utilized to verify cryptographic key (or) to straightforwardly produce cryptographic key from biometric highlights since the biometric estimations got during enlistment and verifications.

A traditional biometric scheme has four essential modules to be specific, sensor module, highlight extraction module, matching module & decision module. Biometrics are more useful in today's life, because we cannot overlook (or) free it, we don't have to recollect (or) keep it secret for secure verification. Biometric cryptosystems are the latest developments in the area of security. A finger print is shaped during the first seven months of fatal growth. Twins are also having unlike fingerprints. However, the fundamental issue with unique finger impression biometric is that it requires a lot of computational properties.

RELATED WORK

R. Cappelli et.al.[3] presented fingerprints images from rebuilding by using ordinary patterns. Also, they identified what amount of extent the recreated images are similar to original images. The efficiency of this mechanism can be evaluated by removing the

success chances of a masquerade attack against nine dissimilar fingerprint recognition systems.

R. Arjona et.al.[4] discussed a fingerprint recognition in the biometric cryptosystem. In this article they connected the total unique finger impression biometric cryptosystem in Field Programmable Gate Array [FPGA] by proposing a variety based two stage highlight gathering strategy. In that pairwise highlight separations are determined. For looking through the high dimensional component examination they utilized Boosting Feature Selection. For acknowledgment execution they utilized a method and it is tried by examining the partition between highlight delineations of the genuine and phony classes. George S.Eskander et.al.[5] suggested a bio - cryptographic scheme is created on offline signature images. In this they used two - step BFS technique and showed recognition rate as 97%. Emanuele Maiorana[6] presented online signature based biometric recognition system. They showed that by using this cryptosystem, secured and inexhaustible signature patterns can be legitimately created and utilized for acknowledgment purposes.

S. Sharma et.al.[7] reported that biometric cryptosystems joins cryptography and biometrics give security to the data. Generally Fuzzy commitment scheme is utilized for this and it creates parallel fixed length highlight vector. But separating highlight vector from finger print is troublesome because of vulnerability amid catching. Along these lines, in this paper she proposed an arrangement free bio-cryptosystem depends on adjusted VNS. At that point the paired element is utilized with FCS consolidating ECC of bio measurements. Biometric dependent key mechanism is developed by using biometric cryptosystem. This code amends if any mistake is there. Coordinating is additionally accomplished for this.

A.K. Jain et.al.[8] introduced an abnormal state order of the different vulnerabilities of a biometric framework. Mainly they examined biometric format security since it is an imperative issue in light of the fact that dissimilar to passwords and bargained biometric layouts can't be reissued. In this paper they noted different biometric format insurance plans and their focal points, restrictions regarding security, reputability and effect on coordinating exactness. Christian Rathgeb and Andreas Uhl[9] discussed overview on biometric cryptosystems and Cancellable biometrics. Biometric cryptosystem and drop capable biometrics speak to developing advances of biometric layout security and furthermore improving open certainty, acknowledgment.

M.Edwin, O. Neill[10] revealed that the estimation of fingerprints is a strategy for distinguishing and indicting offenders that relies upon a significant degree upon the thought given to this kind of proof by researching officers. Once a finger print has been erased expert can do nothing because we can’t re-establish the unique finger impression. This loss of important proof can be averted. So, it is used for multilevel purpose.

U. Uludag et.al.[11] exhibited the exploration issues identified with consolidating biometrics into a cryptographic framework with regards to DRM applications. Number of difficulties engaged with brushing biometric into a cryptographic framework. Existing exploration in biometric cryptosystems is centred around the savage power multifaceted nature of ill-disposed assaults. In a restricted setting, straightforward techniques are utilized for biometric confirmation to discharge a biometric enter are not valuable in numerous cryptographic applications since they include sharing decoded biometric data through a shaky channel.

