IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 74-77

A Review of Multimodal Biometric Technology based on Fusion of Iris and Fingerprint Traitsfor Identification of Person

A. A. Halder[1], Dr. S. R. Pande[2]
Department of Computer Science
SSES Amt's Science College Congress Nagar, Nagpur, Maharashtra, India.

Abstract: *Biometric features are widely used for unique identification of any person. Iris is considered as the most reliable feature for identification of an individual with greatest accuracy because iris is the most discriminatory of facial biometrics. It is also found that biometrics is combined with cryptography for security to the greater extent. For greater precision of security many researchers are mixing other biometrics and hence multimodal biometric system has come into existence. In multimodal biometrics one or more features are combined together and using feature extraction technique features are extracted and fused together thereafter these fused feature set is matched using various matching algorithm with the feature of the person who will be identified. This paper presents an insight on issues with the biometrics which may help the researchers and other organizations working on biometrics.*

Keywords*: Biometrics, Fusion, trait, gait, Multimodal, HDC, FRR*

I. Introduction

Biometric traits are classified as physiological and behavioral traits of human being which are used to distinguish person's identity. These traits can be obtained from palm, iris, face, fingerprint etc. later on voice, gaitand other traits are considered for further more securities these traits are combined and multimodal biometric system has come into existence. Multimodality means where more than one modal is considered such as iris and palm, iris and fingerprint, voice and face etc. for identifying any person with great accuracy. The real world application of biometric system is to restrict anybody who tries to breach the security, only who is permitted to access the system whose extracted features get matched with the dataset stored in the database. Biometrics can be combined with cryptography for secured communication in the real world network [2]. If at all any security breach occurs due to compromise in biometric trait then to overcome this problem cancellable biometric approach has come into existence [7], [13], [14]. Hamming Distance Classifier (HDC) is introduced for calculating false rejection rate (FRR) and false acceptance rate (FAR) [11] also ocular biometrics got importance over the period of time [5]. Invention of multimodal biometric based on iris and fingerprint, iris and palm and other combinations are carried out [8].

THE CANCELLABLE TRANSFORMATION: In multimodality based on iris and voice data they applied three transformation functions BioHashing, Interpolation and BioConvolving. The Biohashing algorithm transforms the original biometric into a non-invertible binary sequence. This technique has originally used in other biometric modalities, such as fingerprint, palm and face. Interpolation technique is based on polynomial interpolations and it consists of generating a new biometric model through the extraction of points of an interpolation process based the attributes that compose the original biometric model. It is a simple method and it makes the inversion of the transformed function difficult, generating a reasonable level of security to the system. This method is then very efficient in satisfying two of the main requirements for transformation techniques, which are simplicity and efficiency at the same time [3]. The BioConvolving method was originally proposed for signature and, in this work, it is adapted to iris and voice data [15]. In this method, the transformed functions are created through linear combinations of sub-parts of the original biometric template. They are using decision-level fusion with three different approaches. In the first approach, multi-algorithm uni-modal fusion, the results of different cancellable transformations of the same biometric modality are combined. In the second approach, uni-algorithm multi-modal fusion, one cancellable transformation is chosen and the results of it in more than one modality are combined. Finally, the third approach, multi-algorithm multi-modal fusion, results of different cancellable transformations for more than one modality are combined [7]. The structure of proposed methodology is given in fig1.

