ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Multibiometric Authentication system using Fuzzy Vault Technique

Abdul Aziz Khan J[1], Jayalilly[2]

Assistant Professor, Dept. of EEE., V.R.S College of Engineering &Technology, Villupuram, Tamilnadu, India

Associate Professor, Dept. of ECE., V.R.S College of Engineering &Technology, Villupuram, Tamilnadu, India

ABSTRACT: This paper is secured fuzzy vault implementation for different biometrics such as Finger Print, Iris and Finger Vein. To enhance the security and accuracy of identification, a novel fuzzy vault algorithm is implemented. Firstly, Enrollment stage the feature is extracted from finger print, Iris, finger vein respectively the extracted features is fused together. The fused image is encrypted and stored in the database. Secondly, Recognition stage the same person unique identity pattern is decrypted and simultaneously matched for providing high level secure authentication using Fuzzy vault encryption and decryption technique. Person unique identity pattern and verification is show that a recognition system which gives 0 percentages FAR (False Acceptance Rate) and FRR (False Rejection Rate) is not applicable still now. To demonstrate the novel proposed algorithm has been stimulated form the result it is concluded the new fuzzy vault technique has further reduced 46% of FAR (False Acceptance Rate) to enlarge the security level. Another term, the accuracy of identification has been improved to reduced 40% of FRR (False Rejection Rate)

KEYWORDS: Finger Print Trait, Iris Texture, Finger vein Texture, FAR, FRR, Novel Fuzzy vault**.**

I. INTRODUCTION

Automated human identification using physiological and/or behavioural characteristics, i.e. biometrics, is increasingly mapped to new civilian applications for commercial use. The tremendous growth in the demand for more user friendly and secured biometrics systems [2] has motivated researchers to explore new biometrics features and traits.

Biometric Authentication technology is the one that conduct a personal identification by using human physiological characteristics and behavioral characteristics. Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employed some of the imaging technologies. The major minutia features of fingerprint ridges are ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates.

II. RELATED WORK

Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint.[1] Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical [2] Vein is free from the impact of external contamination and minor injuries and information characteristic is insensitive to the changes in humidity and temperature. What is more, it is easy to collect, readable and so on. Because of the above unique advantages, the vein recognition is widely used in biometric identification. In recent years, vein recognition has become the most innovative and sophisticated hand biometric identification technology.[2] Iris recognition is the best of breed authentication process available today. While many mistake it for retinal scanning, iris recognition simply involves taking a picture of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

the iris; this picture is used solely for authentication. But what makes iris recognition the authentication system of choice?

1. Stable – the unique pattern in the human iris is formed by 10 months of age, and remains unchanged throughout one's lifetime
2. Unique – the probability of two rises producing the same code is nearly impossible
3. Flexible – iris recognition technology easily integrates into existing security systems or operates as a standalone
4. Reliable – a distinctive iris pattern is not susceptible to theft, loss or compromise
5. Non-Invasive – unlike retinal screening, iris recognition is non-contact and quick, offering unmatched accuracy when compared to any other security alternative, from distances as far as 3″ to 10″

In particular, the systems require high accuracy and fast response times. In practice, however, biometric data are rarely uniform. Biometric data used in fuzzy-commitment-based systems, e.g., in the literature mentioned above, do not satisfy the criteria of being uniform and memory less. Nevertheless, it is assumed that these systems are secure. Also privacy preserving properties of these systems are hardly investigated. The fuzzy commitment scheme is only optimal for the totally symmetric memory less case and only if the scheme operates at the maximum secret-key rate. Moreover, we show that for both the general memory less and stationary ergodic cases the scheme reveals information on both the secret and biometric data. We are not able to determine the achievable rate-leakage regions for these two cases and only provide outer bounds on the corresponding achievable rate-leakage regions. These bounds are sharpened for systematic parity-check codes [4]