Zhe Jin et.al.[12] suggested an ECC - free key restricting plan alongside cancellable changes for particulars based unique mark biometrics instead of fluffy responsibility. M.A. Murillo-Escobar et.al.[13] exhibited a fine print format security plot dependent on disordered encryption by applying calculated guide and Murillo-Escobar's calculation. This framework is implanted confirmation framework and it is secure, successful and requiring little to no effort. We can likewise execute this framework in a genuine secure access control frameworks. Yanqing Yao, Zhoujun Li[14] constructed a Fuzzy personality based signature scheme which depends on little whole number arrangement issues. In this FIBS scheme a client is having personality id with that identity id a signature will issue and this signature is checked under character id^1 if and only if id and id^1 are near one another.

R. Dwivedi et.al.[15] explained the concept of crypto biometric system for secure communication through finger print recognition. P. Kaur et.al.[16] proposed an algorithm in the combination of the fields like biometric and cryptosystem, the biometric will authenticate the data and cryptosystem will provide security. The proposed algorithm is designed using the concept BCS (Biometric and Cryptosystem). This BCS prevents attacks and this study covers 30 such attacks.

Ibrahim Hashem et.al.[17] and Srdan Barzut et.al.[18] presented a comprehensive overview of biometric cryptosystems which covers the concepts like fuzzy commitment, fuzzy vault, and convolutional neural networks CNN.[19]

S.Prabhakar et.al.[20] built up an example acknowledgment framework that perceives an individual dependent on an element vector which got from a particular physiological (or) social attributes of an individual. Marta Gomez-Barrero et.al.[21] proposed a multi-biometric format insurance which depends on homomorphic probabilistic encryption. In this scheme only encrypted data is handled. Peng Li et.al.[22] proposed a novel parallel length fixed component age technique for unique mark.

B. Prasanalakshmi et.al.[23] developed a scheme that includes a thought of including three biometric qualities of an individual where in the sense regardless of whether one comes up short the other characteristic could be used for check (or) personality. In this paper cryptosystem idea is additionally included, where one of the bio-metric quality itself goes about as a key to use the put away format database. It is a valid key no one can misuse.

A. Nagar et.al.[24] suggested an improved acknowledgment act and furthermore security of a fingerprint based on biometric cryptosystem, called finger print fuzzy vault. They showed the fingerprint matching performance improves from an FAR of 0.7% to 0.01% at a GAR of 95%. O. Ghita et.al.[25] Suggested an object recognition by using Eigen vectors. The approach which is discussed is a variant on current approaches to Eigen image analysis. Compared to traditional approach which will give best recognition rate. In this recognition process the Eigen values and Eigen vectors of the image set is calculated. The image set is nothing but the different positions of the object. Our approach is also followed the above process. When compare to other methods

it is a simple implementation and double-quick recognition. We can implement this approach easily in hardware for a real time application.

OUTLINE OF THE PAPER

The rest of the paper is organized as follows. In section2, we propose a Biometric cryptosystem based on fingerprint recognition. In section 3, we discussed the strength of the algorithm. In section4, we demonstrated the simulation results with Eigen space method. In section5,we emphasis the main conclusions of the paper.

PROPOSED BIOMETRIC CRYPTOSYSTEM WITH FINGER PRINT RECOGNITION

In this proposed method, first we have to consider different positions of finger print images of persons. Then we have to find the average image for the training set. Later we have to compare the random image with the image on the Eigen Space. Based on the comparison we have decided whether we have to accept or reject the given image.

Let us consider a picture namely I(x, y) in a two dimensional N by N array. Then convert the above image into N^2*1 dimension. Let the image I can be defined as $[p_1, p_2, p_3, ..., p_N]$ where $p_1, p_2, p_3, ..., p_N$ are the pixel values. Let us pick up p is the quantity of positions in space then the image set is defined as $[I_1, I_2, I_3, ..., I_p]$. Every pixel is having different mean and variance in an image, for getting uniform decoration we done the normalization. Then the normalized image is calculated by using the formula $\phi = \sqrt{\sum_{n=1}^{N} p_n{}^2}$ & $p_n{}' = \frac{p_n}{\phi}$. Now the normalized image is $I' = [p_1', p_2', ...p_N']$.

