ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Multi Biostatistics Scheme at Security Purpose by Using SDS Algorithm

H.Lookman Sithic[1], R.Kalpana[2]

Associate Professor, Department of BCA, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India [1]

Research Scholar, Dept. of CS, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India[2]

ABSTRACT: A growing concern regarding identity theft, national security, and on-line terrorism. Biometrics is seen by many researchers as a solution to a lot of user identification and security problems now days. Biometric identification is any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identify of an individual. Biometric science utilizes the measurements of a person's behavioral characteristics (keyboard strokes, mouse movement) or biological characteristics (fingerprint, iris, nose, eyes, jaw, voice pattern, etc). Modern biometric systems still face much reliability and efficiency related issues such as reference database search speed, errors while recognizing of biometric information or automating biometric feature extraction. In this paper fusion of fingerprint, iris and face traits are used at security purpose in order to improve the accuracy of the system, and then these securities are fused using Fuzzy and weighted logic, that weighted fuzzy logic gives excellent accuracy equal to 99.99 %. The SDS algorithm will generate the random shares of biometric images with a minimal computation without using any keys for crypto system. It will produce the original minutes to compare the biometric images in database and user biometrics.

KEYWORDS: Fingerprint, Iris, Face traits, Biometric, SDS algorithm, Fuzzy logic, Accuracy.

I. INTRODUCTION

A lot of decades ago, biometric characteristics have become very important tools in field of identity verification or identification. This is for its stability for long time and the ability to cope with theft or forgery or forgetfulness. Due to most of biometric systems are far from satisfactory in terms of user confidence and user friendliness and have a False Rejection Rate (FRR). So there is a need to develop novel algorithms for human recognition. Multimodal biometric systems use multiple modalities to overcome the challenges that arise when use single biometric trait such as: noise, non universality, lack of individuals and spoof attacks. Multimodal biometric systems perform better than unimodal biometric systems. In our work, three public biometrics are used "fingerprint, iris and face". In first stage image pre-processing is performed on fingerprint, iris and face images using different techniques for each biometric. In the second stage three feature extraction techniques are applied: Minutia based algorithm are used for fingerprint which extracts two types of points, ridge ending and ridge bifurcation. Modified Daugman's algorithm is used for iris recognition where enhanced iris image is segmented first to localize circular iris and pupil region, The extracted iris region was then normalized into a rectangular block with constant dimensions to account for imaging inconsistencies. Finally, the phase data from 1D Log-Gabor filters were extracted and quantized to four levels to encode the unique pattern of the iris into a bit-wise biometric template using Daugman's rubber sheet model. Local Binary Pattern LBP is performed for face images where face image is divided into cells then for each cell an 8-digit binary number is computed which converted to decimal form then histogram is computed over cells, finally all histograms are concatenated to give feature vector. In the third stage: matching scores from each matcher are arrived. In the fourth stage: each subsystem produce its individual decision, in our work every subsystem has two decision values either low or high. Then fusion of these decisions is executed using Fuzzy logic to get unary decision in the end. The objective of this research is as follow: Designing and implementing a multimodal biometric system of the combined biometrics "fingerprint, iris and face" and then fusing them at the security level by fuzzy logic. The reason to use three biometric traits is the desire to get high degree of discrimination when we have large number of users or population. Then we proposed a SDS algorithm to encrypt the image without using any keys. In this technique an image is splitted into random shares and the secret

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

image is recovered back by using all the generated random shares. The SDS (Sieving, Division, Shuffling) algorithm involves 3 steps. In the first step, the secret image is split into primary colors. In the second step, the split images are divided randomly. In the third step, the divided shares are shuffled within itself. Ultimately these shuffled shares are combined to generate the desired random shares. The use of SDS algorithm will reduce the computation of biometric system at security level.

