DOI: 10.13140/RG.2.1.3324.8881

A Study of Multi-model Fusion Biometric Authentication System and Levels

Kiranjeet Kaur[1], Rupinder Kaur[2]
Student, M.Tech (Scholar), Doaba Institute of Engineering and Technology, Kharar
Assistant Professor, Doaba Institute of Engineering and Technology, Kharar

Abstract - The quality improvement technique, data fusion has been gradually improved in recent years. In data fusion is distinct as a formal structure which includes conveyed means and tools for combining and utilizing data originating from different sources. Image fusion technology has been widely used in the fields of remote sensing, medical imaging, mechanismidea, and army applications in current years. And the research on performances evaluation of different fusion techniques has been realized as an urgent requirement. In the previous framework, the biometric modalities are organized sequentially such that the tougher biometric modality has advanced priority for being processed. Since fusion is required only when all unmoral classifiers are rejected by the SVM classifiers, the average computational time of the planned framework is significantly concentrated. On different multimodal databases involving face and thumbprint show that the planned quality-based classifier collectionstructure yields good performance even when the quality of the biometric sample is sub-optimal.

Keywords - Data fusion, quality improvement technique, biometric authentication and SVM classifiers.

I. INTRODUCTION

Multi-model based verification systems use two or more classifiers affecting to the same biometric modality or dissimilar biometric modalities[1]. Biometric data of a user is typical to the user. The security of the stored biometric data when it is stored in the central verification agency' database is an area of concern. Simplistic means to protect the biometric template by storing the feature set in encrypted form may not yield the desired result as it has been noticed that multiple acquisitions of the feature sets do not yield the same results. Small variations due to inherent intraclass variations of the biometric feature sets may lead to disproportionate variations in the encrypted domain resulting in unacceptable matching score assessment. The inherent nature of the biometric data ensures non-transferability as biometric data is permanently bound to a user and it is almost impossible to produce a new set of biometric sorts for a genuine user [2].

Multi model bio-metric fusiondepicts the outline of multi-modal biometric system in parallel fusion mode, with reference to the one considered in this study, namely a standard bi-modal confirmation system based on a expression and a thumbprint matcher. In multi-modal schemes, information fusion can be approved out at sensor, feature mining, matching score or conclusion level.

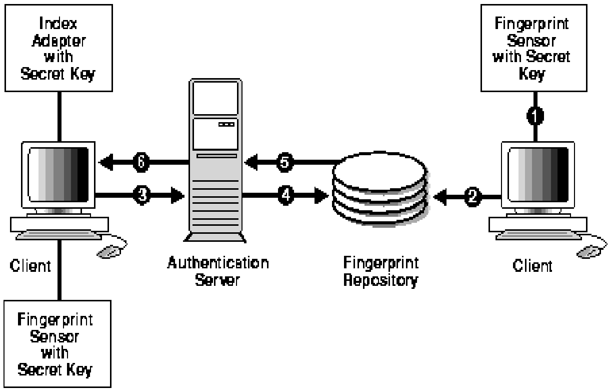
Index Adapter with Secret Key
Fingerprint Sensor with Secret Key
1
6
5
3
4
2
Client
Authentication Server
Fingerprint Repository
Client
Fingerprint Sensor with Secret Key

Fig.1: Biometric authentication

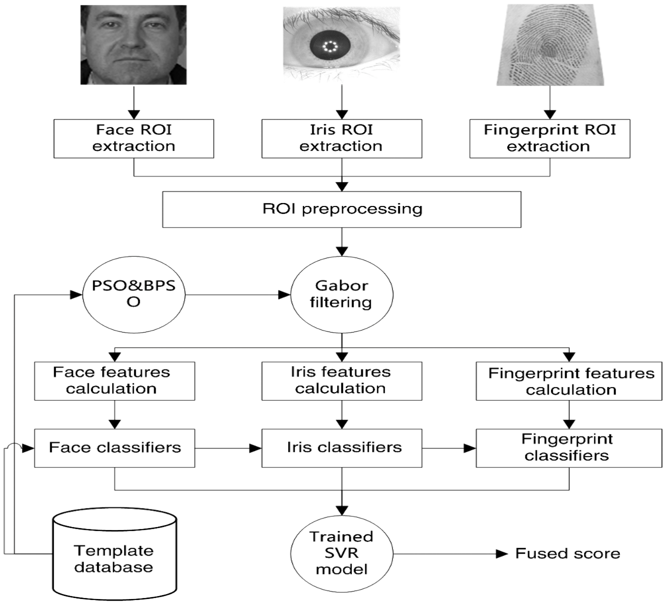

Fig.2: Multi model biometric fusion

Due to ease in accessing and combining of identical scores, fusion at identical score level is the most normally adopted method in the collected works, and is also accepted in this study. In a verification setting, each user presents his face and fingerprint to the respective devices, and claims his uniqueness. Each matcher then distinctly compares the offered trait with the consistent template of the claimed uniqueness, and produces a face and a fingerprint matching score.[3]