Next compute average image (A) for all images by doing the sum of all images by p i.e., $A = \frac{1}{p}\sum_{i=1}^{p} I_i'$. After finding average image then calculate the matrix U by using the formula square root of the sum of the squares of the difference between each image and average image and divide it with i, i.e., $U = \sqrt{\sum_{i=1}^{p} \frac{1}{i}(I_i' - A)^2}$.

Here, the dimension of matrix U is PXN, Where P is the quantity of positions and N is the quantity of pixels. Next find the co-variance matrix C by using the formula $U^T U$.

i.e., $C = U^T U$

Here the dimension of matrix C is $N^2 * N^2$. For a typical image sizes calculating Eigen values and Eigen vectors is an intractable task. We need a computationally reasonable technique to discover these Eigen vectors. If the number of images P is smaller than N then construct the p by p matrix Q= UU^T.

Next, construct the Eigenvalues by computing the characteristic equation of the matrix and by finding the roots of such equation we can obtain the Eigen values. Then for each Eigen value find the corresponding Eigen vectors of the matrix Q. Then compute $Qt_i = v_i t_i$. Where t_i is the i[th] Eigen vector and v_i is the corresponding Eigen value. Now the Eigen space is obtained by multiplying matrix of Eigen vectors with the matrix U.

i.e., W = XU

Where $X = [t_1, t_2, ..., t_p]^T$. X is pXp dimensional.

The dimension of Eigen space W is PXN. By using this approach we can reduce the number of calculations. Compare to other methods this method will give high success rate.

After calculating Eigen space venture all pictures from the set on this subspace. i.e., $W = [e_1, e_2, ..., e_p]^T$. Before projecting the image set onto Eigen space calculate $h_i = [e_1, e_2, ..., e_p]^T \left(\sqrt{\sum_{i=1}^{p} \frac{1}{i}(I_i' - A)^2} \right)$.

Here $e_1, e_2, ..., e_p$ are the Eigen space vectors and each vector is N dimensional.

Then project an unknown input image onto Eigen space the result will be a p-dimensional point which is denoted by 'h'. Next calculate the Euclidean distance between an unknown image (h) and the image on Eigen space (h_i). If this distance is below a threshold value then the image is known, otherwise it is an unknown.

STRENGTH OF THE ALGORITHM

For huge gathering of images the best methodology is to calculating universal Eigen space which contains all pictures. But the universal Eigen space will be hard to calculate figure on the grounds that the quantity of pictures for an extensive accumulation of pictures is vast. For this reason, we are calculating the largest p Eigen values and the corresponding Eigen vectors. By using these Eigen vectors we are calculating Eigen space.

In the existing techniques, U is calculated by subtracting average image from each image. In this computation, Euclidean distance coming considerably more. In our research work we concentrated to improve the image metrics using the parameter U and we have investigated U as follows $\sum_{i=1}^{n} \frac{\Gamma_i - \Psi}{i}, \sqrt{\sum_{i=1}^{n} \frac{(\Gamma_i - \Psi)^2}{i}}$ and so on.

Finally formulated and concluded as $\sqrt{\sum_{i=1}^{n} \frac{(\Gamma_i - \Psi)^2}{i}}$ based on accuracy of image metrics. This will give better Euclidean distance to match with the random image. Random image is the image of

particular person at any moment. By using this formula, we can trim down the error value like Euclidean distance.

ADVANTAGES: FINGER PRINT

By using biometric fingerprint we have several advantages and some of them are

- Finger print images minimize drastically the amount of work and simultaneously maintenance cost is also will become low.
- Every person has distinct finger print; even twins will have different finger prints.
- Finger print images are designed in the fetal stage and their Structures are unchanged throughout life.
- To recognize members of an organization, it supports and preserves security such that only authorized individuals can move from the secured checking point and it will hold off any other individuals.
- Finger print images help significantly to detect criminals in Forensic Department of Crime Scenes.
- To implement fingerprint mechanism it requires in significant memory space.
- Finger print images can't be vanished or cannot be mimicked, and hence information is safe from hackers.

COMPARISON: FINGERPRINT RECOGNITION OVER FACE RECOGNITION

In the current security scenario, we are watching a huge quantity of news about finger print &face recognition in distinct media channels. So, we will put our effort seriously to diminish variances between fingerprint biometric and face recognition today.