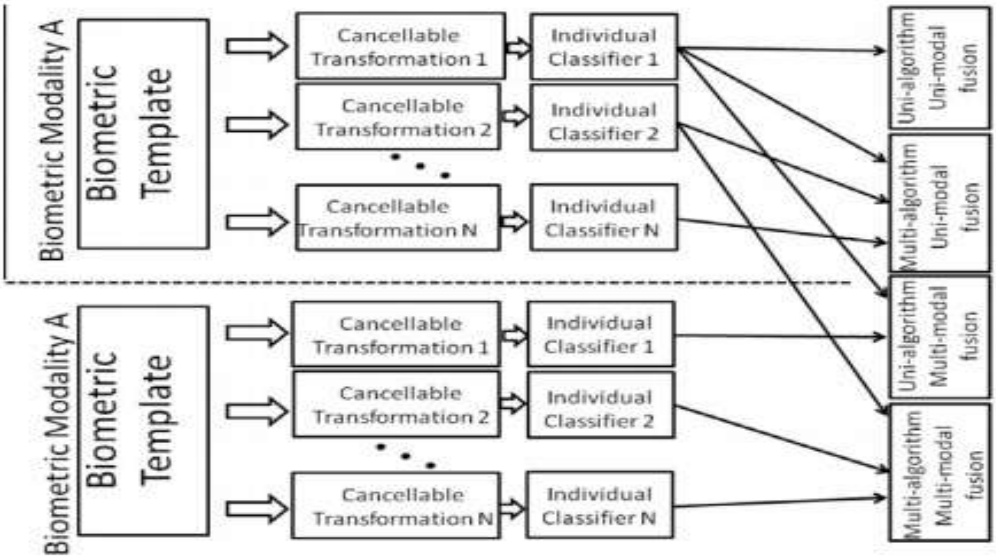

Fig.1.*The general structure of the proposed methodology*[7]

II. Methodology

MULTI-MODEL BIOMETRICS: Multi modal biometric systems are more reliable as it works on more than one modality. The biometric features of more than one modal are fused together to store in database for matching with the one who will be identified. The classification of biometrics is done in terms of both categories and levels. What inputs or processes are being used for fusion defined by categories and the levels define methods of fusion [17]. The fusions are categorized as multi-sample, multi-instance, multi-modal and multi-algorithm where as levels of fusion are categorized as data-sensor level, feature-extraction level, matching-score level and decision level [16]. The proposed multimodal system based on iris and fingerprint having two modules shown in fig.2 and fig.3

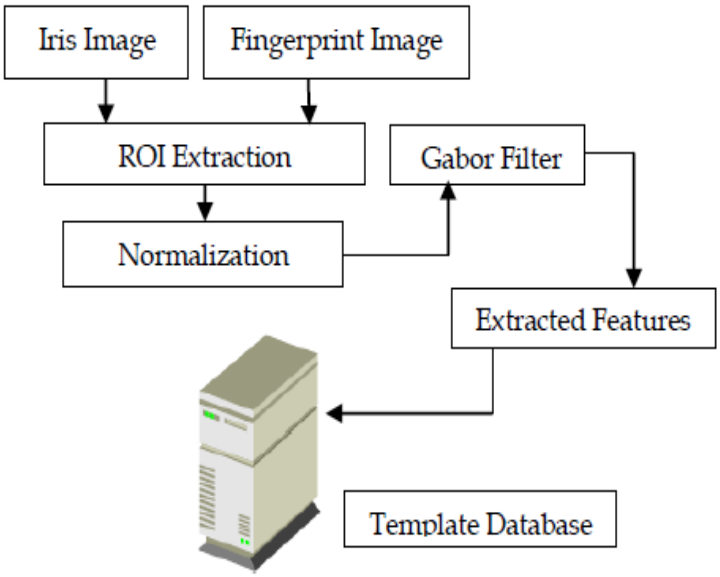

Fig.2 Enrollment Module[16]

The modules are of two types Enrollment module and identification module. The enrollment module contains preprocessing stage and identification module contains preprocessing stage as well as matching stage. The identification module is shown below [16].

