IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-5, Issue-11 E-ISSN: 2347-2693

Multimodal Approach on Finger Vein and Fingerprint by Using Visual Steganography for Efficient Biometric Security

P. Anitha[1*], M. Grace[2]

[1*] Department of Computer Science, Soka Ikeda College of Arts & Science for Women, Chennai-99, India
[2] Department of Computer Science, Soka Ikeda College of Arts & Science for Women, Chennai-99, India

**Corresponding Author: anithajoy81@gmail.com*

Available online at: www.ijcseonline.org

Received: 16/Oct/2017, Revised: 29/Oct/2017, Accepted: 22/Nov/2017, Published: 30/Nov/2017

***Abstract*-**Nowadays our systems need strong security to protect data and resources access from unauthorized persons. For that purpose, biometric-based authentication system provides more security than other approaches. Uni-modal biometric systems use only one biometric trait such as fingerprint, finger vein, voice, face, ear, iris, retina etc., which has some limitations due to noise, spoof attacks etc., The multimodal biometric system is the combination of more than one biometric trait to authenticate an individual. In this paper, a multimodal approach has been proposed by integrating the finger vein and fingerprint to enhance the performance of personal recognition system. Preserving the privacy of stored biometric templates in a centralized database is of more important at present. Visual Steganography provides a very powerful technique by which one secret can be distributed in two or more shares. When the shares on transparencies are superimposed exactly together, the original secret can be discovered without computer participation. In the enrollment procedure, the secret key is encrypted by using AES algorithm and by using the visual steganographic technique, the encrypted secret key is shared between the two images. The share1 is kept as the users' ID card and the share2 is stored in the database. In the verification procedure, new finger vein and fingerprint images are obtained and verified with the images stored in the database. It is computationally hard to obtain the biometric image from any individual stored sheets. This paper explores the possibility of using visual steganography for efficient biometric security in the multimodal approach.

Keywords: *Uni-modal approach, Multimodal approach, Visual Steganography, finger vein, fingerprint, AES.*

I. INTRODUCTION

A. Biometrics

The use of biometrics to identify personnel is widely adopted in the current day scenario. Automated recognition of individuals based on their biological and behavioural characteristics are termed as biometrics. The term biometrics is derived from Greek words, “bio” means “life” and “metrics” means “measure”. So biometrics is the measurement and statistical analysis of people’s physical and behavioural characteristics.

Uni-modal systems use single biometric trait for recognition purposes suffer from several practical problems like noisy data, spoof attacks etc., Multimodal biometric systems make use of different biometric traits simultaneously to authenticate a person’s identity. From the Table 1, it is clear that the combination of fingerprint and finger vein biometric traits is both an attractive alternative in comparison to other biometrics [1].

Table 1. Comparison of different biometric technologies [1]

Biometrics	**Universality**	**Uniqueness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvention**
Face	H	L	M	H	L	H	L
Finger print	M	H	H	M	H	M	H
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Retina	H	H	M	L	H	L	H
Finger vein	H	M	M	M	H	M	L

L-Low, M-Medium, H-High

Preserving the privacy of stored biometric templates in a centralized database is of more important at present. This paper investigates on the multimodal biometric authentication methods used for fusion of two biometric traits, fingerprint and finger vein and the importance of visual steganography for enhancing the security.

B. Visual Steganography

Fusion of fingerprint and finger vein multimodality provides the following advantages [2] like, the two biometrics are mature and independent, enabling an efficient fusion, increase spoof resistance as two biometrics need to be reproduced including one which is not directly accessible. The simultaneous acquisition of two sets of biometric data can be captured and processed at the same time using a single device, improves both FAR and FRR compared to uni-modal technologies.

Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. In order to improve the security features in data transfers over the internet, many techniques such as Cryptography, Steganography etc., have been developed. Steganography is the art of hiding the existence of the communication message before sending it to the receiver. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words “steganography means hiding one piece of data within another” [3].

