Chapter 6
Multibiometric Template Security

The main focus of this chapter concerns the biometric template security in multibiometric systems. A brief introduction to cancelable biometrics and BioHashing approaches are discussed here. In this chapter, a cancelable multibiometric (CMB) based on BioHashing is introduced as a multibiometric template protection method. The performance of the proposed CMB is analyzed both in biometric and multibiometric systems under different scenarios. The chapter concludes with the chapter summary.

6.1 Introduction

The main advantage of biometrics over traditional security systems is intrinsic based recognition and consequently the individual is to be physically present at the point of the authentication. However, biometric systems are vulnerable to a wide range of attacks (Jain *et al*., 2008a). Attacks against the (stored) biometric templates are one of the most potentially damaging on a biometric system. Stolen biometric templates can be used to compromise the security of the system in many ways including gaining unauthorized access by impostors, preparation of physical spoof templates, covertly track a person by cross-matching across different application databases etc. Multibiometric systems provide significant improvement in the recognition accuracy by combining evidence from multiple biometric sources. However, biometric template security is still critical in biometric as well as multibiometric systems.

As a result of the growing demand for security of stored biometric data, cancelable biometric has attracted considerable attention. Cancelable biometrics has advantages over other template protection methods because of easily diversity, revocability and non-invertibility. A number of approaches such as feature transformation and biometric cryptosystems have been proposed to secure templates (Maltoni *et al*., 2009, Rathgeb *et*

al., 2013). A review of template protection schemes can be seen at Section 2.7. In this work, a cancelable biometric is proposed in which biometric features is combined with a tokenized (pseudo-) random number (TRN).

6.2 Cancelable Biometrics

Ratha *et al*. (2001b) introduced cancelable biometrics in which biometric signals are distorted intentionally, repeatedly based on transforms and comparison of biometric templates is performed in the transformed domain. The distortion of biometric signal is carried out in the same fashion for enrollment and for every authentication. In contrast to biometric cryptosystem algorithms, in cancelable biometrics the transformed templates are never decrypted as the transforms are noninvertible and unlinkability of biometric templates. Hence, the original (undistorted) biometrics cannot be recovered even the transform function and the transformed biometric data are known. If one variant of the transformed biometric data is compromised, then the transform function can simply be changed to create a new variant (transformed representation) for re-enrollment as, essentially, a new person. Furthermore, it can be prevented from tracking subjects by cross-matching databases by applying different transforms for different applications. In general, transformed biometric templates are difficult to align in order to perform a proper comparison and as result, loss system accuracy. Hence, the challenge is to construct transform functions which provide secure biometric templates, while maintaining recognition rates of the original biometric algorithm.

In cancelable biometrics, transforms can be applied at two stages of biometric system i.e. signal domain and feature domain. In the signal domain, transformations are either applied to raw biometric measurements (e.g., face image in Ratha *et al*., 2001b) or to preprocessed biometric signals (e.g., iris texture in Hammerle-Uhl *et al*., 2009). Common signal domain transformation includes grid morphing and block permutation of biometric signal or image (Ratha *et al*., 2001b). Feature domain transform can be repeatable perturbations of feature points, transformation based on some (non-invertible) functions or random projection with or without a key like BioHashing (Goh and Ngo, 2003). In case of signal domain transforms, comparators do not need to be adapted whereas in case of feature domain transforms, the extracted biometric features (e.g., face features in Teoh *et al*., 2008) are transformed, thus, a compromise of

transforms requires further effort in reconstructing the original biometric from the template.

Furthermore, cancelable biometrics is commonly categorized as biometric *salting* in which transform is carried out with user-specific key and *non-invertible* in which transform is non-invertible. Biometric *salting* and *non-invertible* transforms have been already discussed in Section 2.7.

Performance of cancelable biometrics (mainly in Biometric salting) can be discussed into three scenarios *viz*.

(i) The best scenario that is, all users have unique keys.
(ii) Stolen-biometric scenario that is, all users share the same biometric feature.
(iii) The worst scenario (stolen-key scenario) that is, imposters share the same genuine users' keys, that is, all users share the same keys.

Chong *et al*. (2006) proposed two iris verification schemes based on cancelable biometrics which was carried out by iterated inner-product between the iris feature and user-specific secret pseudo-random number, and finally deciding each bit on the sign based on a predefined threshold. However, they emphasized the performance improvement rather than the cancelability of the iris biometric including the stolen-biometric and stolen-key scenarios. Generally, in the worst scenario (stolen-key scenario), the performance degrades sharply and can be lower than that obtained using only the biometric data (Kong *et al*., 2006).

6.3 BioHashing

A variant of cancelable biometric using two-factor authentication approach called BioHashing was proposed by Goh and Ngo (2003). The BioHash code were generated by iterated inner product of a tokenized pseudo-random number (TRN) which is generated by a hash key and the user specific biometric features.

BioHashing consists of two major processes (Teoh *et al*., 2004) *viz.* biometric feature extraction and discretization (Figure 6.1). The process of feature extraction includes signal acquisition, preprocessing and feature extraction, as general biometric verification systems. In this stage, different techniques have been employed depending on biometric modality or signals. Discretization, the secret of BioHashing, is conducted in four steps and described in Algorithm 6.1.

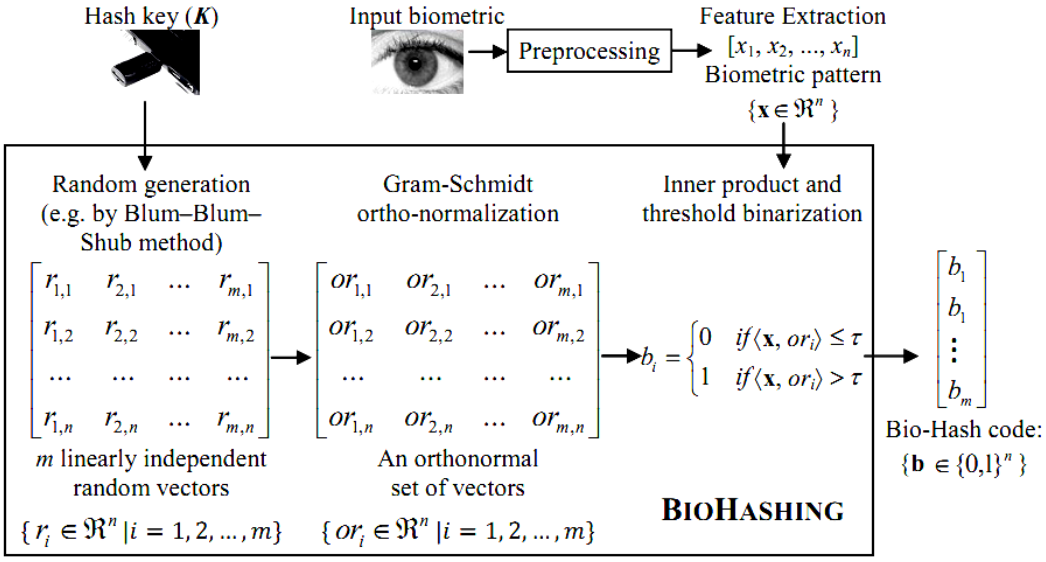


Figure 6.1 Base BioHashing Method

Algorithm 6.1: Base BioHashing

Input: Secret key (**K**), biometric pattern (***x***).