II. LITERATURE SURVEY

Different literatures can be found which present variety of approaches for unimodal and multimodal biometric systems. Multimodal biometrics has been proposed by Ross and Jain in 2003. regarding fingerprint, iris and face biometrics fusion any pair of them" Fingerprint and Iris " , " Iris and Face" or "Fingerprint and Face" has attracted a lot of attention and different researches have proposed many of approaches. Houda benaliouchi et al. in 2014 presented comparative study on fusing iris and fingerprint at score level and decision level. Experimental results have shown that fuzzy logic method at decision level is more accurate than weighted sum rule at score level. Mohamed abdolahi et al. in 2013 had used two uni-modal biometrics, iris and fingerprint as multi-biometrics and found that using these biometrics give good result with high accuracy. Decision level is used for fusion and each biometric result is weighted for participate in final decision. Fuzzy logic is used for the effect of each biometric result combination. Yang and Fan in 2007 used fingerprint, palmprint and hand geometry to implement personal identity verification. These three biometric traits can be taken from the same image. they perform matching score fusion at different levels to establish person, performing a first fusion of the fingerprint and palm print features, and then a matching score fusion between the multimodal system and hand geometry system .the system was tested on a database containing the features self-constructed by 98 subject. Mohamed et al.in 2013 multimodal biometric system fusion using fingerprint and iris are proposed, decision level is used for fusion and each biometric result is weighted for participate in final decision .fuzzy logic is used for the effect of each biometric result combination. The proposed method has achieved high accuracy comparing with unimodal systems. Byungium and Yillbyung in 2005 were presented biometric authentication system based on iris and face; they applied 2-D discrete wavelet transform to extract the feature sets from iris and face. And then Linear Discriminant Analysis is applied to obtain reduced joint feature vector from these feature sets. Databases which used to show experimental results are ORL for face images, and for iris database the images are acquired through CCD camera with LED lamp around lens under indoor light. Ajita and Massimo in 2009 addressed the feature level fusion of multi-modal and multi-unit sources of information by proposing approach computes the SIFT features from both biometric sources. For each biometric trait feature selection on the extracted SIFT features was performed by spatial sampling then the features are concatenated to form a single vector using serial fusion. L.Latha and S.Thangasamy in 2010 they have used left and right irises and retinal features, and after matching process the scores are combined using weighted sum rule. To validate their approach, experiments were conducted on the iris and retina images obtained from CASIA and VARIA database respectively.

III. EXISTING SYSTEM

Biometric-based authentication systems represent a valid alternative to conventional approaches. Unimodal biometric systems made use of a single trait either fingerprints or iris or face traits. But they were not used for recognition; about 8% of people cannot use it and so it's not reliable; as it is single biometric system they can be lost or stolen, attacker can get authentication by forming clone with same features. Existing system enhanced the accuracy and security of Multi-biometric system using code-based cryptosystem. In addition of randomness cryptosystem also probabilistic, and give more susceptibility of template towards brute force attacks. It uses a public key cryptosystem to construct a commitment to achieve non-reputability and authentication.

Disadvantages of existing system:

The stored temple is easily hacked by attackers. In existing, computation is more and more information using in each templates, also more time consuming process.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

IV. PROPOSED SYSTEM

Multi biometric cryptosystem is combination various biometric like face, iris, fingerprint etc. The multi biometrics is used for security purpose and also improves the accuracy by using the weighted fuzzy logic and reduces the computation by using SDS algorithm. In fuzzy logic to provide high accuracy perform minutiae matching based on two types of points, ridge ending and ridge bifurcation. In SDS algorithm to encrypt, split the biometric images into primary RGB colors (Rs, Gs, Bs), second divided the split images randomly (RA, GA, BA), finally divided shares are shuffled itself (RA shuffle, GA shuffle, etc). These shuffled shares are combined to generate the desired random shares. To decrypt split the random shares to retrieves the RGB components then reshuffled the shares (RA, GA, BA) and combine all the shares to get the original biometric images.

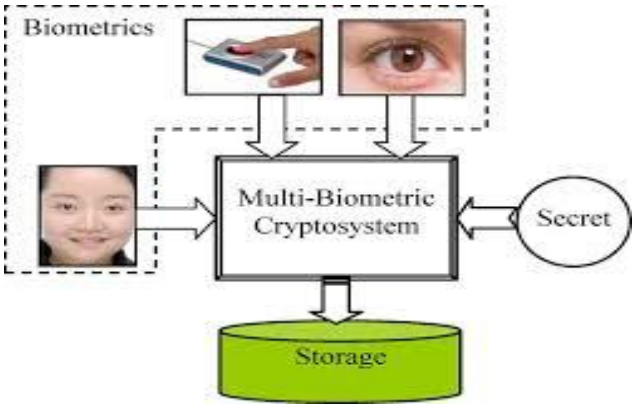

Fig 1: Multi biometric cryptosystem

ADVANTAGES OF PROPOSED SYSTEM:

It improving the accuracy of the biometric verification or identification and it provides a certain degree of flexibility; and resisting spoof attacks. Using of SDS algorithm reduce the computation.

