CHAPTER 2

LITERATURE SURVEY

Fuzzy vault is a recently developed cryptographic method to secure critical data with the biometric information in a way that only the authorized user can access the secret data by providing the valid biometric template. However, attackers can compromise them by cross-matching if they steal multiple vaults of a legal user. If a biometric identifier is compromised, it is lost forever and possibly for every application where the biometric is used.

2.1 MULTIMODAL FUSION

Unimodal biometric systems come across a diversity of security problems and offer sometimes intolerable fault rates. Multimodal biometric have recently attracted significant interest for its high performance in a biometric recognition system (Anil et al., 2008). By setting up multimodal biometric systems, a few of these disadvantages can be overcome. Joining dissimilar biometric sources, Multimodal biometrics offers high identification precision and population coverage (Ruma Purkait, 2007). Several of the latest strategies have been reviewed below:

Monwar M.M and Marina L. Gavrilova (2009) have offered an efficient fusion plan that unites data offered by multiple domain specialists based on the rank-level fusion integration technique. The multimodal biometric system improved by them acquires a number of distinctive qualities, starting from utilizing principal component study and Fisher’s linear discriminant techniques for individual matchers distinctiveness authentication and employing the new rank-level fusion technique in order to strengthen the results attained from dissimilar biometric matchers. The results have pointed out that the fusion of individual modalities can develop on the whole presentation of the biometric system, still in the existence of low quality information.

A human recognition method combined face and speech information in order to improve the problem of single biometric authentication were proposed by Mohamed Soltane et al. (2010). Gaussian mixture modal (GMM) is the main tool used in text-independent speaker recognition, in which it can be trained using the Expectation Maximization (EM)
and Figueiredo-Jain (FJ) algorithms for score level data fusion. The use of finite GMM based Expectation Maximization (EM) estimated algorithm for score level data fusion was proposed. Extracted face and extracted audio is fused to achieve recognition rate. Face speech biometric EER is reduced to 0.087.

Muhammad Imran Razzak et al. (2010) combined the face and finger veins, in which multilevel score level fusion is performed to increase the robustness of the authentication system. The score level fusion of client specific linear discriminant analysis (CSLDA) for fusion of face and finger veins result is performed. CSLDA uses the PCA and LDA to generate a client specific template. The score of face and finger veins are combined using weighted Fuzzy fusion. This system is efficient in reducing the FAR 0.05 and increasing GAR 91.4.

Linlin shen et al. (2011) proposed improve the accuracy by integrating multiple modal biometrics i.e face and palmprint. The both face and palmprint feature are represent by feature code, namely FPCode. FPCode uses fixed length 1/10 bits coding scheme that is very efficient in matching, and at the same time achieves higher accuracy than other fusion methods available. This approach compares with the Gabor+PCA and Gabor+KDRC. Experimental results show that both feature level and decision level strategies achieve much performance with the accuracy of 91.52% and 91.63%.

Pflug A. and Busch C. (2012) have offered a review on the condition of the art in 2D and 3D ear biometrics, covering ear finding and ear identification systems. They have classified large number of 2D ear recognition strategies into holistic, local, hybrid and statistical techniques. They have gathered a structured review of accessible databases, presented ear detection and recognition strategies and unsolved problems for ear recognition in the perspective of smart surveillance system. They have demonstrated that this novel feature was an important extension for face recognition systems on the approach to create invariant automatic recognition.

Kawulok M. et al. (2012) presents a face and eyes using multi-level ellipse detector combined with a SVM verifier. The main contribution is in increasing the accuracy of eye detection in high-quality images. The authors show that the detection error propagation considerably influences the face recognition performance. With the
proposed improvements, face recognition increase the rate by 0.5% for FERET and 7.7% for AR database compared with the publicly available implementation of the well established Viola-Jones face and eye detector.

2.2 MULTIMODAL BIOMETRIC CRYPTOSYSTEM

Multibiometric cryptosystems concurrently defends the two different templates of a user using a single secure sketch (Basha et al., 2010; Christian et al., 2011). Cryptobiometric systems are validation techniques which combine the concepts of cryptography and biometrics. Fig. 2.1 shows the multibiometric cryptosystem. Quantization Index Modulation (QIM) has to bind biometric characteristics with binary keys (Ahmad et al., 2010), providing an increased flexibility in managing the template intra-class variability. Fuzzy vault is a well-established crypto biometric construct, which is credited to the quality of safeguarding the biometric templates (Faundez-Zanuy M., 2005). Moreover, due to the difficulties in managing the intra-class variability of biometric data, the recognition performances of such schemes are typically significantly lower than those of their unprotected counterparts (Lucas et al., 2010).

