Chapter 2

Background and Literature Survey

2.1 Biometric Security Schemes

Biometric systems were originally designed as alternative access granting mechanisms to the conventional token based ones. However as demonstrated in Chapter 1, these systems themselves are exposed to various security threats. Consequently, many novel techniques were developed for providing required security measures to the biometric templates. All these techniques are designed so as to fulfill three important requirements [14] -

- **Irreversibility** - Inverting the protected templates to the original biometric templates should be computationally hard [1]. Alternatively, it can be stated that the transformation of original biometric templates to the protected ones should be 'one-way'.

[1] Computationally hard refers to unavailability of any polynomial time algorithm

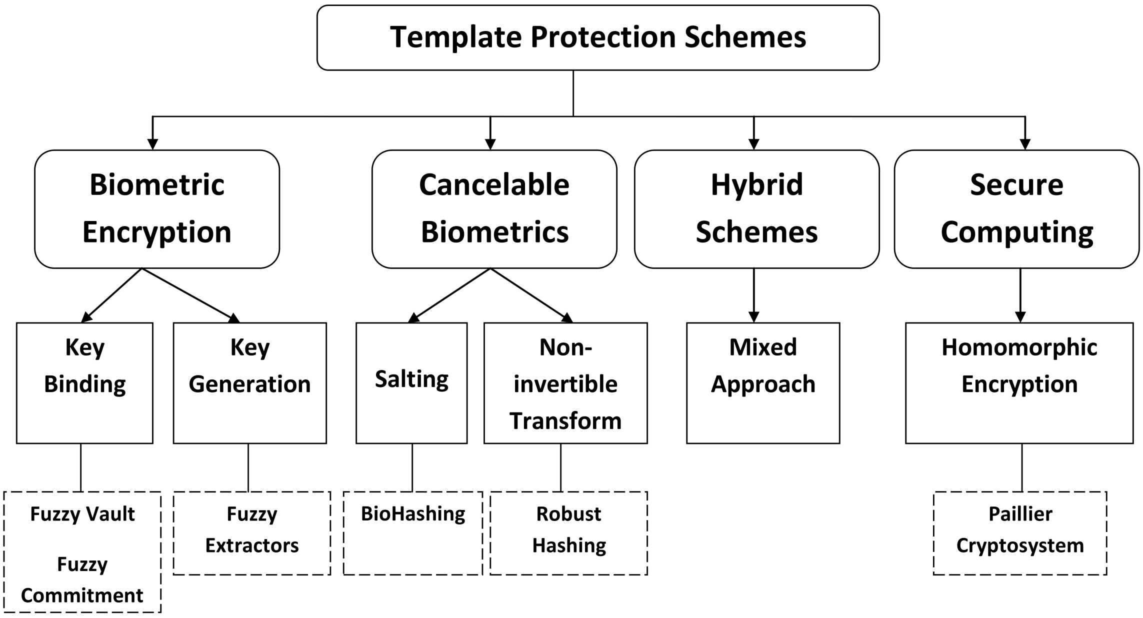

Figure 2.1: Classification of biometric template protection schemes.

- **Unlinkability** - Unlinkability states that there should be no similarity among multiple templates generated from the same biometric feature. This prevents any chance of cross-linking/cross-matching based attacks.
- **Information Leakage** - This requirement states that the stored data should not leak any information about the original biometric templates of the usersf since a simple leakage can potentially lead to major privacy breaches for the enrolled users.

Based on their working mechanism, biometric template protection schemes are divided into four categories: (i) Biometric cryptosystems, (ii) Cancelable biometrics, (iii) Hybrid techniques and (iv) Secure computing schemes. A pictorial depiction of this classification along with their principal working models is presented in Figure 2.1.

Among these four different techniques, schemes based on the concept of biometric cryptosystems and cancelable biometrics have garnered widespread attention and recognition. The popularity of these techniques is demonstrated by the detailed researches accomplished in these areas. As such, an elaborate discussion involving these two schemes is presented as follows.

2.2 Biometric Cryptosystem

A Biometric Cryptosystem (BC) is a generic framework in which a key is associated with the biometric sample data to obtain a 'secure sketch' or 'helper data'. Ideally, this auxiliary piece of data should not disclose any information about the biometric data. However, rigorous theoretical analysis shows that it does indeed leak some critical information about the data, either due to the limitations of coding techniques or due to faulty framework constructions. Based on the procedure of generating the helper data, BCs can be further subdivided into two categories: (i)*Key Binding* and (ii) *Key Generation*. In the key binding based method, the helper data is generated by the process of binding a key or a secret to the biometric template. Prominent examples employing this technique include *fuzzy vault* [15] and *fuzzy commitment* [16]. Alternatively, the key generation technique works in two parts. In the first part, the helper data is generated directly from the biometric sample, whereas in the second part the the same helper data and the query biometric sample (presented during verification) combine to create the key.

