Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Heterogeneous Multimodal Biometric System with Fuzzy Vault Template Security

Mukhwinder Singh*
ECE, BBSEBEC Fatehgarh Sahib, India

Tripatjot Singh Panag
ECE, BBSEBEC Fatehgarh Sahib, India

Abstract*— Mulimodal Biometrics is more robust and secures then unimodal biometrics. In multimodal fusion at feature level is considered more effective as a wide raw feature set is available and can be manipulated as per requirement. This work focuses on fusion of Fingerprint and Iris biometrics at feature level. The proposed approach is based on the fusion of the traits by extracting independent features from the respective modalities. So far there has been extensive work done on fusion at the match score, sensor level, decision level but fusion of the feature level in heterogeneous environment is still an understudied problem. In this work features are extracted from the respected modalities using the state of art techniques and feature set after fusion is made compatible to fuzzy vault which is a robust template security technique. The prime criticality of this work is to develop a heterogeneous multimodal system and to add fuzzy vault security to it.

Keywords*— Fuzzy Vault, Multimodal biometrics, Template, Mintutae, Fusion.

I. INTRODUCTION

Biometrics are automated methods of recognizing an individual based on their physiological (e.g., fingerprints, face, retina, iris) or behavioral characteristics (e.g., gait, signature). It is the science of establishing the identity of an individual based on the physical, chemical or behavioural attributes or traits of the person like DNA, ear, face, hand, and hand vein, fingerprint, finger vein, gait, palm print, hand and finger geometry, iris, keystroke, odour, signature or voice. An automated system capable of capturing a biometric sample from an end user, extracting biometric data from the sample, comparing the data with one or more stored templates, rejects or accepts on the basis of matching results is called a Biometric System. All biometric traits have their own advantages and disadvantages. Not every biometric trait can be used everywhere, so it has to be decided which biometric trait caters best to the needs of a particular application. Most biometric systems that are presently in use typically employ a single biometric trait to establish identity [1]. A lot of challenges are commonly encountered by biometric systems like noise in sensed data, non universality, lack of flexibility, upper bound on identification accuracy, spoof attacks etc. Multi biometric systems are employed to overcome these problems. Along with these advantages that multi biometric systems provide, there are a lot of challenges too like template security and fusion complexity etc. that need to be taken care of while designing multi biometric systems.

II. RESEARCH BACKGROUND

Unimodal Biometric Authentication System is usually more cost-efficient than a multimodal biometric system. But these systems have various limitations such as intra-class variations, inter-class similarities, non universal data and spoof attacks, noise issues with the data etc. To overcome the drawbacks of Unimodal, Multimodal system were introduced. In Multimodal biometric systems it becomes difficult for an intruder to spoof all the traits simultaneously. Hence they are more robust and provide better performance and accuracy. Multibiometric System relies on the evidences presented by multiple sources of Biometric information. Based on these sources a Multibiometric System can be classified into six categories: multi-sensor, multi-algorithm, multi-instance, multi-sample, multi-modal and hybrid. Based on the type of information available in certain module different levels of fusion are defined as: fusion at sensor level, fusion at feature level, fusion at match score level, rank level and decision level [2]. Feature level fusion has an edge over other fusion techniques as it provides a large set of features extracted from different modalities, which can be combined after selection of appropriate normalization technique [3], [4]. Literature reveals that most of the work focuses on fusion at feature level is in homogeneous environment, instead feature level fusion at heterogeneous environment which is still understudied and forms an important basis of the research work. Heterogeneous System is the system which combines different sources of information and it provides the flexibility of extracting the features from various biometric traits used in multimodal using their specific state of the art techniques rather using same feature extraction techniques as in homogeneous systems from all the traits used in multimodal system just to avoid the curse of dimensionality issue. In heterogeneous environment choosing an appropriate normalization helps in dealing with the issue and is expected to provide better results.