II. TYPES OF FUSION

Automatic personal authentication uses different biometric characteristics to attain robustness to noise, permanence, universality, distinctiveness, rotational invariance, translation or distortion, which in turn, ensures the prevention of spoofing. Since it is almost impossible to meet all these requisitions with a single biometric feature, the utility of multimodal biometric system is firmly acknowledged in the field of programmed personal verification. As multi-modal system consists of scores of different modalities (like face, palm print, iris, ear, speech etc.) for different individuals who are to be authenticated or classified, integration is recommended which guarantees speed and acceptability of the system. This integration or fusion can be done at several levels like sensor level, feature extraction level, score level and decision level.

a) **Score level:** A general rule for multimodal system design states that the integration at an early stage of biometric management i.e. at sensor level might be more accurate than those where the fusion is introduced at later stages. A feature extraction level fusion would be difficult as different features may be incompatible with the others. Hence due to the different natures of the biometric modalities, which might be hardly compatible (e.g., fingerprint and iris), fusion at sensor level is hard to obtain. Most commercial biometric systems do not provide access to the feature sets and hence exclude the possibility of fusion at feature level.

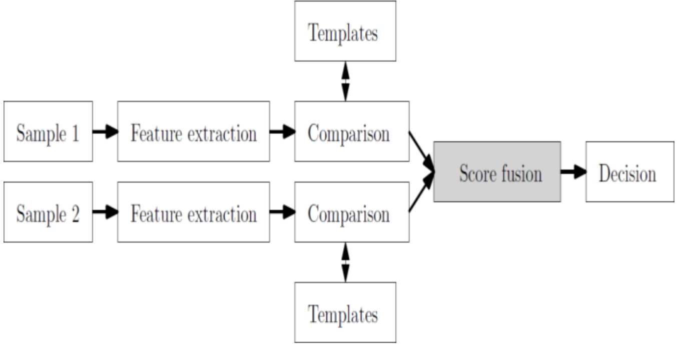

Fig.3: Score level fusion

Consequently, in most applications, fusions at sensor and feature levels are not performed. Fusion at matching level or at decision level does not require the creation of new databases or matching modules. Additionally, it is very difficult to fuse or integrate the scores of different attributes in a decision level methodology due to lack of information[4].

a) **Decision level:**We also propose a decision level fusion model. Basically, we applied learning models for the description of each detection method separately and combine their decision using majority voting as in equation. FD = MV (D(Harris3D), D(Periodic), D(Dense)) Where D is a single decision and FD is a fused decision.

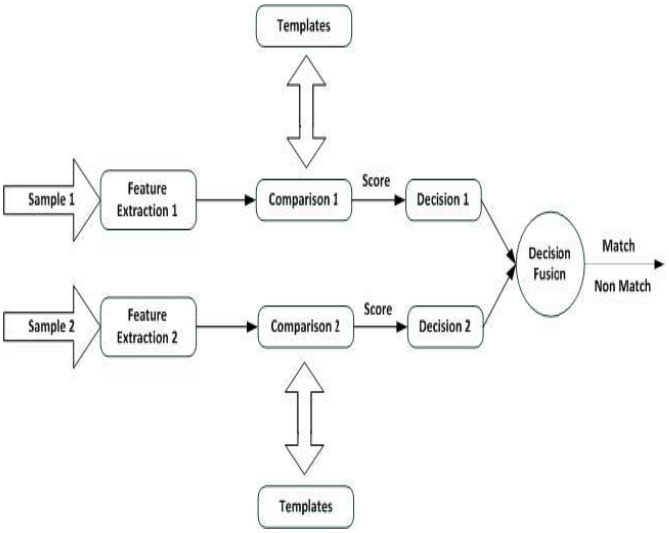

Fig.4: Decision level Fusion

If each model makes a unique decision or in other words there is a tie for all the three decisions, the decision based on Harris3D is selected. This is based on its superior performance as will be discussed later in the section on results. In the following section, the experimental setup and results are discussed [5].

