ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 2, Issue 3, DOI: 10.29027/IJIRASE.v2.i3.2018, 285-291, September 2018

The Usage of Vein and Iris Along with Visual Steganography for Efficient User Authentication

P. Anitha[1], M. Grace

[1]Department of Computer Science, Soka Ikeda College of Arts & Science for Women, Chennai-99, India.
Email: anithajoy81@gmail.com
[2]Department of Computer Science, Soka Ikeda College of Arts & Science for Women, Chennai-99, India.
Email: graceloisjohn@gmail.com

Abstract

Lately biometric based recognizable pieces of proof are broadly received for individual distinguishing proof. Uni-modular biometric frameworks utilize just a single biometric quality, for example, unique mark, finger vein, voice, confront, ear, iris, retina and so forth., which has a few impediments because of clamor, parody assaults and so forth., These downsides can be overwhelmed by setting up multi-modular biometric frameworks comprising of at least two biometric modalities in a solitary recognizable proof framework to enhance the acknowledgment precision. In this paper, a multimodal approach has been proposed by coordinating the finger vein and iris to improve the individual acknowledgment framework. Saving the protection of put away biometric formats in a brought together database is of more vital at present. Visual Steganography gives an intense strategy by which one mystery can be circulated in at least two offers. At the point when the offers on transparencies are superimposed precisely together, the first mystery can be found without PC cooperation. In the enlistment methodology, the mystery key (Aadhaar number) is encoded by utilizing AES calculation and by utilizing the visual steganographicsystem; 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 iris 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:*Multimodal approach, Visual Steganography, Finger vein, Iris, AES.*

I. INTRODUCTION

A. Biometrics

Security of information has been a noteworthy issue from numerous years. The seniority strategy of encryption and unscrambling has been anything but difficult to track for individuals around. Giving security to information utilizing new strategy is the need of great importance. For mechanized individual recognizable proof biometric verification is getting more consideration these days. Computerized acknowledgment of people in view of their natural and social attributes are named as biometrics. From the Figure 1, plainly the use of biometrics is the estimation and measurable examination of individuals' physical and social attributes [1]which gives more prominent security.

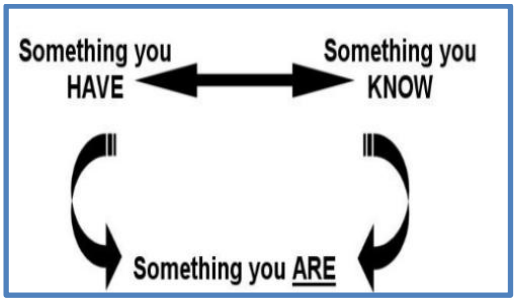

Figure 1: Biometrics

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 iris biometric traits is both an attractive alternative in comparison to other biometrics.

ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 2, Issue 3, DOI: 10.29027/IJIRASE.v2.i3.2018, 285-291, September 2018

Table 1. Comparison of different biometric technologies

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,finger vein and iris and also the importance of visual steganography for enhancing the security.

B. Visual Steganography

Information security essentially implies assurance of information from unapproved clients or programmers and giving high security to avert information change. Keeping in mind the end goal to enhance the security includes in information exchanges over the web, numerous strategies, for example, Cryptography, Steganography and so forth., have been produced. Steganography is the specialty of stowing away and transmitting the information through clearly harmless transporters to disguise the presence of the information [2].The target of steganography is to shroud a mystery message inside a cover-media so that others can't perceive the nearness of the concealed message. In fact in basic words "steganography implies concealing one bit of information inside another" [3].

Visual Steganography gives a ground-breaking strategy by which one mystery can be conveyed in at least two offers as appeared in Figure 2. At the point when the offers on transparencies are superimposed precisely together, the first mystery can be found without PC support [4].

ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 2, Issue 3, DOI: 10.29027/IJIRASE.v2.i3.2018, 285-291, September 2018

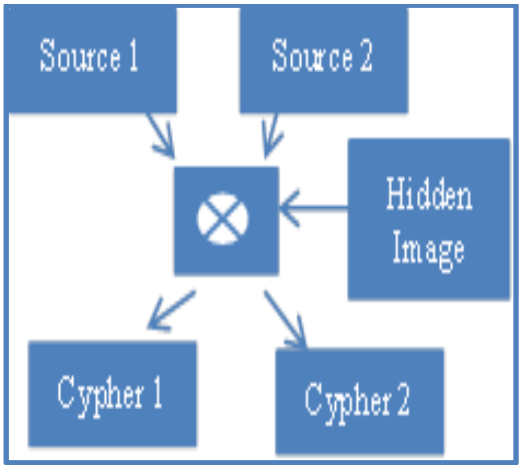

Figure .2. Visual Steganography

I. PROPOSED WORK

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

A. Image Acquisition and Preprocessing of Finger vein

Veins are our special character. As veins are available underthe skin, an endeavor to duplicate a personality is greatly troublesome. These properties of uniqueness,stability and solid insusceptibility to fabrication of the vein designs make it a possibly decent biometric traitwhichoffers more prominent security and dependable highlights for individual distinguishing proof [5].

Finger vein validation is a technique that determines an individual utilizing the vein design inside one's fingers.The independence of finger vein contrasted with other existing biometrics are, it isn't touchy for ecological conditions, for example, wet, earth and it's a cheat verification biometric, stays steady for the duration of the life, non-contact acquisitions and so forth., .. Since de-oxy hemoglobin in the blood retains close infrared lights, vein designs show up as a progression of dull lines as appeared in Figure 3. The close infrared lights joined with an uncommon camera catch a picture of the finger vein designs [6] and [7]. The picture is then changed over into design information and put away as a layout of a man's biometric verification information.

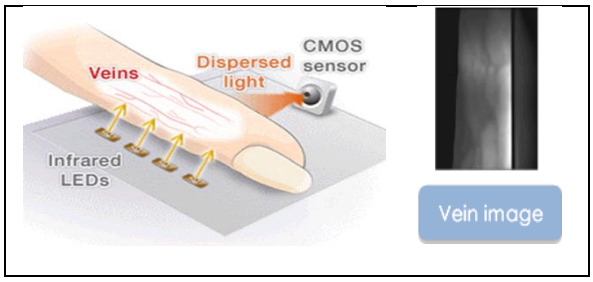

Figure 3. Image acquisition of Finger vein

After the finger vein crude picture caught, it is required to preprocess the crude picture. The caught finger vein pictures are the uproarious and low appear differently in relation to translational and rotational varieties from unconstrained imaging [8]. Finger vein picture preprocessing includes picture ROI identification, picture improvement, and highlight extraction. After the crude picture caught, it is required to be preprocessed before highlight extraction. The undesirable districts have been evacuated by picking the intrigued zone in the picture called locale of intrigue (ROI) and should be possible by removing the centroid and afterward choosing a territory around them [9]. Edge discovery is a picture preparing strategy for finding the limits of articles inside pictures [10]. For division reason, Canny Edge discovery strategy is the best ideal calculation among the edge recognition calculations [11]. It works by identifying discontinuities in brilliance. The crucial criteria of watchful edge recognition calculation are low blunder rate and great restriction [12].

B. Image Acquisition and Preprocessing of Iris

The Iris is a remotely noticeable and all around ensured organ whose one of a kind epigenetic appealing example remains stablethroughout the grown-up life. These qualities make it exceptionally alluring for use as biometric distinguishing individuals.Image handling system can be utilized to extricate the extraordinary iris design from a digitized picture of eye, andencode it in to biometric layout contains a goal numerical portrayal of one of a kind data put away in iris,and enables correlation with be made between formats [13].

In this paper, iris acknowledgment framework predominantly incorporates eye picture catching, picture pre-handling and edge discovery through iris district division, highlight extraction and example coordinating. Among them edge location is one of the real part in iris acknowledgment framework [14]. Edge recognition is partitioned into three primary advances: picture

ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 2, Issue 3, DOI: 10.29027/IJIRASE.v2.i3.2018, 285-291, September 2018

pre-preparing, include extraction of iris picture and layout coordinating. Picture pre-handling comprises picture transformation from RGB picture to dim picture, edge recognition, limitation of iris in a given eye picture, sifting and so on. By and large edge location goes for recognizing focuses in an advanced picture where picture brilliance changes pointedly. The focuses at which picture splendor changes forcefully are regularly sorted out into an arrangement of bended line fragments named edges. Watchful edge location calculation keeps running in a few stages. First in smoothing step, the administrators obscure the picture to expel commotion. At that point in discovering inclinations step when administrator recognizes the vast greatness of slope of picture it denotes the edges. In non-most extreme concealment step the administrator search for neighborhood maxima and stamped it as edges. At that point the administrator applies limit to decide potential edge. In conclusive advance edges are controlled by smothering all edges that are not associated with solid edge as shomwn in Figure 4.