Biometric System itself is not foolproof, there can be number of dangerous security breaches which sometimes lead to irrecoverable losses. There are number of levels/ attack points in biometric system where it can be attacked by an intruder

intentionally or unintentionally. Biometric System can be attacked at Sensor Level, Channel Level, Feature Extraction Level, Matcher Level, and at the stored Template Level. Out of all of them the most challenging and potentially damaging attacks on a biometric system is against the biometric templates stored in the system database. Template Security Techniques in the literature can be broadly classified as Feature Transform and Biometric Cryptosystem based approaches. Fuzzy vault is one of the important and rigorous techniques of Template security. This technique generates the secret data from the registered template and query biometric data. Therefore, it excels not only in template security but also in secret data concealability [5]. The fuzzy vault scheme stores only a transformed version of the template, which makes it applicable to various modalities besides fingerprints. Fuzzy Vault Scheme can also be applied in multimodal biometric systems [6].

Choice of biometric system for an application depends on many factors as performance, acceptability, circumvention and reliability and cost [9]. Fingerprint recognition inherits a rich history of manual methods used by human experts to compare fingerprints. Fingerprint recognition using minutia features is a popular and state of the art method adapted by many research and commercial systems [7]. Iris Biometrics is considered as more reliable and accurate biometrics. It is extremely difficult to surgically tamper the texture of the iris, and spoof attacks (e.g., with prepared contact lenses) are detectable rather easily [9]. Daugman's iris localization and template extraction technique is most widely adapted [8]. Based upon these evidences from literature [10], [11], [12], [13] the work proposed focuses on multimodal based heterogeneous feature extraction from iris and fingerprint, with enhanced security using Fuzzy Vault template security.

III. METHODOLOGY AND RESULTS

A. Methodology

The methodology used in the proposed work is presented in the Fig. 1. Iris and Fingerprint images are taken as input images. Iris template is extracted from iris image using Daugman's Integro differential operator and then the unique patterns of 1's are extracted from iris code. Fingerprint minutia points (ridge endings and bifurcations) are extracted from fingerprint image using CN number technique. Feature sets extracted from iris and fingerprint are then fused and made compatible as input to fuzzy vault to generate the vault.