The key in biometric cryptosystem based techniques is correctly reconstructed only if an accurate query is presented during the identification/verification stage. One important point about biometric encryption is that the BC algorithm should be inherently designed to tolerate some limited disparities between the biometric samples. This criterion is required because two biometric samples from the same person may differ at any given point of time. However, this variation is generally limited within a small threshold value. Alternatively, an impostor will be unable to authenticate correctly because his/her sample will differ considerably from the stored genuine sample and consequently will not be able to retrieve the correct key. The complete process of biometric encryption via key binding is illustrated in Figure 2.2.

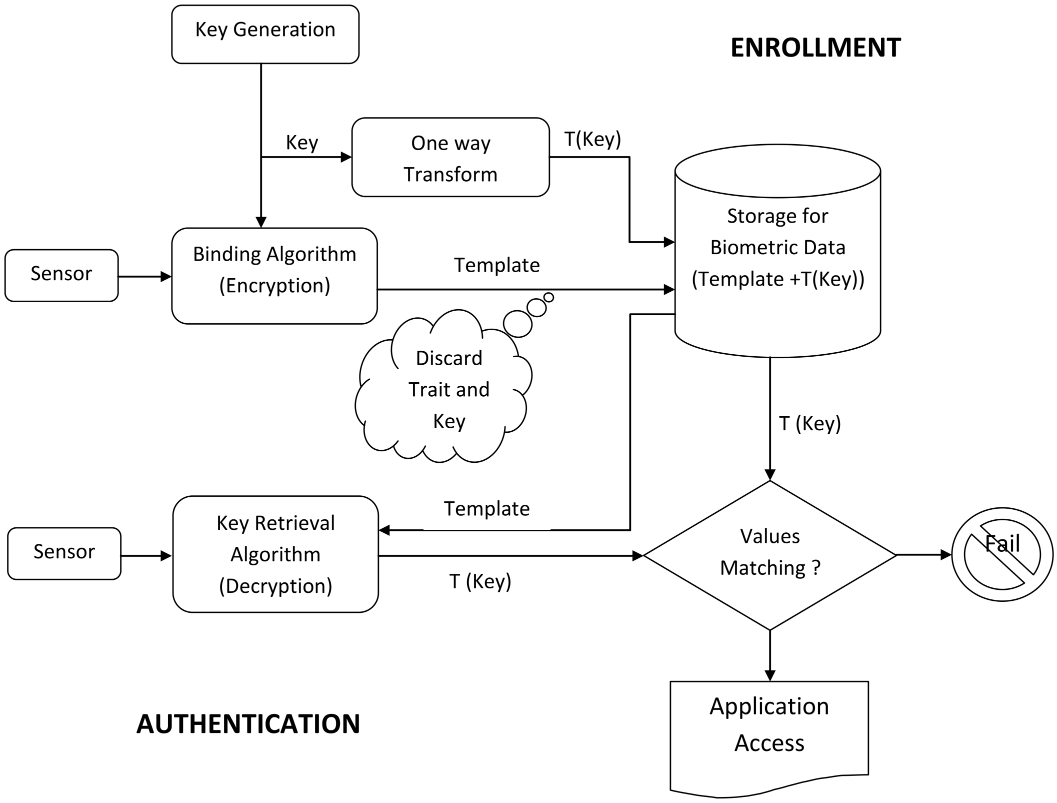

Figure 2.2: Key binding based biometric cryptosystem framework.

2.2.1 Fuzzy Commitment

The fuzzy commitment scheme [16] is widely regarded as a very easy and efficient method for providing security measures to biometric templates. In fuzzy commitment, an enrolled biometric template T^E is assumed to be a N-bit binary string. Next, a key KEY of length L bits ($L<N$) is generated. Care must be taken that this key must be randomly generated according to a uniform distribution. This key is then used to distinctively correspond to a N-bit codeword c of a suitable error correcting code. A sketch is extracted from this template as $y_c = c \oplus T^E$. Here $\oplus$ symbol indicates modulo 2 addition or the XOR operation. The sketch y_c along with a cryptographic hash value $h(KEY)$ gets stored in the database.

During the identification/authentication stage, both the query biometric T^A and the secure sketch are used to facilitate in the computation of a new codeword c' as $c' = y_c \oplus T^A = c \oplus (T^E \oplus T^A)$. The value of c' can then be decoded to obtain a key KEY'. If the value of $h(KEY)$ matches with $h(KEY')$, the authentication is deemed successful. The ability of this system to handle uncertainty or fuzziness lies in the strength of the error correcting codes used. Every error correcting code has an error correcting capacity. The values of KEY and KEY' will be the same only when the hamming distance between T^E and T^A is not greater than this capacity. As observable, the security of fuzzy commitment is measured based on the rank of the error correcting code used in constructing the scheme. The complete technique is diagrammatically illustrated in Figure 2.3.