![Fig. 2.1 Multibiometric cryptosystem](image)

Usually, for the fuzzy vault creation, joint feature vector is primarily created with the assistance of characteristic features (Piotr et al., 2010). To create this collective feature vector, supplementary feature point named ‘chaff points’ is required. A non-organized group of points $R = X \cup C$ furnishes joint feature vector points, where $X$ the unique feature point
of the modalities and the points in $C$ are called chaff points that are arbitrarily chosen from the characteristic feature points [Gandhimathi et al., 2011]. This chaff point creation module is employed to create arbitrary noise points to conceal the biometric features that are gathered from the client’s biometric template. The extraction of a repeatable binary string from biometrics opens new possible applications, where a strong binding is required between a person and cryptographic operations (Kyong et al. 2004). The blend of genuine and chaff points is called the secure fuzzy vault template which safeguards the biometric data as well as the crypto key. For a concurrent accomplishment of the bio-cryptosystem, which is a vital necessity for modern data safety mechanisms, the current technique of chaff generation is grossly insufficient (Abhishek et al., 2012; Karthik et al., 2007). The relevant hassles in chaff point created are successfully tackled by giving shape to a new chaff point generation method that employs an optimizing algorithm for the choice of the new chaff feature points.

Fingerprint fuzzy vault based on chaotic sequence has been proposed by DachengXu et al. (2010). Their proposed method has changed the original template into transformed template by using transformation function. Then, the transformed template was used to construct the vault. In the vault unlocking phase, the transformed input template was generated when the same transformation was applied to the input template. Experimental results have shown that their approach could protect the original template from crossing-matching by different transformed fingerprint templates in different applications.

Sahil Gupta et.al (2013) proposed fuzzy vault using multiple polynomials to the fingerprint biometric to protect the genuine biometric points. Secret keys are generated with the biometric cryptographic framework. Secret key divide into two sub keys, two polynomials apply for the template protection. It works increasingly without falling to the performance of a system for the fingerprint biometric template.

A two-stage geometric approach that is both scale and rotation invariant was implemented by Latha Lakshmanan (2013) for extracting the unique features present in the surface of an ear image. As occlusion because of ear rings and hair significantly affected the efficiency of ear recognition process, only the middle portion of the ear was considered in her work. The resultant matching scores were compared against a threshold
to make a decision for authenticating a person. It was found that the fused scores obtained from the two levels of feature extraction enhanced the recognition accuracy compared with that of the individual stages. Finally, particle swarm optimisation technique was applied on the matching scores in order to optimise the fusion parameters such as decision threshold and weights. It resulted in further improved verification rates compared with the fusion of scores without optimisation. Thus, her proposed method has worked on partial ear images and demonstrated the presence of more unique features in the middle part of the ear (as seen by the increase in recognition accuracy) and the method also helped in reducing the computation time.

Daesung, M et.al (2009) presented the approach to securing the biometric template. The fuzzy fingerprint vault scheme is developed multibiometric cryptography secret key and it reconstruct polynomials to secure the biometric template. It suggested the adaptive degree of the polynomials by considering the number of minutiae extracted from the users. The possible degradation of the template security is avoided by using multiple polynomials.

Meenakshi V.S. et.al (2009) investigated a new approach to achieve the performance improvement in the security analysis of password hardened using fuzzy vault. It includes the combined featured point from the retina and finger print, it has improved by the application non-invertible transformation and multiple biometric traits. Quality-based fusion of fingerprint and retina achieves promising improvement in performance.

A method for enhancing the security in environments has been suggested by Poon H.T. et.al (2009). It describes assail on a fuzzy vault scheme where the attacker is assumed to have access to multiple vaults protected by the same secret key and where a minimum secret key size is used. The attack proficiently reduces the secret key size by recognizing and removing chaff points. As the vault or secret key size decreases, the chances of identifying chaff points are increased. It also discussed the various possible protections against the codeword (Chin et al., 2011).

Abishek Nagar et.al (2010) presented a feature-level fusion framework for the multibiometric cryptosystems that concurrently defends the two different templates of a
user using a single secure sketch. The proposed framework has been detailed using a multibiometric cryptosystem fuzzy vault and fuzzy commitment. This includes a method to enforce limitation such as lowest matching requisite for a particular biometric feature in a multibiometric cryptosystem.

2.3 FACE AND EAR RECOGNITION

Mahoor M. H. et al. (2009) proposed with a 2D face and 3D ear fusion at the match scores level using weighted sum technique. Active Shape Model is used to extract a set of facial landmarks from frontal facial images. For the ear recognition, a set of frames is extracted from a video clip and ear region in each frame is restructured in 3D using Shape from Shading (SFS) algorithm. The resulting 3D ear models are aligned using the iterative closest point (ICP) algorithm. The experiment performed on a database of 402 subjects. The performance of the system is increased to 100%; FAR 0.01%, EER of the multi-modal system is .01%.

A multi-biometric system using face and ear is presented by Darwish A. A. et al. (2009). PCA decorrelate data by finding the eigen vectors of the covariance matrix. MIT, ORL and Yale databases are used for implementation. The individual face and ear images are normalized and preprocessed and then transformed to the PCA space. The system performance is 92.24% with FAR of 10%, FRR of 6.1%, Because of high accuracy and security, it concluded that the fusion of face and ear is a good technique.

