ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Ensuring Privacy and Renewability Using Helper Data Systems on Multibiometric Cryptosystems

[I]M. Beulah, [II]K. Leela Rani
[I]M. Tech Student, [II]Assistant Professor
Dept. of IT, LBRCE, JNTUK University, Mylavaram, Andhra Pradesh, India

Abstract
In novel days, a widely evolving technology can impact on security and privacy issues of people. So for this reason providing highly security and privacy is a great mission to public and private sectors. In recent literature, privacy protection technologies for Multibiometric templates were proposed with cryptosystems concern. Among these is the so-called helper-data system (HDS) based on reliable component selection. Although, Existing system provides security by using cryptosystem technologies but induce some problems like as legislation, cross-matching and identity theft. In this paper we integrate HDS approach with face and fingerprint biometrics such that we achieve a system in which the templates are privacy protected, and multiple templates can be derived from the same facial and fingerprint images for the purpose of template renewability. Extracting binary feature vectors forms an essential step in this process. The binary feature vectors are integrated in the HDS leading to a privacy protected fingerprint feature extraction process and facial recognition algorithm with acceptable FAR and GAR, issued that the intra-class variation is sufficiently small. This suggests that a controlled enrollment procedure with a sufficient number of enrollment measurements is required. The proposed work is to elevate the security using multibiometric cryptosystem in distributed system applications like e-commerce transactions, e-banking and ATM.

Keywords
Multibiometrics, Binary Feature Vector, Renewability, Quantization, Facial Recognition Algorithm

I. Introduction

In recent days person's recognition by means of biometrics is one of the developing phenomena. Biometrics is the science and technology of measuring and analyzing biological data. The term "biometrics" is derived from the Greek words "Bio" (life) and "Metrics"(to measure). Biometrics refers to the physiological or behavioral characteristics of a person to authenticate his/her identity. Physical biometrics as a static biometrics is based on data, derived from the measurement of a part of an individual's anatomy (Fingerprint recognition, Iris scan, Retina scan, Hand Geometry; Palm print, Face recognition, DNA and Vascular Pattern Recognition). Behavioral biometrics is based on data derived from measurements of an action performed by an individual and distinctively incorporating time as a metric (Signature, Keystroke, Handwriting, Voice recognition and Gait). In recent trend, there is an emerging interest in the application of biometric authentication and identification. In this paper we engage in face recognition technology and fingerprint because these are Multibiometric modalities being used in an enlarging number of applications.
Most biometric systems deployed in real-world applications are unimodal. These systems suffer with problems such as noise in sensed data, non-universality, upper bound on identification accuracy and spoof attacks. In order to overcome the problem, the possible performance improvement of biometric systems by using multiple biometrics. These systems can also improve other limitations faced by biometric systems.

II. Literature Review

Nowadays, there is an emerging interest in the application of biometric authentication and identification. For illustration, in recently the inspection of passports in Machine Readable Travel Documents (MRTD) the ICAO [6] standardized the biometric modalities and the related template format. Second issue in electronic travelling and residence cards are widely integrating facial and fingerprint recognition techniques for human identification systems. In another hand, current trend is towards utilization of biometrics as a convenience factor. A global leader in e-security will integrate its biometric authentication service with Baltimore Select Access. It provides secure access control and authorization management using multiple biometrics, such as facial and fingerprint identification. Everything becomes personalized, from preferences in CE equipment to driver seat positioning in the automotive field. The number of PIN codes we need to remember is elevation to a point where especially the elderly can no lengthy cope. Substitute these access mechanisms by biometrics produce not just better security, but essentially more ease-of-use.
In line with the approach of Juels and Wattenberg [1], we recently proposed a new class of template protection technology defined as Helper Data Systems (HDS). In, [8], [9], and, we outlined the fundamentals of these systems, incorporating: basic principles, performance analysis, security analysis etc. A practical translation of the HDS framework was done for fingerprinting, acoustic ear recognition and faces. In this paper we focus on facial biometrics and explore the operational characteristics when integrating a HDS in a facial recognition system. Besides the system performance we also demonstrate some usage scenarios. This paper is organized as follows. In section 3, we briefly review the related process fuzzy vault and fuzzy commitment. In section 4, problem statement under this what are the existing and its drawbacks and proposed with benefits are explained. In section 5, we have to discuss about architecture and internal process .In section 6, modules description, in section 7 conclusion of our system.

