IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 24, 2015, accepted March 16, 2015, date of publication April 30, 2015,
date of current version February 28, 2016.

Digital Object Identifier 10.1109/ACCESS.2015.2428277

A Cell-Array-Based Multibiometric Cryptosystem

AMIOY KUMAR[1], (Student Member, IEEE), AND AJAY KUMAR[2], (Senior Member, IEEE)
[1]Department of Electrical Engineering, IIT Delhi, New Delhi 110016, India
[2]The Hong Kong Polytechnic University, Hong Kong

Corresponding author: A. Kumar (ajay.kumar@polyu.edu.hk)

This work was supported by The Hong Kong Polytechnic University under Project PolyU 5169/13E and under Grant Z0F3.

ABSTRACT This paper presents a new framework for a biometric cryptosystem in which a cryptographic key is concealed with biometric modalities. In this paper, the candidate biometric modality is secured using two functions: 1) BCH encoding, which delivers the parity-code stored for the alignment of the query biometric template and 2) the Hash function to compute hash-code in order to safeguard its integrity. The cryptosystem is formed by creating two different cell-arrays. The hash-code is scattered on one cell-array by a randomly chosen column position, and the secret key is distributed over the second cell-array on the same position. The other cell-array locations are filled with the randomly generated chaff vectors. The parity-code is then jumbled up using a regenerative XORCoding in order to hide it from unauthorized access. At the unlocking stage, the parity-code is regenerated using XORcode and used to align the query template to the original one. If the hashed-code computed from the aligned template can locate the correct locations of the original hashed-code from the feature-array, it can get back the secret-key from the key-array and the correspondingly secret message. The proposed algorithm is implemented and evaluated in two modes: 1) unimodal and 2) multimodal. The experimental results from publicly available databases confirm the superiority of the multimodal cryptosystems over the unimodal cryptosystems.

INDEX TERMS Biometrics, palmprint, iris, cryptosystem, BCH encoding, multimodal cryptosystems.

I. INTRODUCTION

Most security systems are threatened by potential attacks caused by information hacking. Strong authentication systems that could tolerate these potential attacks must be deployed for safeguarding critical security applications such as e-commerce and access to restricted data/buildings. For developing the most secured systems whenever high privacy is demanded, biometrics-based authentication has often been utilized. Biometrics has been employed as an alternative to many security systems based on tokens, smart cards and passwords, which can be either stolen or spoofed. A recent advancement in biometric technology is observed in biometric-cryptosystems [2] which combines cryptography with biometrics. Cryptography is one of the most effective ways to enhance the security of the information system via its encryption and decryption modules [1]. However, the weakest link of cryptography-based security systems is the associated secret key. While the simple memorized key can be easily intercepted, a long and complex key needs extra storage management, like tokens, smart cards, etc. The biometric cryptosystems rely on biometrics based encryption/decryption modules and are therefore more a reliable, convenient, and efficient means of data protection, as they require the physical presence of the person to be authenticated.

A biometric cryptosystem is generally used to safeguard the cryptographic keys, generated to encrypt/decrypt the secret message, by using biometric template. It eradicates the necessity to memorize complex passwords or to carry the tokens. In order to provide a secure cryptographic key, biometric cryptosystems can be divided into two categories: (a) key-merging mode, where the secret key generated from any cryptographic algorithm is locked in a *vault* with biometric modalities [2], [4]–[6], or (b) key-generation mode, in which the key is generated from the user's biometric data and used in any cryptographic algorithm for the encryption and decryption of the secret message [7]–[10].

The usage of biometrics in such cryptosystems also poses challenges: (i) the cryptographic algorithms require the keys to be exactly the same, however, the biometric image acquired at different times from the same person can have significant (intra-class) variations; (ii) a unimodal biometric cryptosystem has its own limitations too. Earlier research has detailed such limitations [11] resulting from noisy sensor data, unacceptable error rates, and emerging spoof attacks from unimodal biometrics [11]. Owing to the intra-class

variations caused due to the different keys each time, one solution is to use Error Correcting Codes (ECC) [4]–[6], [12], which can be tuned to tolerate errors caused due to the variations in genuine biometric templates. Several limitations of unimodal systems can be addressed by using multimodal biometric cryptosystems which utilize two, or more than two, unimodal traits in encryption and decryption. This paper presents a new framework for the biometric cryptosystem in the key binding mode with the provisions of multimodal biometric authentication.

A. RELATED PRIOR WORK AND MOTIVATION

Research on biometric cryptosystems has invited increasing attention in recent years. The key-generating mode of the biometric cryptosystem has been studied by many researchers [7], [10]. The efforts made by Hao *et al.* [7], Sautar *et al.* [8], and Dodis *et al.* [9] have been generated strong cryptographic keys from biometric modalities. The concept of cancelable biometrics also merits a mention here with non-revocable biometrics in [13]. Connie *et al.* [14] used the concept of bio hashing by computing Fisher projections. However, their results are based on the assumption that the generated token or keys will never be stolen or shared. This can be quite unrealistic and can create doubts about real evaluation. A study on such questionable evaluation has been presented by Kong *et al.* in [15]. One of the innovative approaches proposed in this area appears in [16], where the authors utilized random orientation field into the feature extractor to generate cancelable competitive codes.

The basic idea of the key-merging mode was first time presented by Juels and Sudan [17]; called as *fuzzy vault*. Uludag et al. [2], [5] and Uludag and Jain [4] implement the fuzzy vault using the fingerprint biometric as an unordered set. The difficulties associated with the minutiae point alignment is significantly reduced in [6] with the *helper data* in the minutiae point extraction. However, alignment of the query minutiae point with the original one is still an open issue. Further, the polynomial construction/ reconstruction of the fuzzy vault is well suited to the minutiae points and not found much favor for other biometric modalities like palmprint. A modified fuzzy vault is suggested in [18] where the secret key and the biometrics are hidden in separate grids with chaff points added to make the grids fuzzy. The same scheme finds the place in the palmprint [19] and iris [20] based vaults. Palmprint cryptosystem is created using DOG code using Gaussian derivative filters [31]. Reed Solomon coding and XOR operations are used for encryption and decryption of palm data. Various promising approaches are utilized for cancelable palmprint cryptosystem in literature [32]–[34].

In recent study on biometric cryptosystems, the palmprint cryptosystem [12] made by Wu *et al.* is very impressive in terms of low error rates. They applied BCH encoding to the palmprint and stored the ECC to correct the query template at the time of decryption. They further used a hash function to generate the key which can be utilized in any cryptographic algorithm. If the errors in the query image (genuine user) are within the correcting capabilities, the hash function computed from the corrected image can decrypt the secret message. Their scheme to store ECC for the correction of the query biometric template is quite impressive and an automatic way to utilize the decision threshold, learned from the biometric database to differentiate the genuine and the imposter users. However, one weak link of their system may be the attacks on the computed ECC. If the ECC stored for the decryption phase can be attacked by a hacker even an imposter can be corrected and the spoofed features with transmitted ECC can be used to derive the secret message.