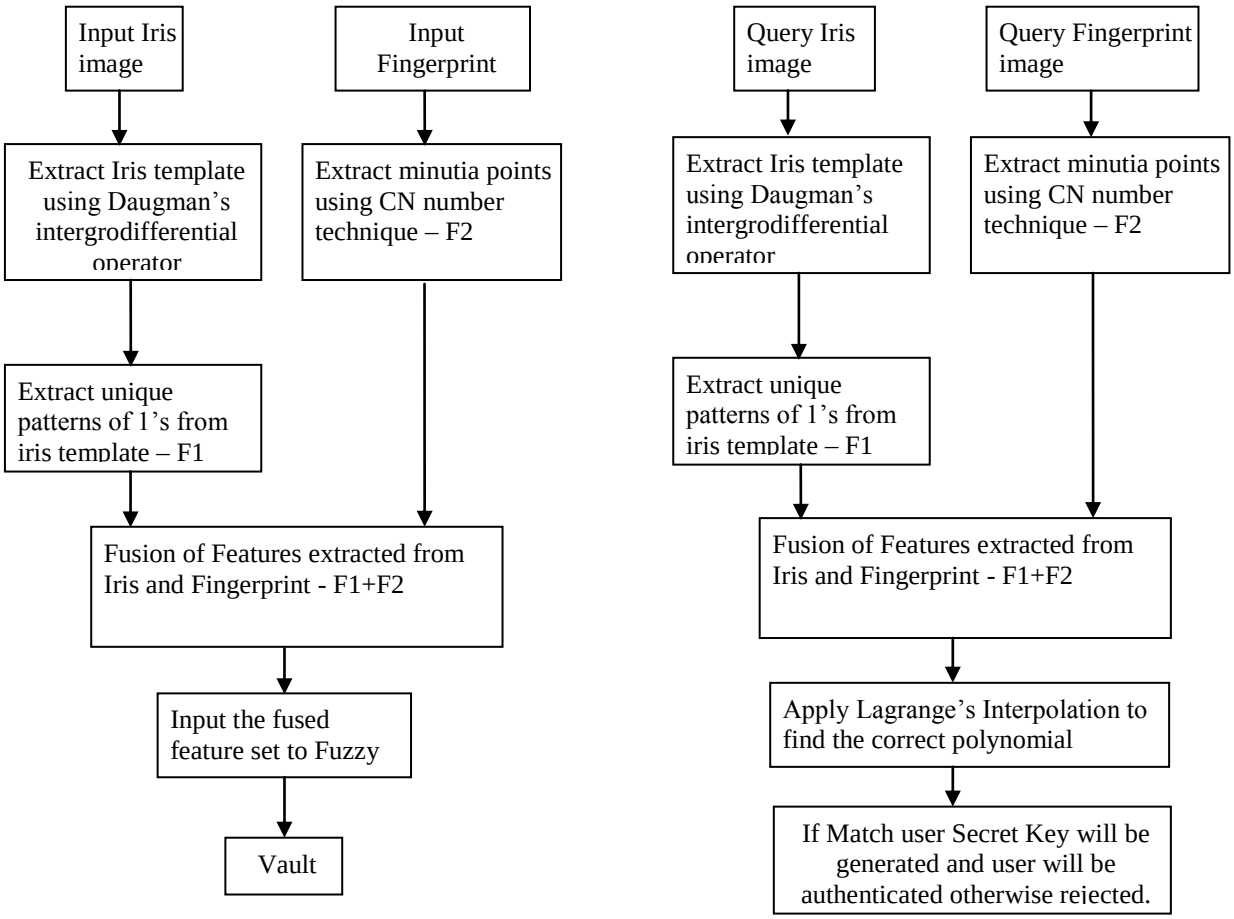

Fig. 1: Heterogeneous fuzzy vault encoding and decoding.

B. Implementation Case Study

The proposed work is implemented in Matlab. Figures below represent one case study following all the steps of the proposed system. Fig. 2 represents the proposed system with input fingerprint image loaded. Fig. 3 represents the system with genuine minutia points extracted out of it using Crossing Number technique. Fig. 4 represents the system with iris image loaded and Fig. 5 is the template extracted from iris using Daugman's intergrodifferential operator.