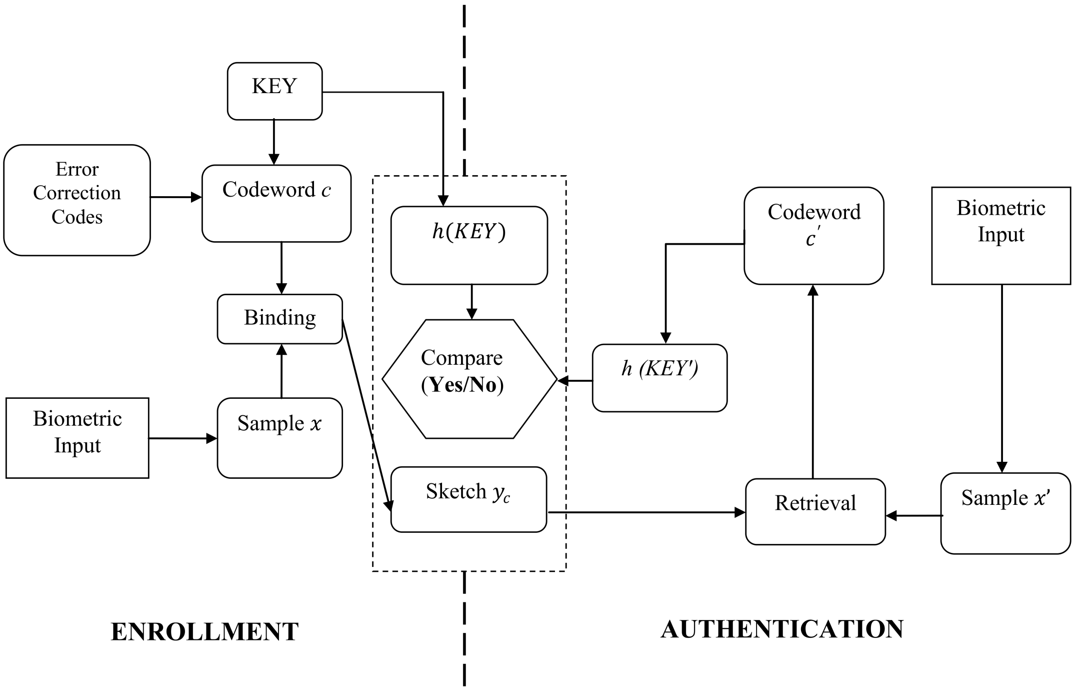

FIGURE 2.3: The fuzzy commitment framework.

2.2.1.1 Developed Schemes

The security of the fuzzy commitment technique was rigorously studied in [17] by estimating the security capacity and entropy loss parameters. Due to some constraints (e.g. keys having low entropy) and difficulties in the practical implementation of error correction coding techniques, the fuzzy commitment scheme has not been extensively used for template protection. Even so, this scheme was tested on iris templates [18] to bind 140-bit keys generated from both Hadamard and Reed-Solomon error correction coding. Iris based systems were again studied by the authors in [19] where two-dimensional iterative min-sum decoding was introduced and in [20, 21] where keys were constructed from the templates via a mechanism based on context based reliable component selection. Regarding fingerprints, a quantization based transformation (randomly generated from a user specific token) for binarizing fingerprint templates was employed in [22] which were in turn generated from a multi-channel Gabor filter. The work in [23] achieved similar objectives by quantizing and approximating the template's Fourier phase spectrum. Finally, face biometrics based fuzzy commitment technique was presented in [24] where the binarization of the facial features was done by thresholding followed by a reliable bit selection method and in [25] where Principal Component Analysis (PCA) was applied for achieving the same goal. Utilizing a more unconventional biometric trait, [26] proposed a fuzzy commitment scheme based on online signatures. All these methodologies differed only in the techniques by which a binary code was generated from the raw biometric feature templates. The rest of their framework followed the original fuzzy commitment scheme. In a different direction, the authors in [27] used lattice functions instead of the traditional error correction codes for handling discrepancy between the biometric samples.

2.2.1.2 Security Evaluation and Attacks

Information leakage is an important property which is considered while measuring the safety of a biometric system, especially for the fuzzy frameworks. This property for fuzzy commitment was extensively studied and information theoretically analyzed in [28]. After a thorough analysis, the authors concluded that the fuzzy commitment framework was optimal when it operated at a rate equal to the maximum key length. It was also shown that the scheme leaked information regarding both the biometric data and the key for memoryless biometric sources. On the basis of these theoretical formulations, attacks such as decodability attacks [29], error correction code histogram attacks and nearest imposter attacks [30] have been performed. These attacks exploit the structures of the error correcting codewords used in the fuzzy commitment scheme. As a preventive measure, [31] suggested applying a bit-permutation structure for protecting the scheme from cross matching. Additionally, a novel scheme for averting information leakage was suggested in [32] which utilized techniques from Multi Party Computation relying on the additively homomorphic property of the underlying Pailler's cryptosystem.

2.2.2 Fuzzy Vault

The fuzzy vault framework was initially proposed in [15]. It has been successfully employed by many researchers to encrypt a variety of biometric traits including fingerprint, face, iris and retina. The principal reason for the success of this technique was due to it's efficient ability to handle uncertainty or fuzziness associated with biometric data. The original fuzzy vault scheme uses the Reed Solomon error correction coding to obtain its goal of managing uncertainty. It has two parts, namely encoding and decoding. In the encoding part, the biometric traits are evaluated on a generator polynomial which in turn is derived from a randomly generated key. The pairs consisting of the traits and their corresponding evaluations are subsequently stored in a vault. Finally, some chaff points are added to complete the encoding step. Importantly, the generation of chaff points is based on two constraints - i) they should not overlap with any valid points in the vault and ii) they must not lie on the polynomial that was derived from the cryptographic key/secret [33].