Output: Bio-hash Code (***b***)

Step 1: Given a secret key ***K*** (the Hash key), generate a set of tokenized (pseudo-) random number (TRN) vectors $\{r_i \in \Re^n \mid i = 1, 2, \ldots, m\}$ based on a key. The Blum–Blum–Shub method (Blum *et al*., 1986) is commonly adopted.

Step 2: Apply the Gram-Schmidt ortho-normalization process to $\{r_i \in \Re^n \mid i = 1, 2, \ldots, m\}$ and thus obtain orthogonalized TRN, a set of orthonormal vectors $\{or_i \in \Re^n \mid i = 1, 2, \ldots, m\}$.

Step 3: Calculate the inner product of the biometric pattern (**x**) obtained from the process of feature extraction and each orthnonormal vector (or_i) in TRN, such that $\langle x, or_i \rangle$.

Step 4: Use a threshold τ to obtain Bio-hash Code, ***b*** whose elements are defined as

$$b_i = \begin{cases} 0 & if \quad \langle x, or_i \rangle \le \tau \\ 1 & if \quad \langle x, or_i \rangle > \tau \end{cases}$$

where, i is between 1 and m, the dimensionality of ***b***.

The BioHash code is dependent on both biometric and TRN and it is irreproducible without presenting the two simultaneously. The inversion of BioHash to recover biometric data is impossible because factoring the inner products of biometrics feature and TRN is intractable. Furthermore, this method delivered extremely low error rates when the genuine token was used.

6.4 Proposed Cancelable Multibiometrics based on BioHashing

Similar to cancelable biometrics, the proposed cancelable multibiometrics (CMB) consists of two major steps: (i) Pre-processing and feature extraction and (ii) Cancelable transform. During Pre-processing, biometric pattern is generated by performing a set of pre-processing operations which are depended on the biometric modality and feature extraction. Cancelable transform is the secret of cancelable multibiometrics. Researchers have proposed several cancelable transforms as security tool of the stored biometric templates. It includes image deformation, feature projection with or without user key. During cancelable transform, (weighted) sum of biometric pattern and inner product of the biometric pattern with a set of orthonormalized vectors based on a user key is performed. In the present work, a cancelable transform using user key (k) is proposed and its steps are illustrated in Figure 6.2 and described in Algorithm 6.2.

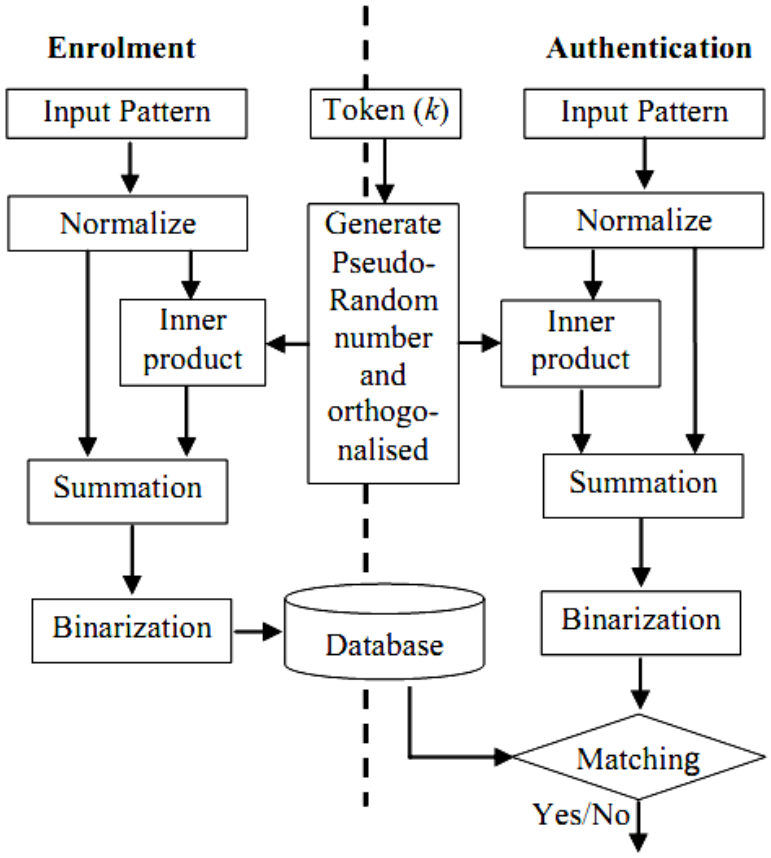


Figure 6.2 Proposed Cancelable Transform

Algorithm 6.2: Proposed Cancelable Biometric

Input: Secret key (**K),** biometric pattern (**P**).

Output: Cancelable biometric (***b***)

Step 1: The biometric pattern (**P**) is normalized using their norm as

$$\mathbf{p} = \mathbf{P}/\,|\mathbf{P}| = [p_1, p_2, ..., p_n]$$

where, |**P**| denotes the L_2 norm of vector **P**.

Step 2: Given the input key (**K**), generate a set of pseudo-random vectors $\{r_i \in \Re^n \mid i = 1,\ 2,\ \ldots,\ m\}$ using the Blum-Blum-Shub method (Blum *et al*., 1986).

Step 3: Apply the Gram–Schmidt ortho-normalization procedure to transform the basis $\{r_i \in \Re^n \mid i = 1, 2, \ldots, m\}$ into a set of orthonormal vectors $\{or_i \in \Re^n \mid i = 1, 2, \ldots, m\}$.

Step 4: Calculate the inner product of **p,** the normalized biometric pattern obtained from Step (1) and orthonormal vectors **or** obtained from Step (3), such that $\langle \mathbf{p}|\mathbf{or_i}\rangle$, $i = 1, 2, ..., m$.

Step 5: The inner product $\langle \mathbf{p}|\mathbf{or_i}\rangle$ is normalized using their norm as

$$\mathbf{I} = \langle \mathbf{p}|\mathbf{or_i}\rangle \,/\, |\langle \mathbf{p}|\mathbf{or_i}\rangle| = [I_1, I_2, ..., I_m]$$

where, $|\langle \mathbf{p}|\mathbf{or_i}\rangle|$ denotes the L_2 norm of vector $\langle \mathbf{p}|\mathbf{or_i}\rangle$.

Step 6: Compute a weighted sum of the normalized vectors **p** obtained in step (1) with **I** obtained in step (5) as

$$CB = \alpha\mathbf{p} + \beta\mathbf{I}$$

where, α and β are constant ($\alpha = \beta = 1$ in the present work).

Step 7: Finally, the cancelable iris pattern (***b***) is generated using a threshold τ as

$$b_i = \begin{cases} 0 & if \quad \langle CB_i \rangle \le \tau \\ 1 & if \quad \langle CB_i \rangle > \tau \end{cases},$$

where, i is between 1 and m, the dimensionality of ***b***.

6.5 Experimental Results and Discussion

Experiments have been carried out in Matlab 7.9 environment. The performance of the proposed cancelable biometric (CB) algorithm is analysed in biometric and multibiometric systems. In biometric system, iris and fingerprint modalities are employed. Multibiometric systems are based on (i) multiple features of iris and (ii) iris and fingerprint modalities. Each system is discussed in the following subsections.

6.5.1 Cancelable Iris Biometrics

In the present work, iris images are taken from the CASIA-IrisV1 and CASIA-IrisV3-Interval database (CASIA, 2006) collected by the Chinese Academy of Sciences' Institute of Automation. Performance evaluation of the proposed cancelable iris biometric is carried out with 350 iris images (of 50 subjects/classes) from both databases i.e. CASIA-IrisV1 and CASIA-IrisV3-Interval. For each class, five instances are used in the training and the remaining two for testing.