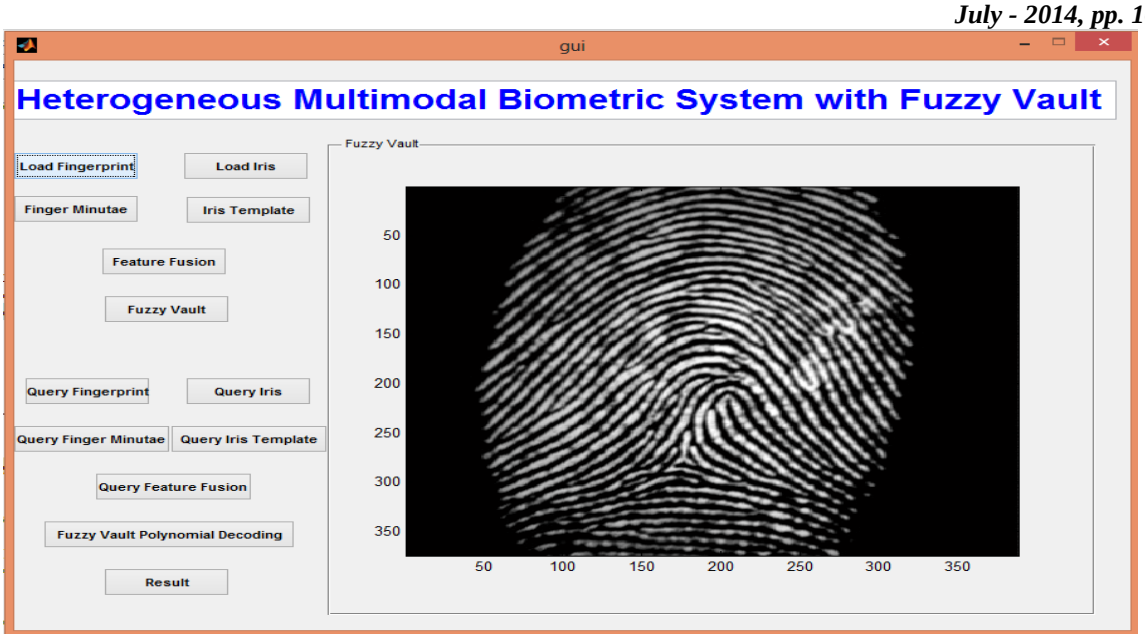

Fig. 2: Heterogeneous Multimodal Biometric System with Fingerprint image loaded.

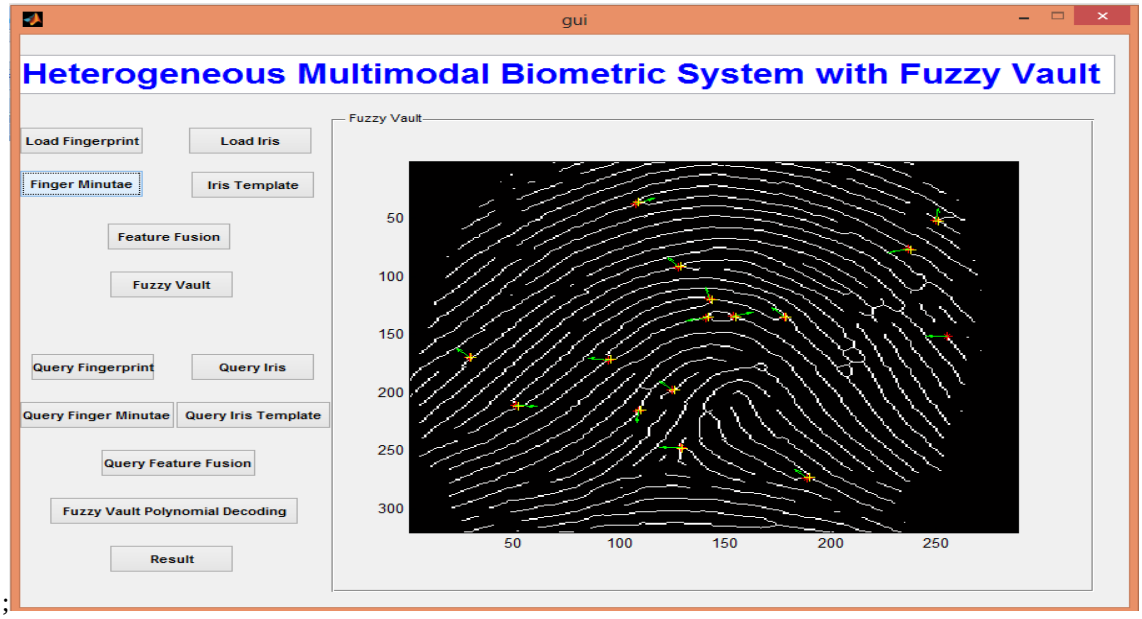

Fig. 3: Heterogeneous Multimodal Biometric System with Fingerprint minutia computed.