The routine removal of local 3D features (L3DF) from ear and face biometrics and their arrangement at the feature and score levels for robust identification has been offered by Islam S. M. S et al (2013). They are the foremost to offer feature level fusion of 3D features removed from ear and frontal face information. Scores from L3DF based matching were furthermore fused with iterative closest point algorithm based matching by means of a weighted sum rule. They have in addition attained recognition and verification (at 0.001 FAR) rates of 99.0% and 99.4%, correspondingly, with neutral and 96.8% and 97.1% with non-neutral facial expressions on the major public databases of 3D ear and face.
### Table 2.1 Multimodal Biometric Studies

<table>
<thead>
<tr>
<th>Source (year)</th>
<th>Databases</th>
<th>Biometric sources</th>
<th>Technique Adopted</th>
<th>Performance of Classification in percentage</th>
<th>No. of subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Muhammad Imran Razzak (2010)</td>
<td>CAIRO</td>
<td>Face + Finger Veins</td>
<td>client specific linear discriminant analysis (CSLDA)</td>
<td>FAR 0.05% and GAR 91.4%</td>
<td>35 subjects,</td>
</tr>
<tr>
<td>Mohamed Soltane (2010)</td>
<td>UYVY. AVI 640 x 480, 15.00 fps</td>
<td>Face + Speech</td>
<td>Gaussian mixture modal (GMM)</td>
<td>EER: Face 0.44935, Speech 0.00269, Face + Speech (fusion) 0.08728</td>
<td>30 subjects</td>
</tr>
<tr>
<td>Piotr Dalka (2010)</td>
<td>Faces are recorded using web camera</td>
<td>Lip movement + Gestures</td>
<td>Artificial Neural Network (ANN)</td>
<td>Recognition Rate 93.7%</td>
<td>176 subjects</td>
</tr>
<tr>
<td>S.M.S. Islam (2013)</td>
<td>UWA, UND-FRGC, UND-F and FRGC V2</td>
<td>Face + Ear</td>
<td>L3DF, Iterative closet point</td>
<td>FAR 0.001 Recognition: 96.8% Verification: 97.1%</td>
<td>UWA – 56 subjects UND-FRGC : 326 UND-F and FRGC V2: 100</td>
</tr>
<tr>
<td>Zengxi Huang (2013)</td>
<td>MD I: Yale B and USTB. MD II: AR and USTB</td>
<td>Face + Ear</td>
<td>Sparse Representation based Classification (SRC), Robust Sparse Coding (RSC)</td>
<td>MDI MSRCW : 95.732% MRSCW:97.86% MD II MSRCW: 98.39% MRSCW: 99.0%</td>
<td>MD I : 38 MD II: 79</td>
</tr>
<tr>
<td>Xu Xiaona (2009)</td>
<td>USTB database</td>
<td>Face + Ear</td>
<td>KPCA, Kernel Fisher Discrimant Analysis (KFDA)</td>
<td>Recognition Rate fusion KPCA 94.52%, KFDA 96.84%</td>
<td>79 subjects</td>
</tr>
<tr>
<td>M.H. Mahoor (2009)</td>
<td>West Virginia University database</td>
<td>2D Face + 3D Ear</td>
<td>Weighted sum technique</td>
<td>EER .01%, FAR .01%, Rank one identification 100%,</td>
<td>402 subjects</td>
</tr>
<tr>
<td>M. Kawulok (2012)</td>
<td>FERET, AR database</td>
<td>Face + Eye</td>
<td>multi-level ellipse detector combined with a SVM verifier</td>
<td>Increase the recognition rate by 0.5% for FERET and 7.7% for AR.</td>
<td>FERET: 3657 images AR: 3313 images</td>
</tr>
<tr>
<td>Linlin Shen (2011)</td>
<td>AR, PolyU database</td>
<td>Face + Palmprint</td>
<td>FPCODE</td>
<td>Feature level fusion : 91.52% Decision level fusion : 91.63%</td>
<td>AR : 119 subjects PolyU : 386 palms</td>
</tr>
</tbody>
</table>
Zengxi Huang et al. (2013) have progressed a robust face and ear based multimodal biometric system by Sparse Representation (SR), which has incorporated the face and ear at feature level, and can successfully correct the fusion rule based on dependability difference among the modalities. SR-based classification methods were used in multimodal classification phase, i.e., Sparse Representation based Classification (SRC) and Robust sparse Coding (RSC). Lastly, they have obtained a group of SR-based multimodal recognition techniques, together with Multimodal SRC with feature Weighting (MSRCW) and Multimodal RSC with feature Weighting (MRSCW).

Features of the face or other parts of the human have dissimilar properties for different sensors. Each parameter of the biometric can be characterized as better or worse depending on the data of the individual is acquired for identification purposes. The important features of multi-modal biometric studies are summarized in Table 2.1.

2.4 SUMMARY

Multimodal studies using the different biometric feature are reviewed in the context of person recognition. The prior work has shown the performance evaluation of the multimodal system under the different trait combination scheme, identification rate, technique adopted, databases and number of subjects used. Important attributes are summarized in Table 2.1. The combination of face and ear modality are suggested. Among the studies reported in the previous section, it claims that multi-biometric improve over a single biometric system and uncorrelated modalities are used to achieve performance in multimodal system.