Visual Steganography provides a very powerful technique by which one secret can be distributed in two or more shares as shown in Figure 1. When the shares on transparencies are superimposed exactly together, the original secret can be discovered without computer participation [4].

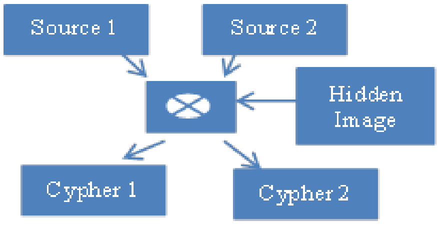

Figure .1. Visual Steganography

II. PROPOSED WORK

This paper consists of four modules such as Image acquisition and pre-processing of Finger vein, Image acquisition and pre-processing of Fingerprint, Enrollment process and Verification process.

A. Image Acquisition and Preprocessing of Finger vein

The individuality of finger vein compared to other existing biometrics are, it isn’t sensitive for environmental conditions such as wet, dirt and it’s a fraud-proof biometric, remains constant throughout the life, non-contact acquisitions etc., .Finger vein authentication is a method that specifies an individual using the vein pattern inside one's fingers. Since de-oxy hemoglobin in the blood absorbs near-infrared lights, vein patterns appear as a series of dark lines as shown in Figure 2. The near-infrared lights combined with a special camera capture an image of the finger vein patterns [5] and [6]. The image is then converted into pattern data and stored as a template of a person's biometric authentication data.

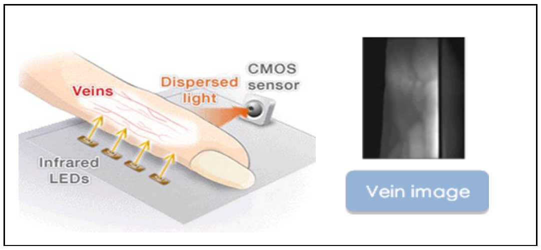

Figure 2. Image acquisition of Finger vein

After the finger vein raw image captured, it is required to preprocess the raw image. The captured finger vein images are the noisy and low contrast with translational and rotational variations from unconstrained imaging [7]. Finger vein image preprocessing involves image ROI detection, image enhancement, and feature extraction. After the raw image captured, it is required to be preprocessed before feature extraction. The unwanted regions have been removed by choosing the interested area in the image called region of interest (ROI) and can be done by extracting the centroid and then selecting an area around them [8]. Edge detection is an image processing technique for finding the boundaries of objects within images [9]. For segmentation purpose, Canny Edge detection method is the best optimal algorithm among the edge detection algorithms [10]. It works by detecting discontinuities in brightness. The fundamental criteria of canny edge detection algorithm are low error rate and good localization [11].

B. Image Acquisition and Preprocessing of Fingerprint

One of the most commercially available biometric technologies is fingerprint recognition, devices for desktop and laptop access are now widely available, users no longer need to type passwords instead, and only a touch provides instant access [12]. The fingerprint image contains minutiae points, core points, ridges and valleys, local features such as bifurcation, termination, bridge, hook etc., and global features such as core and delta. It has four types of patterns such as whorl, right loop, left loop and arch as shown in Figure 3.

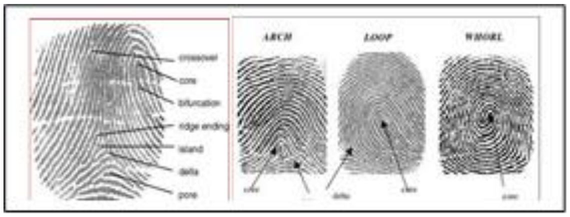

Figure 3. Finger print structures

In this paper, the image enhancement is done using intensity adjustment method based on the threshold. This method is used to adjust the intensity levels of a fingerprint image. After selecting a specific area, create the intensity level of that specific area and calculate the threshold value of intensity levels. The threshold value decides how much intensity should be adjusted or not. Binarization process converts a grey level image into the binary image to improve the contrast between the ridges and valleys in a fingerprint image which leads to the extraction of minutiae [13]. The segmentation process is to define which part of fingerprint image belongs to the background (furrows or irrelevant part) and foreground area (ridges and relevant area).