In the decoding step, the biometric samples are first obtained from the users who want to claim their identity. If the user is a genuine one, the freshly presented samples will comprehensively overlap with the traits present in the vault. The error correction codes will correct (via the Berlekamp- Massey algorithm [34] or the Guruswami-Sudan RS decoding algorithm [35]) any errors which might occur between the two matching samples. After a successful matching, the original trait points are identified along with their corresponding evaluation of the generator polynomial. Finally, the polynomial (and subsequently the key) is reconstructed from these available points by the usage of Lagrange Interpolation method. On the other hand, the biometric trait points of any impostor will not match with the points present in the vault and consequently, the correct polynomial (key) will not be generated. The security of fuzzy vault depends on the number of chaff points in the vault. The greater the number of such points, the more 'noise' there is to conceal the genuine polynomial from an attacker. The fuzzy vault scheme is diagrammatically represented in Figure 2.4.

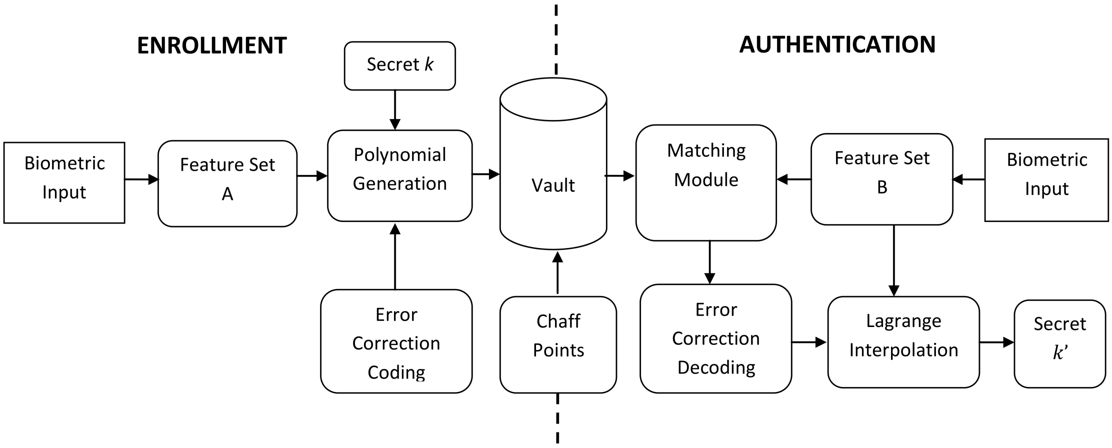

Figure 2.4: The fuzzy vault framework.

2.2.2.1 Developed Schemes

The fuzzy vault technique has stood the test of time to become one of the most widely researched and implemented technique for providing security measures to biometric templates. Some of the most noticeable works involving this versatile framework are mentioned as follows.

- **Fingerprint** - Fingerprints are the most popular and widely used biometric trait in use. The first practical implementation of the fuzzy vault framework for fingerprints was done in [36] by integrating fingerprints in smartcards - the *fingerprint vault*. The work mainly focused on the protection of smart cards containing personal information and a private key corresponding to their users. However, this framework had some disadvantages, the problem of image pre-alignment being the major one. This situation was addressed by a host of works including the geometric hashing based technique in [37], reliable reference points alignment technique in [38] and a rotation and translation invariant minutia representation scheme in [39]. Also, the authors in [40] developed their automatic alignment system taking minutiae descriptors [41] into consideration. A modified fuzzy vault technique was introduced in [42] to make use of asymmetric cryptosystems like RSA. The main drawback of the original fuzzy vault system (which provided the motivation for this work) was the ignorance of the order of the input templates, which in turn decreased the attainable security levels.

The authors in [43] rejected the idea of using Reed-Solomon error correcting codes and subsequently replaced it by Cyclic Redundancy Check (CRC) codes. Owing to the limitations of the fuzzy vault framework, another work introduced passwords in the existing architecture [44]. The distribution of the transformed templates in this scheme was more similar to the normal distribution which provided better resistance against attacks on the vault. The idea of using 'helper data' was envisioned in [45] owing to the problem of aligning a query template with a transformed domain template. The helper data used by the authors in their work are the Orientation Field Flow Curves (OFFC) proposed in [46]. On a different note, the idea of combining minutiae descriptors with contemporary fuzzy vault was explored in [47], thereby improving both the security and performance of the existing fuzzy vault based systems.