The multimodal biometric cryptosystem has also been attempted in the literature. However, most of them utilize feature level combination of biometric modality to build a cryptosystem. Sutcu *et al.* [21] proposed a technique of integrating face and fingerprint at the feature level to obtain a secure template based on known secure sketch schemes. Nandakumar and Jain [22] derived a vault by integrating the fingerprint and the iris templates at the feature level. Camlikaya *et al.* [23] demonstrated a privacy protection technique by hiding the fingerprint minutiae points amongst the voice features. Yanikoglu and Kholmatov [24] combined two fingerprint features extracted from different fingers to get a combined biometric ID. A feature level combination of biometrics may have added complexity of normalization when two features are in different domain of representations. In recent approaches on multi-biometric cryptosystems Li *et al*. [34] have presented a promising feature level fusion approach [35]. The attempt by Rathgeb and Busch [3] on addressing issues and challenges in multi biometric template protection also merits a mention.

B. OUR WORK

This paper focuses on the design and development of a multi-biometric cryptosystem to meet the higher security requirements. However, the basic structure of the cryptosystem can be considered as hybrid of approaches in [12] and [18], and we have made a number of significant modifications in the earlier approaches. The main contributions from this paper can be summarized as follows:

Firstly, a new framework for the biometric cryptosystem is developed in key binding mode. Here, the candidate biometric modalities are subjected to two functions: (i) BCH encoding which delivers the *parity-code* stored for the alignment of the query biometric template, (ii) Hash function, used to compute *hash-code* to ensure its integrity. The cryptosystem is made by creating two different *cell-arrays*. The *hash-code* is scattered on one *cell-array* by a randomly chosen column-position and the secret key is distributed over second *cell-array* on the same positions. The other locations of the *cell-arrays* are filled with the randomly generated chaff vectors.

Secondly, the *parity-code* is encoded using a regenerative XORCoding in order to hide it from the unauthorized access. At the unlocking stage, the parity-code is regenerated using XORcode and used to align the query template to the original

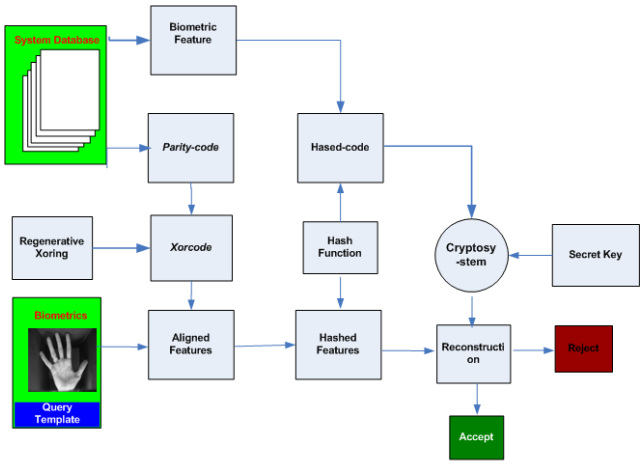


FIGURE 1. Block diagram of the proposed crypto system.

one. If the query *hashed-code* computed from the aligned template can locate the correct locations of the original *hashed-code* from the *feature-cell* it can get back the secret-key from the *key-cell* and the correspondingly secret message.

Finally, but most importantly, this paper presents a multimodal biometric cryptosystem operationalized in two modes: (i) *Feature-Mode*: the cryptosystem is locked by concatenating two extracted biometric features and unlocked by collecting them from the claimed identity (ii) *Decision-Mode*: The secret key is locked in two different cryptosystems with two different modalities. At the unlocking stage, the cryptosystem is attempted to open using both the query biometric modalities. The unlocking is said successful if both the attempts can correctly retrieve the respective keys. The proposed approaches are implemented on two publicly available databases: palmprint [25] and iris [26]. The experimental results confirm the superiority of the multimodal cryptosystems over the unimodal cryptosystems. Further, in two modes of multimodal the performance of *Decision-mode* is found to be superior then those from using *Feature-mode*.

The rest of the paper is organized as follows: The details on the locking and unlocking of the proposed cryptosystem are provided in Section *II*, the modes of multimodal cryptosystem is described in Section *III*, the experimental results on the publicly available databases are illustrated in Section *IV*. The security analysis and relevant discussion on the presented approach is provided in Section *IV* while the key conclusions from this paper are summarized in Section *V*.

II. CONSTRUCTION OF THE PROPOSED CRYPTOSYSTEM

The block diagram of the complete system is shown is Fig. 1. The proposed construction of the biometric cryptosystem consists of three stages: (1) the BCH encoding is applied on biometric features to create the *parity-code* which is then jumbled up using regenerative XORCoding, (2) The locking stage, in which Hash function is used to compute the *hashed-code* and is locked with the secret key for the cryptosystem (*cell-arrays*), (3) the unlocking stage, in which *parity-code* is regenerated using XORCoding and used to align the query features from the locked ones. The *hashed-code* is computed from aligned features to unlock the secret key from the cryptosystem. These stages are detailed in the following *four* subsections.

A. THE BCH CODE

The BCH encoding is used for the biometric features to generate the encoded features. The parameters of the BCH code are n, k and t. Where, n denotes the length of the encoded message, k is the length of the uncoded (original) message, and t denotes the number of the errors to be corrected respectively. The parameter t can be chosen according to the error rates incorporated/expected in the database. Let s be the size of biometric features and let T be the decision threshold (Hamming distance) chosen by considering acceptable error rates. The parameter t can be computed using T as follows:

$$t = s \times T \tag{1}$$

The parameter k should also satisfy constraint $k \geq s$. In case when $k < s$, then (k – s) zeros are appended to the s to get the features with length k and then encode it using BCH encoding. One advantage of this method is that the error correcting capability of the system depends on the T which is learned from the acquired biometric database and can be chosen according to the expectations of the application.

The encoded features consist of two parts: the features of length k and the *parity-code* of length (n-k). The p*arity-code* is sent to the unlocking stage in order to align the query features with the locked ones. The direct transmission of the *parity-code* from locking stage to unlocking stage increases the possibility of security breach. If an attacker can intrude the *parity-code,* a query features could be generated whose errors would be under the error correction capabilities of the (n, k, t) BCH code. Therefore, to reduce such drawbacks we introduce regenerative XORCoding method to compute XORcode from the *parity-code*. The XORcode can regenerate the *parity-code* at the unlocking stage and very difficult predicted by brute force attacks.