Principal Component Analysis (PCA) is used for reducing dimensions of the fingerprint image (ie) from higher dimensional space to lower dimensional space. The drawback of PCA is it works only in linear fashion leads to the development of new method called Kernel PCA (KPCA) which represents nonlinear mappings in a higher dimensional feature space. The KPCA method produced the better result with less error when compared to PCA [14]. A Gabor filter is a linear filter used for edge detection and is applied to extract feature vectors [15]. The feature vectors generated using Gabor filters form feature maps which are used for the matching process.

C. Enrollment Process

Enrollment and verification of authorized personnel are the important functions of the recognition systems. The recognition systems enroll authorized personnel based on the data provided by the biometric sensors and store the data for future verification or matching. In this paper, the new user needs to register with the system and the existing users' can login into the system in order to access the system features. The new user needs to specify the basic personal information such as name, email id, aadhaar number and his/her finger vein image and fingerprint image. As the images were obtained from different sources, it is necessary to keep the template secure. A cryptographic algorithm can be used to secure the template [16]. Here the aadhaar number can be used as the secret key and it was encrypted by using the AES algorithm.

The Figure 4, explains the enrollment part, where the administrator will collect the finger vein and fingerprint image. Those enrolled biometric images are required to undergo certain processing steps and then pass on to visual steganography technique, where it can be divided into two shares. Along with the two shares, the encrypted secret key is also divided and kept with the two shares. The first share of the encrypted secret key is stored on the user’s identity card (ID) and the other share is stored in the database. On superimposing these two shares perfectly, the encrypted secret key is visible to us. On next time when the user comes for authentication, he has to provide his/her ID card, finger vein, and fingerprint as he is already enrolled in the system.

D. Verification Process

In this verification or authentication part, as shown in Figure 5, the user has to provide the ID card allocated to him/her and the finger vein and their fingerprint image in order to complete the authentication process. When the user provides ID card, by using the share on the card and the other share in the database, we create the temporary image having the features from the original image obtained during the enrollment process. This temporary image is then matched with the newly captured finger vein and fingerprint image which is provided in the authentication. The result shows either the user is authenticated or not.