The authors in [48] were the first to develop a fully automatic implementation of the fuzzy vault. They extracted high curvature points derived from fingerprint orientation field to align fingerprint templates, thereby increasing the recognition accuracy of the system. The work in [49] introduced hybrid techniques for template security based on orientation positions of minutiae points, whereas the authors in [50] proposed three useful and effective solutions for fingerprint based fuzzy vault namely - *geometric hash table*, *secure fuzzy fingerprint vault* and *fuzzy fingerprint vault* using a special technique termed as *One Time Template (OTT).* Also, the authors in [51] developed their own system where not only the degree of the generating polynomial was considered, but also the total number of templates required for arriving at the reliable reference points were examined. The authors in [52] expanded the fuzzy vault framework to include minutiae information of several fingerprints arguing that a single finger does not hold sufficient information for secure implementation of the framework. Also, the authors in [53] used the fuzzy vault mechanism to construct a private key from the user sample itself and used an adjustable degree of the underlying polynomial which directly depended on the number of minutiae points obtained from every user. It addressed the situations where the framework failed because the fingerprints had few number of minutiae points (this result is very much impressive as it was claimed that the new framework could make possible attacks 2^{192} times more difficult).

- **Face** - Face is the foremost technique used by human beings to uniquely identify each individual. A fuzzy vault framework for facial data based system in 3D domain was first proposed in [54]. The design itself was inspired by the basic fuzzy vault [15] and the work proposed in [43]. The schematic layout of the system included three stages namely - binarization, encoding and decoding. Although the encoding and decoding processes were similar to previously proposed schemes, the novel idea of binarization was included to transform the raw real-valued facial feature vectors into an appropriate format which can be used as input to the fuzzy vault. The authors in [55] proposed a secure technique for changeable cryptographic key generation utilizing facial data on the basis of fuzzy vault framework. This study was based on the primary work done in [56] which introduced a technique for mapping facial feature to bits. However, these works suffered from many shortcomings which mainly stemmed due to the intra-class variations in biometric data. In their novel approach, the authors attempted to overcome this problem by introducing a binarization technique which quantized the distance measure between pairs of random vectors and biometrics templates. In another work, a facial image based generic fuzzy vault scheme for online authentication was proposed [57]. In this work, a random transformation was made based on the angle measurements between the face feature templates and a set of orthogonal vectors which were randomly generated. This technique prevented the face templates from being exposed during successful authentication. The authors extended their original work

[57] into [58] by considering the ordering of biometric feature characteristics. It prevented cross matching of the features and reduced the resulting FAR. Other notable techniques include the fuzzy eigenface vault developed in [59] and the Reed-Solomon code based face template protection scheme of [60]. Most recently, an exciting new prospect of using face based fuzzy vault for securing data in a distributed cloud computing environment was explored in [61].

- **Iris** - Iris is the most reliable of all the biometric modalities. Additionally, it provides the maximum accuracy among all the other utilized biometric traits. The main reason for such high accuracy stems from the fact that iris is placed inside the body [10]. The authors in [62, 63] were the first to explore the merging of fuzzy vault with iris templates. In their model, a key was inserted in a vault and was subsequently locked with a locking set. Subsequently, the vault was embedded in a smartcard. An unlocking set was used afterward for unlocking the vault and subsequently extracting the stored key. Here, both the unlocking and locking sets were constructed out of Iris Pseudo Codes (IPCs). The IPCs are binary code sequences consisting of 2048 bits and are extracted out of the raw iris images of the enrolled users. Another remarkable work in this field was done in [64], where the iris shuffling algorithm [65] and the modified fuzzy vault framework [42] were combined for solving the challenges involving iris based biometric systems. The authors in [66, 67] came up with their own fusion of iris data and the fuzzy vault framework by dividing the iris texture (after preprocessing) into 64 blocks and calculating the mean gray scale value for each block. This resulted 256 features which were subsequently normalized to integers for the purpose of reducing noise. Reed-Solomon codes and hash functions were also used to transform the feature vector into a cryptographic key. Another direction of work included that of [68] where the authors proposed an iris texture based hardening scheme similar to the hardening of fingerprint based fuzzy vault by using passwords [44]. Finally, the work in [69] requires a mention where the iris templates (after some permutations and translations) were randomly transformed via 64-bit passwords, which were in turn derived by combining soft biometrics and user defined passwords.

- **Retina** - The history of usage of retina as a biometric trait is quiet similar to that of the iris. Although it provides a very accurate system, it is rarely used because of the complexity in obtaining and extracting features from the human retina. In-spite of the difficulties, retina has many benefits when compared to other biometric traits, thus making it suitable for use in highly secure applications. The most prominent advantages are the difficulty in spoofing retina, the difference in retinal patterns between the right and the left eye and the invariance in retinal patterns with age [70]. The feature which is extracted from retinal scan is the blood vessel patterns in the eye. The most noticeable work regarding integration of fuzzy vault with retinal templates was done in [70]. This system systematically combined ideas from [43, 44, 68] and extended them in the field of the retina. This work measured the security strength of the resulting vault by estimating the min-entropy and used single template minutiae for encoding and decoding purposes.