B. THE XORCODING OF THE PARITY-CODE

The XOR code is generated to protect the parity bits from unauthorized access. At decryption stage, the parity bits are first regenerated using XORCoding and then used to align the claimed identity with the registered identity. The XORCoding utilizes the XOR operation to alter the *parity-code* which is basically the combination of 1s and 0s to some other combinations. The two consecutive bits of the *parity-code* is first *Xored* to get a code of length (n-k)/2. The weights of each Xoring is then computed and appended with right bit of the code, called as XORcode in order of make it to the desired length n. The XORcode is then transmitted to the unlocking stage. At the unlocking stage, the XORcode is Xored in

the reverse direction and the weights are then assigned to the left bit of the XORcode to regenerate the *parity-code*. The XORCoding is shown in Fig. 2 with an example of string 100001. The consecutive *Xored* bits are 101 with weights 100. The defined weights are illustrated in Table 1. With these weights and *Xored* bits, the XORcode is generated as 1100010. At the unlocking stage, the *XORcode* is again *Xored* to get 001 and the weights are assigned to left bit to regenerate the *parity-code*.

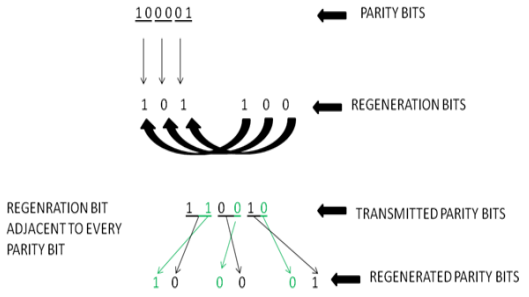


FIGURE 2. An Example of XORCoding.

TABLE 1. Weights assigned during XORCoding.

Parity bits	Xored Output	Weights Assigned
00	0	0
11	0	1
01	1	0
10	1	1

The weights are 1 or 0 assigned according to the presence of 1 or 0 in the parity bit. In order to create the strong XORcode, we introduced random cycles in its computation. At the time of the locking, a random number r is generated between 8 and 15 (in order to represent it in 4 bit) and the XORcode is generated by employing r cycles. The r is then represented in a 4 bit binary string and append to the XORcode. The number r is then deleted and the position of the appended bit is kept secret. At the unlocking end, after recovering the position of the appended bit, the r cycles are employed in the reverse order to regenerate the *parity-code*.

C. LOCKING OF THE CRYPTOSYSTEM

The locking of the proposed cryptosystem consists of candidate biometric features and the secret key generated using a cryptographic algorithm. Let the extracted features be of the length $1 \times N$. We utilized MD5 as a hash function which is applied to the features in order to obtain the hashed feature-vector of the same length $1 \times N$, called as *hashed-feature*. Let a secret key of the size $1 \times S$ is generated using any of the cryptographic algorithms. We then partition the features and the secret key in to four different parts, each of the length *N/4* and *S/4* respectively. Two *cell-arrays* of the size $4 \times Z$ are then created and out of the Z columns, only one of these is randomly selected to distribute the first part of the feature inside it. This *cell-array* is called as *feature-array.* Here, the Value of Z can be chosen as per security requirement. In our work, we have chosen $Z = 100$ to have sufficient number of chaff points associated with genuine feature points [5]. On the second *cell-array*, the first part of the secret key is put on the same column position and this array is referred to as *key-array*. The rest of the 99 columns of the same row are then filled by randomly generated *chaff string* of the same size. The other 3 parts of the key and the features are inserted on the randomly selected columns with the restriction that the key parts and the feature parts will locate at the same column positions. Our specific reason of referring the arrays as *cell-array* is that each cell of the array contains a string of size $1 \times N/4$. The formation of the *cell-arrays* and the placement of the key and the features are shown in Fig. 3.

The two *cell-arrays* joined together constitute main part of our biometric cryptosystem. The biometric image of any user from the database can then be used to compute *XOR-code* using BCH encoding. The MD5 function is used to get *hashed-code* which is scattered to the two separate *cell-arrays* at the same column positions generate the secret key. At the end of the locking stage, the cryptosystem consists of two *cell-arrays*: *feature-array* and *key-array* both of the size 4×100, and the *XORcode*. The complete block diagram for the locking is illustrated in Fig. 4.

D. UNLOCKING OF THE CRYPTOSYSTEM

At the unlocking stage, the extracted features of the query image are firstly aligned to the original ones using BCH encoding. The *parity-code* can be regenerated using XORCoding (Discussed in Section II b). The aligned features are then used to compute *hashed-code* (by using MD5) of the length $1 \times N$. The *hashed-code* is then divided into four parts and each part is matched with the all the 100 column positions of the *feature-array*. In case the claimed/matched identity is from the genuine user, the extracted features are within the error correcting capabilities of the BCH encoding. Hence, the computed *hashed-codes* would match with the original *hashed-codes* hidden in the cell array.

A perfect match helps in retrieving the original *hashed-code* from the *feature-array* and its position helps in achieving the original key from the *key-array* as they were placed at the same row positions during locking stage. Whereas the biometrics from an imposter user is not expected to be corrected from the BCH encoding as the error content in its feature is expected to exceed the error correction capabilities. Hence, the computed *hashed-code* would not match with the ones scattered in the *feature-array* and such non-match is considered to be authentication failure at the unlocking stage. Even if, in the worst cases, the claimed *hashed-code* parts matches with the erroneous column positions, the locations so extracted will lead to the wrong key. The block diagram of the unlocking is shown in Fig. 5.

III. THE PROPOSED MULTIMODAL CRYPTOSYSTEM

The multimodal system proposed in this paper has two modes of operations that can combine or fuse multiple biometrics.

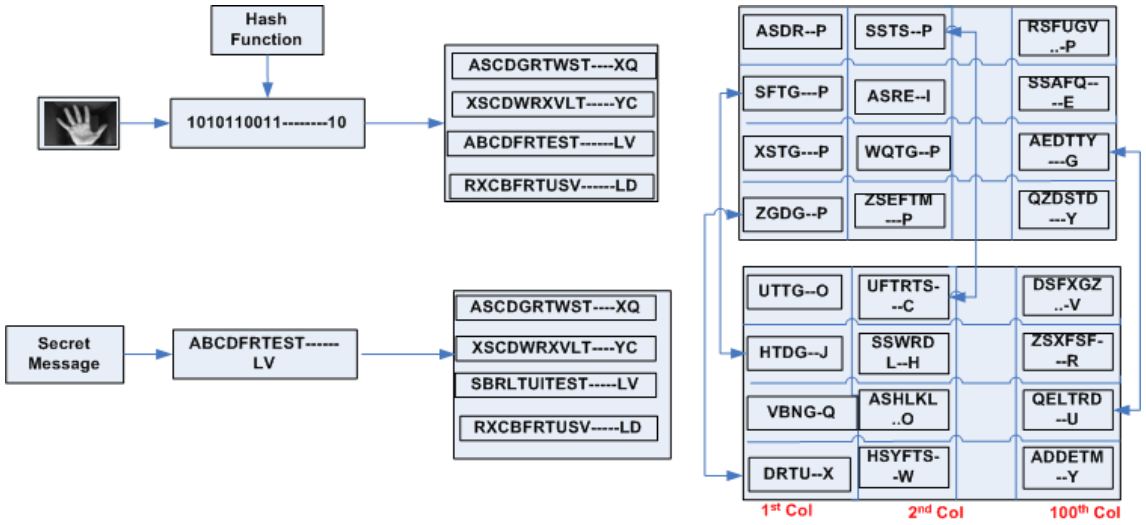


FIGURE 3. Cell-Array construction of the cryptosystem (Arrows shows the same column positions).