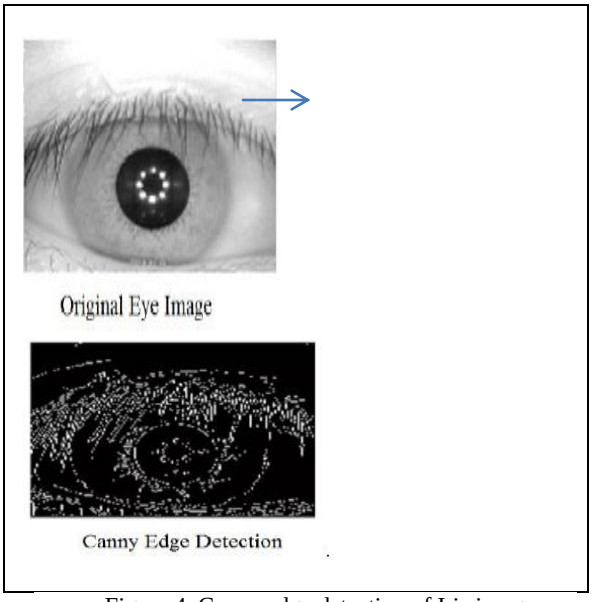

Figure 4. Canny edge detection of Iris image

The Canny edge location system is more productive to recognize both the moderate variety of dark level and solid variety of dim level of the picture.

C. Enrollment Process

Enlistment and check of approved faculty are the vital elements of the acknowledgment frameworks. The acknowledgment frameworks select approved work force in view of the information given by the biometric sensors and store the information for future confirmation or coordinating. In this paper, the new client needs to enroll with the framework and the current clients' can login into the framework keeping in mind the end goal to get to the framework highlights. The new client needs to determine the fundamental individual data, for example, name, email id,aadhaar number and his/her finger vein picture and iris picture. As the pictures were acquired from various sources, it is important to keep the layout secure. A cryptographic calculation can be utilized to anchor the layout [15]. Here the aadhaar number can be utilized as the mystery key and it was scrambled by utilizing the AES calculation.

The Figure 5, clarifies the enlistment part, where the overseer will gather the finger vein and iris picture. Those selected biometric pictures are required to experience certain preparing steps and after that pass on to visual steganography system, where it very well may be separated into two offers. Alongside the two offers, the scrambled mystery key is likewise isolated and kept with the two offers. The main offer of the scrambled mystery scratch is put away on the client's personality card (ID) and the other offer is put away in the database. On superimposing these two offers splendidly, the encoded mystery key is noticeable to us. On next time when the client seeks verification, he needs to give his/her ID card, finger vein, and iris picture as he/she is as of now selected in the system.

D. Verification Process

In this confirmation or validation part, as appeared in Figure 6, the client needs to give the ID card assigned to him/her and the finger vein and their iris picture keeping in mind the end goal to finish the verification procedure. At the point when the client gives ID card, by utilizing the offer on the card and the other offer in the database, we make the brief picture having the highlights from the first picture acquired amid the enlistment procedure. This brief picture is then coordinated with the recently caught finger vein and iris picture which is given in the confirmation. The outcome indicates either the client is validated or not.

ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 2, Issue 3, DOI: 10.29027/IJIRASE.v2.i3.2018, 285-291, September 2018