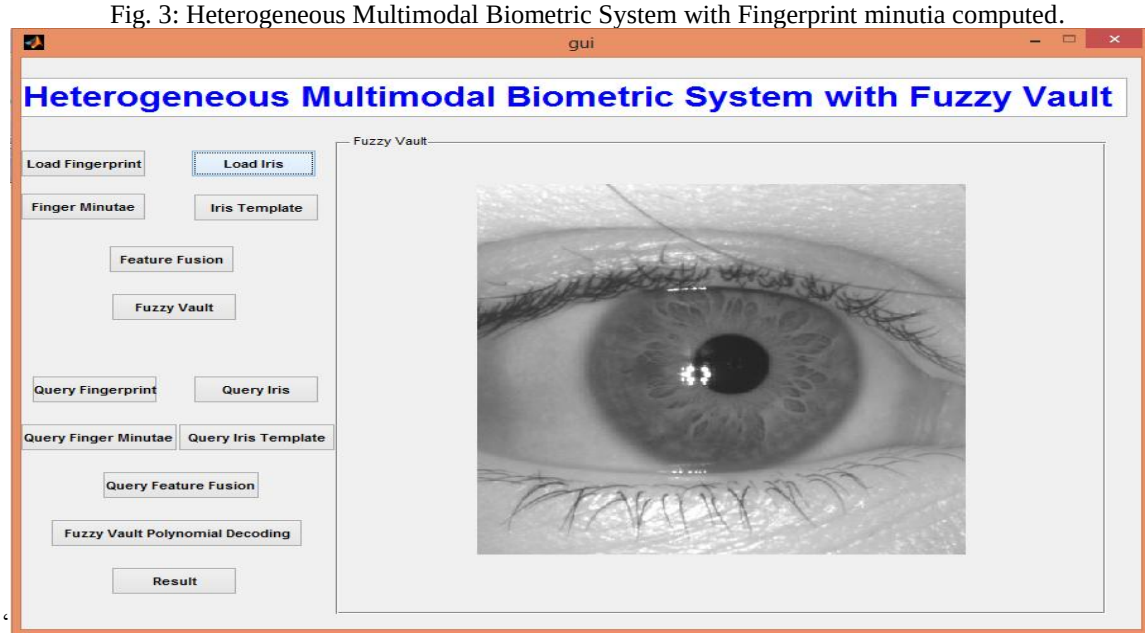

Fig. 4: Heterogeneous Multimodal Biometric System with Iris image loaded.

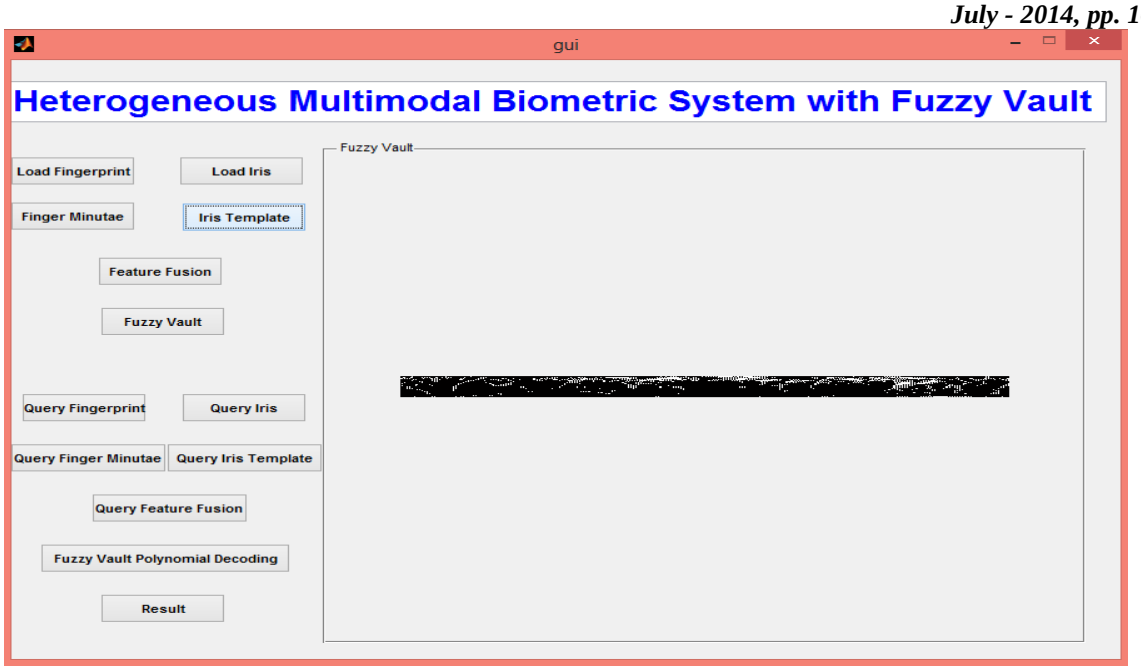

Fig. 5: Heterogeneous Multimodal Biometric System with Iris template extracted.