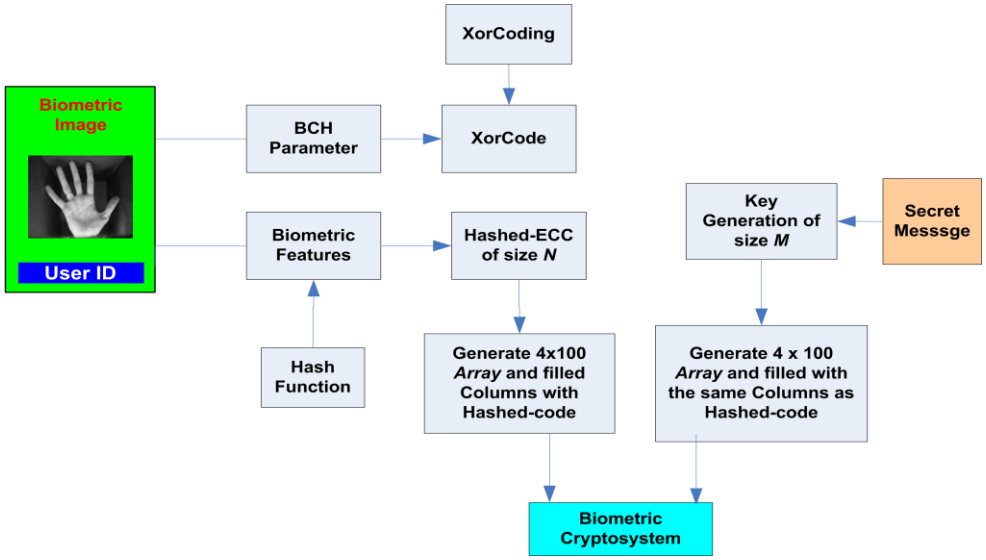


FIGURE 4. Locking of the cryptosystem.

The fusion of multiple biometric modalities can be broadly categorized into four major levels [11]: (i) fusion at the feature level (ii) fusion at the score level, (iii) fusion at rank level, and (iv) fusion at the decision level. The feature level fusion is known to incorporate a rich feature level information while the fusion at score level is difficult to embed in cryptosystems.

We therefore firstly utilize *feature-mode* in which biometric features are concatenated and the locking of the cryptosystem is then performed using the fused features. This multimodal biometrics has also been utilized in the earlier multibiometric systems [23], [24]. However, one drawback of this system is that it needs proper normalization when the concatenated features are in different domain of feature representation. Therefore, another approach of fusion was investigated, *i.e. decision-mode*. In this approach the cryptosystem is simultaneously locked with two modalities involved in fusion. The secret key is broken into two parts and locked with two separate modalities. The unlocking is considered successful if it can be unlocked with both the modalities. The retrieved pieces of the key are then combine to generate final key and hence the secret message.

A. THE FEATURE-MODE OF THE MULTIMODAL SYSTEM

The features are extracted separately from the individual biometrics. Let the feature vectors extracted from the two modalities be of size $1 \times N_1$ and $1 \times N_2$ respectively. The two features are concatenated to obtain a single vector of size $1 \times (N_1 + N_2)$. The new fused feature vector is then encoded using BCH encoding to generate *parity-code*. In order to select proper BCH parameters in case of fused features, the fused features corresponding to each enrolled

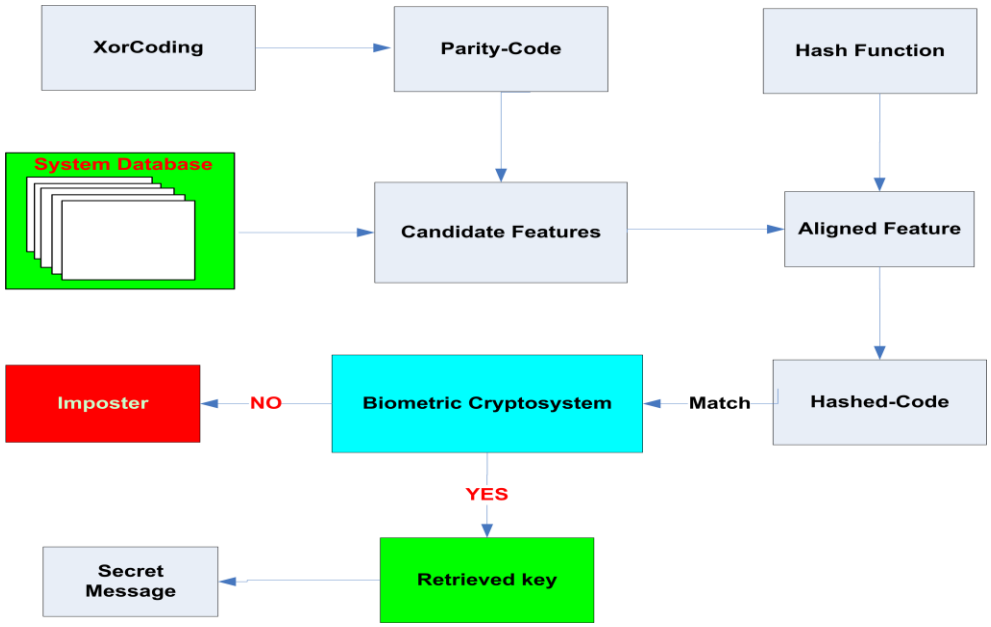


FIGURE 5. Unlocking of the proposed cryptosystem.

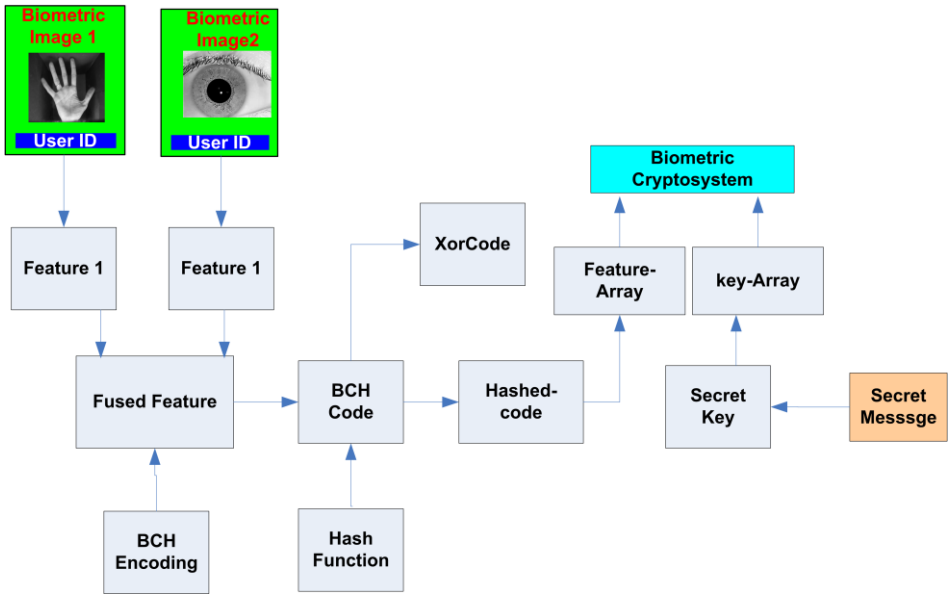


FIGURE 6. Feature-mode multimodal system.

