Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Enhance Technique in Multimodal Biometrics

Garima Sethi*
CSE & Kurukshetra University
India

Ashwinder Tanwar
CSE & Kurukshetra University
India

Abstract-- Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application to which most people associate with biometrics is security. A number of biometric traits have been developed and are used to authenticate the identity of a person. The idea is to use the special characteristics of a person to identify him. By using these special characteristics we mean using the features such as iris, face, fingerprint, signature etc. The method of identification based on biometrics characteristics is preferred over traditional passwords and PIN based methods for various reasons such as: The person to be identified is required to be physically present at the time-of-identification. Here we have used fingerprint and iris traits at feature level extraction. The features are extracted from the pre-processed images of iris and fingerprint. The main goal of optimization in this scenario is to enhance the technique of feature extraction by using better steps.

Keywords—fusion techniques , fingerprint and iris recognition , feature extraction , fuzzy logic, multimodal , encryption.

1. INTRODUCTION

Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to secure systems. However, security can be easily cracked in these systems when a password is revealed to an unauthorized user or a card is stolen by an imitator. Furthermore, simple passwords are easy to guess by an imitator and difficult passwords may be hard to recall by a legitimate user.[18]. The term "biometrics" is derived from the Greek words "bio" which means life and "metrics" which means to measure. Automated biometric systems have only become available over the very last not many decades, due to significant advances in the field of computer processing. Many of these new techniques, however, are based on methods that were originally conceived hundreds, even thousands of years ago. [27] .Biometrics is the science of establishing the identity of a person based on the physical, chemical as well as behavioral attributes of the person. Biometric systems are more convenient than traditional authentication systems since there is no password to be forgotten or smart card to be lost [6]. Biometric system is a pattern recognition system that operates by getting biometric data from an individual, extracting some feature set from the acquired data, and then comparing this feature set against the stored template set in the database.

.A. Modules of Biometric System

1. *Sensor module***:** It captures the biometric data of an individual. Fingerprint sensor is an example of sensor module, it captures the ridge and valley structure of the finger of the user .
2. *Feature extraction* **:** In this module captured biometric data is processed and features sets are extracted.
3. *Matcher module* **:** In this module to generate matching score during recognition , features are compared against the stored templates.
4. *System database module***:** This module stores the templates of users. It stores the various templates of user to account for variations observed in biometric data & templates in database are updated over time. [7]

B. Architecture of Biometric System

There are two phases in a biometric system. A learning phase (enrolment) and a recognition phase (verification). In all cases, the item considered such as finger print or voice, is recorded using a sensor and digital data are then available in the form of table of pixels, a digital signal, etc.. In most cases the data themselves are not used directly; instead the relevant characteristics are first extracted from the data to form a template. This has two advantages: the volume of data to be stored is condensed, and greater anonymity is achieved in data storage (because it is not possible to recover the original signal by referring to these characteristics). The role of the learning module is to create a model of a given person by reference to one or more recordings of the item considered. A large amount of the models used are statistical models, which make it possible to allow for a certain inconsistency in individual data. The recognition unit enables a result to be taken. In identification

mode, the system compares. .The measured signal with the various models contained in the data base and selects the model corresponding most closely to the signal. In the verification mode, the system will compare the measured signal with just one of the data base models and then authorize the person or reject him. Identification may be a very difficult assignment if the data base contains thousands of individuals. Access time problems then become crucial.[28]