Fuzzy vault is secure in the sense that it does not leak information about biometric feature since it uses one-way hash function for encryption like "Cancellable" biometrics. Ability to handle intra-class variations in biometric data. Unlike cryptography, it may allow a match to occur if the difference between the query biometric data and the template is small. The fuzzy vault scheme stores only a transformed version of the template, which makes it applicable to various biometric. To show the improvements of the proposed novel fuzzy vault authentication technique, existing fuzzy commitment authentication is considered as a reference technique. So, the performance of the proposed technique is analyzed using MATLAB simulation and various performance metric are computed to demonstrate its superior performance

This paper is organized as follows: Section1 describes need for finger Print, Dorsa, Vein and existing unimodel biometric Fuzzy commitment technique. Section 2 gives the feature extractions of Multi biometric. Section 4 the simulation results are discussed. Section 5 Finally the conclusion and future work.

III. FEATURE EXTRACTION

Feature extractions of Multi biometric:

a) Finger print

Minutiae refer to specific points in a fingerprint, these are the small details in a fingerprint that are most important for fingerprint recognition. Fingerprint based identification is popular for individual identification because it does not change with age. It is unique to individuals and with the new technologies it is easy and low cost to implement. The uniqueness of a Fingerprint is exclusively determined by the local ridge characteristics and their relationships. The ridges and valleys in a Fingerprint alternate, flowing in a local constant direction. The two most prominent local ridge characteristics are:

- Ridge ending
- Ridge bifurcation

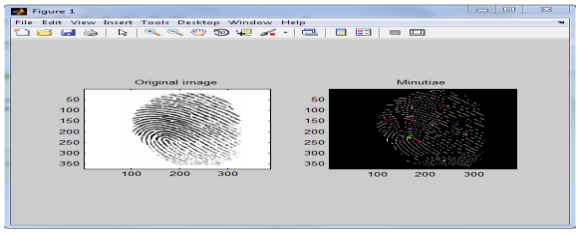

Fig.2.1 Finger print Minutiae Feature

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

b) Finger Vein

Finger vein recognition is a method of biometric authentication that uses pattern-recognition techniques based on images of human finger vein patterns beneath the skin's surface. Finger vein recognition is one of many forms of biometrics used to identify individuals and verify their identity.

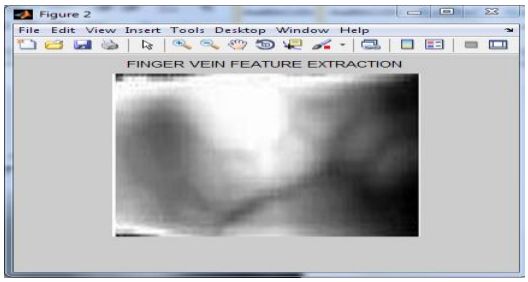

Fig.2.2 Finger Vein Feature Extraction

c) Iris

Iris recognition solutions measure the unique patterns in the colored circle around your pupil to identify and authenticate. Some of the best iris recognition technology out there is deployed in high throughput areas like large international airports. Fast and contactless, iris recognition is on the verge of becoming a consumer biometric modality too, with considerations being made to incorporate scanners on smart phones and wearables in the near future.

Iris recognition is the process of recognizing the person by analyzing the random pattern of the iris (Figure 2.3).The automated method of Iris recognition is relatively young. Existing in patent only since 1994.

The Iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle (Figure 2.4)

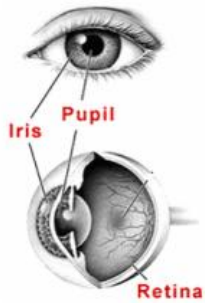

Fig.2.3 Iris Diagram

Fig.2.4 Iris Structure

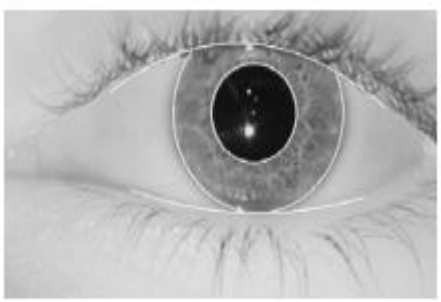

Fig.2.5 White Outlines indicate the localization of the iris and boundaries

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

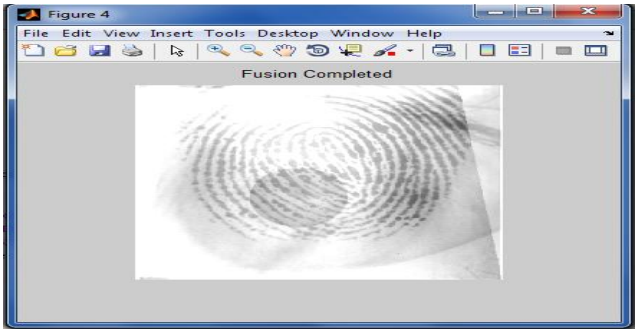

Fig.2.6 Fusion Completed

IV. PROPOSED ALGORITHM

In our multibiometric vault implementation, the biometric features are represented as elements in the Galois Field GF and the key size is set to 16n bits, where n is the degree of the polynomial P [4].we replace the Reed-Solomon polynomial decoding step by a combination of Lagrange interpolation and Cyclic Redundancy Check (CRC) based error detection. During authentication, the query biometric features are used to filter out the chaff points in the vault V resulting in an unlocking set L . Several candidate sets of size (n + 1) are generated from L and polynomials are reconstructed using Lagrange interpolation. CRC based error detection is used to identify the correct polynomial and hence, decode the correct key. Though this method has a higher computational cost due to the large number of interpolations, it has better tolerance to errors. The critical component of our multibiometric vault is the transformation of features from different biometric sources (e.g., fingerprint minutiae, Finger Vein ,Iris) into a common unordered set representation. We first describe how multibiometric can be individually encoded as elements in GF(216) and then show how the multibiometric template can be derived in the following three scenarios: (i) multiple impressions of the same finger, (ii) multiple instances of Finger Vein (iii) multiple traits of Dorsa.

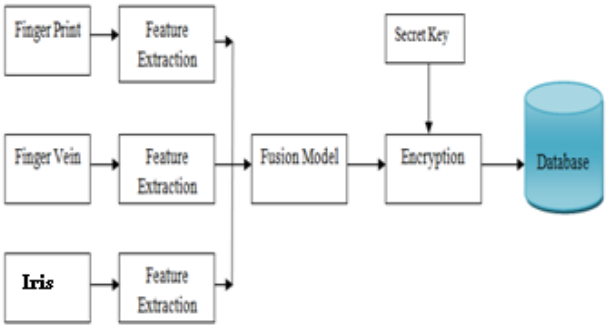

Fig.3.1 Enrollment Stage

Firstly, Enrollment stage the feature is extracted from finger print, Iris, finger vein respectively the extracted features is fused together. The fused image is encrypted and stored in the database as shown in Fig.3.1.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

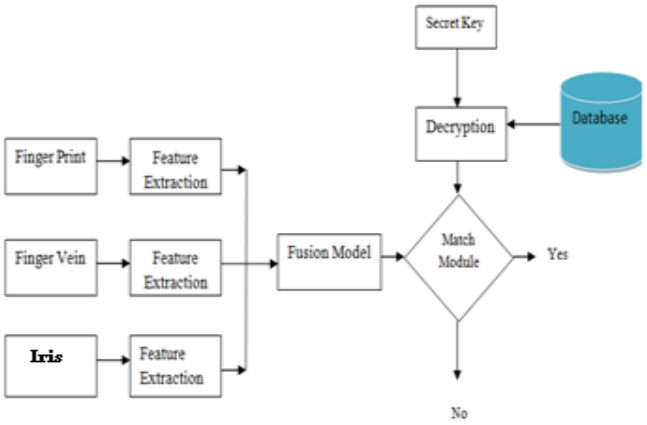

Fig 3.2 Recognition Stage

Secondly, Recognition stage the same person unique identity pattern is decrypted and simultaneously matched for providing high level secure authentication using Fuzzy vault encryption and decryption technique as shown in Fig.3.2.