V. MULTI BIOMETRIC SYSTEM

Fingerprints

Fingerprint has been researched the longest period of time and shows the most promising future in real-world applications. A fingerprint is formed of a group of curves. The most common characteristics include ridge ending and bifurcations called as minutiae. Due to the persistence and individuality of fingerprints, fingerprint recognition has become a popular personal identification technique. However, because of the complex distortions among the different impressions of the same finger, fingerprint recognition is still a challenging problem. Fingerprint is composed of ridges and furrows which are parallel and have the same width. In fingerprint recognition, fingerprint is distinguished by minutiae, which are points on the ridges. There are many types of minutia, but the two basic types are: termination which represents the ending of the ridge and the other is called bifurcation which is the point of the ridge from which two branches derive.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

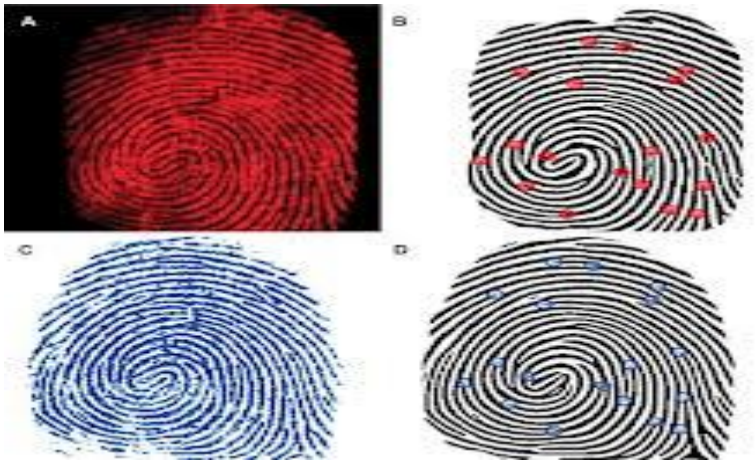

Fig 2: Fingerprint image and minutia points

Minutiae Extraction

The enhanced fingerprint image is binarized and submitted to the thinning algorithm which reduces the ridge thickness to one pixel wide. The skeleton image is used to extract minutiae points which are the points of ridge endings and bifurcations.

Fig 3: Ridge ending and bifurcation extraction

Iris Recognition

The iris system composes of a number of subsystems, which correspond to each stage of iris recognition. The stages include segmentation for locating the iris region in an eye image, normalization for creating a dimensionally consistent representation of the iris region, enhancement by histogram equalization of normalized iris region, feature encoding for creating an iris code containing only the most discriminating features of the iris and finally matching by hamming distance to make a decision of acceptance or rejection.

Segmentation is the first stage in iris pre-processing to isolate the required iris region from the whole eye image by separating the part of an image between the inner boundary and outer boundary.

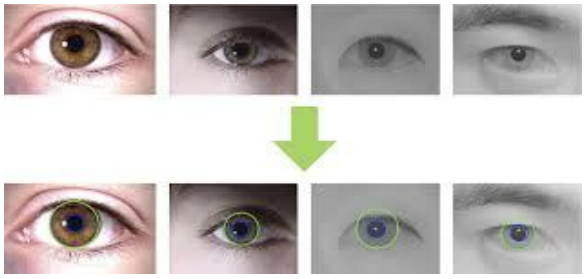

Fig 4: iris segmentation

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Normalization is a process of transforming the segmented iris region into fixed dimension. However, dimensional inconsistencies arise between eye images due to the stretching of iris, caused by pupil dilation from varying levels of illumination. Feature encoding extracts the underlying information from the iris pattern and generates the binary iris template that is used in matching. Matching is a process to determine whether two iris templates are from the same individual or not. Hamming distance is applied for bit-wise comparisons of images.

Face traits

Local Binary Patterns (LBP) is presented as a Strong local descriptor for microstructures of images. In this work local binary pattern are used for face recognition. The face area is first divided into small regions from which Local Binary Pattern (LBP) histograms are extracted and concatenated into a single vector.

