March-April 2020
ISSN: 0193-4120 Page No. 3216 - 3222

# Multi-Biometric Template Transformation Approach Based on Parallel Addition Algorithm

**Thilagavathy -** Associate Professor in the Department of Information Technology,
**Veeramani -** Professor in computer science and Engineering Department,
**Kumaran -** Assistant Professor in the School of Computing, SASTRA Deemed University, Thanjavur

***Article Info***
***Volume 83***
***Page Number: 3216 - 3222***
***Publication Issue:***
***March - April 2020***

***Article History***
***Article Received****: 24 July 2019*
***Revised****: 12 September 2019*
***Accepted****: 15 February 2020*
***Publication****: 21 March 2020*

***Abstract:***
Fingerprint is a physical characteristic which cannot be stolen. Feature vectors are extracted from the left fingerprint, right fingerprint and palm and then encrypting the feature vectors for the verification using parallel addition algorithm along with X-Model X-OR and then perform operations on the linear equation. Multi-biometrics fingerprint system uses more than one fingerprint to identify whether the user is valid user or not a valid user.

***Keywords:*** *Multi-biometrics, Fingerprints, Parallel Addition algorithm, X-Model X-OR.*

## I. INTRODUCTION

Biometric is an automated form of pattern matching system. There are traditional methods which use pin number as there password. These can be easily identified by many attacks namely brute force, snooping, etc., In general, four basic security systems are used such as fingerprint based, iris based, Facial features based, Speech recognition based security system. However, biometric fingerprint will give more accurate outcome and no two fingerprints will have same feature vectors. Moreover, making the system multi-biometric will also increases the uniqueness of the individual and accuracy. The feature vectors must be stored in the encrypted form to safeguard from the attackers.

There is different type of technology which is used in biometrics. Fingerprint recognition is used to identify the uniqueness of ridges and minutiae made by the user fingerprint. Biological measurements qualify to be a biometric for its universality, distinctiveness, permanence and collectability. It can be thought of a pattern recognition system.

**Universality**: Every individual should possess the same set of biometric characteristic.

**Uniqueness**: These characteristics will be unique for every individual and can be easily distinguishable.

**Permanence**: These biometric data remains invariant over a period of time.

**Measurability**: It is possible to acquire the entire biometric feature. The acquired biometric data is used for further processing. From an application perspective, this property should also be considered.

**Acceptability:** Acceptability is the individual's willingness to provide his biometric characteristics.

**Spoof Resistance**: This refers to the degree of difficulty in using the fake biometrics (for example, fake fingers).

Aglika *et al*. [3] proposed a scheme indexing biometric databases. In this scheme, fixed-length codes are generated. By comparison of the match scores between a images and aset of fixed reference images an index score is obtained. But it may not achieve state-of-the-art indexing performance for some biometric modalities but can be easily ported for use on multimodal databases. The major future work in biometrics was made by Tomko*et al.* [4], however, certain issues in biometrics were quickly identified and the proposed system ensured their system is free from the security issues. Dodies et al. [14] define three spaces of metrics. They are Hamming, edit and set difference metrics. The major biometric data will fall in the first and third metric

