symmetry

MDPI

Article

A New Design for Alignment-Free Chaffed Cancelable Iris Key Binding Scheme

Tong-Yuen Chai [1,*], Bok-Min Goi [1], Yong-Haur Tay [1] and Zhe Jin [2]

[1] Lee Kong Chian Faculty of Engineering Science, Universiti Tunku Abdul Rahman, Bandar Sg. Long, Kajang 43000, Malaysia; goibm@utar.edu.my (B.-M.G.); tayyh@utar.edu.my (Y.-H.T.)

[2] School of Information Technology, Advanced Engineering Platform, Monash University, Subang Jaya 47500, Malaysia; jin.zhe@monash.edu

* Correspondence: chaity@utar.edu.my; Tel.: +60-17-500-9917

Received: 18 December 2018; Accepted: 22 January 2019; Published: 1 February 2019

Abstract: Iris has been found to be unique and consistent over time despite its random nature. Unprotected biometric (iris) template raises concerns in security and privacy, as numerous large-scale iris recognition projects have been deployed worldwide—for instance, susceptibility to attacks, cumbersome renewability, and cross-matching. Template protection schemes from biometric cryptosystems and cancelable biometrics are expected to restore the confidence in biometrics regarding data privacy, given the great advancement in recent years. However, a majority of the biometric template protection schemes have uncertainties in guaranteeing criteria such as unlinkability, irreversibility, and revocability, while maintaining significant performance. Fuzzy commitment, a theoretically secure biometric key binding scheme, is vulnerable due to the inherent dependency of the biometric features and its reliance on error correction code (ECC). In this paper, an alignment-free and cancelable iris key binding scheme without ECC is proposed. The proposed system protects the binary biometric data, i.e., IrisCodes, from security and privacy attacks through a strong and size varying non-invertible cancelable transform. The proposed scheme provides flexibility in system storage and authentication speed via controllable hashed code length. We also proposed a fast key regeneration without either re-enrollment or constant storage of seeds. The experimental results and security analysis show the validity of the proposed scheme.

Keywords: cancelable template; iris key binding; indistinguishability; key retrieval; template protection

1. Introduction

Biometric technology, particularly biometric authentication, has been implemented widely in many applications. This refers to individual verification based on their behavioral and physiological characteristics, such iris, fingerprint, facial features, retina, voice, gait, palm-prints, handwritten signatures, and hand geometry. Among other biometrics, iris provides high confidence in the recognition of an individual's identity. The interest in iris comes mainly from its non-contact feasibility and predominantly phenotypic chaotic texture that is unique and stable over a lifetime [1].

With the successful deployment of larger-scale iris recognition systems at the airports and hospitals [2], many concerns have been raised. Biometric applications are often considered unsecure due to the misuse of biometric data and identity management [3]. This concern is acceptable, as the compromised biometric traits will become useless in all the involved biometric applications.

Meanwhile, the practicality and the risk of key management on storage and release remain challenging in cryptography. A simple password is susceptible to dictionary attacks [4], while lengthy passwords are difficult to remember and maintain. The security of generic cryptographic systems is weak due to practicality and nonrepudiation, as the password is not directly tied to a user, thus it is unable to differentiate a legitimate user from an attacker. The limitations of traditional cryptographic key management incorporating passwords can be meliorated by biometric authentication. However, it is still vulnerable, as biometric data can be intercepted, stolen, altered, and replayed. This causes an invasion of identity privacy when unauthorized parties can get access through various attacks such as spoofing, replay attacks, and masquerade attacks [5]. These attacks affect user confidence and lead to a lack of acceptance in biometric technology.

Apparently, encryption of the biometric templates seems to be the solution to this problem. However, cryptography does not tolerate single bit error, but hashed versions of the same users can be different due to the variability of biometric samples. The idea to bind biometrics with cryptographic keys then paves an alternative in managing cryptographic keys and template protection [6]. Biometric template protection is normally categorized into Biometric Cryptosystem (BCS) and Cancelable Biometric (CB). These schemes are designed to fulfill irreversibility, cancelability, and unlinkability for data privacy's preservation.

The main concept of BCS is to securely bind a digital key to a biometric (key binding), or extract a key from the biometric (key generation) to ensure that it must be computationally difficult to retrieve either the key or the biometric from the stored template, which is also known as the "helper data" [7]. The key will be retrieved only if the query template contains sufficient similarity during authentication. BCS will store the biometric-dependent helper data instead of the cryptographic key. All of these properties of BCSs offer substantial security benefits to biometrics [8]. For key generation, keys can be generated directly from the helper data and a given query biometric template. These schemes are also known as fuzzy extractors or secure sketch, as defined in [9,10]. The difficulty in realizing key generation schemes is the high intra-user variability in biometrics that causes contradiction in achieving high key entropy and stability in authentication [7]. The fact that the original design is not catered for cancelability and unlinkability also makes this approach less popular compared to the key binding approach.