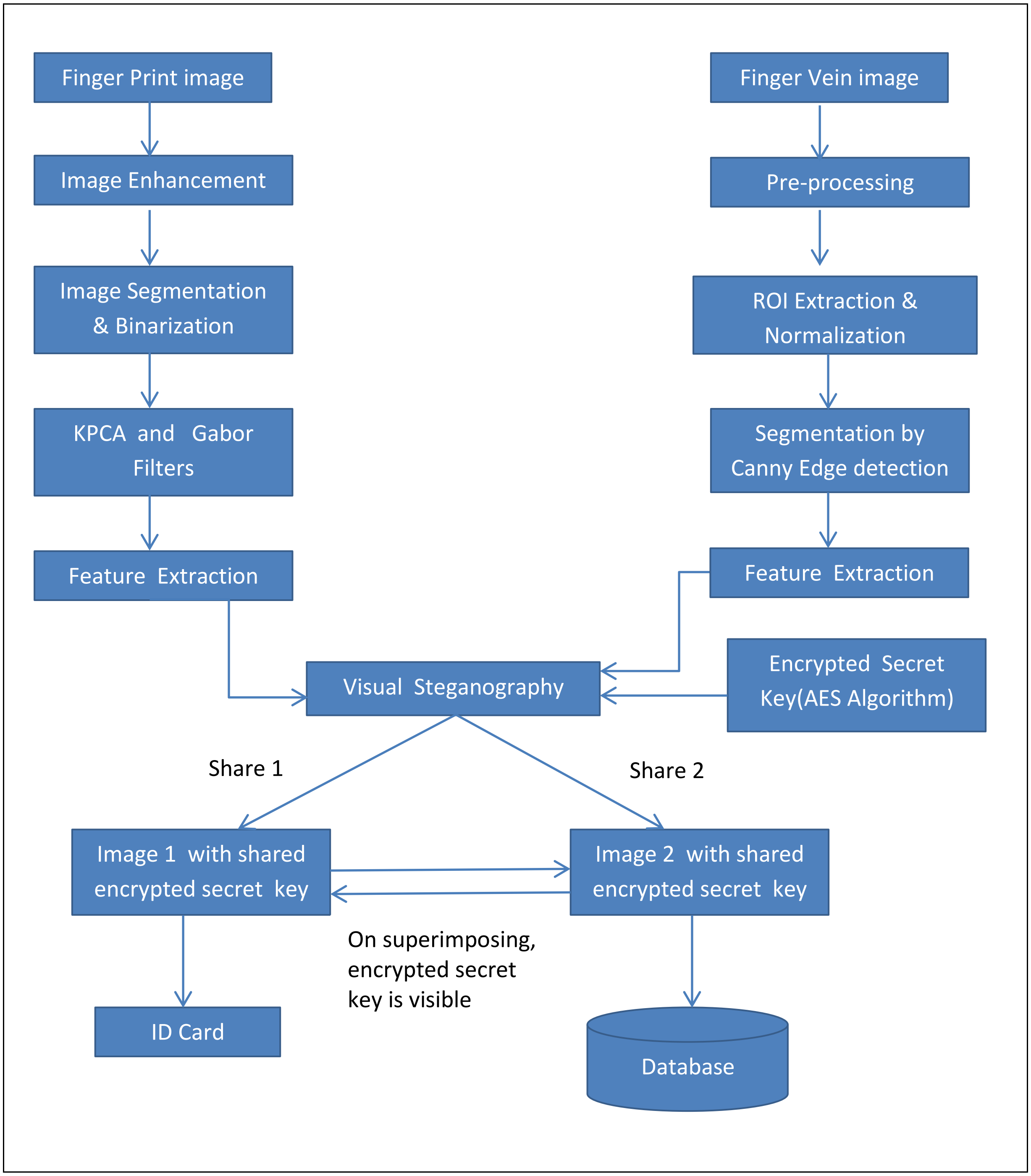
Finger Print image
Image Enhancement
Image Segmentation & Binarization
KPCA and Gabor Filters
Feature Extraction
Finger Vein image
Pre-processing
ROI Extraction & Normalization
Segmentation by Canny Edge detection
Feature Extraction
Encrypted Secret Key(AES Algorithm)
Visual Steganography
Share 1
Share 2
Image 1 with shared encrypted secret key
Image 2 with shared encrypted secret key
On superimposing, encrypted secret key is visible
ID Card
Database