user are computed. The decision threshold with appropriate error rates are computed and used to select the n, k, t for the BCH code (Detailed in Section II *A*). With the BCH encoded features, *parity-code* is used to compute XORcode and stored for unlocking stage. The hash function (MD5) is applied to the fused feature and the *hashed-code* of size $1 \times (N_1 + N_2)$ is computed which is finally incorporated to lock the cryptosystem with the help of the generated secret key.

At the unlocking stage, the two modalities are acquired from the user. The two feature vectors of size $1 \times N_1$ and size $1 \times N_2$ are computed from the modalities and concatenated at the feature level to obtain the feature vector of size $1 \times (N_1 + N_2)$. The *parity-code* is regenerated using XORcode and the fused features are then aligned using the BCH encoding. The MD5 is then used to generate aligned fused features to compute *hashed-code*. The *hashed-code* is finally matched with within the *feature-array* to get the secret key from *key-array*. Block diagram of complete system is given in Fig. 6.

B. THE DECISION MODE OF THE MULTIMODAL SYSTEM

The *decision-mode* is evaluated from two modalities which use two respective cryptosystems. The query modalities are

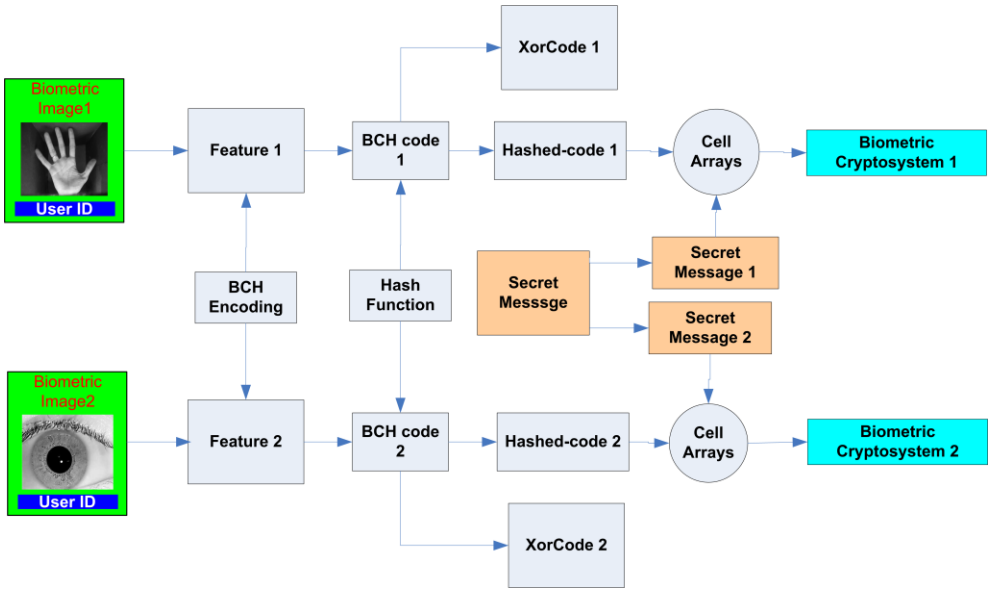


FIGURE 7. Decision-mode multimodal system.

allowed to unlock their respective vaults separately. If both the modalities can correctly unlock their cryptosystems, then the key can be retrieved. The parameters n, k, t of the BCH code (Detailed in Section II A) is learned for both the modalities. The candidate features are encoded using BCH code to generate two *parity-codes*. The XORCoding is applied to generate XorCodes in each case. The Hash function is finally employed separately on the features to generate respective *hashed-codes* of the size $1 \times N_1$ and $1 \times N_2$ respectively. The *hashed-codes* are scattered on the two *feature-arrays of* size 4×100 at the randomly selected column positions. The key of size $1 \times M$ is are scattered in two *key-array*s at similar column positions to *feature-array*. The two *feature-arrays* constitute two cryptosystems corresponding to respective modality. The block diagram of the complete system is shown in Fig. 7.

At the unlocking stage, the two query feature vectors are generated from the presented biometric modalities. BCH codes are then employed on the feature-vectors. The *parity-codes* are regenerated using XorCodes. The XorCodes are then used to align the two features and the application of Hash function provided the two *hashed–codes.* The respective cryptosystem is then attempted to open using both the *hashed-codes*. If both of them are able to correctly locate the column positions of original h*ashed-codes* from the *feature-array* to the secret key is said to be retrieved successfully from the *key-array*. However, if any modality has retrieved it incorrectly, it can be marked as unsuccessful attempt and in that case the claimed user would not be able be allowed to get the secret message back.

The *decision-mode* of the multimodal biometric cryptosystem inherits the two fold security than unimodal and even than feature level biometrics. Both the claimed modalities should correctly locate the key parts from key-arrays. If any of the biometric modalities erroneously retrieved the key, the user will not able to retrieve message.

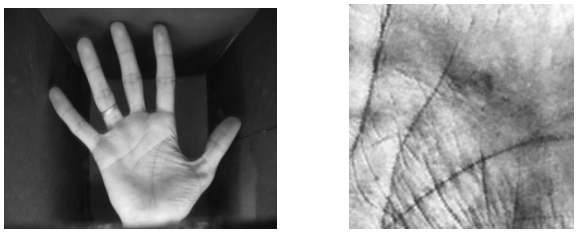
IV. EXPERIMENTAL RESULTS

The increasing popularity of palmprint biometric is due to its high user convenience and high matching accuracy. The research efforts published in the literature [16] and [21] has shown that the palmprint is one of the promising biometric modalities full of complex textural details. The first set of experiments on the proposed cryptosystem is therefore carried out on the unimodal databases from the palmprint and iris. The iris modality has also been utilized as a promising biometric trait with higher textural details and widely employed commercial system with least vulnerability to the imposter attacks as irises are hidden in the eyelids. The combination of palmprint and iris is therefore truly justified as a potential multimodal system. In the second set of experiments, the multimodal cryptosystems using *feature-mode* and *decision-mode* fusion approaches is investigated. The database used for the experimentation purpose is publicly available IITD palmprint [25] and iris [26] which forms an effective bimodal databases acquired from same population.