On the other hand, helper data is generated by binding a cryptographic key to a biometric template. Therefore, helper data is actually the fusion of the cryptographic key and biometric template. Fuzzy commitment [6] and fuzzy vault [11] are two important schemes designed for using the key binding approach. These schemes usually apply Error Correction Code (ECC) to deal with the variance of biometric data in authentication. The independently generated cryptographic key is revocable, but re-enrollment is required whenever an update of the key is necessary. Despite the security properties and stability of this approach, there are several drawbacks and vulnerabilities, which are discussed further in Section 2.

Cancelable biometrics is another method for biometric template protection involving repeated efforts to distort the biometric template through transformation. Authentication can then be conducted in the transformed domain [12]. The transformed templates are irreversible and never decrypted to ensure that the security and privacy of the biometric template are protected. Thus, it is more secure to store the transformed template instead of the original biometric template [13]. New templates can always be regenerated through transformations for compromised cases. There are four important criteria to be fulfilled for the design of the cancelable biometrics scheme:

1. Unlinkability: The protected biometric templates from the same subject should not be differentiable to prevent cross-matching across various applications.
2. Revocability: It should be computationally infeasible to derive its original data from multiple protected templates.
3. Non-invertibility: It should be computationally infeasible to derive its original biometric data from the protected template and/or the helper data.
4. Performance: The accuracy of the cancelable template in recognition performance must be approximately preserved with respect to its original counterparts without the template protection scheme.

While both BCS and CB fulfill the requirement of biometric template protection, there are still remaining issues and drawbacks being raised in terms of security, privacy, and performance. Besides that, BCSs provides an alternative to protecting the secret key in cryptographic applications. In this paper, a new iris key binding scheme is proposed, bridging the gap between biometric cryptosystems and cancelable biometrics. In other words, the proposed scheme aims to leverage these two main approaches while overcoming their respective limitations.

The paper is organized as follows. Previous work related to iris key binding schemes and cancelable iris templates is described in Section 2. Motivation and contribution are also explained under Section 2. The presentation of our proposed iris key binding scheme and its implementation are shown in Section 3. The experimental results, security, and privacy analysis are provided in Sections 4 and 5. Finally, concluding remarks are given in Section 6.

2. Related Work

2.1. Fuzzy Commitment

Juels and Wattenberg [6] introduced the fuzzy commitment scheme by combining knowledge from the area of Error Correction Codes (ECC) and cryptography to protect the cryptography key. The fuzzy commitment scheme has a function F, which is used to commit a codeword $c \in C$ and a witness $w \in \{0,1\}^n$. The witness is the enrolled biometric template represented by n-bits binary string, while C is a set of error correcting codewords c of length n. The difference vector of w and $c, \delta \in \{0,1\}^n$ can be obtained through bit-wise XOR operation: $\delta = c \oplus w$. The δ is denoted as the helper data, which will be stored together with $h(c)$ into the database where $h(.)$ is the hash function. The commitment is termed $F(c, w)$. Given a query biometric template w', a corrupted codeword c' can be reconstructed through $c' = \delta \oplus w'$ using the stored helper data. At the authentication stage, if the query binary string is sufficiently similar to the enrolled template within the capability of the ECC, a hash of the result will be tested against $h(c)$ where a successful authentication yields if $h(c') = h(c)$.

The first application of the fuzzy commitment scheme to iris codes was implemented by Hao et al. [14]. Hadamard and Reed-Solomon error correction codes were used in their scheme to bind 2048-bit iris codes into 140-bit cryptographic keys. The main idea was to apply Hadamard codes to eliminate bit errors caused by the natural variance such as background errors while burst errors were corrected by Reed-Solomon codes. The Genuine Acceptance Rate (GAR) of 99.53% and zero False Acceptance Rate (FAR) are reported in an in-house dataset. Two-dimensional iterative min-sum decoding was then introduced [15] for the iris-based fuzzy commitment scheme with higher correction capacity and efficiency. This was because a high False Rejection Rate (FRR) was discovered on a noisy channel using the Reed-Solomon code. Instead, two different Reed-Muller codes were used to form a matrix for efficient decoding. This approach achieved a GAR of 94.38% and a zero FAR on the ICE 2005 iris database [16] with 40 bits of bound keys. A context-based approach which constructs keys based on reliable bits within the iris codes bound by BCH-code is proposed in [17]. User-specific masks and check bits were used to form the helper data. A variety of techniques focusing on biometric template protection, random bit-permutation, biometric feature binarization, and concatenated coding scheme were then proposed to improve the performance and security of the iris fuzzy commitment schemes, see [18–21] for examples.