Figure 4. Enrollment Process

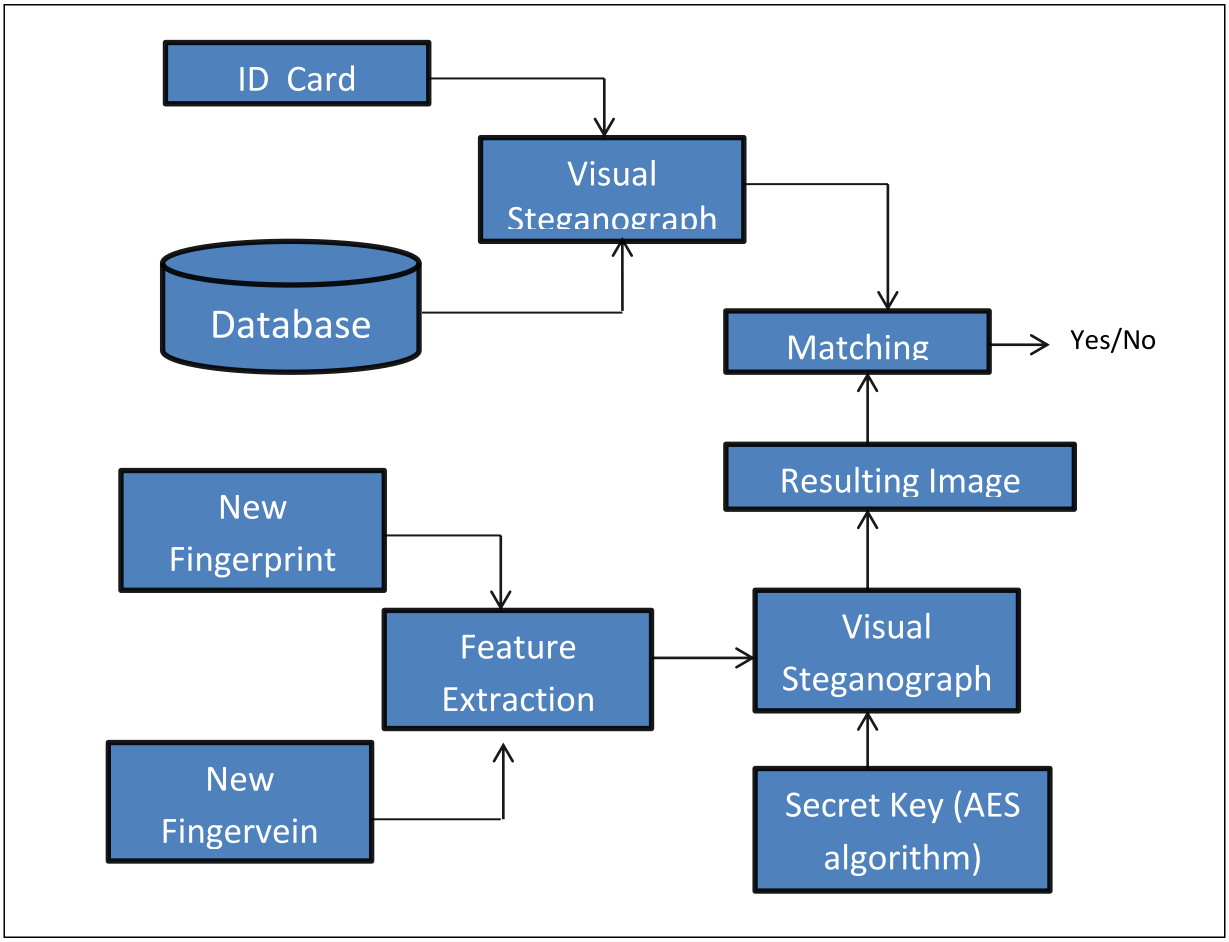

Figure 5. Verification Process

III. CONCLUSION

Various approaches were adopted by researchers nowadays to secure the raw biometric data and the template in a database. In this paper, a method is proposed to store hybrid biometric templates such as finger vein and fingerprint images in the database. The secret key (aadhaar number) is encrypted using the AES algorithm. Using visual steganography, the encrypted secret key is shared between the two images. The finger vein and fingerprint images can be reconstructed only when both sheets are simultaneously available. It is computationally hard to obtain the biometric image from any individual stored sheets. This paper concludes that by applying the visual steganography techniques on the hybrid biometric template provides more security.

REFERENCES

[1] Hatim A. Aboal samh, *"A Multi Biometric System using combined Vein and Fingerprint Identification"*, International Journal of Circuits, Systems and Signal Processing, pp 29-36, Issue 1, Vol.5, 2011.

[2] T.Sheeba, M. Justin Bernard, "*Survey on Multimodal Biometric Authentication Combining Fingerprint and Finger vein"*, International Journal of Computer Applications (0975-8887), Vol.51,No. 5, 2012.

[3] Neha Chhabra, *"Visual Cryptographic Steganography in Images"*, International Journal of Computer Science and Network Security, pp 126-131, Vol.12, No.4, 2012.

[4] K. Sankareswari, S. Arul Jothi, *"Hybrid Approach for Securing Biometric Templates Using Visual Cryptography"*, International Journal of Advance Research in Computer Science and Management Studies, pp 61-65, Vol.3, Issue 9, 2015.