March-April 2020
ISSN: 0193-4120 Page No. 3216 - 3222

region because a biometric template can be appeared either as a set of features or binary string. Abhishek et al. [2] propose a fusion of feature at feature-level to simultaneously safeguard templates of multiple users as a sketch of single secure system using biometrics of two cryptosystems which is fuzzy commitment and fuzzy vault. Nandhakumar and Jain [12] uses fuzzy vault to adopt a fused template fingerprint and the feature vectors of iris among chaff points. Cai Li et al. [5] proposed a method to add security to fingerprint-based multi biometric cryptosystem using a method known as level of the decision fusion. Hash areimplemented in the construction to protect every biometric feature vectors. Since hash functions are used, the hash function should be time efficient. And a bad hash function might become a vulnerability and easy target. Asem Othman et al. [6] proposed a fingerprint security method by combining spiral and continuous components from two fingerprints. This method provides virtual identities and used to generate cancellable fingerprint template. Enhancement of the performance due to mixed fingerprints by exploring alternate algorithms for pre-aligning, selecting and mixing the different pairs must be improved. Abishek Nagar et al. [7] proposed to safeguard the individual template which will be used to store only the secured sketch which is generated from respective template using biometric cryptosystem. Uz et al. [10] proposed a analysis based on hierarchical method and scoring approach which is used to combine many feature vectors into a maximum quality based on super-template set. The Delaunay triangle will provide the hierarchical analysis and scoring which provides higher levels of hierarchy which represents higher levels of minutiae points and lower quality of hierarchy point's medium and lower quality minutiae points. Sheng Li et al.[8] proposed that binary thinned fingerprint embedded with private user information which will not cause any sudden variation. In the authentication stage, the user data which is stored in the form of template provides the query fingerprint. In this process, no boundary pixel is developed in the embedding which results in marke-thinned fingerprint. When the online database is compromised, the attacker cannot extract any information from the raw data in the database. Thus the identity of the user is protected. Kai Cao et al. [9] proposed that the necessity of securing the fingerprint templates, increasing the internal working of the template and also improves the fingerprint analysis. By this system, the purpose of reconstruction utilizes the background analysis of fingerprint ridge structure to increase the fingerprint image. The further working of this system will make the fingerprint more realistic. Juels and Sudan et al. [20]proposed the scheme of fuzzy vault. This systemuses the biometric features using a polynomial and checking is based on polynomial regeneration using a Reed–Solomon Error Correcting Code. Cai Li et al. [11] pointed out some limitation in using entropy-based security system and propose a better security system that merges information-theoretic approach along with the system of computational security. The construction of a fingerprint-based multi-biometric system fuses with levels of decision. Hash functions are also used along with the construction to increase the protection of each biometric trai. Golic et al. [13] represents the average number of min-entropy that doesn't identify the statistical independence of random variable. The system introduces the conditional Shannon entropy. Both the conditional Shannon and average min-entropy calculates the security that comes from the information-theoretic perspective, which will reflects the probability rather than biometric templates actual values. Fang et al.[16] is a cascaded method within the sketch of secure framework. The main advantage of a the approach is that biometric traits can easily be mixed with multi-biometric cryptosystem. The benefit is it allows use of templates which is heterogeneous. Wencheng Yang et al. [15] developed a Delaunay quadrangle which will handle when the Delaunay triangle suffers. This system is used to deal with non-linear local structural change which cannot be handled by triangular approach. Alignment-free

March-April 2020
ISSN: 0193-4120 Page No. 3216 - 3222

features extracted are less sensitive to triangular approach and applied directly only to template protection.

## II. PROPOSED SYSTEM

### A. Preprocessing:

The fingerprint will be preprocessed before using the inputs.

i. Pixel Alignment: During verification the user fingerprint will always not be on same position. So, the pixel has to be align with respect to the nearest matched template, which then can be used for the purpose of verification.

ii. Identification of false minutiae points: The process of identifying the false minutiae points will be helpful in the process of reducing the noise in the fingerprint which can be either left, right or palm.

iii. Reducing the feature vector: Not all the feature vectors are taken under consideration. Only the feature vector which can produce the maximum accuracy and responsible for the identification of the individual are only taken under consideration. Hence identifying the maximum likelihood feature vector plays a vital role in fingerprint recognition.