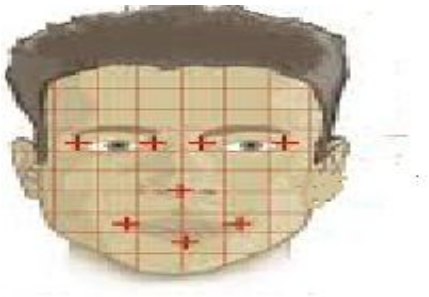

Fig 5 facial image into region

VI. SDS ALGORITHM IN MULTI BIOMETRIC SYSTEM

A SDS algorithm to encrypt the image without using any keys. By using this method in security level, the computation time of the verifying biometric images is reduced. In this technique an image is splitted into random shares and the secret image is recovered back by using all the generated random shares. The SDS (Sieving, Division, Shuffling) algorithm involves 3 steps. In the first step, the secret image is split into primary colors. In the second step, the split images are divided randomly.

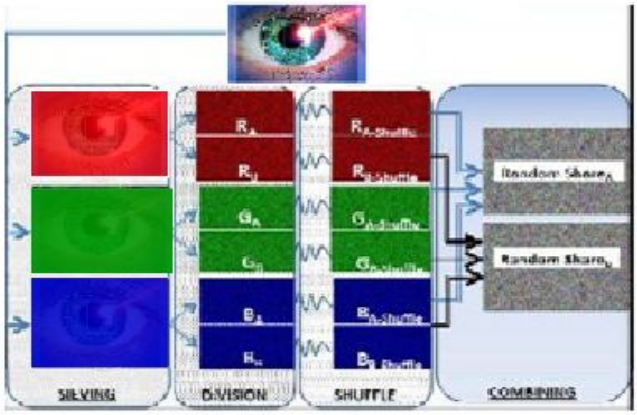

Fig 6: encrypt biometric image using SDS algorithm

In the third step, the divided shares are shuffled within itself. Ultimately these shuffled shares are combined to generate the desired random shares. The steps involved in generating two random shares during encryption are depicted. There

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

are two most preferred models for the representation of colors, additive and subtractive color models. In the additive color models or RGB, the three primary colors namely Red, Green, and Blue colors are mixed to get the desired colors. The example for the additive color model is the colors that visible on the computer monitor. While in the subtractive color model or CMY, Cyan, Magenta, and Yellow pigments are used to get the desired colors. This subtractive color model is widely used in printers. Since the results of encryption and decryption proposed in the technique are viewed on the computer monitors hence, it is natural to use the additive colors in the proposed technique.

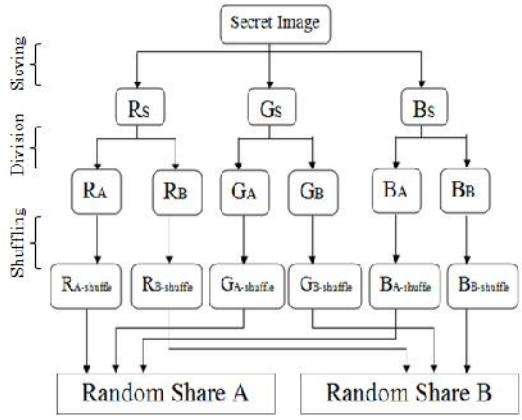

Fig 7: Steps involved in encryption to generate two random shares

To encrypt biometric images split the biometric images into primary RGB colors (Rs, Gs, Bs), second divided the split images randomly (RA, GA, BA), finally divided shares are shuffled itself (RA shuffle, GA shuffle, etc). These shuffled shares are combined to generate the desired random shares.

The decryption process of the SDS algorithm

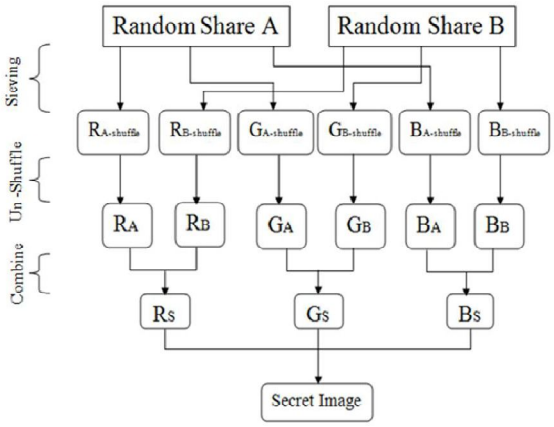

Fig 8: Steps involved in decryption process

To decrypt split the random shares to retrieves the RGB components then reshuffled the shares (RA, GA, BA) and combine all the shares to get the original biometric images.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