Ideally, fuzzy commitment is proven secure under the random oracle model, hence, helper data contains no information about the secret. In other words, the secret is expected to be uniformly and independently distributed where an adversary can only perform brute force attacks. However, practically speaking, this is hard to achieve due to the inherent structure of the biometric data and the correlation between features [22]. Privacy leakage is another concern in fuzzy commitment caused by the redundancy in an ECC, which is unavoidable [22]. Cross matching can happen if large privacy leakage is discovered. There are several attacks, such as decodability attacks [19], statistical attacks [23], and attack via record multiplicity (ARM) [24].

Kelkboom et al. [19] proposed a bit-permutation process for the fuzzy commitment scheme to prevent it from a decodability attack that exploits the correlation of the multiple helper data generated from the biometric data of a same subject. The decodability attack was first initiated by Carter and Stoinov [25] to verify the possibility of whether decoding two helper data leads to a valid codeword. When there are two helper data $\delta_1, \ \delta_2$ being generated by two biometric data from the same subject, $w_1, \ w_2$, in a decommitment process, the attacker can leverage the helper data by performing $\delta_1 \oplus \delta_2 = (w_1 \oplus w_2) \oplus (c_1 \oplus c_2)$, which equates to $\delta_1 \oplus \delta_2 = (w_1 \oplus w_2) \oplus c$. If the two helper data are derived from the same subject, $w_1 \oplus w_2$ is small and the outcome will be most likely close to the correct codeword. In short, the bit-permutation mechanism helps to improve the security through distribution of entropy across biometric feature vectors.

Rathgeb et al. [23] presented a statistical attack against the iris fuzzy commitment scheme. Binary biometric feature vectors of an impostor are randomly chosen, and decommitment is performed successively with the stored helper data, assuming that attackers are knowledgeable about the applied ECC. The frequency of each possible codeword is collected, and a corresponding histogram is generated for each chunk. The ECC based histograms of all the chunks can be analyzed after repeating the chunk-based decommitment processes using an adequate amount of imposter templates. The most likely error correction codeword for a chunk can be decided based on the bin, which corresponds to the histogram maximum.

Scheirer and Boult [24] launched an attack via record multiplicity on the fuzzy vault. This refers to an imposter in possession of multiple invocations of the same secret, which are combined to reconstruct secrets that lead to the retrieval of biometric templates. The introduced attack on the fuzzy vault, namely Surreptitious Key-Inversion (SKI), is an equivalent attack against fuzzy commitment. Under this attack, the biometric string blended with the codeword can be recovered through XOR operation using the compromised cryptographic key (secret) and the secure sketch.

Privacy and security leakages of fuzzy commitment schemes are investigated in [26] for several biometric data statistics. The scheme is found to leak information in bound keys and non-uniform templates. For instance, keys bound of 44 bits in fuzzy commitment schemes [14] suffer from low entropy, reducing the complexity for brute force attacks [20]. Zhou et al. [22] conducted a quantitative assessment on the privacy and security leakage of the fuzzy commitment scheme. Biometric data are not uniformly and independently distributed, which further contributes to the security issue. Several evaluation metrics were proposed to conclude that fuzzy commitment is highly vulnerable due to the inherent dependency on the biometric features. Apart from that, fuzzy commitment is often bounded by the limitations introduced by ECC. The scheme was found to be affected by the tradeoff between security and performance [27]. Similar perspective is reported by Bringer et al. [15], where the decoding accuracy and maximum key length are bounded by the error correction capacity of the adopted ECC. Besides, another limitation comes from the design of the fuzzy commitment scheme in terms of input representation and matching [9]. The input feature to fuzzy commitment is restricted to binary representation in order to conduct matching in the hamming domain. This hinders the scheme from achieving better performance since many effective feature extraction and matching techniques do not comply with this requirement. Considering the discussed attacks and limitations, the security and privacy provided by iris-based fuzzy commitment is doubtable.