### *B. Proposed System Architecture:*

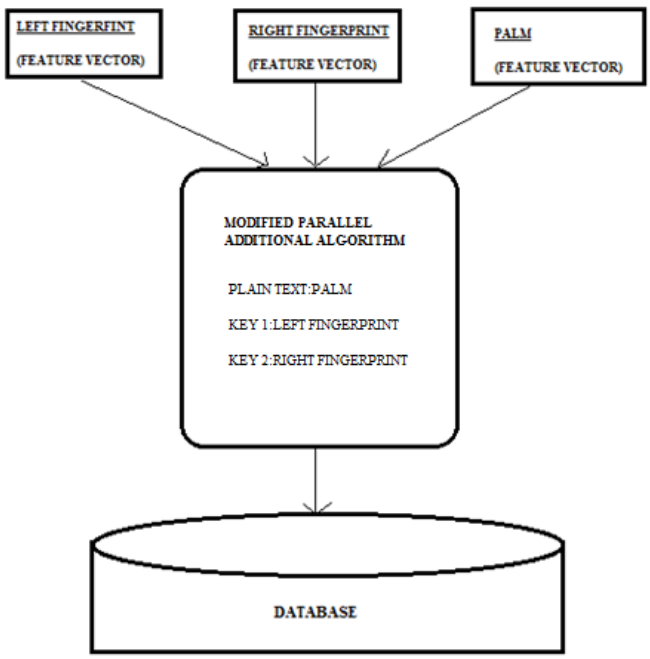


**Fig 1.1 Proposed System Architecture**

In the fig 1.1, the inputs for the parallel addition algorithm are taken by using left fingerprint acts as a plain text, right fingerprint acts as a key1 and palm acts as a key2.The parallel addition algorithm uses X-Model X-OR model which makes the inputs to do XOR operation in the format of X type with the inputs of $2^N$.The X-Model will end when X type cross the value of N=8.The output from the X-OR model will taken and fed to the parallel addition algorithm. The proposed algorithm contains three parts. One algorithm modifies the parallel addition algorithm using x model XOR. Second algorithm modifies the list ranking algorithm using sine model XOR. Third algorithm modifies the butterfly parallel algorithm using cross model XOR.

**Algorithm: Modified Parallel addition algorithm**

**input** :leftprint ,rightprint , palmprint
**plain text** : leftprint
**key 1** : rightprint
**key 2** : palmprint
**Output**: cipher 1(integer)

*1 For i=0 to n*
*2 convert the left[i] and right[i] to binary and store I*
*in an array ,say rem and rem1.*
*3 set k to 0*
*4 while rem[r] != NULL && rem1[s] != NULL*
*result[k++]= rem[r] ^ rem1[s]*
*if rem1[s] is NULL*
*result[k++]= rem[r] ^ rem1[0]*
*while rem[r] != NULL && rem1[s] != NULL*
*result[k++]= rem[r] ^ rem1[s]*
*if rem[r] is NULL*
*result[k++]= rem[0] ^ rem1[s]*
*convert the resultant binary number to integer*
*res1 = right[i] base 3*
*5 res2 = palm[i] base 3*
*6 res3 = res1(x^2)+res2 (x) + res*
*7 res3 = res3 mod 256*
*8 result[i]=res3*
*9 This resultant array of ciphers are then fed to the algorithm (paralell addition)*

March-April 2020
ISSN: 0193-4120 Page No. 3216 - 3222

### *C. Modified parallel Addition algorithm:*

In fig 1.2 parallel addition algorithm each node will be operating on all the three inputs. The inputs for the parallel addition algorithm are taken by using left fingerprint acts as a plain text, right fingerprint acts as a key1 and palm acts as a key2.The plaintext left fingerprint is taken as 8 bit node form and add the adjacent nodes in the first step and then similar steps are carried out for the next step. The process goes on when there are only two nodes remaining. Then Right fingerprint and palm is taken and parallel addition algorithm is repeated. Again there will be 8 bit values for all the three inputs left, right and palm. The output from this stage is send to the X-Model operation.