VII. COMPUTATION

Algorithm

Step 1: Sieving
Input _ Secret Image
Sieve(Secret Image)
Output _(R, G, B components)
Step 2: Division n = total number of pixels (0 to n-1)
Ri / Gi / Bi = individual values of the ith pixel in
the R, G, B components
z = total number of random shares
x =number of bits representing each primary color
max_val = 2x
Repeat 2 for R, G, B component
2(a) for i = 0 to (n-2)
{ for share k = A to (Z-1)
Rki = Random(0, max_val)
Aggr_Sumi = _ Rki
}
Rzi =(max_val + Ri – (Aggr_Sumi % max_val)) % max_val
Step 3: Shuffle
Repeat for RA-Z, GA-Z and BA-Z (all generated shares)
for k = A to Z
{ Rk-shuffle = Rk
PtrFirstVac = 1
PtrLastVac = n-1
For i = 1 to (n-1)
{ If (R(k+1)(i-1) is even)
{ R(k-shuffle)
PtrFirstVac = Rki PtrFirstVac ++, i++
}
Else
{
R(A-shuffle)
PtrFirstVac = RAi i++, PtrLastVac –
} } }

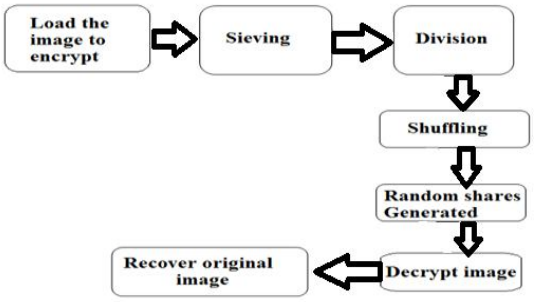

Fig 9: encrypt and decrypt without key

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

VIII. RESULT ANALYSIS

The performance and the computation of the SDS algorithm are compared. This project reduce the computation time compare with the existing system i.e., code based cryptosystem. Using this algorithm in biometric model gives high security and accuracy of the multimodal system.

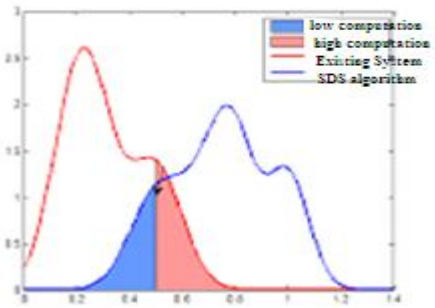

Fig 10: comparison of SDS and Existing system

IX. CONCLUSION AND FUTURE WORK

Many fusion strategies can be executed at different levels as follow: Feature level: The data obtained from sensor is used to extract the feature vector from one biometric trait which is independent from those extracted from the other; these feature vectors are concatenated to produce a single new vector. This process is difficult when feature vectors are heterogeneous. Matching score level: Each system provides a matching score indicating the nearness of the feature vector with the template vector. These scores can be combined to assert the veracity of the claimed identity. While the information contained in matching scores is not as rich as in images or features, it is much richer than ranks and decisions. Further, it is easier to study and implement than image-level and feature-level fusion. It can also be used in all types of biometric fusion scenarios. It will be extended in future to minimize the time consumed than the proposed one.