a) Fuzzy vault using LOCK and UNLOCK Algorithm

Step 1:

- Starting point A secret κ ∈ F k q transformed into a polynomial p ∈ Fq[X] with degree smaller than k
- A set A = {ai ∈ Fq|i = 1..t}
- A security parameter r ≥ t

Step 2:

- Starting point A secret κ ∈ F k q transformed into a polynomial p ∈ Fq[X] with degree smaller than k
- A set A = {ai ∈ Fq|i = 1..t}
- A security parameter r ≥ t

Step3:

LOCK algorithm

- LOCK algorithm Evaluate each element of A by p for i = 1 to t do
  xi = ai
  yi = p(xi)
- Add chaff points
  for i = t + 1 to r do
  xi ∈ Fq \ A
  yi ∈ Fq \ p(xi)
- Final vault
  VA = {(xi, yi)|i = 1..r}

Step 4:

UNLOCK algorithm

Given a set B = {bi ∈ Fq|i = 1..t}, construct V = {(xj , yj) ∈ VA|xj ∈ B}.Use Reed-Solomon decoding over V

- RS codes can be decoded up to t−k 2 errors by Peterson-Berlekamp-Massey algorithm
- If A and B overlap substantially, recover κ 7/

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

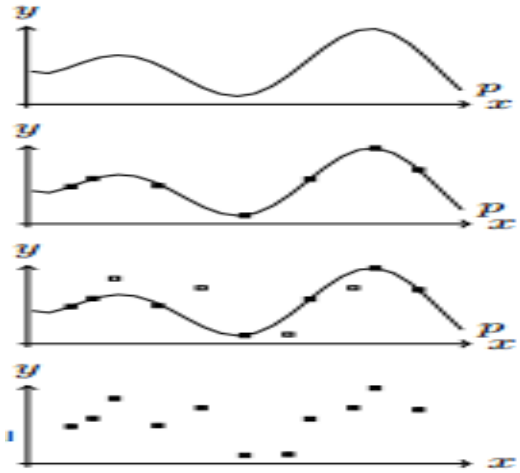

Fig.3.3 Starting Point and LOCK Point

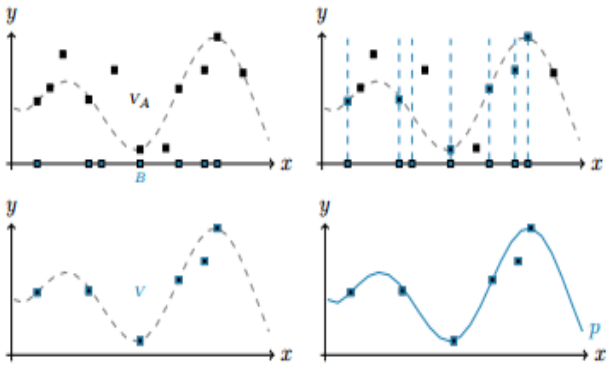

Fig.3.4 Recover UNLOCK Point

V. SIMULATION RESULTS

a) False Acceptance Rate:

False Acceptance can be explained from Fig.5 as imposter person being authenticated as genuine because the criteria of reference threshold is fulfilled and the imposter person is lying in the range of genuine person as shown by dotted arrow. It is defined in (1)

$$FAR = \frac{\text{Wrongly Accepted Individuals}}{\text{Total Number Of Wrong Matching}} \qquad (1)$$

b) False Rejection Rate

Similarly, False Rejection can be explained from the Fig.6 as the genuine person is rejected because the criteria of reference threshold is not fulfilled and the genuine person is lying in the range of imposter person as shown by dotted arrow. It is defined in (2)

$$FRR = \frac{\text{Wrongly Rejected Individuals}}{\text{Total Number Of correct Matching}} \qquad (2)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