Iris segmentation is an important stage of iris recognition and mainly consists of extraction the iris from the input eye images by defining the papillary and sclera boundaries of the iris. An edge map of the input eye image is generated by employing Canny edge detection (Liu *et al*., 2003). From the edge map, the iris inner (pupil) and outer (sclera) circles are detected by applying the circular Hough transform (Wildes, 1997). The eyelid occlusion is removed using a linear Hough transform. The presence of eyelashes is identified using a simple thresholding technique.

Afterwards, a normalization process is required in order to transform the segmentation iris into a fixed dimension. This is done with Daugman's rubber sheet model (Daugman, 2004), which maps the circular iris image into a rectangular.

The performance of the proposed cancelable multibiometric (CMB) is compared with the base BioHashing method described in Section 6.3 and the simple biometric system (Bio), in terms of Equal Error Rate (EER), False Rejection Rate (FRR) at zero False Accept Rate (FAR) and Running time (RT) in sec. and the results are tabulated in Table 6.1. The evaluation is also extended with stolen-key (S-Key) and stolen-biometric (S-Bio) scenarios. Figure 6.3-6.5 shows the ROCs plots that show the performance of the proposed CB with different combination of three feature extraction methods *viz*. PCA, ICA and DWT over CASIA-IrisV1 and CASIA-IrisV3-Interval datasets.

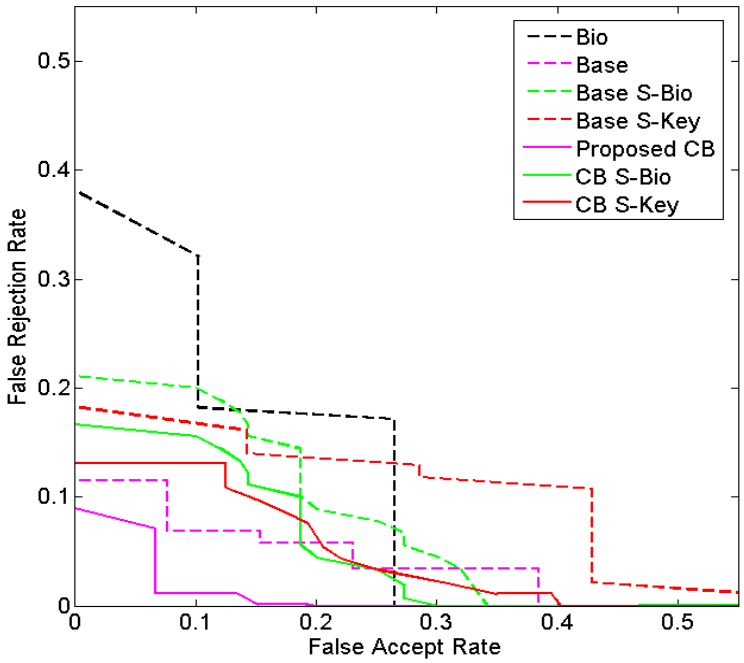
The performance of the proposed CB is compared with performance of base BioHashing at best (i.e. both biometric and key are secured), stolen-key (S-Key) and stolen-biometric (S-Bio) scenarios correspondingly. Table 6.1 shows that the proposed CB achieves the best result with 0.0529 EER and 0.0896 FRR at zero FAR whereas base BioHashing achieves 0.0729 EER and 0.1149 FRR at zero FAR for PCA features extracted over CASIA-IrisV1 dataset. For the same feature, the proposed CB achieves

0.1255 EER and 0.1304 FRR at zero FAR at stolen-key (S-Key) scenario whereas base BioHashing achieves 0.1475 EER and 0.1828 FRR at zero FAR at the same scenario and so on. From the experimental results, it is found that the proposed CB outperforms the base BioHashing in all scenarios.

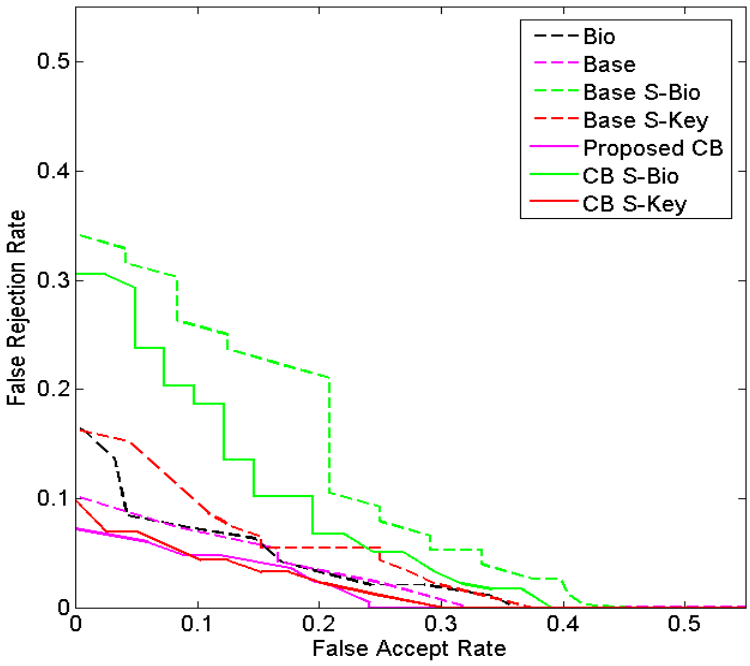
Table 6.1 Performances of Proposed Cancelable Iris Biometrics

Feature Extraction Method	**Algorithm**	**CASIA-IrisV1**			**CASIA-IrisV3-Interval**		
		EER	**FRR at FAR=0**	**RT (in sec)**	**EER**	**FRR at FAR=0**	**RT (in sec)**
PCA	Bio	0.1768	0.3814	0.2311	0.0800	0.1684	0.2300
	Base	0.0729	0.1149	0.2225	0.0800	0.1023	0.2252
	Base S-Bio	0.1494	0.2111	0.2225	0.2092	0.3421	0.2242
	Base S-Key	0.1475	0.1828	0.2251	0.0978	0.1630	0.2248
	Proposed CB	0.0529	0.0896	0.2238	0.0580	0.0723	0.2317
	CB S-Bio	0.1347	0.1667	0.2252	0.1281	0.3051	0.2234
	CB S-Key	0.1255	0.1304	0.2249	0.0659	0.0978	0.2753
ICA	Bio	0.3101	0.6552	0.2322	0.1395	0.4301	0.2220
	Base	0.1064	0.1064	0.2207	0.1010	0.1010	0.2250
	Base S-Bio	0.1368	0.1368	0.2211	0.1546	0.1546	0.2215
	Base S-Key	0.3250	0.7333	0.2345	0.1600	0.4483	0.2305
	Proposed CB	0.0510	0.0510	**0.2205**	**0.0421**	**0.0421**	0.2230
	CB S-Bio	0.0505	0.0505	0.2241	0.1020	0.1020	0.2213
	CB S-Key	0.2906	0.5417	0.2265	0.1300	0.1628	0.2336
DWT	Bio	0.3099	0.8776	0.2302	0.3112	0.8704	0.2387
	Base	0.0690	0.0920	0.2317	0.0904	0.1685	0.2232
	Base S-Bio	0.1304	0.2065	0.2237	0.1327	0.1327	0.2512
	Base S-Key	0.3765	0.7000	0.2636	0.3454	0.7895	0.2453
	Proposed CB	0.0512	0.0843	0.2289	0.0769	0.0769	0.2289
	CB S-Bio	0.0707	0.0707	0.2535	0.0606	0.0606	0.2239
	CB S-Key	0.3765	0.4800	0.2339	0.3112	0.7679	0.2292