III. Related Work

Fuzzy Vault and Fuzzy Commitment:

To secure biometric templates many techniques are there. These techniques are categorized into two classes:

A. Template transformation

These techniques modify the biometric template with a user specific

key so that it is complicated to recover the original template from the transformed template. Throughout authentication, the same transformation is enacting to the biometric query and the matching is performed in the transformed domain to evade exposure of the original biometric template. Normally the secure template should satisfy the properties like: Non-invertibility and Revocability.

B. Biometric cryptosystems

In this technique secure sketch is obtained from given biometric template and stored in database as an alternative of original template. The helper data is usually obtained by binding a key with the template. So such approaches are also known as key binding biometric cryptosystems. To handle intra-user variations error correction coding techniques are typically employed.
Fuzzy vault [2] is well known example of biometric cryptosystem. It is design to secure multibiometric features which are represented as a point set. Main benefit of this, it has ability to secure fingerprint details. In fuzzy vault encoder, the biometric template will be given along with random secret key which is converted to a polynomial degree and polynomial is evaluated in a graph. The set of points is then secured by hiding them with chaff points. The set of genuine points along with polynomial evaluations together with chaff points constitute the sketch or vault. The fig1 shows fuzzy vault scheme process.

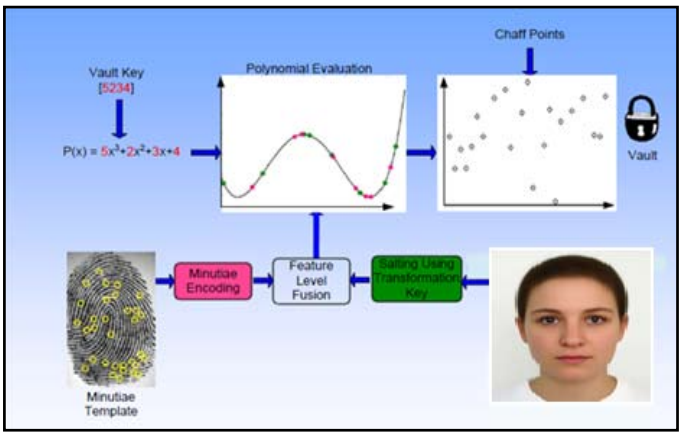

Fig.1 : Fuzzy vault Process

Fuzzy commitment Scheme [7] is a biometric system that can be used to secure biometric traits represented in the form of binary vectors. These vectors can be transformed into binary string. The binary string is divided into a number of segments and each segment is separately secured using a fuzzy commitment scheme. The keys associated with these segment wise fuzzy commitment schemes are then used as additional points in the fuzzy vault constructed using the point-set based features[12].The example shows in the below fig2.

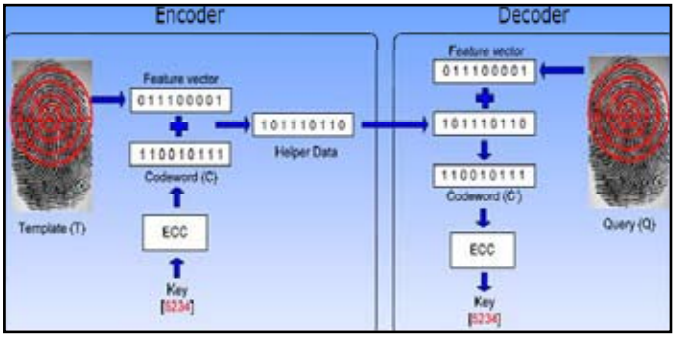

Fig. 2 : Fuzzy Commitment Process

IV. Problem Statement

A. Existing System

(i) Non-invertibility:-specified a secure template, it must be computationally hard to find a biometric feature set that will match with the stated template.
(ii) Revocability:-which means considered two secure templates comes from the same biometric data, it must be computationally difficult to identify that they are derived from the same or obtain the original biometric data.

Disadvantages

1. **Identity theft:** A person has only a less number of biometrics. Storage of the templates in multiple locations (e.g. databases) increases the probability of theft and abuse. This would mean a" theft of identity", that is once the template is compromised it is compromised forever: it cannot be revoked, reissued or even destroyed.
2. **Cross matching:** Especially in networked environment attacks on biometric databases form a serious threat? As soon as identical templates are deployed in multiple databases it would be possible to perform cross matching between them. In this way the privacy of the user is not insured.
3. **Sensitive information:** In some literature it is reported that: biometrics may reveal sensitive medical information. It speaks for itself that this data must be protected in order to intercept misuse. This becomes particular relevant when using DNA like information as a biometric tool.
4. **Legislation:** Although biometrics are not specifically mentioned in the Directive, it is predominant to realize that the Directive protects the privacy rights of individuals who can be "identified by one or more factors specific to his [or her] physiological identity". Consequently, the information biometric technology provides will likely be considered as protected personal data, thus impacting biometric deployment.

