Fusion Based Multimodal Biometrics using Face and Palm print at Various Levels

Sneha A. Taksande[1], Pushpanjali M. Chouragade[2]
M.Tech. Scholar[1], Assistant Professor[2]
Department of Computer Science and Engineering
Government College of Engineering, Amravati
sneha.taksande11@gmail.com, pushpanjalic3@gmail.com

Abstract **- Biometrics have wide applications in the fields of security and privacy. As unimodal biometrics are subjected to various problems regarding recognition and security, multimodal biometrics have been used extensively nowadays for personal authentication. In recent years it is seen that researchers paying enormous attention to design effective multimodal biometric systems because of their ability to endure spoof attacks. Single biometric sometimes fails to extract adequate information for verifying the identity of a person. On the other hand, by combining multiple modalities, enhanced performance reliability could be achieved. In this paper, we have fused face and palm print modalities at all levels of fusion e.g. sensor level, feature level, decision level and score level. For this purpose, we have selected modality specific feature extraction algorithms for face and palm print such as LDA and LPQ respectively. Popular databases AR (for face) and PolyU (for Palm print) were considered for evaluation purposes. Severe experiments were conducted both under clean and noisy conditions to ascertain robust level of fusion and impact of fusion strategies at various levels of fusion for these two modalities. Results are substantiated with appropriate analysis.**

Index Terms **–** Biometric, Face, Palm print, Fusion, LDA, LPQ.

I. INTRODUCTION

Traditionally passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to secure system. However, security can be easily broken in these systems when a password is revealed to an unauthorized user or a card is stolen by a copier. Furthermore, simple passwords are easy to guess by an imitator and difficult passwords may be hard to recall by a legitimate user. The word "biometrics" is derived from the Greek words "bio" which means life and "metrics" which means to measure.

BIOMETRICS now became a key technology for personal authentication in different fields of network security. Biometric technologies provide us friendly and reliable control for accessing computers, network systems and work places. We can define "Biometrics" as the automatic personal recognition based on the physiological and behavioral characteristics of that individual. Biometric-based authentication techniques are given more attention nowadays because of the increased concern in security. Some of the examples for biometric identifiers that have been used for automated recognition include fingerprints, iris, face, hand or finger geometry, palm prints, retina, voice, signature, and keystroke dynamics. The best example of using biometric is ATM system.

Biometric techniques are unique and efficient methods for person identification/authentication; many organizations rely on unimodal biometric systems to identify individuals. Multimodal biometric system is a relatively new application in biometric field, while single (unimodal) biometrics has been used for a long time. For example, fingerprint has been widely used by law enforcement agency for person verification and identification. These biometric systems based on single modality suffers with various challenges such as noise in sensed data, intra-class variations, inter-class similarities, nonuniversal and spoof attacks etc. To overcome drawback of unimodal and to increase the reliability of system, biometric fusion especially multi-modal biometric fusion has drawn a lot of attention recently. Multimodal biometric system is subset of Multibiometric system which depends on multiple source of evidence to identify an individual. The advantages of multimodal systems over the unimodal are increase in the population coverage, high performance, more robust and increase the resistance for spoof attacks.

II. RELATED WORK

Traditionally, unimodal biometrics has been used for personal authentication. But it provides less accuracy in the case of recognition. So we have given more preference to multimodal biometrics. Several feature extraction methods have been implemented to extract the feature vectors of palm print and knuckle print. Mostly Gabor filters are used for extracting features from palm print. Gabor filters can provide better recognition rate, but cannot extract all the features and have high computational cost. Thus Log Gabor filters have been proposed to extract the features of palm print. Performance of Log Gabor filters is limited by marginal matching accuracy and failure to remove all noises in the image.

Some researchers proposed 2D-Fourier Transform (FT) for feature extraction of palm print. Here entire image is

segmented into several narrow-width bands and the task of feature extraction is carried out in each band using two dimensional Fourier transforms.

Yao et al. proposed a system on fusion of palm print and face, on single sample biometrics recognition problem. Initially, features are extracted using Gabor filter for both palm print and face modality than dimension of feature space is reduced using PCA transform. Normalization of features is performed using weighting strategy, however features are combined and nearest neighbor (NN) classifier is employed for classification. Audrey et al. designed small sample biometric recognition based on palm print and face fusion. The fusion of palm print and face is performed at score level; it achieving a correct recognition rate of 98.85% using only two samples per modality.

Ahmad et al. evaluated a multimodal system for face and palm print. Gabor based image processing is utilized to extract discriminant features, while principal component analysis (PCA) and linear discriminant analysis (LDA) are used to reduce the dimension of each modality. Multimodal fusion at the feature level of face and palm print produces better recognition result (99.5%) compared to single modal biometrics method (87% for eigen-faces, 92% for fisher-faces, 91.5% for Eigen-palm and 94% for fisher-palm). Kisku et al. proposed a sensor level fusion

Scheme for face and palm print. Here, face and palm print are decomposed using Haar wavelet and then average of wavelet coefficients are carried out to form a fused image of face and palm print. Finally, inverse wavelet transform is carried out to form a fused image of face and palm print. Then, feature extraction is carried out on this fused image using Scale Invariant Feature Transform (SIFT) technique to make the decision about accept or reject.