- **Signature** - Signature is categorized as a behavioral biometric trait which depends on the behavior patterns of individuals. Efforts have been made to incorporate signature based schemes into the fuzzy vault framework but with a limited amount of success. The majority of such works concentrate on different technique for creating biometric keys from signatures by generating hash extractors [71] and by dividing the complete feature space between subspaces and cells [72]. The inclusion of fuzzy vault in this area was done in [73, 74] which utilized the local parameters of online signatures. More recently, the authors in [75] have proposed a fuzzy vault based on offline signature images by employing a multi-feature extraction and Boosting Feature Selection (BFS) approach based on a dissimilarity representation. This system was evaluated on the standard Brazilian Signature Database with about 97% recognition accuracy and an overall entropy of 45 bits. The same authors later extended their work in [76] by enhancing the accuracy of signature based biometric cryptosystems. They achieved this feat by cascading a novel signature verification system with the fuzzy vault modules.

- **General Modifications** - Now some general modifications made to the original fuzzy vault framework are discussed. These alterations were not done with respect to a particular trait but were performed to improve a specific aspect of the vault. The authors in [77, 78] introduced a generic fuzzy vault design approach based on the theory of classifiers. In this work, the functionality of the primitive fuzzy vault system was formulated as a classifier wherein the distance between the fuzzy vault and the sample query templates composed the classification space. Not only the authors later extended their work in [77] by employing a BFS method for optimizing their model but also tested it in offline handwritten signatures with promising results. This work was further continued in [79], wherein a scheme which dynamically modifies the user key size was proposed. In a different direction, the authors implemented a novel low-complexity scheme [80] to compute the monic polynomial in the modified fuzzy vault during the enrollment process. This was done by using a new interpolation method which reduced both the computational complexity and latency for the verification process.

The notion of using Reed-Solomon (RS) codes instead of the popular CRC codes was revived in [81]. They argued that biometrics based applications that do not depend on CRC codes would have a smaller message space polynomial and would eventually show improved results. As such, they proposed a decoder based on RS codes and the extended Euclidian algorithm which achieved greater decoding speeds than CRC based decoders. Finally, a very interesting study was carried out in [82] where a fuzzy vault based on constant dimension subspace codes was presented. These subspace codes are basically a class of error correcting codes in projective n-space over a finite field F_q.

2.2.2.2 Security Evaluation and Attacks

An in-depth information theoretic analysis of the fuzzy vault scheme has been performed in [83, 84]. In their work, the authors provided upper bounds for the information leakage of the stored data and derived both upper and lower security bounds for any attack that attempt to recover the template from the stored reference data. Besides, not only they showed the selection procedure for optimal parameters of the vault but also estimated the minimum number of minutiae points required for obtaining the desired security rank. However on the flip-side, a large number of attacks on biometric cryptosystems were devised. These attacks mainly fell into three categories namely *Record Multiplicity (ARM)*, *Surreptitious Key Inversion (SKI)* and *Blended Substitution* attacks [85]. Based on these notions, the authors introduced non randomness attack which exploited the non random method for the generation of chaff points [86]. The intuition behind this attack was the fact that chaff points generated during the fuzzy vault scheme tend to have a smaller 'free area'. The SKI and blended substitution attacks in fuzzy vault were discussed in [85] but no practical implementation was given. However, the attack via record multiplicity was studied and experimentally implemented in [87]. The authors empirically quantified the complexity required by an attacker to compromise the vault. Surprisingly, they were able to retrieve the secret key from 59% of corresponding vault pairs in the fingerprint database that they used.

Other attacks to which the fuzzy vault has been subjected to include brute force attack [88], collusion attack [89] and Fast Polynomial Reconstruction attack [90]. Specially, the last attack is very much interesting as it claims that the original polynomial of the vault could be accurately reconstructed if the number of genuine points exceeded the degree of the polynomial by two. A more framework specific attack was performed in [91] which targeted the password and fingerprint based fuzzy vault hardening scheme [44]. The problem of releasing multiple sketches associated with the same biometric data (i.e. a type of ARM attack) was recently analyzed in [92]. The authors examined the improved fuzzy vault scheme [83] and concluded that the relation between these multiple sketches could be determined by solving a system of nonlinear equations. The solutions to these equations were later demonstrated in [93], which also presented a new attack based of the extended Euclidian algorithm. In their work, the authors not only derived lower bounds for the record multiplicity attack but also showed that the devised attack was asymptotically optimal in an information theoretic sense.

2.3 Cancelable Biometrics

On a conceptual level, cancelable biometrics refer to intentionally introducing a repeatable distortion signal to the biometric data to protect it [94]. The distortion, in turn, is regulated by some parameters which are generated from a secret key/token. Hence the key serves as the basis for providing the *cancelibility* property of the schemes. Authentications of the users in these frameworks are performed by matching their biometric data in a transformed domain based on the distortion functions. The distortion functions must themselves be designed in such a way that it should be computationally hard to invert them. The scope of cancelable biometrics based techniques is very diverse. A variety of schemes employing different methodologies regarding the generation of the keys and design of the transformation functions have been proposed in the literature. Since this thesis is focused on developing cancelable schemes for fingerprint and iris based biometric features, only the most popular works based on these two traits are mentioned here. A more comprehensive study of cancelable biometrics based techniques is provided in [95].