B. Proposed System

We propose a feature-level fusion framework to simultaneously secure multiple templates of a user wielding biometric cryptosystems. To demonstrate the viability of this framework, we propose simple algorithms for the following three tasks:

1) Converting different biometric representations into a common representation space using various embedding algorithms: (a) binary strings to point-sets, (b) point-sets to binary strings, and (c) fixed-length real-valued vectors to binary strings.
2) Fusing different features into a single multibiometric template that can be secured using an appropriate biometric cryptosystem such as fuzzy vault and fuzzy commitment; efficient decoding schemes for these biometric cryptosystems were also proposed.
3) Helper data Extraction is the process of generated a random number which is unique. Once encrypted binary features are loaded into the system, HDS can detects and RGN generates automatically at server side.
4) Incorporating a minimum matching constraint for each trait, in order to counter the possibility of an attacker guessing only a subset of the biometric traits.

Advantages

- Differentiated with uni-biometric systems that rely on a single

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

biometric trait, multi-biometric systems can provide higher recognition accuracy and larger population coverage.

- Accordingly, Multi-biometric systems are being extensively affected in many large-scale identification systems.

V. System Architecture

The Architecture shows the main process of our proposed system in fig3.

Block Diagram Description

The sequential process followed both Enrollment and verification stages of multibiometrics are given in below figure5, to achieve the goal of providing security and renewability is given by:

Data Acquisition: Images are collected by using sensor. Raw data can be captured from sensor. The optical sensors are most popular and are inexpensive.

Pre-processing: by using preprocessing image quality will improve. Tasks like image binarization, Segmentation alignment or region of interest (ROI) identification, filtering to remove the high frequency noise, histogram equalization, normalization [5]. Eigen face [11] filtering for face takes place in pre-processing.

Feature Extraction: Features can play a major role for identification/ verification whether a given user is an authentic or not. For multibiometric cryptosystem feature extraction process is done for individual biometric with different feature extraction technologies In fingerprint minutiae extraction algorithm using fingerprint image main features ridges, valley ring, delta point, fork, etc . Likewise Face, The Following that, six key facial feature objects are identified: (i) left eye, (ii) right eye, (iii) left eyebrow, (iv)right eyebrow, (v) mouth and (vi) nose. Face recognition algorithm [13] using for extraction of features.figure4 shows the features of face and fingerprint images.

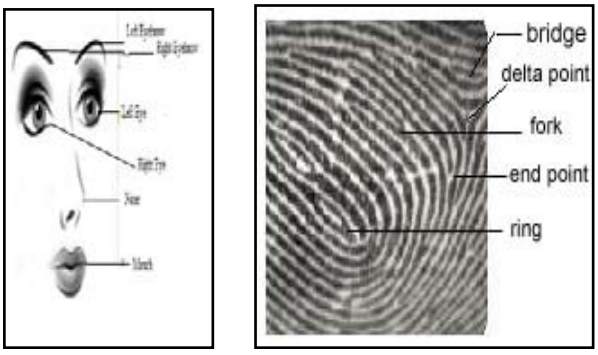

Fig 4 : Main Features of Face and Fingerprint

Feature Vector Binarization: To generate a binary string of length represents the feature vector. Additional information about interval boundaries is necessary. The transformation into bit strings is achieved using dedicated quantizers. All these quantizers operate on a single feature. After all separate features have been transformed into a (short) bit string, all the bit strings can be combined to obtain a binary string representation of the feature vector.

Fusion: Both fingerprint and face templates together as fused. In case, different representation of templates (fingerprint and face) then we have to convert in homogeneous representation using Embedding Algorithm then concatenation apply to both. Otherwise, simply concatenating them [3].

Helper Data System/Extraction: The extraction of feature binary vector from fusion and random generated number.

ECC: In the enrollment stage, an error correcting code (ECC) is binding with key then applied to fused data, to extract a set of parity-check bits. In the verification stage, the new binary feature vector is considered as a noisy version of the enrolled one. The stored parity check bits are used to attempt the correction of binary string. Hamming Distance error-correction technique can applicable [10].