Cheng Lu et al. designed multimodal system on combining face and palm print at match score level fusion. Two feature extraction methods are employed for multimodal biometric identification. The one is based on statistics properties (SP) and the other is two-dimensional principal component analysis (2DPCA). The experimental results indicate that the performance of multimodal biometric identification outperforms to the unimodal system and the accuracy can reach 100%. Shen et al. proposed feature code based approach for multimodal biometrics. Decision level fusion is employed two fusion cases, face & palm print and FKP & palm print are considered to verify the effectiveness of multimodal biometrics. Experimental results show that much better performance than single modal biometrics has been achieved. Yan et al. developed a novel class-dependence feature analysis method for multimodal system, based on Correlation Filter Bank (CFB) technique. Face and palm print are the modalities used and fused at the feature level. Hanmandlu et al. explored a multimodal biometric system based on hand biometrics (i.e. palm print, hand veins, and hand geometry) at score level fusion using t-norm strategy. The experimental results suggest that the score-level approach using t-norm renders fairly good performance and does not require any iteration. The proposed fusion using Hamacher t-norm yields Genuine Acceptance Rate (GAR) (99.9%) at False Acceptance Rate (FAR) of 0% which is remarkable improvement over individual modalities.

III. ARCHITECTURE OF BIOMETRIC SYSTEM

There are two phases in a biometric system. A learning phase i.e. enrolment and a recognition phase i.e. 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 secrecy 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 copies of the item considered. A large amount of the models used are statistical models, which make it possible to allow for a certain variations 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 one of the data base models and then authorize the person or reject him. Identification may be a very difficult task if the data base contains thousands of individuals. Then access time problems become crucial.

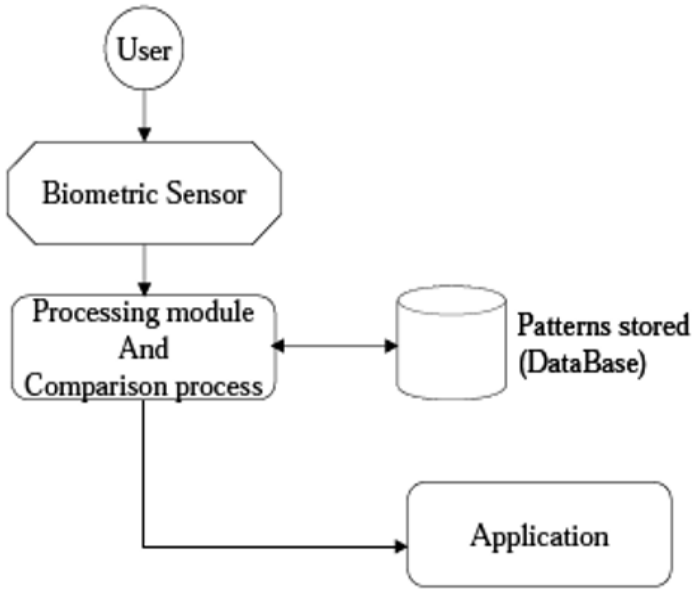

Fig. 3. Architecture of Biometric System

Modules of Biometric System:

1. *Sensor module:* It captures the biometric data of an individual. An example of sensor module is fingerprint sensor, 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.

IV. PROPOSED METHODOLOGY

Gabor wavelets demonstrate two desirable characteristic: spatial locality and orientation selectivity. The structure and functions of Gabor kernels are similar to the two-dimensional accessible fields of the mammalian cortical simple cells indicates that the Gabor wavelet representation of face images should be robust to variations due to brightness and facial expression changes. Matching, and it is just the reason that almost all of the previous work makes use of only the magnitude part for face recognition. Note that, convolving an image with a bank of Gabor kernel tuned to 5 scales and 8 orientations results in 40 magnitude and phase Response maps of the same size as image. Therefore, considering only the magnitude response for the purpose of feature description, each pixel can be now described by a 40 dimensional feature vector by concatenating all the response values at each scale and orientation describing the response of Gabor filtering at that location. Note that Gabor feature extraction results in a highly localized and over complete response at each image location. In order to describe a whole face image by Gabor feature description the earlier methods take into account the response only at certain image locations, e.g. by placing a rough rectangular grid over the image and taking the response only at the nodes of the grid or just considering the points at important facial landmarks. The recognition is then performed by directly comparing the corresponding points in two images. This is done for the main reason of putting an upper limit on the dimensionality of the problem. However, in doing so they indirectly assume a perfect alignment between all the facial images, and moreover the selected points that needs to be compared have to be detected with pixel accuracy. The Gabor based feature description of faces although have shown superior results in terms of recognition, however we note that this is only the case when frontal or near frontal facial images are considered. Due to the problems associated with the large dimensionality, and thus the Requirement of feature selection, it cannot be applied directly in scenarios where large pose variations are present.