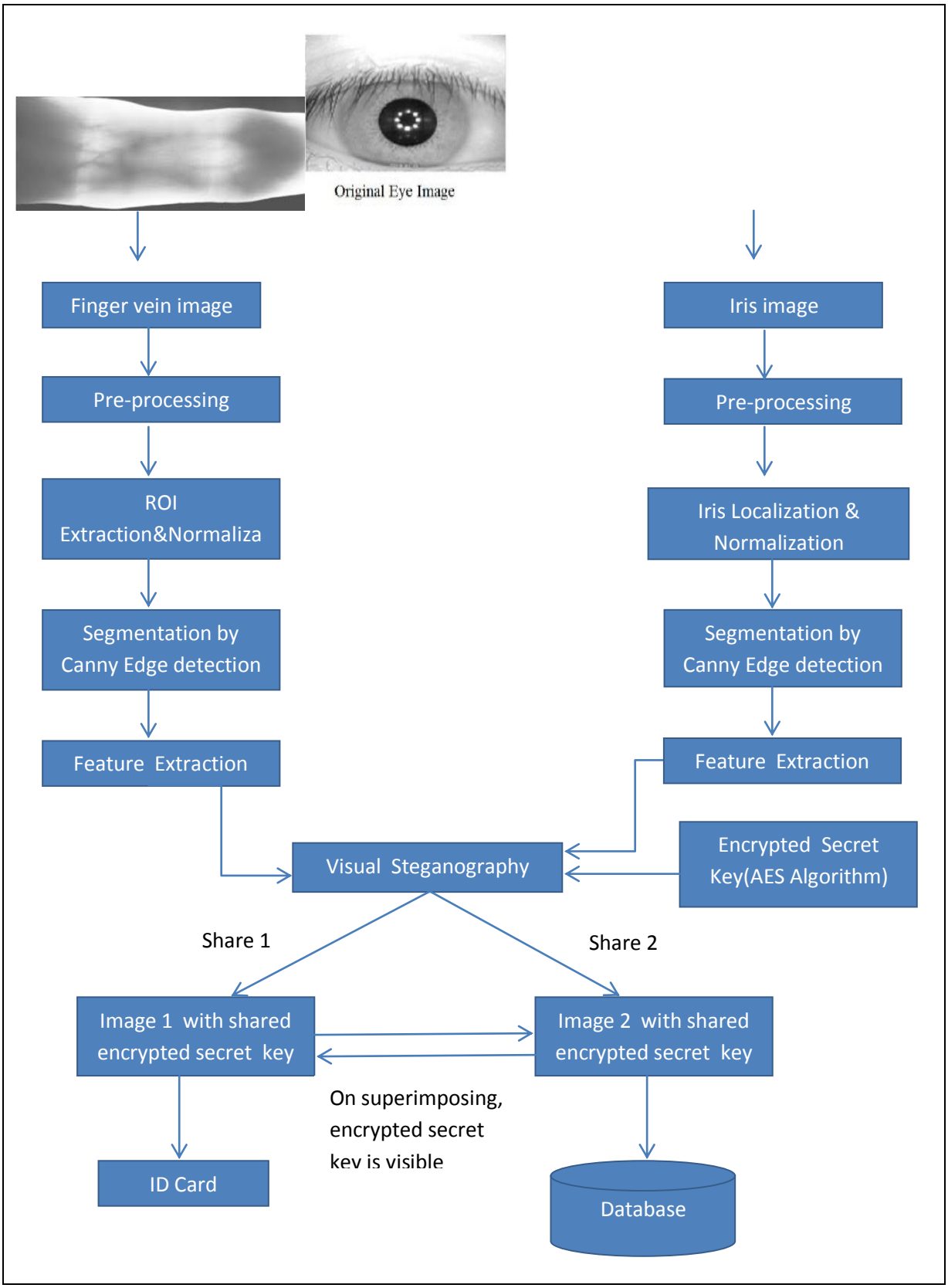

Figure 5. Enrollment Process

ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 2, Issue 3, DOI: 10.29027/IJIRASE.v2.i3.2018, 285-291, September 2018