XOR: In order to provide the system with revocable templates, this module computes the bitwise exclusive OR between a binary feature vector and a randomly generated binary string.

Hash Function: When an individual is enrolled in the system, a hash function H, is applied to template .The output is stored in the system database, ensuring the privacy of binary string. In the verification stage, H is applied to corrected binary string, so that the output can be corrected to the stored hash. SHA-1 provides high security and confidentiality.

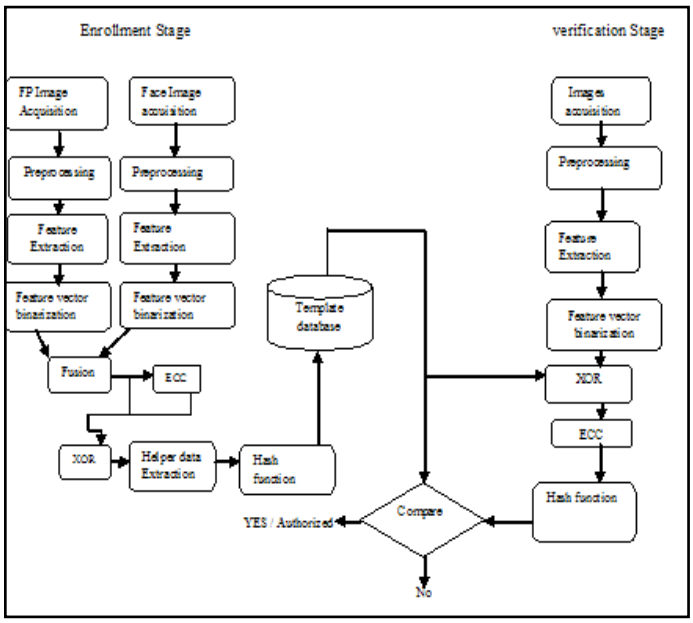

Fig. 5 :Block Diagram Of Our System

Decision: If the stored hash H(z) and H(z') matches, then the user is successfully verified and the key will be regenerated, which is responsible for decision making.

VI. Modules

Modules Description

A. Fingerprint feature Module

In this module, Fingerprint minutiae are extracted to procure the binary string representation from the minutiae set. First the user has to upload and select the fingerprint image from the sample database. Then the Finger print features are loaded into the system database. Then this module, extracts the fingerprint features.

B. Face feature Module

In this module, the Face features are extracted. The user has to upload and select the Face image from the sample database. Then the Binary feature vector from face image loaded into the Database. Then the binary features are extracted.

C. Feature-Level Fusion Module

We propose a feature-level fusion framework to simultaneously

secure multiple templates of a user using biometric cryptosystems. To demonstrate the viability of this framework, we propose simple algorithms for the following three tasks:

1) Converting different biometric representations into a common(homogeneous) representation space using various embedding algorithms: (a) binary strings to point-sets, (b) point-sets to binary strings, and (c) fixed-length real-valued vectors to binary strings.
2) Fusing different features into a single multi-biometric template that can be secured using an appropriate biometric cryptosystem such as fuzzy vault and fuzzy commitment. Generally, a homogeneous representation of feature sets together as a fusion. Efficient decoding strategies for these biometric cryptosystems are also proposed.
3) Consolidating a minimum matching constraint for each trait, in order to counter the possibility of an attacker gaining illegitimate access to the secure system by simply guessing/knowing only a subset of the biometric traits.

D. Secure data forwarding Module

In this module the data is forwarded to the Server securely. The data from the client module is sent/forwarded to the server module. Where, the user has to give the IP address of the server to send the data from client to server. After providing the IP address, the module starts working and the data is sent to the server securely. In the server side, the data reaches and then multi-biometric images are reconstructed there again.

E. Helper Data System Module

In this module, the binary data is already stored in database combined with the encrypted data. Security system will get this stored data known as Helper database by using the user identity and exact the encrypted data from helper data. This data is encrypted with a RGN (Random Generated Number) for every registered user. So security system will decrypt this and derive the RGN. Finally Security system will verify the user identity by compare the decrypted RGN with the stored RGN in Database and send response to the user.