Table 1: Comparison of Face and Fingerprint Recognitions

Parameter	Fingerprint Recognition	Face Recognition
Accuracy	Finger print identification is a greatly reliable system in terms of accurate measurement.	Face recognition system executes in different process. It depicts in compound aspects which include eyes, cheeks, ear etc.
Distance	In this the subject cannot be detected with respect to a distance. i.e., we should associate physically with the device to be enrolled in fingerprint recognition mechanism.	In this The subject should be placed a near distance to be enrolled in face recognition mechanism.
Cost	Face recognition doesn't demand high configured cameras. It can work with the usual cameras such as mobile phones, web-cams etc. Which are integrated without any additional price and are available to public.	Biometric technology more specifically fingerprint recognition is absolutely a very efficient solution to face with the intruders. In addition to the software, an organization should arrange high-quality fingerprint device separately.
Agreement	In fingerprint system, people will be registered in the process by own consent. The registration of users will take place when they put their finger on the device.	In face recognition system, people may be registered in this process even without their authorization. Many governments will be collecting face biometric from public locations without declaring any announcement.
Acceptability	Fingerprint is moderately tolerable in some location.	Face recognition is extremely acceptable in everywhere.
Template Size	Fingerprint image template size is very medium.	Face recognition system essentially requires a large database.
Hardware	This system requires extra hardware in addition to the software.	This system does not require any extra hardware.

SIMULATION RESULTS WITH MODIFIED EIGEN SPACE METHOD

To demonstrate the proposed algorithm first we have to consider the training set. Designing a practical system for person or object recognition require accuracy and speed. The size of the sample set is small, then we have to construct the universal Eigen space. If the size of the sample set is large then we have to construct the universal Eigen space and object Eigen space for each object. C.Puri et.al.[26] presented an Analysis of Rural and Urban Indian Fingerprint images. In the above modified Eigen Space method, we used 8 different finger prints of 75 people. i.e. totally 600 images as a training set. These images are collected from ref [12]. Some of the images in the training set are shown below.

Then the average image is calculated by converting each image into matrices. And by using the program in R software the average image is calculated. It is denoted by the matrix A. For obtaining the uniformity we done the normalization for each pixel of the image.

Average image

Fig.1

Eigen space

Fig.2

Random image

Fig.3

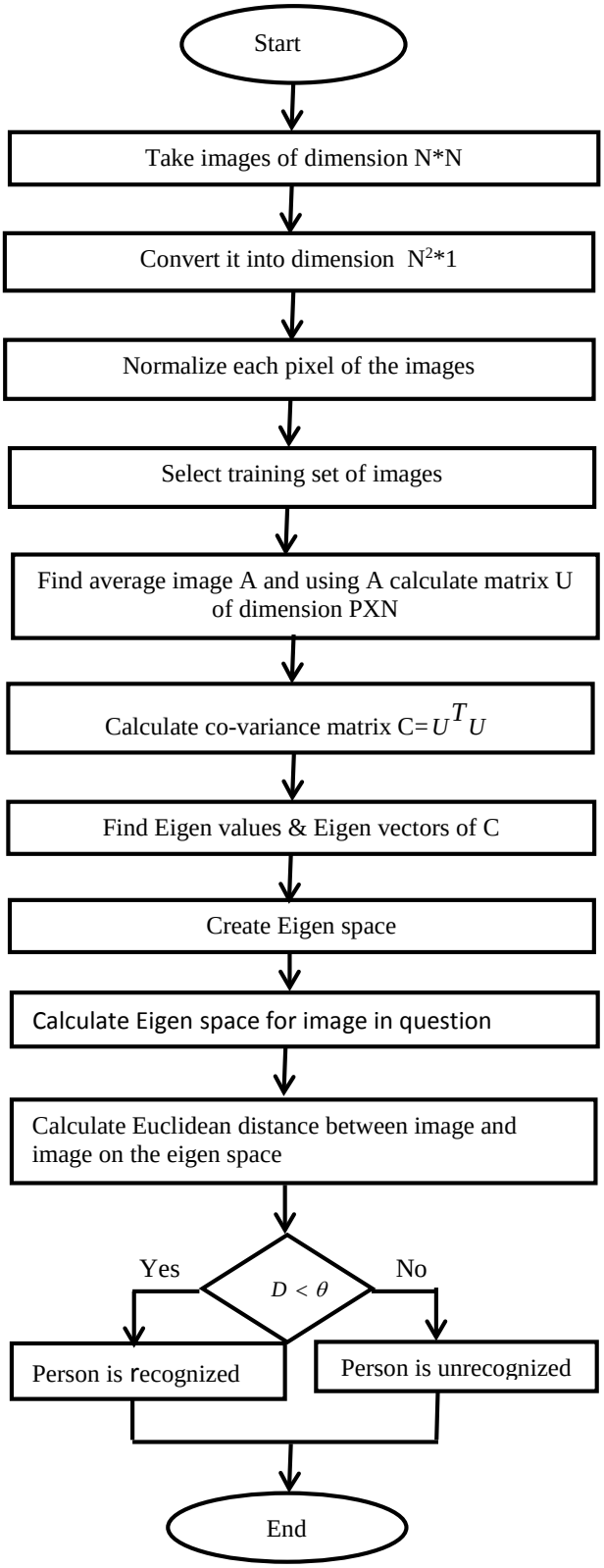
Here the figure1 represent the average image for the above 6oo images training set. Figure 2 represent the Eigen space image and figure 3 is called the random image for testing.