2.3.1 Fingerprint Based Schemes

In a broad sense, fingerprint based cancelable schemes can be categorized under two sub-divisions namely *salting* and *non-invertible transforms.* The most prominent example of salting based technique is the BioHashing scheme, first introduced in [96]. The entire BioHashing process can be divided into two steps. In the first step, a preprocessing is carried out on the biometric data to make the corresponding features invariant to small variations in the input biometric signal. In the second step, a user defined key is used to generate orthogonal pseudo-random vectors (the orthogonalization is generally done by the Gram–Schmidt process). Finally, a biohash value is generated by comparing the inner product of the orthogonal vector and the feature vector extracted against a predefined threshold. The entire BioHashing scheme is illustrated in Figure 2.5. The security strength of the scheme lies in the fact that it is very difficult to reconstruct the original biometric features without knowing the secret key. This follows due to the usage of dot product and the threshold based mechanisms [97]. However, one of the major limitations of BioHashing methods is their low performance (in terms of increased FAR) when attackers are in possession of a secret key [98]. To improve upon this point Nanni and Lumni [99] used the invariant local binary pattern texture operator. However this technique resulted in lower levels of privacy since minutiae comparator was used for alignment.

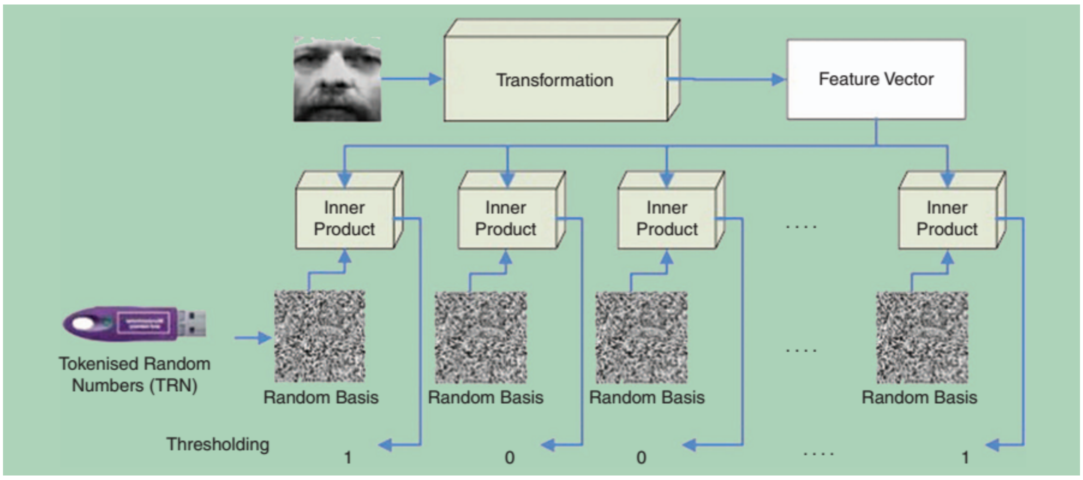

FIGURE 2.5: The BioHashing scheme [97].

Cancelable biometric schemes implementing non-invertible transforms was introduced in [100]. The pivotal idea in these schemes is to secure the biometric template by applying a non-invertible transformation function or one-way functions. Likewise to the salting based techniques, the comparison of the biometric templates take place in the transformed domain. In their original work, the authors compared Cartesian, polar and surface folding transforms in the context of the minutiae positions of fingerprints. It has been shown that the original verification rates were preserved by such schemes while maintaining the irrevocability property. However, practical attacks against the scheme were proposed in [101]. Especially, it was shown the security guarantees were falsified when multiple transformed templates were generated from the same original template. Another work in the same direction exploited the concept of dynamic random projection (RP) [102], wherein a nonlinear projection process was devised which relates a random matrix's assembly to the biometric feature vector itself. In a different study, a key dependent geometric transform function was used to generate cancelable fingerprint templates [103]. The orientation of a line passing through the core points was specified by the key transformation function. The orientation information subsequently served as the basis for generating the cancelable templates.

Cancelable schemes can also be categorized on the basis of the requirement of any pre-alignment procedures. The majority of the schemes described till now employed some form of pre-processing steps which assisted during the alignment of the biometric templates. Now some alignment-free approaches which do not require such measures are presented. The authors in [104] proposed a novel scheme for fingerprints based on *minimum distance graphs.* These 'graphs' comprised of the inter-minutia minimum distance vectors originating from the core point as the feature set. In another work, the authors used curtailed circular convolution for designing an alignment free cancelable fingerprint scheme [105]. The security of the scheme centered around using efficient one-way transforms of input binary strings to length-reduced, convolved output vectors. Information about orientation field around fingerprint minutiae points was utilized in [106] to design a secure system. The relative translation of the points was made invariant to the position of the finger in this approach. The scheme however showed poor results for low quality of fingerprints. Hashing based fingerprint protection scheme was successfully implemented first in [107]. The authors proposed a symmetric hashing based technique wherein the final matching was performed in the hash space. The authors hashed triplets of minutiae points through some linear combinations of the symmetric hash functions, thereby securing the actual points. However, the symmetric hash functions used in the scheme were not theoretically analyzed regarding their capacity against various state-of-the-art attacks.