III. IRIS RECOGNIZATION

Wildes gives accounts ofthe main reasons behind the use of iris images as a trusted and highly reliable human trait for discriminating individuals. In design issues related to the implementation and deployment of an automated iris recognition scheme, founded on sound workstation vision algorithms, talk over in details. Until the past few years, several new procedures for eye feature mining have been suggested. However, very little contributions have been made to propose new identical mechanisms in instruction to improve the precision of iris recognition schemes at large[6].

DOI: 10.13140/RG.2.1.3324.8881

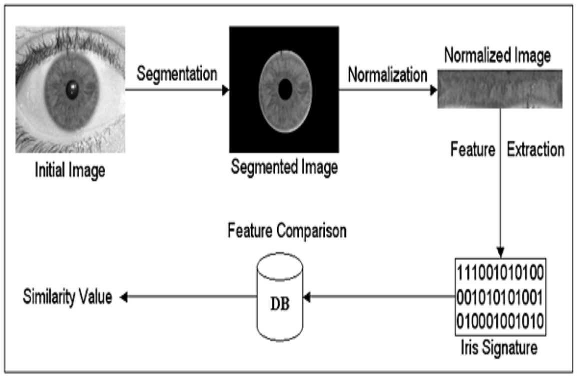

Fig.5: Iris Recognition

IV. FACE RECOGNITION

The human face plays a significant role in our social [9] interface, conveying people's identity. Using the human face as a key to security, biometric face recognition expertise has received significant attention in the past several years due to its potential for a wide variability of applications in both law enforcement and non-law enforcement.As compared with other biometrics schemes using fingerprint/palm print and iris, face recognition has distinct advantages because of its non-contact process. Face images can be caught from a distance without touching the person being identified, and the documentation does not require interacting with the person. In addition, face recognition serves the crime deterrent determination because face images that have been verified and archived can later help identify a person.

Most current facial appreciation systems work with numeric codes called face prints. Such systems identify 80 nodal points on a human face. In this situation, nodal points are end points used to measure variables of a person's face, such as the distance or width of the nose, the depth of the eye sockets and the shape of the cheekbones. These systems work by capturing data for nodal points on a digital image of an entity's face and storing the resulting data as a face print. The face print can then be used as a basis for assessment with data captured from faces in an image or video.

Facial recognition systems based on face prints can rapidly and accurately identify target individuals when the conditions are favorable [10]. However, if the subject's face is incompletely obscured or in profile rather than facing forward, or if the light is deficient, the software is less reliable. Nevertheless, the technology is evolving quickly and there are several emerging approaches, such as 3D modelling, that may overcome current problems with the systems.

V. RELATED WORK

Min Guo et al (2014)[7]image fusion, in which a superposition strategy is practical to concept the coupled wordlists. The shaped coupled wordlists are further developed via an iterative update to guarantee that the HR MS image square can be practically identically rebuilt by multiplying the HR dictionary and the sparse coefficient vector, which is resolved by sparsely on behalf of its counterpart LR MS image patch over the LR wordlist. The fusion effectssince IKONOS and WorldView-2 data show that the proposed fusion method is competitive or even higher to the other state-of-the-art fusion approaches.**P Suresh et ,al(2015)[2]**Biometric system based identity management systems offer advantage over conventional knowledge and possession based systems. Considerable research has been undertaken in the past to classify newer and consistent biometrics for more effective and secure identity management. Fusion of multiple biometrics to achieve better results is also an area of active research. However, making biometric credential systems revocable and unidentified without sacrificing efficacy and efficacy of detection still remains a challenge. This survey paper makes an attempt to give an insight into the approaches that have been made in the direction of multimodal biometric fusion and into the various options that have been explored to make biometric authentication systems revocable and anonymous. **Zahid Akhtar et, al(2012**) [3]the robustness of multi-modal systems, in serial and parallel fusion modes, under spoofing attacks. In specific, we empirically examine the vulnerability of sequential and parallel fusion of face and fingerprint biometrics to actual spoofing attacks. Our results display that multi-modal schemes in both fusion modes are vulnerable to attacks against a particular biometric quality. On the former hand, they show that the serial fusion mode can attain a favorable trade-off among presentation, verification time, and sturdiness against spoofing attacks .**Sudesh Kumar Kashyap (2015**)[8]fuzzy logic operations in context of image combination. Color and ultraviolet images obtained from Enhanced Vision System prototype are exploited for the study. The fused image is assessed for various design cases for fuzzy logic system type 1 and Intermission type 2 fuzzy judgment systems. Constructed on qualitative and logical analysis, it is concluded that Intermissionkind 2 fuzzy senseschemedoes better than fuzzy logic schemekind 1 and in universal Sugeno based fuzzy logic schemes are better than Mamdani based fuzzy logic systems. **Satrajit Mukherjee et al (2014)[4]** a novel adaptive weight and exponent based utility mapping the identical scores from different biometric bases into a single amalgamated matching score to be used by a classifier for additional decision constructing. Differential Development (DE) has been working to modify these tunable constraints with the objective existence the minimization of the overlying area of the frequency distributions of genuine and cheat scores in the fused score space, which are appraised by Gaussian kernel density method to achieve higher level of accuracy. Investigational results show that, the suggested