VERIFICATION AND ACCURACY

Initially we calculated the average image (Fig.1) for the images in the training set (i.e., for 600 images). Next we computed the matrix U by using the average image A. Then the co-variance matrix C is calculated by using the formula that the multiplication of transpose of U and U.

Then we considered P by P matrix Q=UU^T. After that we calculated the characteristic equation and then find the roots of the equation which will give the Eigen values and for each corresponding Eigen value Eigen vectors are calculated for the matrix Q. The Universal Eigen space (Fig. 2) is formed by taking the largest Eigen values and corresponding Eigen vectors. Next, the Euclidean distance between the random image and image in the Eigen space are calculated. By programming the Euclidean distance of the random image (Fig. 3) and Eigen space is 43.99. The time complexity of the proposed Eigen space method is $O(p^{3/2})$. When we compare with other methods this method is simple, fast and reliable. We can implement this approach in any programming languages by using the below algorithm.

Detailed flow chart of the above algorithm is as:



CONCLUSIONS

In this article a biometric cryptosystem based on fingerprint recognition is presented. Any system is giving accurate recognition rate means it involving biometric factor. Because the unique person

identification potential is provided by biometrics. The proposed system is able to perform user recognition by using fingerprint. For recognition person we considered a large data base of 600 images, We implemented the proposed approach on this database. We calculated Time complexity to run the new designed approach is to other methods this implementation is simple, double-quick and trusty. We can easily implement this $O(p^{3/2})$. Compare approach in hardware for a real time application. The future work will focus on increasing success rate for very large databases.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