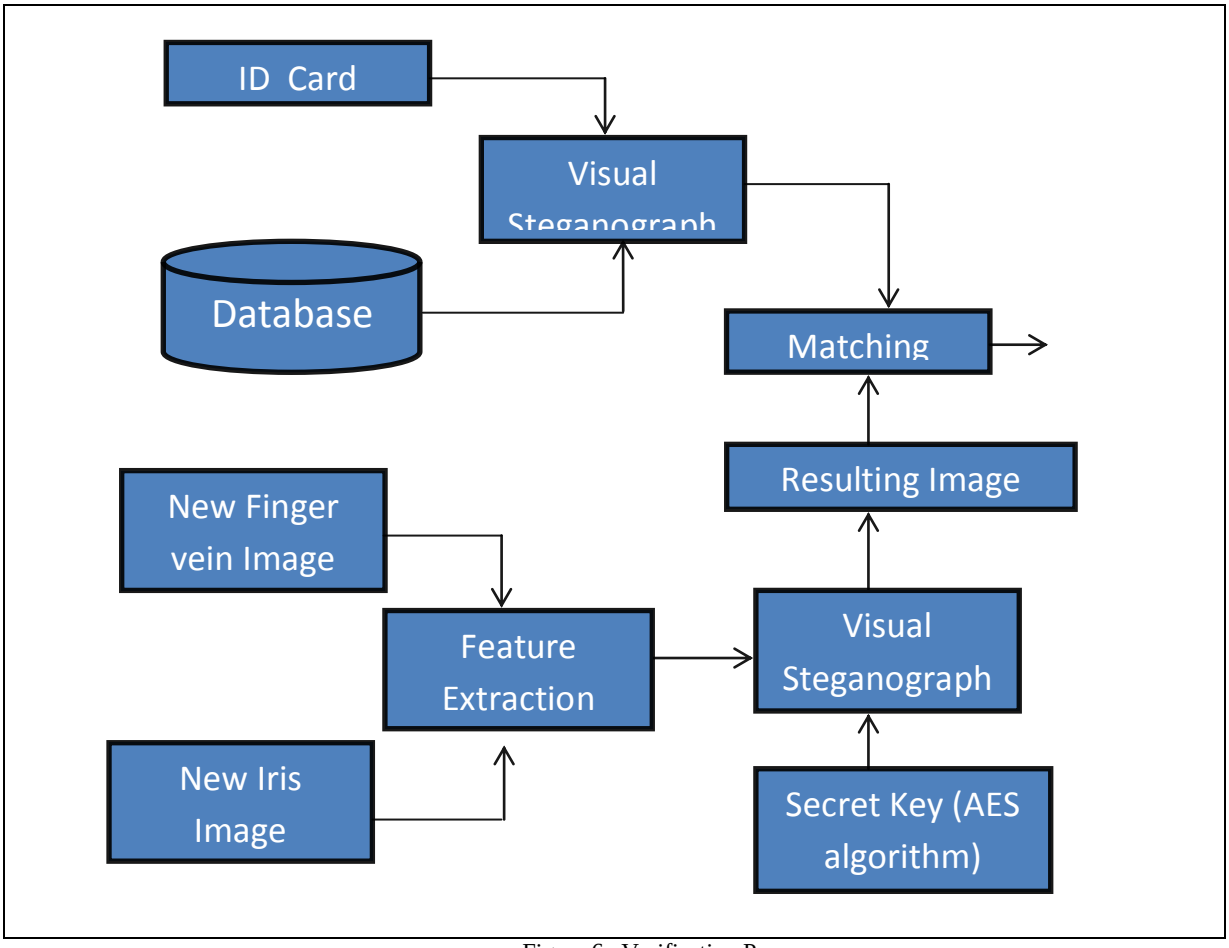

Figure 6. Verification Process

II. 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 iris 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 iris 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. Aboalsamh, *"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]B.B. Gite, DivyaChoksey, Mahesh Jambhulkar, Rahul Ramath, YashovardhanJhamvar, *" Data Hiding Using Steganography And Authentication Using Digital Signatures And Facial Recognition*", International Journal of Engineering Research and Applications, pp**. 364-369**, Vol**.3**, Issue **2**, April **2013**.

[3] NehaChhabra, *"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] Manjiree S. Waikar, Dr. S. R. Gengaje**, "***Infrared Vein Detection System For Person Identification*",International Journal of Recent Trends in Engineering &Research, pp.**305-310**,Vol.**03**, Issue **06**; June –**2017**.

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

[7] 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.**

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

[9] 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.**

[10] ShaikRiyazUlhaq, ShaikImityaz, 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**.

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

[12] 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.**

[13]V. S. Dhongde, M. R. Wargantwar, S.G.Joshi, "IRIS Recognition Using Neural Network", International Journal of Innovative Research in Science, Engineering and Technology, Vol. **3**, Special Issue **4**, April **2014**.

[14]U T Tania, S M A Motakabber and M I Ibrahimy, "*Edge detection techniques for iris recognition system",* 5th InternationalConferenceonMechatronics(ICOM'13) IOP Conf.Series:Materials Science and Engineering,**2013.**

[15]T. SrinivasaRao, 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 SrimathiIndhira 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.