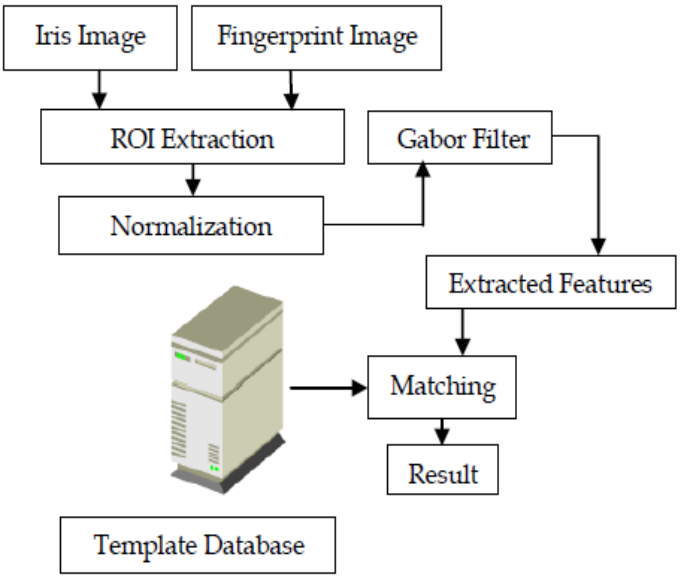

Fig.3 Identification Module [16]

III. Performance Evaluation

The combination of Iris and fingerprint can identify any person with greater accuracy or uniquely throughout the globe. It is shown in the image below-

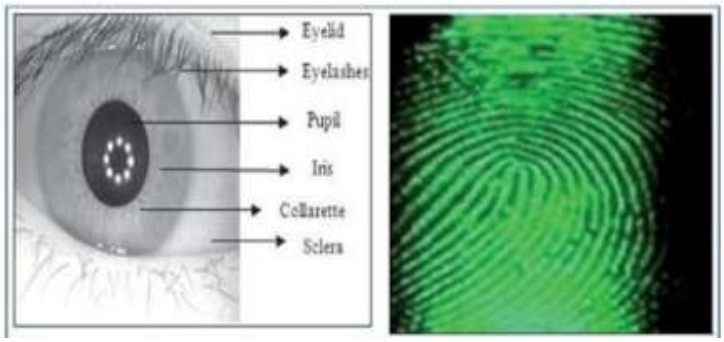

Fig.4. The combination of Iris and Fingerprint is combined together [8].

The fusion of these to traits provides the basis for the greater security in human identification. Though the fusion of these features are quite challenging but in real life combination of both are used; for finding similarity between trained and sample data to be tested two different algorithm are used for distance measure Euclidean distance and Hamming distance. In this way the identity of a person can be recognized in a secure and safest way with greater accuracy [8].

SECURITY ISSUES:

It is reported that those system using multimodal biometric system are face attacked although this mischievous activities are recorded by the system even though direct and indirect attacks are directed towards this multimodal biometric system. Researcher also revealed that biometric systems are getting spoofing attack and also some software attack to break down the security features applied in the system [9]. The targeted attacks are on database, communication channel and feature extraction techniques. Another issue with biometric system is that, it cannot distinguish genetically identical twins iris features as these features are exactly identical [10].

IV. Conclusion

In this paper it is tried to study and reveal the information related to multimodal biometric system based on iris and palm and various techniques that are used to fuse the biometric traits and how challenging these fusion techniques are. The biometrics whish are using facial data are being face attacked and this kind of attack can be overcome by cancellable transformations. Some single module and multi module proposed biometric systems are discussed which can reveal the idea of biometric system functions for the researcher. This

should be made sure that the iris based biometric system may work on ideal and non ideal images efficiently otherwise always there may be a chance of security breach. It is also found during the study that the iris based biometric system provides false data in noncooperative environment and this is to be addressed by the researcher in future research.

References

[1]. Gaurav Bhatnagar, Jonathan Wua, BalasubramanianRamanb (2012). Fractional dual tree complex wavelet transform and its application to biometric security during communication and transmission. Future generation computer systems, 28,1,2012, p254-267

[2]. R. ÁlvarezMariño, F. Hernández Álvarez, L. Hernández Encinas.(2012). A crypto-biometric scheme based on iris-templates with fuzzyextractorse. Information Sciences, 195, p91-102.