F. Performance Evaluation Module

We evaluate the trade-off between recognition accuracy and security of the proposed multibiometric cryptosystems. To validate the multibiometric system using HDS, we enacted a system residing of fingerprint and face modalities. We further assume that the adversary has knowledge about the face and fingerprint biometrics, i.e., person has access to some face and fingerprint images of the enrolled user. Using cryptographic techniques these templates must securely stored on the server. Fuzzy vault employed for minutiae aggregation of fingerprint template where as fuzzy commitment for face template. The degree of polynomial for the fuzzy vault is specified such that the sum of security in bits and GAR in percentage of the resulting system is maximized. Wielding this constrained multi-biometric cryptosystem, it is feasible to attain a security of 35 bits even if the face features of a genuine user are known to the adversary in addition to this, FAR metric used for evaluating the performance.

VII. Experimental Results

To establish the practical efficiency of our system, we implemented them and tested its performance on number of biometric samples (facial and fingerprint images) of each identical person. We have also taken some of invalid biometric samples. These included data used in real time applications. The algorithms were implemented in C# (.Net Framework) and were run on windows7 operating environment. During implementation of these Authentication and verification process, we have provided better security and privacy using HDS for each user. The Input for each side user's biometric samples and the output is to recognition his/her authentity.

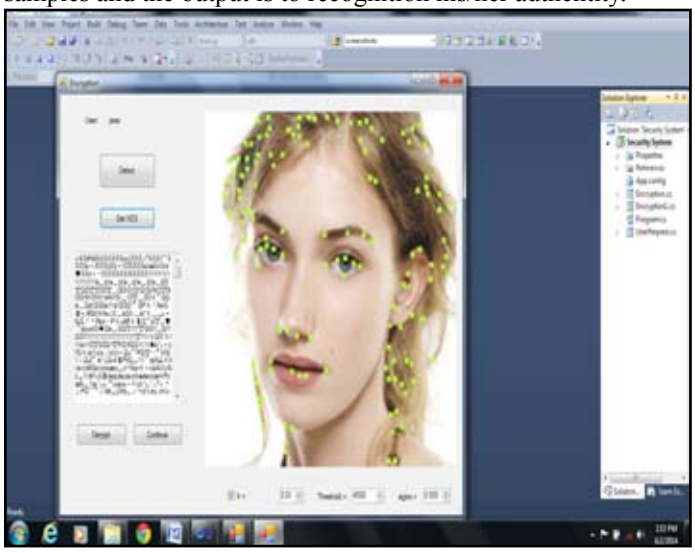

Fig. 6 : HDS for random number generation

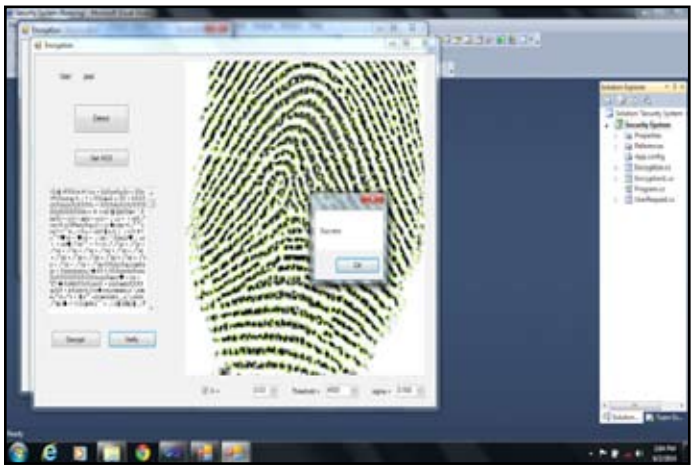

Fig.7 : Result display

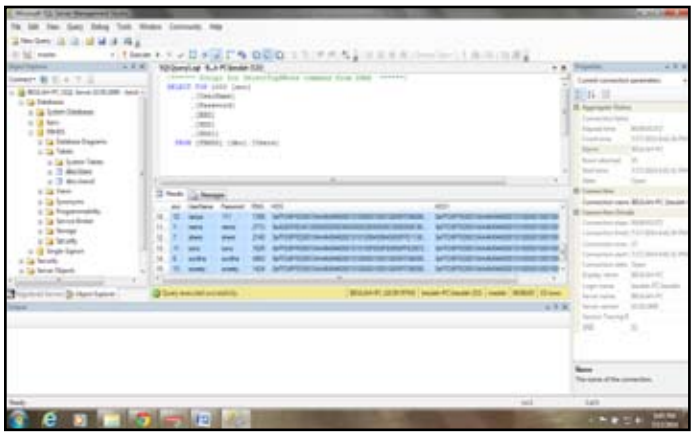

Fig. 8: Storage information of our system in Database.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