Represented below is Fig. 6 in which fuzzy vault is created after fusing the features extracted from iris and fingerprint. Here the genuine features are represented by crosses and chaff points by squares in Galois field. The feature set generated from iris is normalized by extracting specific patterns of 1's from it using Crossing Number technique so that the two sets of features can be fused to form a multimodal feature set as input to the fuzzy vault.

During authentication process the query fingerprint and iris are passed to the system and feature sets from both are extracted following the same procedure and the fused set is used to select the polynomial projections of the fuzzy vault. Feature set and its projections are computed using Lagrange's Interpolation in Galois field to extract the correct polynomial. So, if the set of query images are of the genuine person then the correct secret key would be generated confirming the authenticity of the user. Otherwise the correct secret key will not be generated.

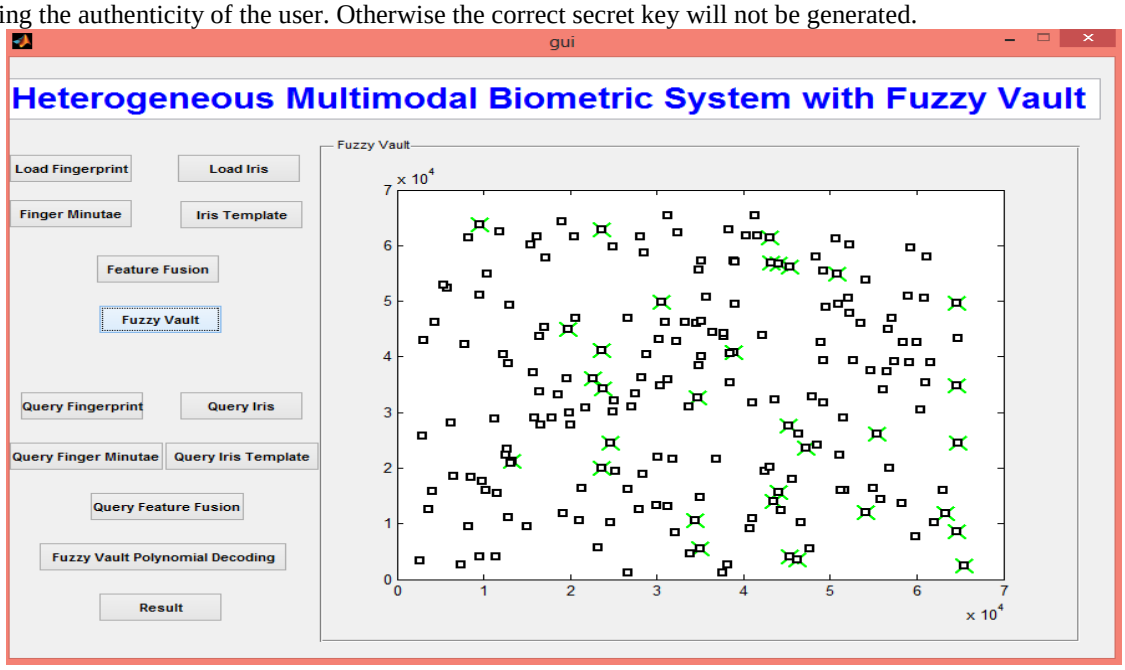

Fig. 6: Heterogeneous Multimodal Biometric System with Fuzzy Vault generated after fusion of features extracted from finger and iris.