DOI: 10.13140/RG.2.1.3324.8881

method outperforms the conventional score-level fusion rules when verified on dualistic databases of 4 modalities (thumbprint, iris, right ear and left ear) of 300 and 516 users and thus settles the efficiency of score level fusion.

Table no: 1 Important Modules

Level Name	Description
Sensor Level	This fusion strategy requires the raw data to be acquired from multiple sensors which can be further handled and unified to generate new data from which features can be extracted. Sensor level fusion can be done only if the numerous cues of the same biometric are obtained from multiple compatible sensors.
Feature level	The feature set is removed from the multiple sources of information and is further concatenated into a joint article vector. This new high dimensional piece vector represents an individual. In case of feature level fusion some decreasemethod must be used in order to select only useful features.
Match score level	Match score is a quantity of the similarity between the input biometric and template biometric feature vectors. Based on the similarity of feature vector and the pattern, each subsystem calculates its own match score value. These individual scores are finally collective to obtain a total score, which is then accepted to the decision module, after which recognition is performed.
Rank level	Rank level fusion is normallyaccepted for the identification of the person rather than verification. Thus, fusion entails consolidating the multiple ranks connected with an identity and determining a new rank that would aid in establishing the final decision

VI. CONCLUSION

The present paper gives a survey of research work in the fields of cancelable biometrics and also has explored the realm of multi-modal biometrics. The use of multi-modal biometrics in enhancing the potency of transformations is a potential area of research. An introduces a novel score level fusion strategy employing DE to minimize the overlapping area of the resultant frequency distributions of the resulting fused genuine and imposter scores. To the best of our knowledge, no such met heuristic optimizer based parameter tuned mapping function has been deployed for blending individual scores in a multimodal biometric authentication system

VII. REFERENCES

[1] Bhatt, Himanshu S., et al. "A framework for quality-based biometric classifier selection." Biometrics (IJCB), 2011 International Joint Conference on.IEEE, 2011.

[2] Suresh, P., and K. R. Radhika. "Bio-metric credential system: Multimodal cancelable anonymous identity management." Advance Computing Conference (IACC), 2015 IEEE International.IEEE, 2015.

[3] Akhtar, Zahid, et al. "Evaluation of serial and parallel multibiometric systems under spoofing attacks." Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on. IEEE, 2012.

[4] Mukherjee, Sayan, et al. "Differential evolution based score level fusion for multi-modal biometric systems." Computational Intelligence in Biometrics and Identity Management (CIBIM), 2014 IEEE Symposium on. IEEE, 2014.

[5] Abouelenien, Mohamed, Yiwen Wan, and Abdullah Saudagar. "Feature and decision level fusion for action recognition." Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on.IEEE, 2012.

[6] Ghouti, Lahouari, and Ahmed A. Bahjat. "Iris fusion for multibiometric systems." Signal Processing and Information Technology (ISSPIT), 2009 IEEE International Symposium on.IEEE, 2009.

[7] Guo, Min, et al. "An online coupled dictionary learning approach for remote sensing image fusion." Selected Topics in Applied Earth Observations and Remote Sensing, IEEE Journal of 7.4 (2014): 1284-1294.

[8] Kashyap, Sudesh Kumar. "IR and color image fusion using interval type 2 fuzzy logic system." Cognitive Computing and Information Processing (CCIP), 2015 International Conference on.IEEE, 2015.

[9] Mikhaylov, Dmitry, et al. "Face Detection and Tracking from Image and Statistics Gathering." Signal-Image Technology and Internet-Based Systems (SITIS), 2014 Tenth International Conference on.IEEE, 2014.

[10] Han, Dan, and Yue Ming. "Facial expression recognition with LBP and SLPP combined method." Signal Processing (ICSP), 2014 12th International Conference on. IEEE, 2014.