VIII. Conclusion

We have proposed a feature-level fusion framework for the outline of multibiometric cryptosystems that protects the multiple templates of user by using single secure sketch. The feasibility of such a framework has been demonstrated using both fuzzy vault and fuzzy commitment, which are two of the most well-known biometric cryptosystems. We have also proposed variant embedding algorithms for transforming biometric representations, efficient decoding strategies for fuzzy vault and fuzzy commitment, and a mechanism to impose constraints such as minimum matching requirement for specific modalities in a multibiometric cryptosystem. A realistic security process of multibiometric cryptosystems known as Helper Data System (HDS) has proposed for providing privacy and renewability. Which leads to authenticate user can have securely entered into the server for storaging multibiometric data. One of the important observation here The RGN (Random Generated Number) was completely hidden from the viewers. Experiments on two different multibiometric databases containing fingerprint and face modalities demonstrate that it is indeed possible to raise both the matching performance and template security using the multibiometric cryptosystems.

There are four critical issues that need to be investigated further:1) Embedding schemes for transforming one biometric representation into another, while preserving the discriminative power of the original representation; 2) a better feature fusion scheme to generate a compact multibiometric template that retains most of the information content in the individual templates; 3)methods to improve the security analysis by accurately modeling the biometric feature distributions; and 4) evaluation of the proposed cryptosystem on large multimodal databases.

References

[1]. *A. Juels, M. Wattenberg.A Fuzzy Commitment Scheme. In G. Tsudik, Ed., 6th ACM Conf. Computer and Communication Security, pp28- 36,1999*

[2]. *A. Juels and M. Sudan, "A fuzzy vault scheme," in Proc. IEEE Int. Symp. Information Theory, Lausanne, Switzerland, 2002, p.408.*

[3]. *E. Kelkboom, X. Zhou, J. Breebaart, R. Veldhuisand C. Busch,"Multi-algorithm fusion with template 2 protection,"ain Proc. IEEE 3rd Int. Conf.aBiometrics: Theory, Applications, and Systems, Washington, DC, Sep. 2009.*

[4]. *F. Zuo, P.H.N. de With, Towards fast feature adaptation and localization for real-time face recognition systems, Visual Communicationsaand Image Processing 2003. Edited by Ebrahimi, Touradj; Sikora, Thomas Proceedings of the SPIE, Volume 5150, pp.1857-1865 (2003)*

[5].a *F. Zuo, P.H.N. de With, Fast facial feature extractionausing a deformable shape model with Haar-wavelet based local texture attributes, Proc. ICIP,pp1425-1428, 2004.aaa*

[6]. *ICAO, International Civil Aviation Organization (ICAO), http://www.icao.int*

[7]. *Juels and Wattenberg, —A Fuzzy Commitment Scheme—, in proc, 6th ACM conf, Computer and Communication Security, 1999.*

[8]. *J.Goseling, P. Tuyls, Information- Theoretic Approach to Privacy Protection of BiometricTemplates Manuscripts, Proc. IEEE International Symposium on Infomation Theory 2004 (ISIT2004),p172.*

[9]. *J.-P. Linnartz and P. Tuyls, New shielding functions to enhance privacy and prevent misuse of biometric templates, 4th International conference on audio and video based biometric person authentication (AVBPA), 2003.*

[10]. *M. Purser, Introduction to Error-Correcting Codes, Artech House, Boston, 1995.*

[11]. *M. Turk and A. Pentland, "Eigenfaces for recognition," J. Cognitive NeuroSci., vol. 3, no. 1,pp.71–86,1991.*

[12]. *Moses Okechukwu Onyesolu and Ignatius Majesty Ezeani, — ATM Security Using Fingerprint Biometric Identifier: An Investigate Study‖, IJACSA Vol.3,No.4,2012*

[13]. *Michiel van der Veen, Tom Kevenaar, Geert-Jan Schrijen, Ton H. Akkermans, Fei Zuo "Face Biometrics with Renewable Templates".*

Authors Profile

Mundlapati.Beulah pursuing M.Tech Degree in Software Engineering from Lakireddy Bali Reddy College of Engineering, Vijayawada, AP, INDIA. Her research Interests include Software Engineering, Image Processing and Biometrics.

Leelarani Kommareddy is an assistant professor of Information Technology at Lakireddy Bali Reddy College of engineering. She obtained her M.Tech from JNTUK. Her research interests include Artificial intelligence, Neural Networks, Data Mining and Information security.