C. Results

The results are tested on Fingerprint FVC database and CASIA Iris database taking 100 samples from each. The performance of the system was assessed by means of the standard error rates, False Rejection Rate (FRR), which accounts for the percentage of falsely rejected users, the False Acceptance Rate (FAR), which corresponds to the percentage of falsely accepted impostors. There exists a trade-off among these two performance metrics i.e. reducing the FAR results in an increase of the FRR and vice versa. Table 1 shows the results for the system accuracy in term of FAR, FRR and GAR for the proposed system.

TABLE 1: FAR, FRR AND GAR VALUES

Performance Metrics	**Values on Multimodal System Fingerprint+ Iris**
FAR	2.3
FRR	7.6
GAR	92.4

IV. CONCLUSIONS

Reliable and efficient identity management system has become very important in this highly interconnected world with increased concerns of identity fraud and national security. Biometric systems provide a greater degree of security and user convenience than the traditional authentication methods. Moreover, biometric systems also provide negative recognition and non-repudiation that is not provided by traditional systems. Multibiometric systems, if properly designed, are able to increase the matching accuracy of a recognition system, increase population coverage and deter spoofing attacks. The experimental results demonstrate that fusing information in multimodal heterogeneous environment at the feature level made the application of fuzzy vault possible producing satisfactory results increasing system security. The system can also be explored for other set of biometric traits.

REFERENCES

[1] Anil K. Jain, Ruud Bolle and Sharath Pankanti, *Biometrics Personal Identification in Networked Society*, Kluwer Acedmic Publishers, Print ISBN: 0-792-38345-1, created in United States of America, 2002.

[2] Arun Ross, Anil K. Jain, "Multimodal Biometrics: An Overview", Appeared in Proc. Of 12th European Signal Processing Conference (EUSIPCO), pp. 1221-1224, September 2004.

[3] Robert Snelick, Umut Uludag, Alan Mink, Michael Indovina and Anil Jain, "Large Scale Evaluation of Multimodal Biometric Authentication using State-of-the-Art Systems", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 27, No. 3, pp 450-455, , Mar 2005.

[4] Anil K. Jain, Patrick Flynn, Arun R. Ross, *Handbook of Biometrics*, Springer Science and Business Media LLC, ISBN-13: 978-0-387-71041-9, 2008.

[5] Ari Juels, Madhu Sudan, "A Fuzzy Vault Scheme", IEEE International Symposium Information Theory, Lausanne, Switzerland, pp. 408, 2002.

[6] Anil K. Jain, Karthik NandaKumar and Abhishek Nagar, " Biometric Template Security", in Journal on Advances in Signal Processing, Michigan State University, pp 1-17, 2007.

[7] Nalini Ratha and Ruud Bolle, *Automatic Fingerprint Recognition System*, ISBN 0-387-95593-3, Springer-Verlag New York, Inc., 2004.

[8] Oad Percy, Ahmad Waqas, "Iris Localization using Daugman's Algorithm", Thesis presented to Electrical Engineering Department of Bleking Institute of Technology School of Engineering, 2002.

[9] Martin Adolf, "Biometrics and Standards", ITU-T Technology Watch Report, Telecommunication Standardization Policy Division, ITU Telecommunication Standardization Sector, December 2009.

[10] 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.

[11] Ujwalla Gawande, Anushree Sapre, , Apurva Jain, , Sanchita Bhriegu, Shruti Sharma, "Fingerprint-Iris Fusion Based Multimodal Biometric System Using Single Hamming Distance Matcher", International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491, Volume 2, Issue 4 , pp: 54-61, February 2013.

[12] Hunny Mehrotra, Ajita Rattani, Phalguni Gupta, "Fusion of Iris and Fingerprint Biometric for Recognition", Proceedings of International Conference on Signal and Image Processing, 1-6, 2006.

[13] P.U. Lahane, Prof. S.R. Ganorkar, "Efficient Iris and Fingerprint Fusion for Person Identification", International Journal of Computer Applications (0975 – 8887), Volume 50– No.17, July 2012.