[5] Jinfeng Yang, Yihua Shi, *"Towards Finger Vein Image Restoration and Enhancement for Finger Vein Recognition",* Elsevier, Information Sciences, pp 33-52, 268, 2014.

[6] Wenming Yang, Xiaola Huang, Fei Zhou, Oingmin Liao, *"Comparative and competitive coding for personal identification by using finger vein and finger dorsal texture fusion"*, Information Sciences, pp 20-32, 268, 2014.

[7] Lu Yang, Gang ping Yang, Yilong Yin, Rongyang Xiao, *"Sliding Window-Based Region of Interest Extraction for Finger Vein Images",* Sensors, 2013.

[8] Humairah Hamid, V.K. Narang, Priti Singh, *"Review on Vein Pattern Based Biometric Systems"*, International Journal of Innovative Research in Science, Engineering and Technology, Vol.6, Issue 5, 2017.

[9] Shaik Riyaz Ulhaq, Shaik Imityaz, Selvakumar, L.Gopinath, *"Multimodel Biometric Template Authentication of Fingervein and Signature using Visual Cryptography"*, International Journal of Engineering and Techniques, Vol. 3, Issue 3, 2017.

[10] A. L. Kabade, *"Canny edge detection algorithm"*, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), 5(5):1292-1295, 2016.

[11] Kayode A. Akintoye, M. Rahim M. Shafry, Abdul Hanan Abdullah, *" A Novel Approach for Finger Vein Pattern Enhancement using Gabor and Canny Edge Detector"*, International Journal of Computer Applications (0975 – 8887), Vol. 157, No 2, 2017.

[12] Shanthakumar, Janardhan Naidu, *"An Efficient Personnel Authentication Through Multi modal Biometric System"*, International Journal of Scientific Engineering and Applied Science (IJSEAS), Vol.2, Issue 1, ISSN: 2395-3470, pp. 534-543, 2016.

[13] Sangeetha Narwal , Daljit Kaur, *"Comparison between Minutiae Based and Pattern Based Algorithm of Fingerprint Image"*, International Journal of Information Engineering and Electronic Business, 2, pp. 23-29, 2016.

[14] Mohammad Mohsen Ahmadinejad, Elizabeth Sherly, *"A Comparative Study on PCA and KPCA Methods for Face Recognition",* International Journal of Science and Research (IJSR), ISSN: 2319-7064, Vol. 5, Issue 6, 2016.

[15] Kondreddi Gopi, J.T. Pramod, *"Fingerprint Recognition Using Gabor Filter and Frequency Domain Filtering",* IOSR Journal of Electronics and Communication Engineering, Vol. 2, Issue 6, pp.17-21, 2012.

[16] T. Srinivasa Rao, E. Srinivasa Reddy, "*A Multimodal Biometric Authentication Technique using Fused Features of Finger, Palm and Speech",* International Journal of Computer Sciences and Engineering, Vol. 5, Issue 8, E-ISSN:2347-2693, 2017.

Author's Profile

P. Anitha, received the M.Phil degree in Computer Science from Alagappa University in 2011, MCA., degree in Computer Applications in Alagappa University in 2008 and B.Tech., degree in Polymer Technology in Madurai Kamaraj University in 2002. From 2015, she is working as an Assistant Professor in Soka Ikeda College of Arts and Science for Women, Chennai, India. Her area of interest is Information Security, Computer Networks and Biometric systems.

M. Grace, received the M.Phil degree in Computer Science from Alagappa University in 2006, MCA degree in Computer Applications in Bharathidasan University 2002, and ME., degree in Computer Science in 2013. From 2002 to 2005, she worked as an Assistant Professor in Srimathi Indhira Gandhi College of Arts and Science for Women, Trichy and from 2006 to 2011, worked as a Lecturer in Jaya Engineering College in Chennai. From 2012, she is working as an Assistant Professor in Soka Ikeda College of Arts and Science for Women, Chennai, India. Her area of interest is Information Security and Computer Networks.