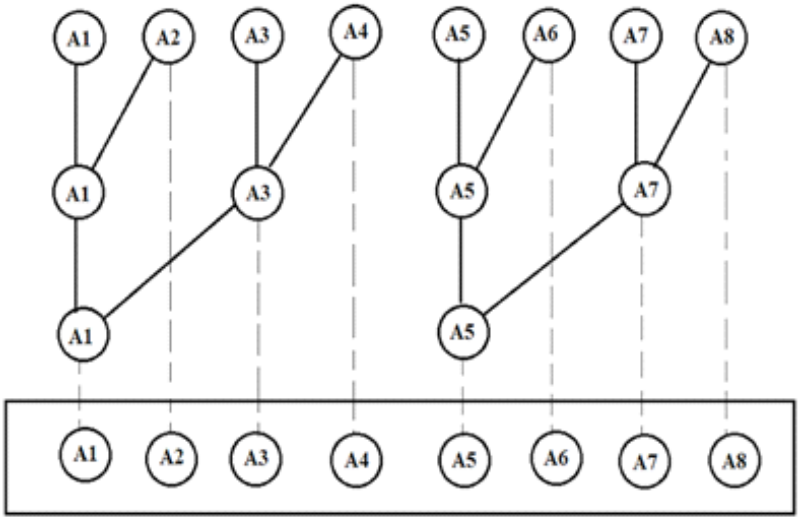


**Fig. 1.2 Parallel addition**

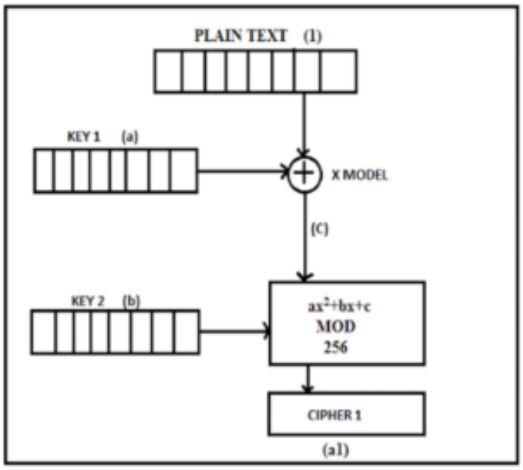


**Fig. 1.3 Node operation of parallel addition**

The working process of each nodes is shown in fig 1.3.Here the plaintext which is the left fingerprint's feature vector and the key1 which is the right fingerprints feature vectors are extracted by parallel addition algorithm and are then X-OR'ed by a method called X-model X-OR. The key2 which is palm and the feature vectors of 8 bit are generated from the parallel addition algorithm and send through the linear equation $(ax^2+bx+c)$Mod 256 along with result generated from the feature vectors of plaintext and key1. The result for the first step will be the cipher text1 generated during the proposed process.

March-April 2020
ISSN: 0193-4120 Page No. 3216 - 3222

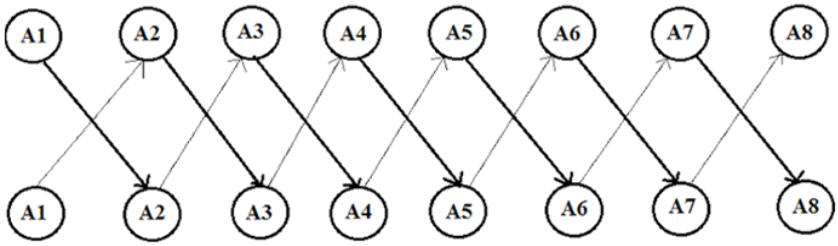


**Fig 1.4 X model XOR**

Normally the XOR returns true if both the inputs are different else the XOR will return output as false. Fig 1.4 shows the bit representations of the integer from the feature vectors. The parallel addition algorithm uses X-Model X-OR model which makes the inputs to do XOR operation in the format of X type with the inputs of 2N.The X-Model will end when X type cross the value of N=8.The output from the X-OR model will taken and fed to the parallel addition algorithm. These vectors are then combined with key 2 which is palm using the linear equation ax2+bx+c.

***D. Matching and Scoring:***

The Table 1.1 compares the proposed system with existing system databases FAR, FRR and ERR. The proposed system found to provide higher security when compared with existing system.

| Method | 2002 DB1 | 2002 DB2 | 2002 DB3 | 2004 DB2 | 2006 DB2 | 2006 DB3 |
|---|---|---|---|---|---|---|
| | FRR/FAR | FRR/FAR | FRR/FAR | FRR/FAR | FRR/FAR | FRR/FAR |
| Wenchang yang et al 2014 | 4.73 | 4.92 | 5.213 | 5.56 | 5.78 | 6.32 |
| Theproposed System | 3.2 | 4.5 | 4.7 | 5.2 | 5.4 | 5.7 |

**Table 1.1 ERR of different existing system and the proposed system**

## III. SECURITY ANALYSIS

***A. One Way Encryption:***

Parallel addition algorithm is used for transforming the input to another form and X-Model X-OR reduces the number of inputs by X-OR operation. If there are 16 nodes then after performing X-Model X-OR only 8 will be present. Since it provides one way encryption, the process cannot be reversed to produce the original input. The verification of the user is also done at the encrypted range only. So, there is no possibility of regenerating the inputs. Even if the database is compromised, the hacker cannot get any information regarding the fingerprints. During process these feature vectors will be represented in another form. Because after applying three algorithms, all the features are merged to form new vectors. Hence the reverse is not possible because many of the feature vectors will be missing so that it make in non-invertible.