/

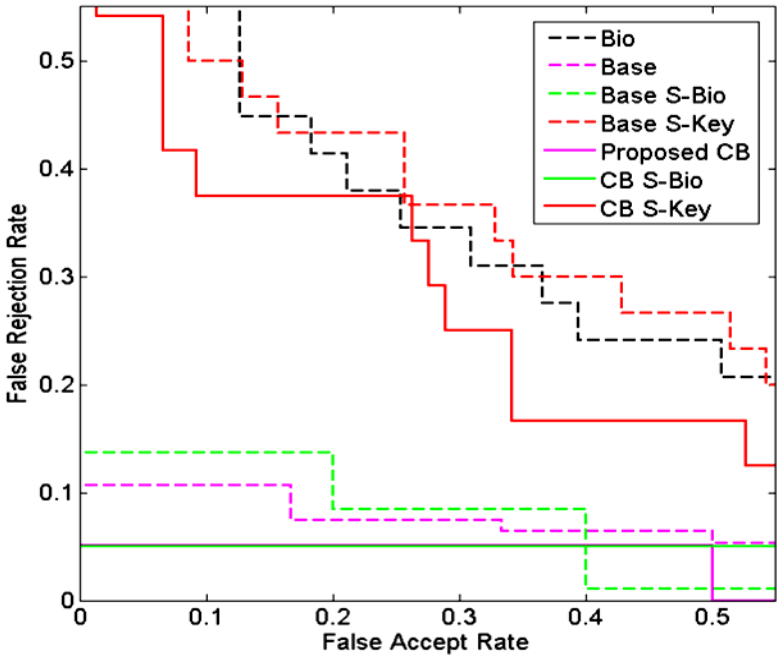


(a)

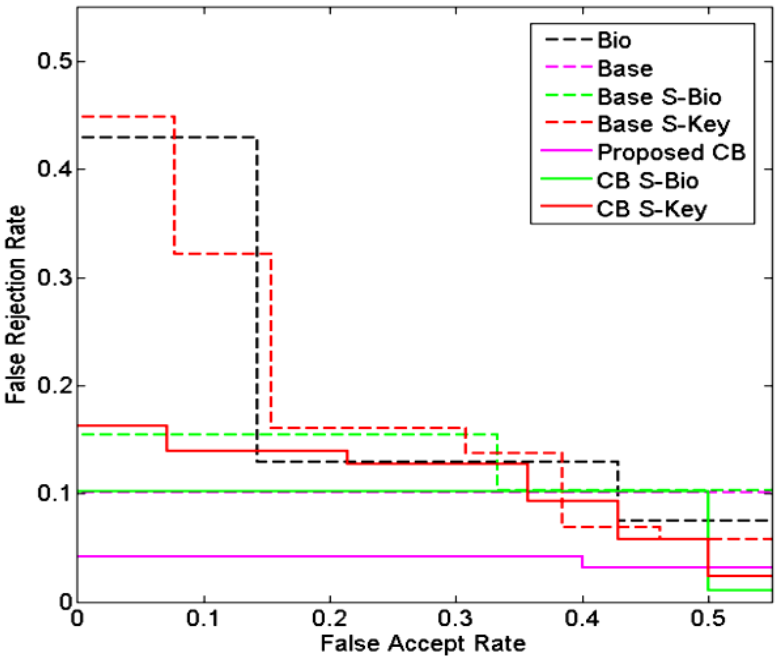


(b)

Figure 6.3 ROCs of Different Template Protection Algorithms in Iris Recognition System on PCA Features from (a) CASIA-IrisV1 (b) CASIA-IrisV3-Interval

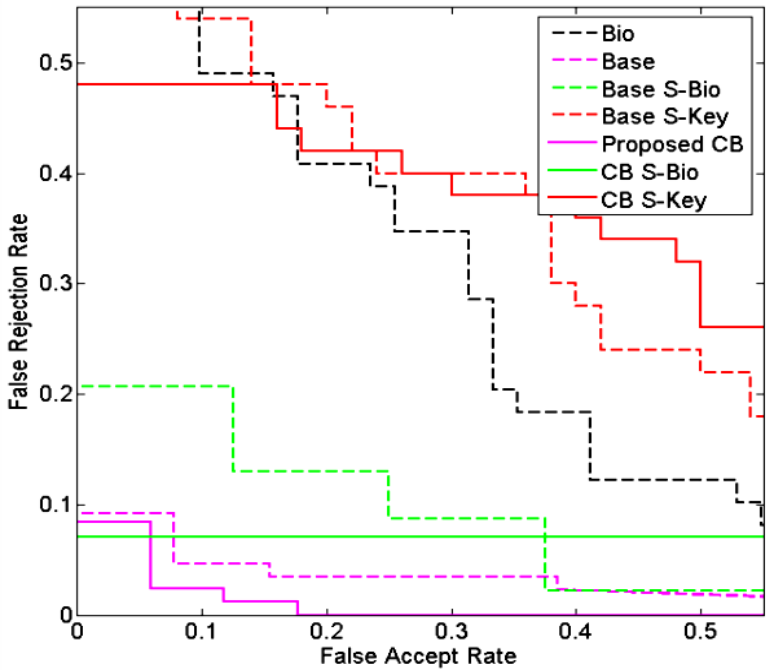


(a)

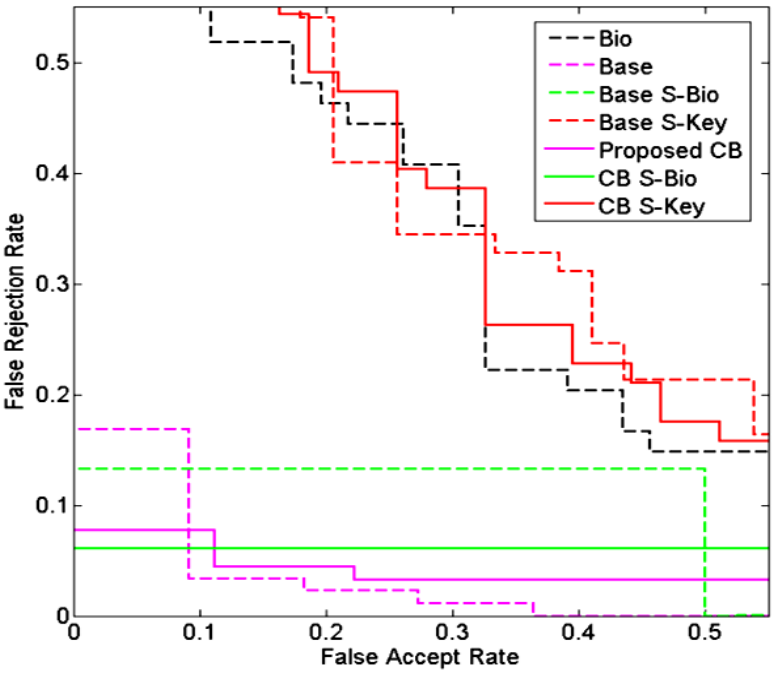


(b)

Figure 6.4 ROCs of Different Template Protection Algorithms in Iris Recognition System on ICA Features from (a) CASIA-IrisV1 (b) CASIA-IrisV3-Interval



(a)



(b)

Figure 6.5 ROCs of Different Template Protection Algorithms in Iris Recognition System on DWT Features from (a) CASIA-IrisV1 (b) CASIA-IrisV3-Interval

6.5.2 Cancelable Fingerprint Biometrics

In this experiment, fingerprint images are taken from FVC2004 DB3 (Maio *et al*., 2004). The fingerprints of FVC2004 DB3 were acquired through thermal sweeping sensor "FingerChip CD4B14CB" by Atmel. It consists of 800 gray scale fingerprint images of size 300×480 pixels. Performance evaluation of the proposed CB is carried out with 350 iris images (of 50 subjects/classes, 7 instances each class). For each class, five instances are used in the training and the remaining two for testing.