A. Existing system:

- Initially unimodal biometrics systems were depend on a single source of information such as a single iris or fingerprint or face for authentication.
- The selection of a particular biometric for use in a specific application involves a weighting of several factors.
- It was identified that seven such factors to be used when assessing the suitability of any trait for use in biometric authentication.
- Single biometric will not meet all the requirements of every possible application.
- Since it has several problems multimodal biometrics was introduced.

B. Proposed system:

- Here we are providing new methods in fusion of palm print and face images.
- Here preprocess will be done for input images. Then feature extraction is executed for preprocessed images by bifurcation extraction and Gabor feature.
- Then bifurcation feature will be found for palm print images and Gabor feature for face images.
- Multimodal sparse representation method, the test data by a sparse linear combination of training data, while making the observations from different modalities of the test subject to share their sparse representations.
- Then score will be find for input images.
- The input images for palm print and face will be fused.

V. DIFFERENT LEVELS OF FUSION OF FACE AND PALM PRINT

Following Figure shows the block diagram of the proposed multimodal biometric system based on the fusion of face and palm print at various levels of fusion. Fusion of information in biometric can be performed in different form: a) Fusion prior to matching. b) Fusion after the matching. In the case of prior to matching, the multiple information of biometric sources can take place either at sensor level or at the feature level. On the other hand, combining the information after the matching/classification can be performed at score level and decision level. In our multimodal biometric system, the fusion is performed at all four levels. There are different kinds of approaches for consolidating information from two different modalities. At sensor level we have used wavelets based image fusion scheme to fuse palm print and face images, at feature level we employed different normalization techniques namely Min-Max, Z-Score and Hyperbolic tangent. At score level, we considered fusion rules, such as sum, max and min rule, to combine the two matching scores. Finally, at decision

level we adopted logical AND and OR to combine the output decisions by different matchers.

The proposed system for personal authentication based on palm and face print identifiers have been illustrated in the below block diagram and the steps are described below:

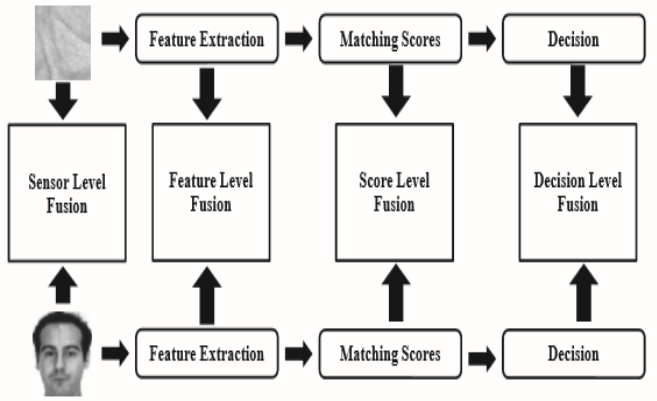

Fig 5: Block diagram of Different levels of fusion of Face and Palm print

Fusion at the feature extraction level: The data obtained from each sensor is used to compute a feature vector. As the features extracted from one biometric attribute are independent of those extracted from the other, it is reasonable to concatenate the two vectors into a single new vector. The new feature vector now has a higher dimensionality and represents a person's identity in a different hyperspace.

Fusion at the matching scores level: Matching score provided by each system indicating the proximity of the feature vector with the template vector. These scores can be combined to assert the veracity of the claimed identity. Techniques such as logistic regression may be used to combine the scores reported by the two sensors.

Fusion at the decision level: Each sensor can capture multiple biometric data and the resulting feature vectors individually classified into the two classes i.e. accept or reject.

VI. CONCLUSION

In the recent past, there is a tremendous interest shown by researchers towards implementation of multimodal system adopting various fusion strategies. However, to the best of our knowledge, there is minimal reporting in the literature that addresses all levels of fusion in a single paper. This paper addressed fusion of face and palm print modalities at all levels of fusion to determine best level of fusion for these two modalities of face and palm print. In addition, for every level of fusion, we ascertained the optimal fusion strategy for these two modalities. We believe that this study helped us to know the robust level of fusion for face and palm print modalities. Thus Biometrics provides security benefits across the spectrum, from IT vendors to end users, and also from security system developers to security system users.

REFERENCES

[1] Mohamed A. Kassem, Nagham E. Mekky and Rasheed M. EL-Awady "An Enhanced ATM Security System Using Multimodal Biometric Strategy", *International Journal of Electrical & Computer Sciences IJECS*- IJENS Volume 14 No. 04, August 2014.

[2] Garima Sethi and Ashwinder Tanwar, "Enhance in Multimodal Biometrics", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 4, Issue 6, June 2014.

[3] S Noushath, Mohammad Imran, Ashok Rao and Hemantha Kumar G, "Multimodal Biometric Fusion of Face and Palm print at Various Levels", *IEEE*, 2013.

[4] Ephin M, Shreya Mohan, N. A. Vasanthi, "Survey on Multimodal Biometric using Palm prints and Fingerprint'', *International Journal of Computer Applications* (IJCA):2013.

[5] Harbi Al, Mahafzah, Mohammad, Imran, and H.S Sheshadri; "Multibiometric: Feature level fusion using FKP Multi Instance biometrics", *IJCSI International Journal of Computer Science Issues*, Vol. 9, Issue 4, No 3.2012.

IJSER