2.2. Fuzzy Vault

Another design that provides protection and error-tolerant verification is the fuzzy vault scheme that was introduced by Juels et al. [11]. The first implementation of a fuzzy vault scheme on iris was presented in [28]. In this method, independent component analysis (ICA) was employed to extract important coefficients from multiple local regions in an iris image. The K-mean based pattern clustering method aimed to solve the variance of the extracted iris features, while ICA created unordered sets for fuzzy vault. On a challenging CASIAv3-Interval iris database [29], a GAR of 80% was achieved at a zero FAR employing 128 bit keys. Reddy et al. [30] hardened the fuzzy vault using the user’s password to prevent from attacks via record multiplicity. Iris features were extracted from minutiae-like coordinates obtained through image enhancement steps. At zero FAR, a degradation of 2% to 90% GAR was reported for CASIAv1 [31] and the MMU iris database [32] when the degree of polynomial was set to seven or eight. More proposals on iris vaults [33,34] omitted a detailed explanation about iris feature encoding or protocols. The majority of the proposed approaches to biometric cryptosystem lack a thorough security analysis, for example, larger entropy loss can be possible, especially for neighboring bits dependencies, and this can reduce the security all the way to 40 bits [14].

The implementations of the fuzzy vault scheme by Juels and Sudan [11] in biometrics exposed its vulnerability to correlation attacks and linkage attacks [24,35]. This conflicts with the unlinkability and irreversibility requirements defined for biometric template protection. The basic idea of fuzzy vault fingerprint systems to include auxiliary data was to help alignment issues affected by translation, rotation, and non-linear distortion. However, the attacker can make use of the publicly unprotected auxiliary alignment data in performing linkage attacks. An implementation for absolute fingerprint pre-alignment that resists any correlation between related records of the fuzzy vault scheme was proposed as the countermeasure [36]. In designing an effective fuzzy vault-based cryptosystem, a practical decoding strategy is important. The error correcting capacity of the Reed-Solomon decoder in the original fuzzy vault is insufficient to achieve practical implementation for biometrics, especially single finger. To overcome this, the Lagrange-based decoder [37] was proposed, but the decoding complexity would then become infeasible for implementation.

2.3. Cancelable Biometrics

Ratha et al. [12] were the first to introduce cancelable biometrics. They applied a smooth but non-invertible surface folding transformation to preserve the accuracy performance. The proposed scheme preserved the change in minutiae position after the transformation while introducing many-to-one mapping for non-invertibility. Despite the satisfactory accuracy performance that was reported, the non-invertibility was found vulnerable [38]. Since then, this work has inspired more research works into biometric template protection. In short, cancelable biometrics can be categorized into biometric salting and non-invertible transformation.

Any invertible transform of a biometric template can be referred to as biometric salting, even if the extraction is applied in a way that it is not feasible to reconstruct the original biometric template [39]. Independent auxiliary data such as user specific token are blended with the biometric data to form a distorted version of the original template. Chong et al. [40] proposed S-IrisCode encoding, which combines two authentication factors, iris feature and tokenized pseudo-random number via iterated inner-product and thresholding, to produce a set of cancelable binary codes per person. Noise mask is developed to eliminate the weaker inner-product and improve the accuracy in matching.

Another salting method by Zuo et al. [41] can be applied to either real-valued (GRAY-SALT) or binary (BIN-SALT) iris data. For GRAY-SALT, the real-valued iris data and a random pattern are combined pixel-wise through addition or multiplication. Similar techniques can be applied to the binary iris code using XOR operation for BIN-SALT. In this case, the original iris pattern is concealed and cancelable iris template can be realized by replacing the auxiliary data. However, deterioration of accuracy performance is inevitable without the pre-alignment process. Another idea to achieve cancelable iris biometric is based on sectored random projections [42]. In this method, an unwrapped iris image is first divided into different sectors where random projections will be applied on each sector separately via user specific random Gaussian matrix. The random matrices will then be concatenated to form the cancelable template. The sectored based strategy not only limits the effect of noise but also reduces the size of useful information. New templates can be generated by using different random projection matrices if the existing one is compromised. However, further research [43,44] found that the accuracy performance degraded if the same random matrix was applied to different users. Moreover, the cancelable template is likely to be inverted when the user-specific random matrices are disclosed.

In short, biometric salting is feasible for cancelable biometrics if and only if the auxiliary data is kept secret.