A. THE BIOMETRIC MODALITIES

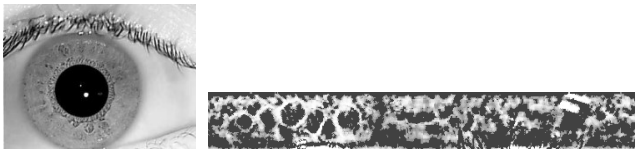
The palmprint database of 200 subjects with 5 samples each is used for experiments. The ROI extraction, normalization, and Gabor based feature extraction method is same as in [27]. The palmprint images of size 384×384 whereas ROIs are of size 128×128, shown in Fig. 8 (a) and 8 (b) respectively.

The 200 subjects from iris database with 5 samples per user are used. A sample iris image of size 340×240 is illustrated in Fig. 9 (a). The image normalization, enhancement, and Gabor based feature extraction is the same as detailed



(a) (b)

FIGURE 8. (a) Sample Image from IITD database (b) Corresponding ROI image.

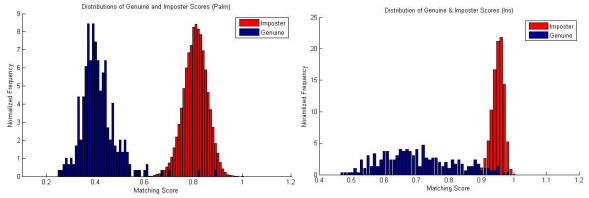


(a) (b)

FIGURE 9. Iris Images (a) sample image (b) Iris strip.

in [28]. A normalized iris image of size 50 × 512 is shown in Fig. 9(b).

The feature extraction from the palmprint is based on the Gabor filter based method as detailed in [27]. The palm images are down sampled to the size 32 × 32 and reshaped to get the string of size 1024. The log Gabor based feature extraction from iris is same as in [28]. We further reshaped the iris image to size 50 × 50 in order to generate the binary string of size 2500.



(a) (b)

FIGURE 10. Histogram for genuine and imposter scores (a) Palmprint (b) iris.

In order to select the parameters n, k, t, for the BCH encoding, we first computed genuine and the imposter scores from both the databases. The Hamming distance based matching between two palmprint and iris is same as in [27] and [28]. Each of the 200 users is compared with other and the matching scores from same user are marked as genuine otherwise as imposter. Out of total 499, 500 (1000 × 999/2) matches, 2000 matches are genuine matching scores. The histograms of the genuine and imposter matching scores are shown in Fig. 10 (a) for palmprint and 10 (b) for iris.

B. THE UNIMODAL CRYPTOSYSTEMS

The False Acceptance Rate (FAR) and False Rejection Rate (FRR) corresponding to different thresholds for the palmprint is shown in Table 2 while for the iris is shown in Table 3. A suitable decision threshold for palmprint and iris modalities could be chosen from these tables (Table 2 and table 3 respectively) according to the requirement of FAR and FRR. The parameters of BCH encoding for palmprint are: (n = 8191, k = 4928,

TABLE 2. Error rates using IITD palmprint database.

Threshold	No of Error Bits	FAR (%)	FRR (%)
0.2451	251	.00099	9.4000
0.2460	252	.00089	9.2667
0.2470	253	.00076	8.9733
0.2480	254	.00075	8.6000
0.2490	255	.00069	7.9667
0.2666	273	.0027	7.2000
0.2675	274	.0036	6.9500
0.2685	275	.0036	6.2000
0.2695	276	.0036	5.8667
0.2705	277	.0054	5.4667
0.2714	278	.0054	5.4667
0.2724	279	.0072	5.4667
0.2744	281	.0089	5.3333
0.2753	282	.0089	5.3333
0.2763	283	.0116	5.3333
0.2773	284	.0125	5.2000
0.2783	285	.0143	4.9333
0.2792	286	.0143	4.9333
0.2802	287	.0170	4.9333
0.2832	290	.0242	4.8000

TABLE 3. Error rates for iris.

Threshold	No of Error Bits	FAR (%)	FRR (%)
0.440	1100	0.0065	10.9520
0.441	1102	0.0085	10.5333
0.442	1105	0.0095	10.4476
0.443	1107	0.0151	10.0381
0.444	1110	0.0572	9.9762
0.445	1112	0.0743	9.8090
0.446	1115	0.0951	9.9238
0.447	1117	0.1957	9.7857
0.448	1120	0.2352	9.9042
0.449	1122	0.3525	9.5371
0.450	1125	0.3525	9.0489
0.451	1127	0.4262	8.9286
0.452	1130	0.5767	8.5619
0.453	1132	0.6102	7.8257
0.454	1135	0.9000	6.4143
0.455	1137	0.9515	6.1762
0.456	1140	1.0524	5.8095
0.457	1142	1.1562	5.0381
0.458	1145	1.3231	4.8810
0.459	1147	1.4835	4.2381

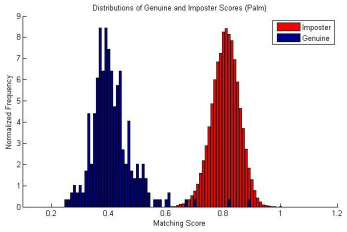


FIGURE 11. Histogram for genuine and imposter scores for PolyU Palmprint.

TABLE 4. Error rates fusing PolyU palmprint database.

Threshold	No of Error Bits	FAR (%)	FRR (%)
0.342	350	0.00193	4.4595
0.344	352	0.00185	4.1892
0.346	354	0.00187	4.1892
0.354	362	0.00763	4.1892
0.356	364	0.00858	3.9189
0.358	366	0.0993	3.6486
0.360	369	0.0983	3.3784
0.370	379	0.0563	2.9730
0.380	389	0.0593	2.5676
0.390	399	0.0491	2.0270
0.400	410	0.0353	1.6216
0.420	430	0.0343	1.4865
0.440	450	0.0393	0.9459
0.460	471	0.0393	0.8108
0.480	491	0.0202	0.6757
0.500	512	0.0285	0.2703
0.520	532	0.0469	0.2703
0.540	553	0.1103	0.2703
0.560	573	0.2583	0.1351
0.580	594	0.5736	0.1351

$t = 285$) while for iris are: ($n = 32767$, $k = 9324$, $t = 2341$). Note that the high error rates for palmprint based system in comparison with the earlier work in [12] may be due to contactless imaging, as detailed in [25]. We therefore examined the palmprint database from the Hong Kong PolyU [30]. The ROI extraction and Gabor filter based features are same as in [27]. The genuine and imposter distributions of the PolyU palmprint are shown in Fig. 11. The other processing for cryptosystem is the same as for IITD palmprint database. The error rates for PolyU database is shown in Table 4.

The parameters for this database are as follows: decision threshold = 0.520, FAR = 0.0469%, FRR = 0.2703%. The BCH parameters are: ($n = 2047$, $k = 1277$, $t = 532$) approximately.