The fingerprint features are extracted as follows: a fingerprint image is preprocessed to enhance the image by Short Time Fourier Transform (STFT) analysis (Sharat *et al*., 2007). Then, texture features consist of three sets of invariant moment features are extracted from three different sizes of Region of Interest (ROI) areas based on the reference point from the enhanced fingerprint image. Each set of invariant moments contains three invariant moments. Thus, texture pattern of 128 features are extracted from fingerprint image. The fingerprint patterns are transformed into cancelable fingerprint patterns using Algorithm 6.2. Then, the cancelable fingerprint patterns are classified by using SVM with RBF Kernel. The performance of the proposed cancelable fingerprint biometric (CB) is compared with the base BioHashing method described in Section 6.3 and the simple biometric system (Bio), in terms of Equal Error Rate (EER), False Rejection Rate (FRR) at zero False Accept Rate (FAR) and Running time (RT) in sec. and the results are tabulated in Table 6.2. The evaluation is also extended with stolen-key (S-Key) and stolen-biometric (S-Bio) scenarios. Figure 6.6 shows ROC couves that show the performance of the proposed CB with fingerprint modality.

Table 6.2 shows that the proposed CB achieves the best result with 0.0638 EER and 0.0638 FRR at zero FAR whereas base BioHashing achieves 0.1146 EER and 0. 1146 FRR at zero FAR for fingerprint modality over FVC2004 DB3 dataset. From the experimental results, it is also found that the proposed CB outperforms the base BioHashing in all scenarios.

Table 6.2 Performance of the Proposed Cancelable Fingerprint Biometrics

Algorithm	**FVC2004-DB3**		
	EER	**FRR at FAR=0**	**RT (in sec)**
Bio	0.2285	0.5455	0.2354
Base	0.1146	0.1146	0.2364
Base S-Bio	0.1667	0.1667	**0.2324**
Base S-Key	0.1875	0.2143	0.2434
Proposed CB	**0.0638**	**0.0638**	0.2326
CB S-Bio	0.1184	0.1316	0.2264
CB S-Key	0.1236	0.1910	0.2443

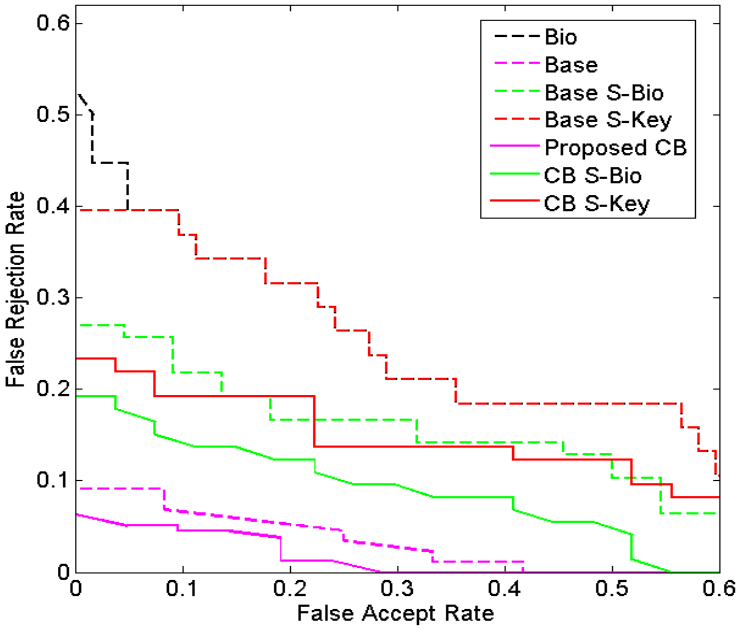


Figure 6.6 ROCs of Different Template Protection Algorithms in Fingerprint Recognition System

6.5.3 Cancelable Multibiometrics: Multi-algorithm Approach

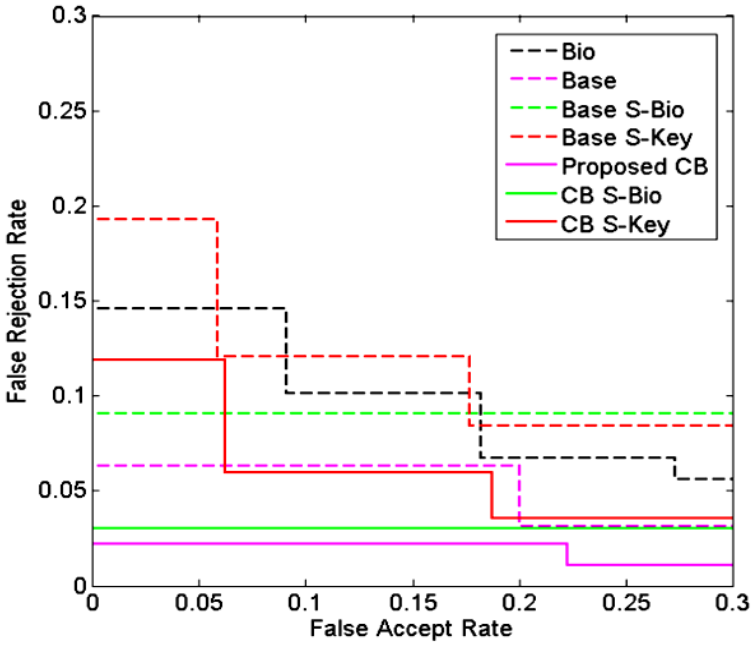
In this experiment, the iris patterns extracted in Cancelable Iris Biometrics Experimentation (Section 6.5.1) are employed as input patterns. The iris patterns are extracted using three feature extraction methods *viz*. PCA, ICA and DWT over CASIA-IrisV1 and CASIA-IrisV3-Interval datasets. The multibiometric templates are generated by concatenating each pair of iris templates from two feature extraction methods. Hence, there are three possible combinations of feature extraction methods *viz*. (i) PCA + ICA, (ii) PCA + DWT and (iii) ICA + DWT.

The multibiometric templates are transformed into cancelable multibiometrics using Algorithm 6.2. Then, the cancelable multibiometric templates are classified by using SVM with RBF kernel. The performance of the proposed cancelable multibiometrics (CMB) is compared with the base BioHashing method described in Section 6.3 and the simple multibiometric system (Bio), in terms of Equal error rate (EER), False Rejection Rate (FRR) at zero False Accept Rate (FAR) and Running time (RT) in sec. and the results are tabulated in Table 6.3. The evaluation is also extended with stolen-key (S-Key) and stolen-biometric (S-Bio) scenarios. Figure 6.7-6.9 shows ROC curves that show the performance of the proposed CB in multibiometric systems.