***B. Computational security:***

If the left fingerprint contains 24 features and right fingerprint contains 24 feature and palm also contains 24 features (totally 72 feature vectors) after performing X-Model X-OR with left and right fingerprint only 24 feature are made from 48 feature vectors then this 24 feature vectors are then passed through the linear equation along with palm(24

March-April 2020
ISSN: 0193-4120 Page No. 3216 - 3222

feature vectors),then these 48 feature vectors are again reduce to 24 feature vectors. Hence finally from 72 feature vectors, the proposed system reduces to 24 feature vectors. Hence during comparison the computation found to lesser than normal comparison of 72 feature vectors ie.,

$$K(x) = \left( \sum_{i=3} FV(i) \right) / 3 \quad \text{------(1)}$$

Where FV (i) is a feature vector K(x) is the total of unique feature vectors produced by parallel addition algorithm. Since the proposed system uses multi level security, even if the user has fault in left fingerprint or right fingerprint or palm, the other two fingerprints can help the proposed system to identify the valid user. There will be a peak value for the valid user in the verification process which will make the system to identify the user's validity.

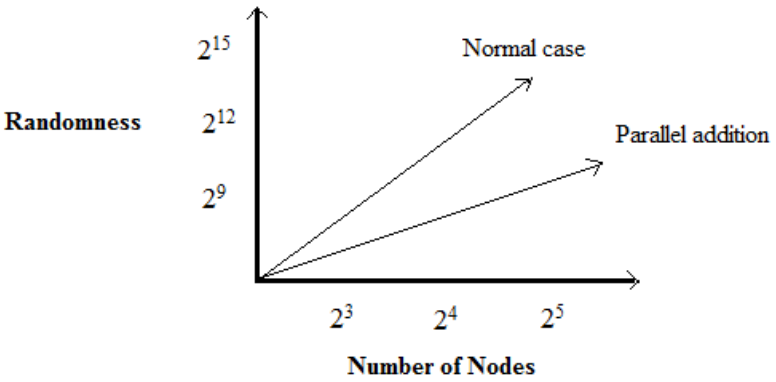


**Fig 1.5 Randomness vs. Number of Nodes**

| Left Fingerprint | Right Fingerprint | Palm | Total feature vectors | Output of parallel addition feature vectors |
|---|---|---|---|---|
| 23 | 23 | 23 | 24 | 23 |
| 24 | 24 | 24 | 25 | 24 |

**Table 1.2 Effectiveness of the Proposed Model**

In Fig 1.6, as the number of inputs keeps on increasing, the output will also contain the total average of the total number of number of inputs and so that the computation time complexity reduces as the number of output node keeps on decreases. The randomness will also keeps on increasing as the output produced will the addition of the node in 2N.

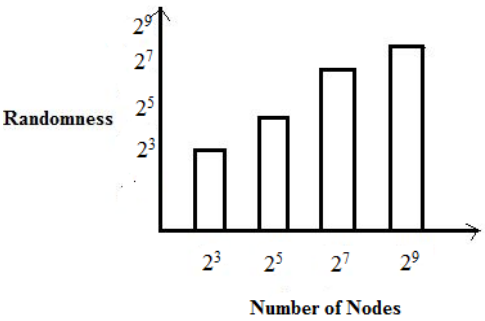


**Fig 1.6 Randomness vs. No.of nodes**

*March-April 2020*
*ISSN: 0193-4120 Page No. 3216 - 3222*

## IV. CONCLUSION

The proposed system uses parallel addition algorithm and X-Model X-OR to provide security using the encryption. The X-Model X-OR will make X-OR in the diagonal pattern and redefine the nodes values. The security will further be enhanced by the linear equation ax2+bx+c.The linear equation will further enhance the security by increasing the making key2 as palm feature vectors. So, the combinations cannot regenerate which provides a higher level of security for the database. Even if the hacker stoles the database, the attacker cannot able to identify the logic behind the security system.