REFERENCES

1. B. Shanthini, S. Swamynathan "A Novel Multimodal Biometric Fusion Technique for Security", (ICIKM 2012) IPCSIT vol.45 (2012) © (2012) IACSIT Press, Singapore.
2. Jain, R. Bole and S. Pankanti, BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Press, Boston (1999).
3. Farhat Anwar, Md. Arafatur Rahman, Md. Saiful Azad "Multibiometric Systems Based Verification Technique", ISSN 1450-216X Vol.34 No.2 (2009), pp.260-270 © EuroJournals Publishing, Inc. 2009
4. Karthik Nandakumar and Anil K. Jain "Multibiometric Template Security Using Fuzzy Vault", BTAS 2008
5. Ajay Sharma , Deo Brat Ojha " A Multi-Biometric Template Security: An Application of Code-Based Cryptosystem", IJCIM Vol. 19. No.1 (January-April, 2011) pp 14 -24
6. Abhishek Nagar, Karthik Nandakumar, Anil K. Jain "Biometric Template Transformation: A Security Analysis"
7. B. Fu, S. X. Yang, J. Li, and D. Hu, "Multibiometric cryptosystem: Model structure and performance analysis," IEEE Trans. Inf. Forensics Security, vol. 4, no. 4, pp. 867–882, Dec. 2009.
8. Rahib Hidayat Abiyev and Kemal Ihsan Kilic "Robust Feature Extraction and Iris Recognition for Biometric Personal Identification", Department of Computer Engineering, Near East University, Nicosia, North Cyprus
9. Chaohong Wu, "Advanced Feature Extraction Algorithms for Automatic Fingerprint Recognition Systems", April 2007.
10. Bhumika G. Bhatt, Zankhana H. Shah "Face Feature Extraction Techniques: A Survey", May 2011 B.V.M. Engineering College, V.V.Nagar,Gujarat,India
11. Liliana Ferreira, Niklas Jakob and Iryna Gurevych "A Comparative Study of Feature Extraction Algorithms in Customer Reviews" , © 2008 IEEE DOI 10.1109/ICSC.2008.40
12. Shailesh Kumar, Joydeep Ghosh, and Melba M. Crawford, Member, IEEE "Best-Bases Feature Extraction Algorithms for Classification of Hyperspectral Data", IEEE, VOL. 39, NO. 7, JULY 2001.
13. Sunil Chawla and Aashish Oberoi. 2011 "A robust algorithm for iris segmentation and normalization using hough transform." Global Journal of Business Management and Information Technology, 1(2):69–76.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

14. Zhenhua Guo, Lei Zhang, and David Zhang. 2010 "Rotation invariant texture classification using lbp variance (lbpv) with global matching". Pattern recognition, 43(3):706–719.
15. Anil K Jain, Arun Ross, and Salil Prabhakar. 2004 "An introduction to biometric recognition. Circuits and Systems for Video Technology", IEEE Transactions on, 14(1):4–20.
16. Philippe Parra. "Fingerprint minutiae extraction and matching for identification procedure". University of California, San Diego La Jolla, CA, pages 92093–0443.
17. BG Sherlock, DM Monro, and K Millard. 1994 "Fingerprint enhancement by directional fourier filtering". In Vision, Image and Signal Processing, IEEE. Proceedings-, volume 141, pages 87–94. IET.
18. wuzhili. 2002 "fingerprint recognition".
19. Heng Fui Liau and Dino Isa. 2011 "Feature selection for support vector machine-based face-iris multimodal biometric system". Expert Systems with Applications, 38(9):11105–11111.
20. Hugo Proenc¸a and Luıs A Alexandre. 2006. "Iris recognition: An analysis of the aliasing problem in the iris normalization stage". In Computational Intelligence and Security, 2006 International Conference on, volume 2, pages 1771–1774. IEEE.

BIOGRAPHY

Mr.H.LOOKMAN SITHIC M.S(IT).,M.Phil.,[Ph.D]., He received him MS(IT) degree from Jamal Mohamed College, Bharathidasan university and M.Phil(c.s)degree from Periyar University, Salem. He is having 14 years of Experience in Collegiate Teaching and He is the Associate professor in depart of BCA in Muthayammal College of Arts and Science, Rasipuram, Affiliated by Periyar University, Salem, Tamilnadu, India. His main research interested include Data Mining.

Ms.R.KALPANA has born on 28.05.1991 in Tamilnadu, India. She received BSc in 2011 from Vivekanandha College of Arts & Science for Women, Elayampalayam, Affiliated to Periyar University, Salem, Tamilnadu, India. She received B.Ed in 2012 from Vivekanandha College of Education for Women, Elayampalayam, Affiliated to Tamilnadu Teachers Educational University,Chennai, Tamilnadu, India. She received M.Sc in 2014 from Muthayammal College of Arts & Science, Rasipuram, Affiliated to Periyar University-Salem, Tamilnadu, India. She is Pursuing M.phil (full time) from Muthayammal College of Arts & Science in Periyar University, Salem, Tamilnadu, India. Her interested area is Computer Networks.