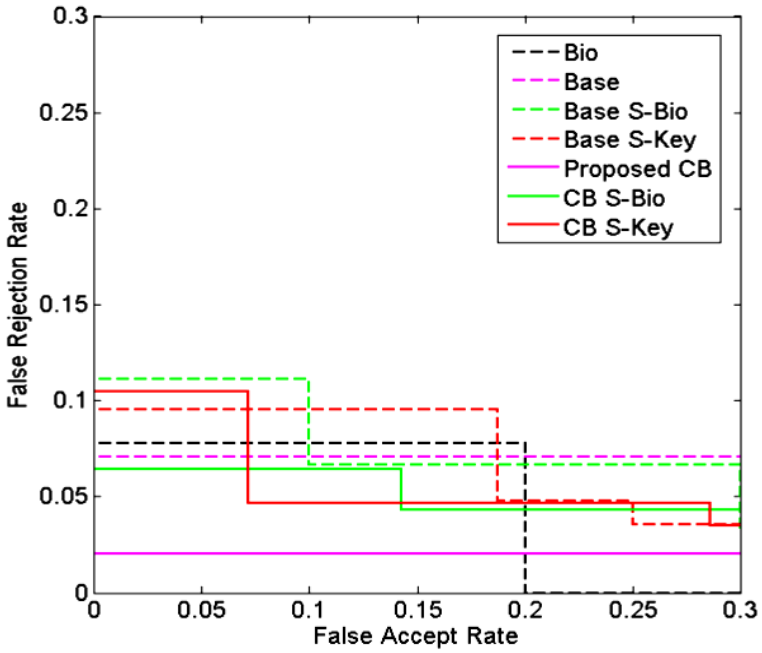
Table 6.3 shows that the proposed CMB achieves the best result with 0.022 EER and 0.022 FRR at zero FAR whereas base BioHashing achieves 0.0632 EER and 0.0632 FRR at zero FAR for combined PCA + ICA features extracted over CASIA-IrisV1 dataset. For the same feature, the proposed CMB achieves 0.0595 EER and 0.1190 FRR at zero FAR at stolen-key (S-Key) scenario whereas base BioHashing achieves 0.1185 EER and 0.1928 FRR at zero FAR at the same scenario and so on. From the experimental results, it is also found that the proposed CMB outperforms the base BioHashing in all scenarios.

Table 6.3 Performances of Cancelable Multibiometrics: Multi-algorithm Approach

Multi-biometric System	Algorithm	CASIA-IrisV1			CASIA-IrisV3-Interval		
		EER	FRR at FAR=0	RT (in sec)	EER	FRR at FAR=0	RT (in sec)
PCA + ICA	Bio	0.1011	0.1461	0.3036	0.0778	0.0778	0.2200
	Base	0.0632	0.0632	0.2477	0.0707	0.0707	0.2084
	Base S-Bio	0.0909	0.0909	0.2926	0.1000	0.1111	0.2052
	Base S-Key	0.1185	0.1928	0.2713	0.0952	0.0952	0.2515
	Proposed CB	0.0220	0.0220	0.2395	0.0202	0.0202	0.2481
	CB S-Bio	0.0303	0.0303	0.3425	0.0645	0.0645	0.2108
	CB S-Key	0.0595	0.1190	0.2512	0.0698	0.1047	0.2321
PCA + DWT	Bio	0.0435	0.0435	0.3482	0.0978	0.0978	0.2847
	Base	0.1010	0.1010	0.2473	0.0737	0.0737	0.2545
	Base S-Bio	0.1100	0.1100	0.2006	0.0737	0.0737	0.2154
	Base S-Key	0.1190	0.2143	0.2270	0.0941	0.0941	0.2318
	Proposed CB	**0.0200**	**0.0200**	0.2029	0.0326	0.0326	0.2212
	CB S-Bio	0.0512	0.0512	0.2039	0.0430	0.0430	0.2195
	CB S-Key	0.0697	0.1047	0.2156	0.0404	0.0404	0.2256
ICA + DWT	Bio	0.1615	0.2234	0.2043	0.1277	0.1277	0.2087
	Base	0.0625	0.0625	0.2543	0.0645	0.0645	0.2499
	Base S-Bio	0.1000	0.1111	0.2036	0.0714	0.0714	0.2032
	Base S-Key	0.2286	0.4143	0.2679	0.1333	0.2706	0.2309
	Proposed CB	0.0219	0.0219	0.2430	0.0219	0.0219	0.2099
	CB S-Bio	0.6452	0.6452	0.2195	0.0303	0.0303	**0.1976**
	CB S-Key	0.1111	0.1341	0.2125	0.1149	0.1494	0.2252

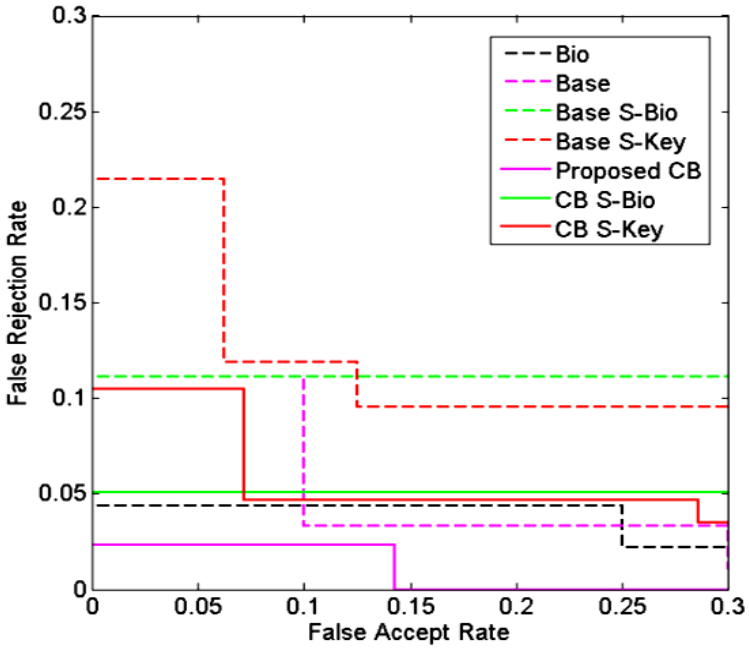


(a)

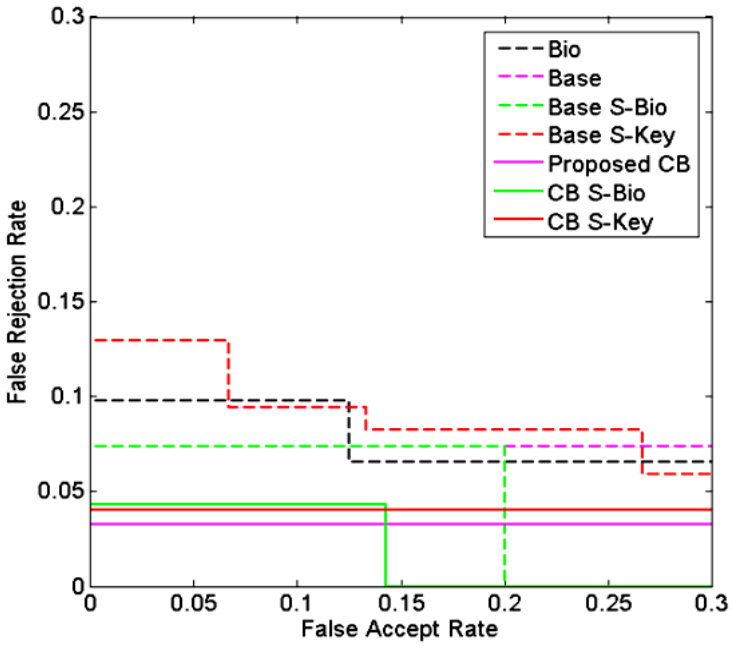


(b)