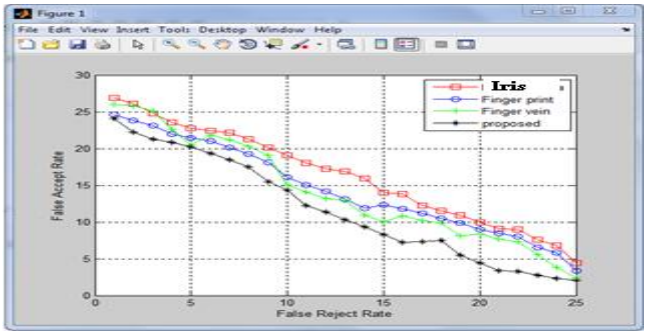

Fig.4.1 FAR vs FRR

The above figure represents the unimodel authentication and multimodal authentication techniques are compared in terms of FAR and FRR. From the simulated results it was inferred that proposed novel fuzzy vault technique as less FAR when compare to unimodel authentication and FRR is comparatively reduced as shown in figure 4.1

Table 4.1 Comparison of FRR and FAR

Biometric traits	FRR (%) (Corresponding reference point FAR 15%)	FAR (%) (Corresponding reference point FRR 15%)
Iris	14	14
Finger print	12	13
Finger vein	10	10
Proposed Technique	9	8

The Table 4.1 shows FRR and FAR Comparison between unimodel Biometric and Multimodal Biometric. The Corresponding Reference Point of FAR is 15% then the multimodal biometric increased the rejection rate and improves security. Simultaneously Corresponding reference point FRR 15% is decreased 40% to improve accuracy. The FRR and FAR of Proposed technique is improved 40% and 46% compare to Existing System of unimodel biometric authentication techniques.

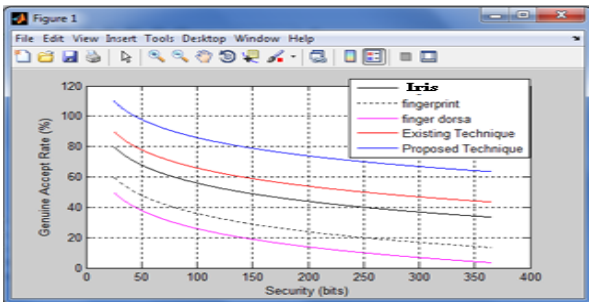

Fig.4.2 GAR vs SECURITY

The above figure represents the Fuzzy Commitment and Fuzzy Vault authentication technique are compared in terms of GAR vs SECURITY. From the simulated results it was inferred that proposed novel fuzzy vault technique has more GAR when compare to existing authentication technique shown in figure 4.2

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Table 4.2 Comparison of GAR and Security

Security (bits)	50	150	250	350
GAR(%) (Existing Technique)	78	60	50	42
GAR (%) (Proposed Technique)	98	80	70	62

The Table 4.2 shows GAR (Genuine Acceptance Rate) and Security. Comparison between Existing Fuzzy Commitment and Proposed Novel Fuzzy Vault Technique. The security of 250 bits is taken to achieve 28% of GAR which outperforms Fuzzy commitment authentication technique in terms of accuracy of identification.

VI. CONCLUSION AND FUTURE WORK

In this project an efficient authentication technique has been proposed for Finger print, Finger Vein and Iris. A novel Fuzzy vault approach is proposed to reduce the FAR (False Acceptance Rate) of 46% and Genuine Acceptance Rate is improved 20% Approximately .The Experimental Results obtained indicates that the proposed authentication technique not only reduced FAR And FRR but also gives good identification accuracy.