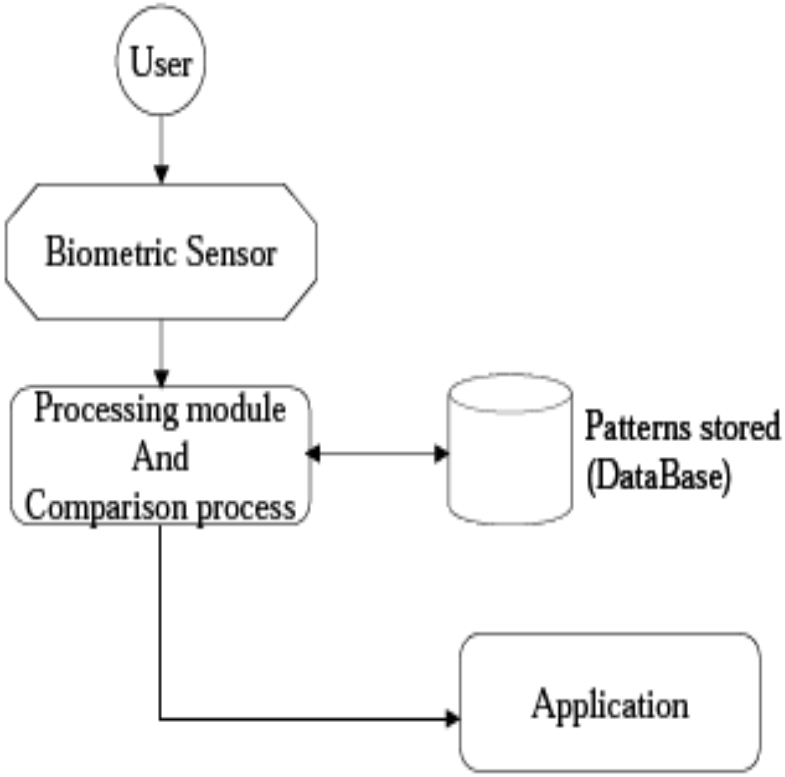

Fig1. Architecture of biometric system

C. Drawbacks Of Biometrics Systems

1) *Noise in sensed data.* A fingerprint with a scar and a voice distorted by a cold are examples of noisy inputs. Noisy data could also outcome from defective or unacceptably maintained sensors (for example, gathering of dirt on a fingerprint sensor) and adverse ambient conditions (for example, poor lighting of a user's face in a face recognition system). Noisy biometric data may be mistakenly matched with templates in the database resulting in a user being inaccurately rejected.
2) *Intra-class variations.* The biometric data acquired from an individual during authentication may be very different from the data used to generate the template during enrollment, thereby moving the matching process. This dissimilarity is typically caused by a user who is incorrectly interacting with the sensor, or when sensor characteristics are customized (for example, by varying sensors, that is, the sensor interoperability problem) during authentication.
3) *Distinctiveness.* While a biometric character is expected to change significantly across individuals, there may be very large similarities in the feature sets used to represent the traits. Thus, each and every biometric trait has some theoretical upper bound in terms of its intolerance capability.
4) *Non-universality.* While every user is likely to have the biometric trait being acquired, in actuality it is possible for a subset of the users to not acquire that particular biometric. Let us take an example that is a fingerprint biometric system may be incompetent to extract features from the fingerprints of certain individuals, due to the poor superiority of the ridges. Thus, there is a failure to enroll (FTE) rate associated with using a single biometric character. There is experimental evidence that about 4% of the population may have poor quality fingerprints that cannot be easily imaged by some of the existing sensors.
5) *Spoof attacks.* An impostor may try to spoof the biometric trait of a justifiably enrolled user in order to circumvent the system. This type of attack is especially applicable when behavioral traits such as signature and voice are used. However, physical character like fingerprints are also susceptible to spoof attacks.
   In the case of iris recognition, the user must be helpful. Further, iris images must meet harsh quality criteria, so the images of very poor quality (e.g., iris with large pupil, or off center images) are discarded at the time of acquisition. Consequently, more than a few attempts may be necessary to obtain the iris image, which not only delay the enrollment and verification, but also annoys the user. The rate of rejection of poor quality images is termed as the failure to enroll rate (FTE). Like any other biometric, the iris can change (such as a consequence of eye disease), in which case, even a very high-quality iris based identification system can fail.[9]

D. Why Multimodal Biometrics?

Uni-modal biometric system performs person recognition based on a single source of biometric information. Such systems are often affected by the subsequent problems:

1. Noisy sensor data
2. Non- universality
3. Lack of individuality
4. Lack of invariant representation
5. Susceptibility to circumvention

Such factors escort to the usage of multimodal biometric for identifying individuals. Combining the proof obtained from different modalities using an effective fusion scheme can significantly improve the usually accuracy of the biometric system. A multimodal biometric system can decrease the FTE/FTC rates and provide more battle against spoofing because it is difficult to simultaneously spoof multiple biometric sources.[8]

II. LITERATURE SURVEY

1) Kankrale R.N. , Jawale M.A "Fuzzy Logic Concatenation in Fingerprint and Iris Multimodal Biometric Identification System",(2013) International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 10, October 2013. The author aims on concatenating two biometric features that is iris and fingerprint at decision level with Fuzzy logic. Multimodal biometric identification system is used for concatenating two or more physical traits to minimize False Accept Rate(FAR) as well as False Reject Rate (FRR). In greater aspect, fuzzy logic based approach by decision level is used for concatenation and each biometric result is then weighted for participate in final decision. Fuzzy logic is mainly used for the effect of each biometric result combination. This proposed multimodal system achieves remarkable results with several commonly used databases. For example, the author had obtained an interesting working point by FAR = 0% and FRR=3.43% using entire CASIA Fingerprint and a randomly extracted same size subset of the CASIA Iris database.

2) Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari"Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic" , (2013)International Journal of Soft Computing and Engineering ISSN: 2231-2307, Volume-2, Issue-6, 2013
   Single biometric systems have a range of problems such as spoof attacks,noisy data, non-universality and unacceptable error rate. These limitations can be solved by using multimodal biometric systems. Multimodal biometric systems uses two or more individual modalities, such as face, iris, retina and fingerprint. Multimodal biometric systems develop the recognition accuracy more than uni-modal methods. In this research the author had used two biometrics, iris and fingerprint are used as multi-biometrics and illustrate using this biometrics has excellent result with high accuracy. Decision level was used for fusion and each biometric result was weighted for participate in final decision. Fuzzy logic was used for the effect of each biometric result combination.

3) N. Radha , A. Kavitha(2012) "Rank Level Fusion Using Fingerprint And Iris Biometrics" Indian Journal Of Computer Science And Engineering (IJCSE), ISSN : 0976-5166 Vol. 2 No. 6 Dec 2011-Jan 2012.`Authentication of users is an essential and difficult to achieve in all systems. Shared secrets like Personal Identification Numbers (PIN) or Passwords and key devices such as Smart cards are not presently sufficient in little situations. The biometric improves the capability to recognize the persons. A biometric identification system is an automatic recognition system that recognizes a person based on the physiological (e.g., fingerprints, face, retina, iris, ear) or behavioral (e.g., gait, signature, voice) characteristics. In many real-world applications, uni-modal biometric systems often face has significant limitations due to sensitivity to noise, intra class variability, data quality and other factors. Multimodal biometric systems overcome a number of these limitations. Multimodal biometric system provides supplementary accuracy when compared to uni-modal biometric system. The main goal of multimodal biometric system is to develop the security system for the areas that require high level of security. The proposed system mainly focused on developing a multimodal biometrics system, which uses biometrics such as fingerprint and iris. Fusion of biometrics were performed by the means of rank level fusion. The features from the biometrics are obtained by using the FLD (Fisher Linear Discriminant). The experimental result shows the performance of the proposed multimodal biometrics system. In this paper, the decision is made using rank level fusion and the ranks of individual persons are calculated using the Borda count, and Logistic regression approaches.

4) P.U.Lahane, S.R.Ganorkar(2012)"Fusion of Iris & Fingerprint Biometric for Security Purpose" International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012 ISSN 2229-5518. The main aim of a biometric system is to automatically distinguish between subjects as well as to protect data. It also protects resources that accessed from unauthorized users. The authors developed a biometric identification system which represents a valid alternative to conventional approaches. In biometric system , physical or behavioral traits are used. Multimodal biometric identification system aims towards fuse two or more physical or behavioral characteristics. Multimodal biometric system

is used in order to develop the correctness. Multimodal biometric identification system based on iris & fingerprint trait is projected. In a multimodal biometric system each biometric character processes its information separately. The processed information is combined using an suitable fusion scheme. in succession, the relationship of data base template and the input data is done with the help of Euclidean-distance matching algorithm. If the templates would matched, the author can allow the person to access the system. Multimodal biometric system also provides optimal False Acceptance Rate (FAR) & False Rejection Rate (FRR), therefore improving system accuracy & reliability.

5) Rupesh Wagh and Arti P choudhary(2013) "Analysis of Multimodal Biometrics with Security Key" , (IJARCSE) International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013. According to this research paper the author has focused on biometrics template security. Multimodal biometrics used two modalities that is Fingerprint and Iris biometrics characteristics. The significant features were taken from biometric template. That features were stored using feature level fusion and that fused vector is then encrypted using different security technologies. The author had also done the fusion using extracting important features of modalities. Author had discussed that how their system was secured when they have used selective encryption method to encrypt the biometric template. Authors took the biometrics samples tested from two database named Virtual database and Real database. Virtual database means the database that is generated from doing the operation where as the real database is the database for testing of the biometric system. The authors concluded that Multimodal biometrics gives accuracy in providing results as compared to unimodal system. By experimental results it was proved that accuracy of multimodal system was improved than fingerprint and Iris unimodal system. They use using digital image processing with cryptography i.e. two technologies were combined.