Figure 6.7 ROCs of Different Template Protection Algorithms in Multi-algorithm Approach on (PCA+ICA) Features from (a) CASIA-IrisV1 (b) CASIA-IrisV3-Interval

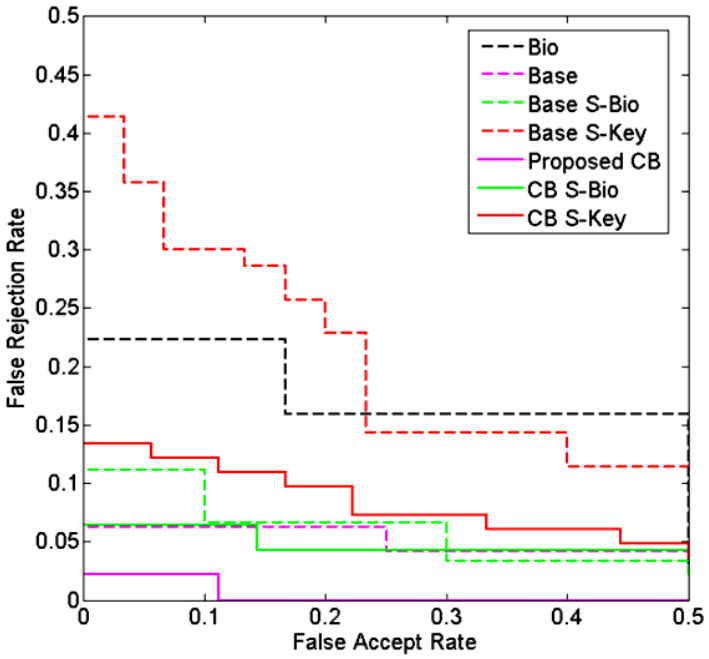


(a)

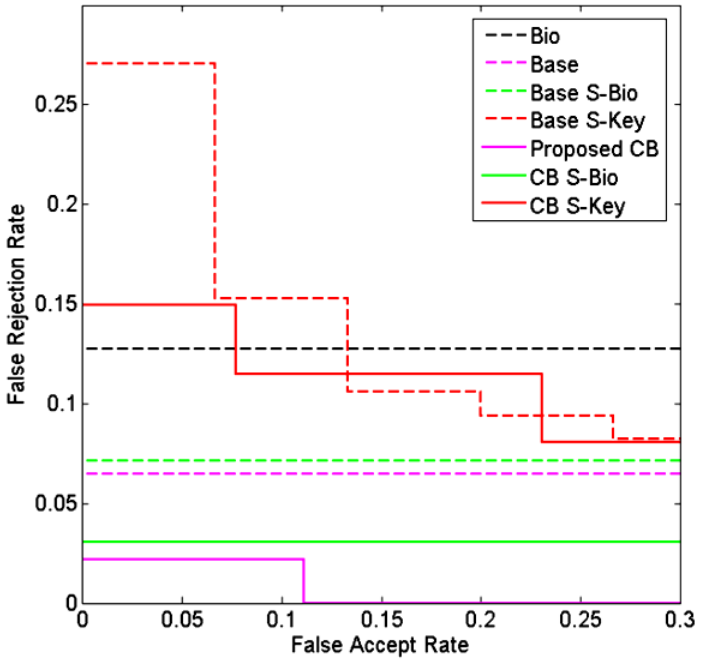


(b)

Figure 6.8 ROCs of Different Template Protection Algorithms in Multi-algorithm Approach on (PCA+DWT) Features from (a) CASIA-IrisV1 (b) CASIA-IrisV3-Interval



(a)



(b)

Figure 6.9 ROCs of Different Template Protection Algorithms in Multi-algorithm Approach on (ICA+DWT) Features from (a) CASIA-IrisV1 (b) CASIA-IrisV3-Interval

6.5.4 Cancelable Multibiometrics: Multimodal Approach

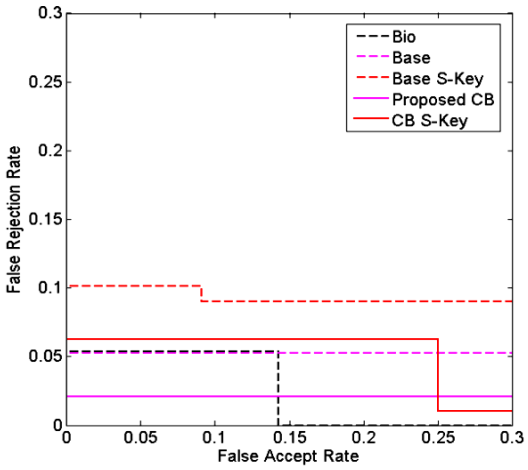
In this experiment, the multibiometric system is based on fingerprint and iris modalities and, the modalities are fused in feature level. The fingerprint features (FP) are taken from the experiment conducted in Section 6.5.2 and the iris features from the experiment conducted in Section 6.5.1. The iris features extracted using three feature extraction methods *viz*. PCA, ICA and DWT over CASIA-IrisV3-Interval datasets are employed in this experiment. The multibiometric templates are transformed into cancelable multibiometrics using Algorithm 6.2. Then, the cancelable multibiometrics are classified by using SVM with RBF kernel. The performance of the proposed cancelable multibiometric (CMB) is compared with the base BioHashing method described in Section 6.3 and the simple multibiometric system (Bio), in terms of Equal Error Rate (EER), False Rejection Rate (FRR) at zero False Accept Rate (FAR) and Running time (RT) in sec. and the results are tabulated in Table 6.4. The evaluation is also extended with stolen-key (S-Key) scenarios. Figure 6.10 shows ROC plots that show the performance of the proposed CMB in multibiometric systems.

Table 6.4 shows that the proposed CMB achieves the best result with 0.02 EER and 0.02 FRR at zero FAR whereas base BioHashing achieves 0.0526 EER and 0.0526 FRR at zero FAR for multibiometric (FP + PCA) system. For the same system, the proposed CMB achieves 0.0625 EER and 0.0625 FRR at zero FAR at stolen-key (S-Key) scenario whereas base BioHashing achieves 0.0909 EER and 0.1011 FRR at zero FAR at the same scenario and so on. From the experimental results, it is also found that the proposed CMB outperforms the base BioHashing in all scenarios.