Techniques for creating anonymous and revocable representation from binary string representations of fingerprints was first described in [108]. Although this method was proved to fulfill the criteria of re-usability and diversity, it required calculating all the possible invariant features which resulted in higher computation costs. The authors in [109] also proposed a method for minutia based bit strings. Their main idea was to map the minutiae into a predefined 3 dimensional array which consists of small cells. Subsequently, one of the minutiae was selected as the reference minutiae, while other minutiae points were translated and rotated with reference to the reference minutiae. However the stored template became insecure in the stolen token scenario. This idea was further explored in [110], wherein a polar grid based 3-tuple quantization technique was utilized. A permutation component was employed here to randomize a user bit-string with user- specific tokens. Although the scheme was efficient, neither the permutation sequence was explicitly stated anywhere nor was it theoretically analyzed.

A densely infinite-to-one mapping technique for pair minutiae vectors was used in [111] for protecting stored fingerprint templates. The quantized minutiae vectors were protected by hiding the true solution from an infinite number of alternative solutions. In another work, an alignment-free method based on multi-line neighboring relation generation was proposed in [112]. Several rectangles were constructed by considering each minutia as reference minutiae, and then calculating the rotation and translation invariant neighboring relations. However the scheme was not theoretically analyzed for the fulfillment of the *diversity* property, which undermines the guarantee of cancelability in the first place. A fingerprint bio-cryptosystem was suggested in [113] which exploited local Voronoi neighbor structures (VNSs) of the fingerprints. The dual structural notion of Delaunay triangles was used in [114] to provide similar security guarantees. The authors in [115] developed a randomized graph based hamming embedding technique, which used a minutiae descriptor called *minutiae vicinity decomposition* to derive a set of randomized geometrical invariant features. Finally, a method in pair-polar coordinate space using polar transformations was proposed in [116] wherein a vector containing radial distance and two angles were generated by making one minutia as a center in the polar coordinate space. A many-to-one mapping was applied to ensure non-invertibility of the raw templates.

2.3.2 Iris Based Schemes

The notion of non-invertible geometric transforms [94] was utilized for iris based biometric systems in [117]. In their work, the authors proposed a mesh warping based approach for generating the transformed templates. Iris texture extracted from an iris image was remapped according to a distorted grid mesh laid over it, whereas distortions were specified by a key that offsets each vertex in the original mesh by some unspecified amount. Another work utilizing non-invertible transforms based on random projections was proposed in [118]. In this method, a biometric features $x \in \mathbb{R}^N$ was projected into a random subspace $A \in \mathbb{R}^{n \times N}, n < N$. Importantly in random projection based schemes, the distance between the feature points in the original feature space is preserved in the random output space by the guarantee of Johnson-Lindenstrauss (JL) lemma [119]. The proposed scheme of [118] was extended in [120] by utilizing sparse representation-based classification. It was illustrated therein that the sparse representation of iris features before and after applying random projections was similar, thereby dismissing any chance for degrading the overall performance.

An approach for the generation of iris based cancelable templates via random permutations was introduced in [121]. In their work the authors proposed two novel techniques named GRAY-COMBO and BIN-COMBO for generating cancelable iris features. The first method transforms Gabor features obtained from the iris textures by circularly shifting and adding rows at random, whereas the second method applies similar transformations on the iris codes by random shifting and XOR-ing. However, these schemes were sensitive to outliers like eyelids, eyelashes, and specular reflections due to the usage of linear transformations. In every permutation based scheme, securing the key is a primary objective since it forms the basis for protecting the privacy of the individual users.

More recently, a novel cancelable approach for iris features involving adaptive Bloom filters was proposed in [122]. A Bloom filter is a space-efficient probabilistic data structure which represents a set in order to support membership queries [123]. This primitive was modified since traditional Bloom filters are suitable for conditions where a probability of false positives is tolerable (biometric recognition systems not being one of them). Their proposed technique efficiently mapped binary biometric feature vectors to an alignment free transformed domain; additionally providing some irreversibility guarantees. At its optimal configuration, the modified Bloom filter based scheme provided a GAR of 96.36% corresponding to a FAR of 0.01% for the CASIA-v3-Interval iris database [2]. The authors subsequently expanded their idea in [124] to include iris-codes obtained from both eyes of a single subject. In later works, the authors [125] proposed a Bloom filter based multi-biometric scheme wherein they performed a feature level fusion between face and iris templates to a single protected template. In-spite of the claims of unlinkability and irreversibility in their original work, the study of Hermans et.al [9] demonstrated that it was vulnerable to cross-matching based attacks, thereby refuting the claim of unlinkability.

[2] The Center of Biometrics and Security Research, http://www.idealtest.org

In particular, the authors presented a practical attack that distinguishes two Bloom filters (b, b') generated from the same data from two independent ones (c, c') with a probability of at least 96%.