III. METHODOLOGY

A. Matlab

MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment and fourth-generation programming language , a high-level language and interactive environment for numerical calculation, visualization, and programming. Using MATLAB, you can examine data, generate models and applications and , develop algorithms. The tools , languages and built-in math functions permit you to explore multiple ways and reach a solution faster than with spreadsheets or traditional programming languages, such as C/C++ or Java. You can also use MATLAB for a variety of applications, including image and video processing, control systems, test and measurement, signal processing and communications, computational biology and computational finance. Many engineers and scientists in industry and academia use MATLAB, the language of technical computing. Developed by MathWorks, MATLAB allows plotting of functions and data, implementation of algorithms, matrix manipulations, creation of user interfaces, as well as interfacing with programs written in other languages, including C, C++, Java. MATLAB is widely used in academic and research institutions as well as industrial enterprises.

B. Fuzzy logic

Fuzzy logic is used for the fusion of two feature extracted templates. Fuzzy logic enables us to process iambuses information in a way like human thinking, i.e. big versus small or high versus low. It makes intermediate values to be defined between true and false by partial set memberships. As an primary step, we consider fuzzy variables and fuzzy sets in a fuzzy inference system for iris and fingerprint images. Using fuzzy logic for fusion at decision level has many advantages like soft inputs while the crisp outputs are achieved. Fuzzy system used in this paper with simplest way gives an brilliant result. This system gives an acceptable percentage output for every acceptable range of inputs for which using a threshold for the best states are accepted.

IV. PROPOSED ARCHITECTURE

The basic idea behind the problem is to improve the performance and feature extraction of multimodal biometric systems using different methods. In the propose approach, the two biometric template will fuse before matching to generate multimodal biometric template. The template stored in the database is not secure as a number of attacks are possible like modification of template etc. In order to provide database security different technique will be used to generate secure template. This secure template will be encrypted using algorithm to increase the security at this level.

Step 1: Fingerprint and Iris biometric sample will be enrolled using different sensors.

Step 2: Features will be extracted differently from both the biometrics.

Step 3: Fusion of both extracted features will take place at this level (i.e fusion at feature extraction level) using neural network or fuzzy vault or genetic algorithm. The feature sets originating from multiple biometric algorithms will consolidate into a single feature set by the application of appropriate attribute normalization, reduction and transformation schemes.

Step 4: Generated template will be stored in the database.

Step 5: Above stored template will be protected via Cancellable Biometric.

Step 6: Security will further increase by encrypting the template using cryptography.

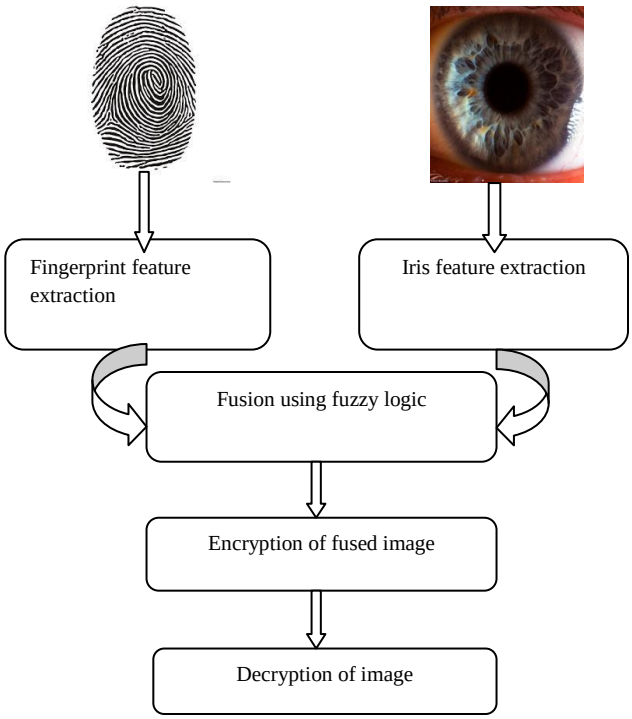

Fig. 2 Proposed Architecture

V. RESULTS & DISCUSSION

We work in the MATLAB to get the extracted features of fingerprint and iris. Both the extracted characteristics are then fused using fuzzy logic and encryption is done by using AES technique.