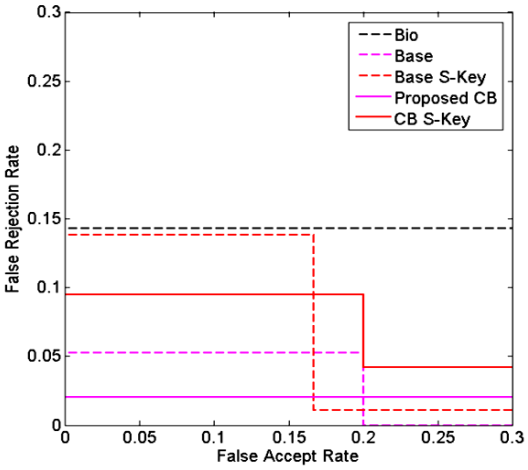
Table 6.4 Performances of Cancelable Multibiometrics: Multimodal Approach

Multibiometrics	Algorithm	EER	FRR at FAR=0	RT (in sec)
FP + Iris (PCA)	Bio	0.5376	0.5376	**0.2148**
	Base	0.0526	0.0526	0.2231
	Base S-Key	0.0909	0.1011	0.2326
	Proposed CB	**0.0200**	**0.0200**	0.2451
	CB S-Key	0.0625	0.0625	0.2530
FP + Iris (ICA)	Bio	0.1400	0.1429	0.2210
	Base	0.5263	0.5263	0.2484
	Base S-Key	0.1383	0.1383	0.2190
	Proposed CB	0.0204	0.0204	0.2518
	CB S-Key	0.0947	0.0947	0.2274
FP + Iris (DWT)	Bio	0.1489	0.1489	0.2301
	Base	0.0778	0.0778	0.2290
	Base S-Key	0.1263	0.1263	0.2283
	Proposed CB	0.0208	0.0208	0.2389
	CB S-Key	0.0895	0.1236	0.2353

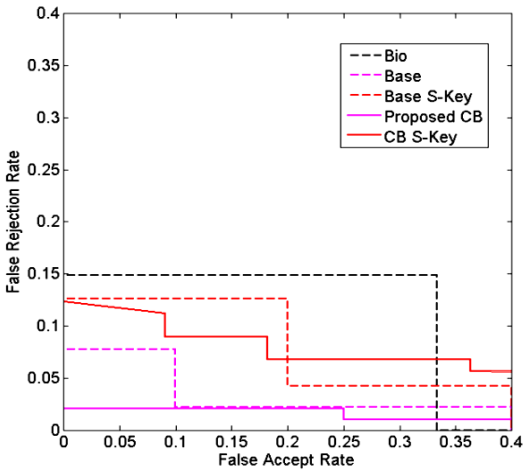
A summary of the performance of the proposed CB in biometric and multibiometric systems in terms of EER is tabulated in Table 6.5 and is graphically represented in Figure 6.11. From the table, it is found that the proposed CB attains its best performances with the values of 0.0421 EER and 0.0978 FRR at zero FAR with Iris (ICA over CASIA-IrisV3-Interval) and Iris (PCA over CASIA-IrisV3-Interval) respectively among the biometric systems. Among multibiometric systems, M2 and M7 show the best performance of 0.02 EER and, M5 attains 0.0404 FRR at zero FAR. It is also observed that



(a)



(b)



(c)

Figure 6.10 ROCs of Different Template Protection Algorithms in Multi-Modal Approach (a) FP + PCA (b) FP + ICA (c) FP + DWT

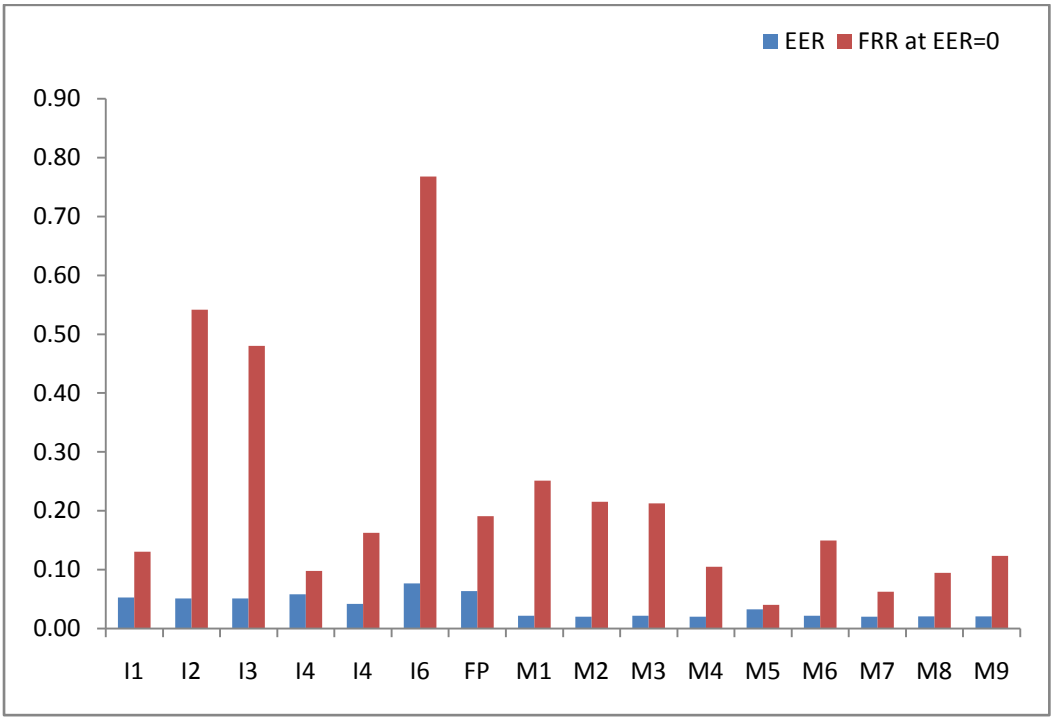


Figure 6.11 Performance Summary of the Proposed Cancelable Multibiometrics

Table 6.5 Performance Summary of the Proposed Cancelable Multibiometrics

	Biometric System	Code	EER	FRR at FAR=0
Biometric	Iris (PCA over CASIA-IrisV1)	I1	0.0529	0.1304
	Iris (ICA over CASIA-IrisV1)	I2	0.0510	0.5417
	Iris (DWT over CASIA-IrisV1)	I3	0.0512	0.4800
	Iris (PCA over CASIA-IrisV3-Interval)	I4	0.0580	0.0978
	Iris (ICA over CASIA-IrisV3-Interval)	I5	0.0421	0.1628
	Iris (DWT over CASIA-IrisV3-Interval)	I6	0.0769	0.7679
	Fingerprint	FP	0.0638	0.1910
Multibiometric	Multibiometric (I1 + I2)	M1	0.0220	0.2512
	Multibiometric (I1 + I3)	M2	**0.0200**	0.2156
	Multibiometric (I2 + I3)	M3	0.0219	0.2125
	Multibiometric (I4 + I5)	M4	0.0202	0.1047
	Multibiometric (I4 + I6)	M5	0.0326	**0.0404**
	Multibiometric (I5 + I6)	M6	0.0219	0.1494
	Multibiometric (FP + I4)	M7	**0.0200**	0.0625
	Multibiometric (FP + I5)	M8	0.0204	0.0947
	Multibiometric (FP + I6)	M9	0.0208	0.1236

6.6 Chapter Summary

In this chapter, biometric template protection methods mainly cancelable biometrics and BioHashing are discussed. A new approach to cancelable multibiometric based on BioHashing is proposed and is tested with biometric systems including iris recognition system and fingerprint recognition system. Iris recognition system is based on PCA, ICA and DWT feature extraction methods and, CASIA-IrisV1 and CASIA-IrisV3-Interval databases are employed. FVC2004 DB3 dataset is employed in fingerprint feature extraction. In multibiometric systems, the iris and fingerprint templates are concatenated. The proposed cancelable biometric is employed to transform the unibiometric and multibiometric template and the transformed cancelable templates are classified using SVM with RBF Kernel. The performance of the proposed CMB is compared with the base BioHashing method at best, stolen-key (S-Key) and stolen-biometric (S-Bio) scenarios. From the experimental results, it is observed that the proposed CMB outperforms base BioHashing method in terms of EER and FRR and is a promising approach for biometric template protection.

In the next chapter, the overall summary of the investigation with future scope is presented.