## REFERENCES

1. Maneesh Upmsnyu, Anoop M. Namboodri, Kannan Srinathan and C.V.Jawahar, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, June2010.
2. Abhishek Nagar, KarthikNandakumar and AnilK. Jain "Multibiometric Cryptosystems Based on Feature-Level Fusion" in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL.7, NO.1, FEBRUARY 2012.
3. AglikaGyaourova and Arun Ross "Index Codes for Multi biometric Pattern Retrieval" in IEEE TRANSACTIONSON INFORMATION FORENSICS AND SECURITY, VOL.7, NO.2, APRIL 2012.
4. G. J. Tomko, C. Soutar, and G. J. Schmidt, "Fingerprint controlled public key cryptographic system," U.S. Patent 5 541 994, Jul. 30, 1996.
5. Cai Li, Jiankun Hu, Josef Pieprzyk and Willy Susilo "A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion" in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL.10, NO. 6, JUNE 2015.
6. Asem Othman and Arun Ross," On Mixing Fingerprints",Published as IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO.1, JANUARY 2013
7. Abishek Nagar, KarthikNandakumar and AnilK. Jain, "Multibiometric Cryptosystems Based on Feature-Level Fusion" Published as IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1.Year, FEBRUARY 2012.
8. Sheng Li and Alex C. Kot, "Privacy Protection of Fingerprint Database", Published as IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 2, FEBRUARY 2011.
9. Kai Cao and Anil K.Jain," Learning Fingerprint Reconstruction:FromMinutiae to Image", Published as IEEEE Transactions on Information Forensics and Security,Vol. 10, January 1,2015.
10. T. Uz, G. Bebis, A. Erol, and S. Prabhakar, "Minutiae-based template synthesis and matching for fingerprint authentication," Comput. Vis.Image Understand., vol. 113, no.9, pp. 979–992, Sep. 2009.
11. Cai Li, Student Member, IEEE, Jiankun Hu, Josef Pieprzyk, and Willy Susilo, Senior Member, IEEE, "A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion", VOL. 10, NO. 6, JUNE 2015.
12. K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in Proc. IEEE Int. Conf. Biometrics, Theory, Appl. Syst., Arlington, VA, USA, Sep./Oct. 2008, pp. 1–6.
13. J. D. Golic and M. Baltatu, "Entropy analysis and new constructions of biometric key generation systems," IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2026–2040, May 2008.
14. Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in Proc. Eurocrypt, 2004, pp. 523–540.
15. Wencheng Yang, Jiankun Hu, and Song Wang, "A Delaunay Quadrangle-Based Fingerprint Authentication System With Template Protection Using Topology Code for Local Registration and Security Enhancement", IEEE transactions on information forensics and security, vol. 9, no. 7, july2014.
16. Abhishek Nagar, Student Member, IEEE, KarthikNandakumar, Member, IEEE, and AnilK. Jain,"Multibiometric Cryptosystems Based on Feature-Level Fusion", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012.
17. C. Fang, Q. Li, and E.-C.Chang, "Secure sketch for multiple secrets," in Proc. Int. Conf. Applied Cryptography and Network Security, Nejra, Spain, 2010.

*March-April 2020*
*ISSN: 0193-4120 Page No. 3216 - 3222*

18. Benjamin Tams, Preda Mihailescu, Axel Munk, "Security Considerations in Minutiae-Based Fuzzy Vaults," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, May 2015.
19. Aglika Gyaourova, Student Member, IEEE, and Arun Ross, Senior Member, IEEE, "Index Codes forMultibiometric Pattern Retrieval," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY , April 2012.
20. A. Juels and M. Sudan, "A fuzzy vault scheme," Designs, Codes Cryptograph., vol.38, no. 2, pp. 237–257, Feb. 2006.
21. Prakash,S., Ali, S.S., and Ganapathi, I.I.. Robust technique for finger print template protection. IET Biometrics, 7(6), pp.536-549.
22. Wong, K., Dong, X.B., and Jin, Z., 2018, November. "A Generalized Approach for Cancellable Template and Its Realization for Minutia Cylinder-Code",In 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) (pp. 908-915) IEEE.