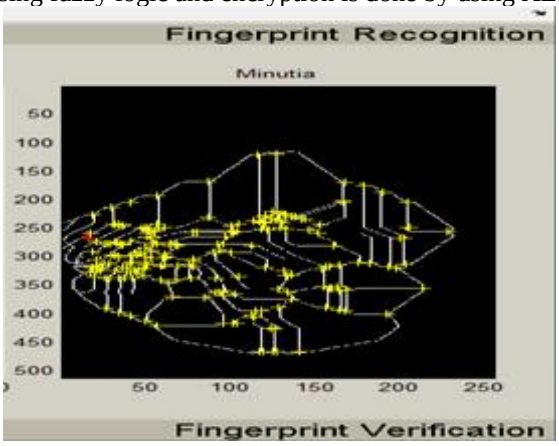

Fig3 minutia extraction of fingerprint

fig4 segmented image of iris.

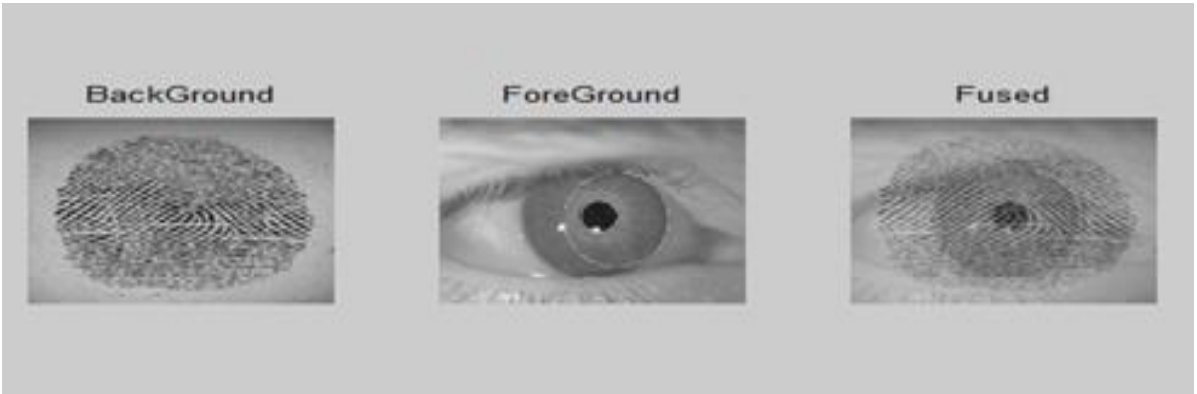

Fig 5 fused image

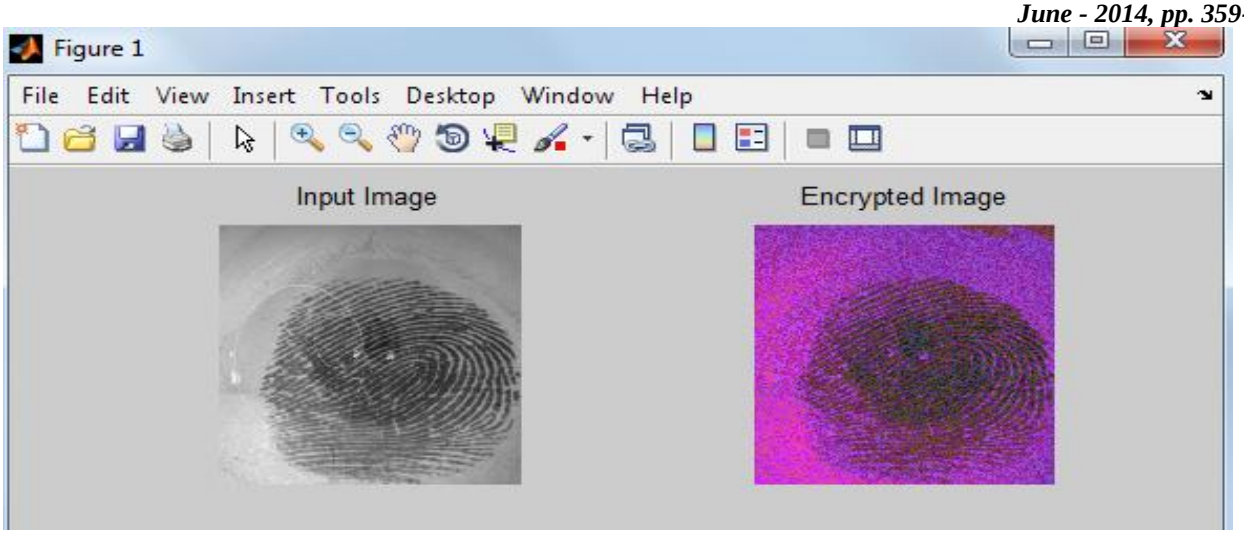

Fig 6 encrypted image

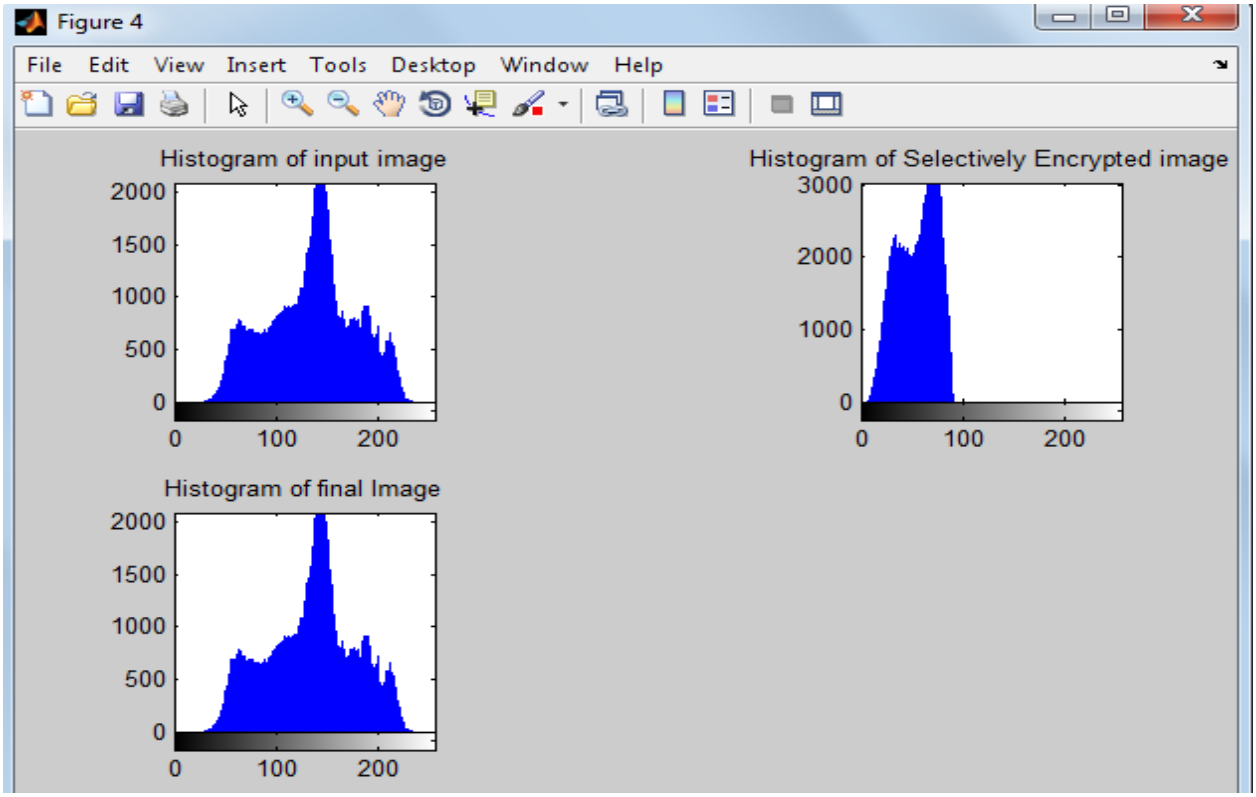

Fig7. Histogram Of Images

VI. CONCLUSION

Biometrics provides security benefits across the spectrum, from IT vendors to end users, and also from security system developers to security system users. For last many years, many highly secure environments also have used biometric technology for entry access. Today, the main application of biometrics is in physical security: to control access to secure locations (rooms or buildings) .Nowadays, biometric systems are widely used for authentication purposes, but the uni-modal biometric system has some limitations like noisy sensor data, be deficient in of individuality, non universality, susceptibility to circumvention and lack of invariant representation . So to overcome these disadvantages, multimodal biometric system are used. Multi biometrics is a new technique used to accurate identification of the person. This paper presents a multimodal biometrics combining fingerprint and iris with feature extraction level and fusion is done by fuzzy logic. Efficient security system by using iris and fingerprint traits has been design. The extraction is such that we have many fingerprint recognition steps and iris recognition steps. These steps increase the extraction of features from both the features. Then the extracted features are then combined using fuzzy logic. This fused template is then encrypted using AES technique and we can also match the original fused image and the encrypted image to check whether it is encrypted or not.