C. THE MULTIMODAL CRYPTOSYSTEMS

The multimodal cryptosystems in the *feature-mode* and *decision-mode* were also implemented. The error rates for *feature-mode* are given in Table 5. In our experiments, we choose the decision threshold as .387. The corresponding FAR, FRR, and the corrected bits are: 0.1172%, 2.800% and 793. The BCH parameters for the systems are ($n = 16383$, $k = 7339$, $t = 793$). *For the decision-mode, the parameters for the two modalities are to be selected. We chose a distance threshold for palmprint as 0.2783 and for iris as 0.441 from Table 2 and Table 3 respectively. Matching scores are generated for all the genuine and imposter matchers. An imposter match is said to be falsely accepted if the score is accepted with both the thresholds. Similarly, a genuine score is said to be falsely rejected if it rejected by both the thresholds. The error rates for decision-mode are given in Table 6. The BCH parameters defined for palm and for the iris using decision-mode are ($n = 8191$, $k = 4928$, $t = 285$) and ($n = 16383$, $k = 5085$, $t = 1102$) respectively.*

TABLE 5. Error rates for feature-mode.

Threshold	No of Error Bits	FAR (%)	FRR (%)
0.369	756	.0089	4.1333
0.370	758	.0089	4.0000
0.371	760	.0098	3.7333
0.372	762	.0116	3.6000
0.373	764	.0143	3.4667
0.374	766	.0152	3.4667
0.375	768	.0179	3.4667
0.376	770	.0215	3.4667
0.377	772	.0268	3.2000
0.378	774	.0304	3.2000
0.379	776	.340	3.0667
0.380	778	.0438	3.0667
0.381	780	.0528	2.9333
0.382	782	.0635	2.8000
0.383	784	.0734	2.8000
0.384	786	.0895	2.8000
0.385	788	.0949	2.8000
0.386	790	.1074	2.8000
0.387	793	.1172	2.8000
0.388	794	.1342	2.8000

V. SECURITY ANALYSIS AND DISCUSSION

In this section we provide the security analysis of the proposed unimodal and multimodal biometric cryptosystems. We firstly consider the case of palmprint based cryptosystem and the analysis made here is according to the parameters of the palmprint. The possibility of the attacks is considered stepwise. The first possibility is the attack on the candidate biometrics, i.e. if the attacker used any random palmprint to attack the system. We have a IITD database of 200 users with 5 images each for IITD palmprint (See Section *IV-A*). In this case, the probability to successfully decrypt the message is about 0.001 (1 out of 1000 palm images) $\approx 10^{-3}$. Thus, to decrypt the message, a cracker has to find about (10^3) different palmprint which is very difficult to manage in a short time. This probability decreases to $0.0005 \approx 10^{-4}$ for Hong Kong PolyU dataset where we used a database of 200 users with 10 images each. Secondly, the attack on the *parity-code* is possible in two ways. If the *parity-code* is attacked directly from the system, the XORCoding

TABLE 6. Error rates for decision-mode.

Threshold (Iris)	Threshold (Palm)	FAR (%)	FRR (%)
.440	.2451	0	2.5760
.441	.2460	0	2.2700
.442	.2470	0	2.2000
.443	.2480	0	2.0000
.444	.2490	0	1.8667
.445	.2666	0	1.5600
.446	.2675	0	1.4500
.447	.2685	0	1.3333
.448	.2695	0	1.2978
.449	.2705	0	1.1453
.450	.2714	0	1.0300
.451	.2724	0	0.9500
.452	.2744	0	0.9500
.453	.2753	0	0.9140
.454	.2763	0.00089	0.9030
.455	.2773	0.00089	0.5240
.456	.2783	0.0980	0.2200
.457	.2792	0.0980	0.2200
.458	.2802	0.0720	0.2200
.459	.2832	.00720	0.2200

TABLE 7. Results for the comparison.

Approach	Threshold	FAR (%)	FRR (%)
Palm [13]	0.2949	0.0012	3.0169
Iris [21]	-	0	8.333
Palm (PolyU)	0.520	0.0469	0.2703
Palm (IITD)	0.2783	0.0143	4.9333
Iris (IITD)	0.450	0.3825	9.0489
Feature-mode	0.387	0.1172	2.800
Decision-mode	0.453	0	0.9140

(Section *II B*) can safeguard it as without knowing the random cycles or appended bit positions, the regeneration of XORcode is very difficult. If the *parity-code* is attacked by randomly generated string, the probability is $2^{(n-k)}$ where n and k are the parameters of the BCH codes. Finally, the possibility for an attacker in recovering the original *hashed-code* from the *feature-array* by brute force attack is p which can be computed as:

$$P = \frac{100 \times 99 \times 98 \times 97}{100^{100} \times 100^{99} \times 100^{97}} \cong 0.941 \times 10^{-387} \quad (2)$$

The summary of experimental results is presented in the Table 7. This table shows that the presented approach operates on very small error rates and that error rate is for the *decision-mode* multimodal cryptosystem (FAR = 0%, FRR = 0.9140%).

The proposed approach is also comparable to earlier reported work by [12] on palmprint cryptosystem with FAR = 0.0012% and FRR = 3.0169% and from [20] on iris cryptosystem with FAR = 0% and FRR = 8.333%. However, the PolyU palmprint database used in [12] is expected to perform better than IITD contactless database [25]. The multimodal system made using IITD palmprint and iris in our work is a multimodal database. The results from the presented approach using the PolyU palmprint database achieved FAR of 0.0469% at FRR of 0.2703% and are quite encouraging.

It may be noted that even if the iris database operated on high error rates as compared to the palmprint, the multimodal modes can operate on significantly smaller error rates. The Gabor filter based features extracted from the palmprints have performed quite well on the PolyU and IITD database; and has been one of the key reasons for superior performance from the multi modal systems. It should also be noted that the *decision-mode* of multimodal cryptosystem investigated in this paper is not only is capable of operating with smaller error rate than both the unimodal cryptosystems and the *feature-mode,* but also strengthens the cryptosystem; as it is very difficult to simultaneously forge multi cryptosystems than those based on single modality.

VI. CONCLUSIONS

This paper has investigated a new framework for biometric cryptosystem which include the BCH encoding to compute *parity-code* in order to align the query features during unlocking; and the Hash function to transform the feature vector to the *hashed-code.* The *hashed-code* is then locked with secret key on two different *cell-arrays* at randomly chosen locations. However, their positions on the respective arrays are same. If the query features can separate exact locations of the original features from the *feature-array,* it can retrieve the secret key from the *key-array* and hence the message.