[3]. Javier Galbally, Arun Ross, Marta Gomez-Barrero, Julian Fierrez, Javier Ortega-Garcia. (2013). Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms. Computer Vision and Image Understanding, 117 (1), p1512-1525.

[4]. Farmanullah Jan, Imran Usman, Shahrukh Agha. (2012). Iris localization in frontal eye images for less constrained iris recognition systems. Digital Signal Processing, 22 (1), p971-986.

[5]. Simona Crihalmeanu and Arun Ross. (2012). Multispectral sclera patterns for ocular biometric recognition. Pattern Recognition Letters, 33(1), p1860-1869.

[6]. Maria De Marsico, Chiara Galdi, Michele Nappi, Daniel Riccioc.(2014). FIRME: Face and Iris Recognition for Mobile Engagement. Image and Vision Computing. p1161-1172.

[7]. Anne M.P. Canuto, Fernando Pintro, João C. Xavier-Junior. (2013).Investigating fusion approaches in multi-biometric cancellablerecognition. Expert Systems with applications, 40, 6, p1971-1980.

[8]. UjwallaGawande, MukeshZaveri, Avichal Kapur. (2013). Bimodal biometric system: feature level fusion of iris and fingerprint. Biometric Technology Today, p7-8.

[9]. Marta Gomez-Barrero, Javier Galbally, Julian Fierrez. (2014). Efficientsoftware attack to multimodal biometric systems and its application toface and iris fusion. Pattern Recognition Letters, 36 (1), p243-253.

[10]. Karen Hollingsworth, Kevin W. Bowyer, Stephen Lagree, Samuel P.Fenker, Patrick J. Flynn. (2011). Genetically identical irises have texturesimilarity that is not detected by iris biometrics. Vision and ImageUnderstanding, 115 (1), p1493-1502.

[11]. C.Chen and R.Veldhuis. (2011). Extracting biometric binary strings withminimal area under the FRR curve for the hamming distance classifier.Signal processing, 91, 4, p906- 918.

[12]. Farmanullah Jana, Imran Usman, Shahid A. Khana, Shahzad A.MalikaaDepartment. (2013). Iris localization based on the Houghtransform, a radial-gradientoperator, and the gray-level intensity. Optik -International Journal for Light and Electron Optics, 124 (1), p5976-5985.

[13]. C. Rathgeb and C. Busch. (2014). Cancelable multi- biometrics: Mixingiris-codes based on adaptive bloom filters. Computers & Security, 42(1), p1- 12.

[14]. Maltoni, D.Maio. A.k. Jain, S. Prabhakar.(2009). Handbook ofFingerprint Recognition, (2nd ed.). Springer publishing Company, Incorporated.

[15]. Maiorana, E., Martinez-Diaz, M., Campisi, P., Ortega-Garcia, J., &Neri, A. (2008). Template protection for hmm-based on-line signature authentication. In IEEE conference on computer vision and pattern recognition workshops (CVPRW) (pp. 1– 6).

[16]. P.U.Lahane, Prof. S.R.Ganorkar International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012 2 ISSN 2229-5518

[17]. Austin Hicklin, Brad Ulery, Craig Watson ―A Brief Introduction to Biometric Fusion‖ 16 June 2006.

[18]. HengFuiLiau and Dino Isa. (2011). Feature selection for support vector machine-based face-iris multimodal biometric system. Expert Systems with Applications., 38 (1), p11105-11111.

[19]. D.M. Rankin, B.W.Scotney,P.J.Morrow a, B.K. Pierscionek. (2012). Iris recognition failure over time: The effects of texture. Pattern Recognition, 45 (1), p145-150.

[20]. Shaaban A. Sahmoud, Ibrahim S. Abuhaiba 2013. Efficient irissegmentation method in unconstrained environments. PatternRecognition, 46 (1), p3174-3185.