REFERENCES

[1] Zhi Liu , Shanging Song, "An Embedded Real Time Finger- Vein Recognition System For Mobile Devices", *IEEE Transaction on Consumer Electronics*,Vol .58 ,No. 2, May 2012.

[2] D. D. Hwang , I. Verbauwhede, "Design of portable biometric authenticators - energy, performance,and security tradeoffs", *on Consumer Electronics*, vol. 50, no. 4, pp. 1222-1231, Nov.2004.

[3] Tanya Ignatenko, Frans M. J. Willems, Fellow, "Information Leakage in Fuzzy Commitment Schemes", *IEEE Transactions On Information Forensics and Security*,*vol*. 5, No. 2, June 2010.

[4] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based Fuzzy Vault: Implementation and Performance," *IEEE Trans. on Info.Forensics and Security*, vol. 2, no. 4, pp. 744–757, December 2007.

[5] K. Nandakumar, A. K. Jain, "Multibiometric Template Security Using Fuzzy Vault," *IEEE Second International Conference on Biometric: Theory, Applications and systems (BTAS 08).*

[6] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in Proc.6th *ACM Conf. Computer and Communications Security*, Singapore, Nov. 1999, pp. 28–36.

[7] Karthik Nandakumar*," "* Fingerprint-Based Fuzzy Vault: Implementation and Performance" *IEEE Transactions On Information Forensics And Security*, Vol. 2, No. 4, December 2007.

[8] Jai,Anil k,Flynn,Patrick,Ross and Arun A*,"Handbook of Biometrics,"*Chapter 15,pp.529-548, 2008.

[9] http://en.wikipedia.org/wiki/Fingerprint recognition

[10] Information on: Biometric feature Extraction, http://Biometric .csc.msu.edu/.

.

BIOGRAPHY

J. Abdul Aziz Khan received the B.E. degree in Electronics and Communication Engineering from V.R.S College of Engineering Affiliated to Anna University, Chennai, India in 2011 and M.E degree in Embedded System Technologies V.R.S College of Engineering Affiliated to Anna University, Chennai, India in 2015. He presented paper on International Conference on ACCCAS-2015 on the topic "Secure Authentication for Finger print, Finger Vein and Finger Dorsa using Fuzzy Vault Technique" conducted by AL-AMEEN Engineering College, Erode. He also presented paper on National level conference on the topic "Readiness of Helper Monitoring for Home Alone Disabled and Elderly Persons" conducted by Vivekanandha College of Engineering for women [Autonomous], Namakkal. He is currently working as an Assistant professor in Electrical and Electronics Engineering department in V.R.S College of Engineering and Technology, Arasur, Villupuram District, Tamilnadu, India. He published 2 International Research Journal and National Journal.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

S.Jayalilly received the B.E. degree in Electronics and Communication Engineering from Mookambigai College of Engineering, Trichy, Tamilnadu, India in 1992 and M.Tech degree in Embedded Systems Technology from SRM University, Chennai, India in 2013. She presented paper on International Conference on "Real time Biometric security system Through Finger vein recognition" conducted by J.K.N.N College of Engineering and Technology, Kumarapalayam, Erode . She has presented paper in the 16th ISTE TN & P Section Annual Convention for Faculty Members of Engineering College-2014, on the topic "Enhancing Effectiveness of Teaching /Learning Process-Pedagogical Techniques Held at National Engineering College, Kovilpatti. She has presented paper in the 17th ISTE TN & P Section State Level Faculty Convention 2014 & National level Seminar on "Quality in technical Education-Industries Expectations" held at Excel college of Engineering and Technology and won first prize, Komarapalayam She has more than 10 years experience in Teaching Profession. She is currently working as an Associate professor in Electronics and Communication Engineering department in V.R.S College of Engineering and Technology, Arasur, Villupuram District, Tamilnadu, India. She has a Life Member ship in ISTE. She published 1 International Research Journal and National Journal.