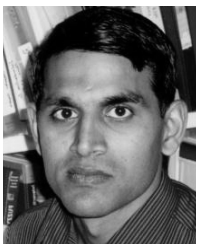
In order to safeguard the *parity-code* from unauthorized closure, we introduced regenerative XORCoding with random cycles. The information of the cycles is appended with the XORcode but its position kept secret. At the unlocking stage, the parity-code can be regenerated using XORcode for query features alignment. The presented approach has been evaluated on publicly available palmprint and iris databases. Two modes of multimodal cryptosystem is also presented and found to be superior then both the unimodal cryptosystems.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2010.
[2] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948–960, Jun. 2004.
[3] C. Rathgeb and C. Busch, "Multi-biometric template protection: Issues and challenges," in *New Trends and Developments in Biometrics*. Rijeka, Croatia: InTech, 2012, pp. 173–190.
[4] U. Uludag and A. Jain, "Securing fingerprint template: Fuzzy vault with helper data," in *Proc. Conf. Comput. Vis. Pattern Recognit. Workshop (CVPRW)*, New York, NY, USA, Jun. 2006, p. 163.
[5] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," in *Audio- and Video-Based Biometric Person Authentication*

(Lecture Notes in Computer Science), vol. 3546. Berlin, Germany: Springer-Verlag, Jul. 2005, pp. 310–319.
[6] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 744–757, Dec. 2007.
[7] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081–1088, Sep. 2006.
[8] C. Sautar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. K. V. Kumar, "Biometric encryption," *Inf. Manage. Comput. Secur.*, vol. 9, no 5, pp. 205–212, 2001.
[9] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008.
[10] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," in *Proc. 6th ACM Conf. Comput. Commun. Secur.*, 1999, pp. 73–82.
[11] K. Nandakumar, "Integration of multiple cues in biometric system," M.S. thesis, Dept. Comput. Sci. Eng., Michigan State Univ., East Lansing, MI, USA, 2005.
[12] X. Wu, D. Zhang, and K. Wang, "A palmprint cryptosystem," in *Advances in Biometrics* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, Aug. 2007, pp. 1035–1042.
[13] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, Apr. 2001.
[14] T. Connie, A. Teoh, M. Goh, and D. Ngo, "PalmHashing: A novel approach for cancelable biometrics," *Inf. Process. Lett.*, vol. 93, no. 1, pp. 1–5, Jan. 2005.
[15] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of BioHashing and its variants," *Pattern Recognit.*, vol. 39, no. 7, pp. 1359–1368, Jul. 2006.
[16] A. Kong, D. Zhang, and M. Kamel, "Three measures for secure palmprint identification," *Pattern Recognit.*, vol. 41, no. 4, pp. 1329–1337, Apr. 2008.
[17] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes Cryptography*, vol. 38, no. 2, pp. 237–257, Feb. 2006.
[18] A. Nagar and S. Chaudhury, "Biometrics based asymmetric cryptosystem design using modified fuzzy vault scheme," in *Proc. ICPR*, Hong Kong, Aug. 2006, pp. 537–540.
[19] A. Kumar and A. Kumar, "Development of a new cryptographic construct using palmprint-based fuzzy vault," *EURASIP J. Adv. Signal Process.*, vol. 2009, pp. 1–11, Sep. 2009, Art. ID 967046.
[20] X. Wu, N. Qi, K. Wang, and D. Zhang, "An iris cryptosystem for information security," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Harbin, China, Aug. 2008, pp. 1533–1536.
[21] Y. Sutcu, Q. Li, and N. Memon, "Secure biometric templates from fingerprint-face features," in *Proc. CVPR*, Minneapolis, MN, USA, Jun. 2007, pp. 1–6.
[22] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in *Proc. BTAS*, Arlington, VA, USA, Sep./Oct. 2008, pp. 1–6.
[23] E. Camlikaya, A. Kholmatov, and B. Yanikoglu, "Multimodal biometric templates for verification using fingerprint and voice," *Proc. SPIE*, vol. 6944, pp. 69440I-1–69440I-9, Mar. 2008.
[24] B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in *Proc. ICPR-BCTP Workshop*, Cambridge, U.K., Aug. 2004, p. 43.
[25] A. Kumar, "Incorporating cohort information for reliable palmprint authentication," in *Proc. ICVGIP*, Bhubaneswar, India, Dec. 2008, pp. 583–590. [Online]. Available: http://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Palm.htm
[26] (2013). [Online]. Available: http://web.iitd.ac.in/~biometrics/Database_Iris.htm
[27] D. Zhang, W.-K. Kong, J. You, and M. Wong, "Online palmprint identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 9, pp. 1041–1050, Sep. 2003.
[28] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal identification," in *Proc. CVPR*, Anchorage, AK, USA, Jun. 2008, pp. 1–7.
[29] X. Wu, D. Zhang, and K. Wang, *Palmprint Recognition*. Beijing, China: Scientific Pub., 2006.
[30] *PolyU Palmprint Database*. [Online]. Available: http://www.comp.polyu.edu.hk/?biometrics/
[31] X. Wu, K. Wang, and D. Zhang, "A cryptosystem based on palmprint feature," in *Proc. ICPR*, Dec. 2008, pp. 1–4.
[32] L. Leng and J. Zhang, "Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security," *J. Netw. Comput. Appl.*, vol. 34, no. 6, pp. 1979–1989, Nov. 2011.
[33] H. Li and L. Wang, "Chaos-based cancelable palmprint authentication system," *Procedia Eng.*, vol. 29, pp. 1239–1245, Mar. 2012.
[34] H. Li, J. Zhang, and Z. Zhang, "Generating cancelable palmprint templates via coupled nonlinear dynamic filters and multiple orientation palmcodes," *Inf. Sci.*, vol. 180, no. 20, pp. 3876–3893, Oct. 2010.
[35] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 255–268, Feb. 2012.

AMIOY KUMAR received the M.Sc. degree in industrial mathematics and informatics from the Department of Mathematics, IIT Roorkee, India, in 2006. He is currently pursuing the M.S. (Research) and Ph.D. (Research) degrees with the Department of Electrical Engineering, IIT Delhi, India. He joined the Biometrics Research Laboratory, Department of Electrical Engineering, IIT Delhi, in 2006. His research interests include pattern recognition with an emphasis on biometric-based personal authentication and multibiometric systems.



AJAY KUMAR (S'00–M'01–SM'07) received the Ph.D. degree from the University of Hong Kong, in 2001. He was an Assistant Professor with the Department of Electrical Engineering, IIT Delhi, India, from 2005 to 2007. He is currently working as Associate Professor in the Department of Computing, The Hong Kong Polytechnic University. His current research interests are in biometrics with an emphasis on hand biometrics, vascular biometrics, iris, and multimodal biometrics. He has authored extensively in biometrics and computer vision-based industrial inspection, and holds five U.S. patents. His research interests include pattern recognition with an emphasis on biometrics and defect detection using wavelets, general texture analysis, neural networks, and support vector machines. He is currently on the Editorial Board of the *Pattern Recognition* journal, and serves on the IEEE Biometrics Council as the Vice President (Publications). He was on the Editorial Board of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (2010–2013), and served on the program committees of several international conferences and workshops in the field of his research interest. He was the Program Chair of the Third International Conference on Ethics and Policy of Biometrics and International Data Sharing in 2010, and the Program Co-Chair of the International Joint Conference in Washington, DC, in 2011, and the International Conference on Biometrics in Madrid in 2013. He served as the General Co-Chair of the International Joint Conference in Tampa in 2014.