1. M. Singh, R. Singh, A. Ross. A comprehensive overview of biometric fusion. *Inf. Fusion* **2019**, 52 (1), 187–205.
2. A.K. Jain, A. Ross, S. Prabhakar. An Introduction to Biometric Recognition. In *IEEE Transactions on Circuits and Systems for Video Technology*; **2004**; Vol. 14, pp 4–20.
3. R. Cappelli, A. Lumini, D. Maio, D. Maltoni. Fingerprint image reconstruction from standard templates. In *IEEE Transactions on Pattern Analysis and Machine Intelligence*; **2007**; Vol. 29, pp 1489–1503.
4. R. Arjona, I. Baturone. A fingerprint biometric cryptosystem in FPGA. *Proceedings of the IEEE International Conference on Industrial Technology*. 2015, pp 1554–1559.
5. G.S. Eskander, R. Sabourin, E. Granger. A bio-cryptographic system based on offline signature images. In *Information Sciences*; **2014**; Vol. 259, pp 170–191.
6. E. Maiorana. Biometric cryptosystem using function based on-line signature recognition. In *Expert Systems with Applications*; **2010**; Vol. 37, pp 3454–3461.
7. S. Sharma, A. Saini, S. Chaudhury. A survey on biometric cryptosystems and their applications. *Comput. Secur.* **2023**, 134, 103458.
8. A.K. Jain, K. Nandakumar, A. Nagar. Biometric Template Security. *EURASIP J. Adv. Signal Process.* **2008**, 2008 (1), 579416.
9. C. Rathgeb, A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *Eurasip Journal on Information Security*. 2011.
10. M.E. O'Neill. Fingerprints in Criminal Investigation. *J. Crim. Law Criminol.* **1940**, 30 (6), 929.
11. U. Uludag, S. Pankanti, S. Prabhakar, A.K. Jain. Biometric cryptosystems: issues and challenges. *Proc. IEEE* **2004**, 92 (6), 948–960.
12. Z. Jin, A.B.J. Teoh, B.M. Goi, Y.H. Tay. Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation. In *Pattern Recognition*; **2016**; Vol. 56, pp 50–62.
13. M.A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiérrez. A robust embedded biometric authentication system based on fingerprint and chaotic encryption. In *Expert Systems with Applications*; **2015**; Vol. 42, pp 8198–8211.
14. Y. Yao, Z. Li. A novel fuzzy identity based signature scheme based on the short integer solution problem. *Comput. Electr. Eng.* **2014**, 40 (6), 1930–1939.
15. R. Dwivedi, S. Dey, M.A. Sharma, A. Goel. A fingerprint based crypto-biometric system for secure communication. *J. Ambient Intell. Humaniz. Comput.* **2020**, 11 (4), 1495–1509.
16. P. Kaur, N. Kumar, M. Singh. Biometric Cryptosystems: a Comprehensive Survey. *Multimed. Tools Appl.* 82, 16635–1690,.
17. M.I. Hashem, K. Alibraheemi. Literature Survey: Biometric Cryptosystems Based on Fingerprint Processing Techniques. *2022 Int. Conf. Data Sci. Intell. Comput. ICDSIC 2022* **2022**, 198–201.
18. S. Barzut, M. Milosavljević, S. Adamović, et al. A novel fingerprint biometric cryptosystem based on convolutional neural networks. In *Mathematics*; **2021**; Vol. 9.
19. V. Jalaja, G.S.G.N. Anjaneyulu, L. Narendra Mohan. New Digital Signature scheme on Non-Commutative Rings using Double Conjugacy. *J. Integr. Sci. Technol.* **2023**, 11 (2), 471.
20. S. Prabhakar, S. Pankanti, A.K. Jain. Biometric recognition: Security and privacy concerns. In *IEEE Security and Privacy*; **2003**; Vol. 1, pp 33–42.
21. M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, J. Fierrez. Multi-biometric template protection based on Homomorphic Encryption. In *Pattern Recognition*; **2017**; Vol. 67, pp 149–163.
22. P. Li, X. Yang, H. Qiao, et al. An effective biometric cryptosystem combining fingerprints with error correction codes. *Expert Syst. Appl.* **2012**, 39 (7), 6562–6574.
23. B. Prasanalakshmi, A. Kannammal, B. Gomathi, K. Deepa, R. Sridevi. Biometric cryptosystem involving two traits and palm vein as key. In *Procedia Engineering*; **2012**; Vol. 30, pp 303–310.
24. A. Nagar, K. Nandakumar, A.K. Jain. A hybrid biometric cryptosystem for securing fingerprint minutiae templates. In *Pattern Recognition Letters*; **2010**; Vol. 31, pp 733–741.
25. O. Ghita, P.F. Whelan. Object recognition using eigenvectors. In *Proc. SPIE 3208, Intelligent Robots and Computer Vision XVI: Algorithms, Techniques, Active Vision, and Materials Handling*; Casasent, D. P., Ed.; **1997**; pp 85–91.
26. C. Puri, K. Narang, A. Tiwari, M. Vatsa, R. Singh. On analysis of rural and urban Indian fingerprint images. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; **2010**; Vol. 6005 LNCS, pp 55–61.