REFERENCES

[1] Kankrale R.N. , Jawale M.A" Fuzzy Logic Concatenation in Fingerprint and Iris Multimodal Biometric Identification System", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 10, October 2013

[2] Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari "Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic" , International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013

[3] N. Radha , A. Kavitha "Rank Level Fusion Using Fingerprint And Iris Biometrics" Indian Journal Of Computer Science And Engineering (IJCSE), ISSN : 0976-5166 Vol. 2 No. 6 Dec 2011-Jan 2012

[4] P.U.Lahane, S.R.Ganorkar " Fusion of Iris & Fingerprint Biometric for Security Purpose" International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012 ISSN 2229-5518

[5] Rupesh Wagh and Arti P choudhary "Analysis of Multimodal Biometrics with Security Key" , International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013

[6] Taruna Panchal and Ajit Singh "Multimodal Biometric System", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[7] Shweta Malhotra and Chander Kant "A Novel approach for securing biometric template" ,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[8] Kande Archana1,A .Govardhan "Enhance the Security in the ATM System with Multimodal Biometrics and Two-Tier Security", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 10, October 2013

[9] Shanthini, B. and S. Swamynathan "Multimodal Biometric-based Secured Authentication System using Steganography" , Journal of Computer Science 8 (7): 1012-1021, 2012 ISSN 1549-3636 © 2012 Science Publications

[10] K P Tripathi "A Comparative Study of Biometric Technologies with Reference to Human Interface", International Journal of Computer Applications (0975 – 8887) Volume 14– No.5, January 2011

[11] Ajay Kumar, Vivek Kanhangad , David Zhang "A New Framework For Adaptive Multimodal Biometrics Management" IEEE Transactions on Information Forensics and Security vol. 5, pp. 92-102, Mar. 2010

[12] Nageshkumar.M, Mahesh.PK and M.N. Shanmukha Swamy, "An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image",IJCSI International Journal of Computer Science Issues, Vol. 2, 2009

[13] K.Sasidhar, Vijaya L Kakulapati, Kolikipogu Ramakrishna & K.KailasaRao, "Multimodal Biometric Systems – Study To Improve Accuracy And Performance" ,International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010

[14] Eugen Lupu ,Petre G. Pop, "Multimodal Biometric Systems Overview", Acta Technica Napocensis ,Volume 49, Number 3, 2008

[15] Tobias Scheidat, Claus Vielhauer, "Analyzing A Multimodal Biometric System Using Real And Virtual Users",SPIE Vol. 6505, 650512, © 2007 SPIE-IS&T · 0277-786X/07/$18

[16] Anil Jaina, Karthik Nandakumara, Arun Rossb , "Score Normalization In Multimodal Biometric Systems", Pattern Recognition , The Journal Of The Pattern Recognition Society,18 January 2005

[17] Kresimir Delac , Mislav Grgic, "A Survey Of Biometric Recognition Methods", 46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June 2004

[18] Anil K. Jain And Arun Ross, "Multibiometric Systems"Communications Of The ACM ,January 2004/Vol. 47, No.1,

[19] Karine Pellerin, "Increasing Accuracy In Multimodal Biometric Systems" GIAC Security Essentials Certification (GSEC) ,Version 1.4c Option 1

[20] Michael Goh Kah Ong, Tee Connie, Andrew Teoh Beng Jin, David Ngo Chek Ling, "A Single-Sensor Hand Geometry And Palmprint Verification System" , WBMA '03, November 8, 2003, ACM 1-58113-779-6/03/00011

[21] Robert Snelick, Mike Indovina, James Yen, Alan Mink," Multimodal Biometrics: Issues In Design And Testing" ICMI'03, November 5–7, 2003,ACM 1-58113-621-8/03/0011

[22] Arun Ross and Anil Jain, "Information Fusion in Biometrics"Appeared in Pattern Recognition Letters, Vol. 24, Issue 13, pp.2115-2125, September, 2003