Non-invertible transformation is a one way transformation function that can be implemented on the iris template to achieve non-invertibility so that the transformed template can be stored securely in the database [7]. Zuo et al. [41] provided two methods to ensure that the transforms are non-invertible and revocable. GRAY-COMBO and BIN-COMBO can be applied on the unwrapped iris image and binary iris codes, respectively. For GRAY-COMBO, rows are shifted circularly in a horizontal direction using random offsets. Then, two randomly selected rows are combined via addition or multiplication operation. A similar transform is adopted by BIN-COMBO, but the combination is changed to XOR or XNOR. The non-invertibility criterion is achieved through the distortion caused by data shifting. The shifting is always shifted in same orientation, hence no alignment is necessary for matching. Performance degradation is experienced due to the decrease in the valid iris area and occlusions. Nonetheless, this transformation shares the same risk as the salting approach, where stolen-token can happen since they use user-specific key.

A block remapping method was proposed by Hammerle-Uhl et al. [45] to perform non-invertible transformation. The iris image is first normalized and partitioned into image blocks. Then, random permutation is applied to the each block, followed by the image remapping technique. The random and repeated remapping process prevents the reconstruction of the original iris image. Although the non-invertibility criterion was fulfilled through the block remapping process, Jenisch et al. [46] demonstrated that 60% of the original iris image could be reconstructed from the stolen template.

Ouda et al. [47] proposed a cancelable biometrics scheme—BioEncoding—without user-specific keys or tokens. The consistent bits, $w \in \{1,0\}^n$ where n denotes the length of the bit vector, are first determined from a series of iris codes of each user. This allows the elimination of bits with a higher probability to flip within several iris samples of the same individual. The positions of all consistent bits are stored. The bit vector is grouped n/m into m binary codewords and each codeword is mapped to a single bit value generated by a random sequence S of length $l = 2^m$. The mapped binary bit values are then used to construct the final BioCode according to their associated positions. For the non-invertibility requirement, the many-to-one nature of the mapping guarantees its irreversibility. To improve the scheme's resistance against correlation attacks, the original biometric template could be permuted or XORed with a different random sequence of the same length before applying BioEncoding transformation. However, Lacharme [48] pointed out that restoration was feasible if the Boolean function used to generate the random sequence was discovered.

An alignment-free cancelable iris biometrics based on adaptive Bloom filters was introduced by Rathgeb et al. [49]. Bloom filter-based representations of biometric templates such as iris codes enable an efficient alignment-invariant biometric comparison at matching stages. Besides, the many-to-one mapping of biometric features to a Bloom filter is non-invertible. For cancelable template refreshment, they applied an application-specific secret key—for example, seed values—to fulfill the unlinkability criterion. The accuracy performance of Bloom filter was comparable to its original counterparts. However, restoration of the biometric template was reported successful with low complexity of 2^{25} [50]. This was followed by possible unlinkability attacks where two Bloom filters generated from the same iris codes were identified with high probability when smaller key space was used to preserve the accuracy performance [51]. Recent work from Gomez-Barrero et al. [52] suggested an alternative to preventing cross-matching attacks in Bloom filter-based template protection schemes. Cancelable biometrics generation based on randomized look-up table mapping was initiated by Dwivedi et al. [53]. Rotation invariant iris templates are first selected based on the minimum hamming distance. The row vector is then divided into l groups of m bits binary codewords. The corresponding decimal values for all the groups are encoded through a look-up table with m randomly generated bits for all possible decimal values ranging from 0 to $2^m - 1$. The newly mapped binary codeword becomes the final cancelable template. The iris codes are at risk with information about block size and m being stolen, since look-up table and cancelable templates are stored in the database as well. The author emphasized the need to further secure the look-up table generation for stolen-token scenarios. Recent work from Umer et al. [54] demonstrated a feature learning method for a cancelable iris recognition system. Among other feature representations, a sparse representation coding technique showed better discriminability, employing a multi-class linear support vector machine (SVM) classifier. The existing BioHashing scheme is applied and extended by using two tokens, which are subject specific and subject independent, respectively. Despite the flexibility in template renewal, no in-depth security analysis was discussed regarding the proposed scheme.

Our proposed scheme incorporated Bloom filter [49] and Indexing First One hashing (IFO) [55] for the purpose of alignment-free biometric template generation, as explained in our recent work [56]. Thus, a brief introduction about IFO and Bloom filter are given to facilitate the understanding of our proposed scheme in the methodology section. For a detailed explanation of these two techniques, the reader is referred to [49,55].

In order to resolve the head rotation issues in IrisCode, the Bloom filter technique [49] can be adopted to transform the original IrisCode $\boldsymbol{I} \in \{0,1\}^{n_1\times n_2}$ into an alignment-free binary matrix named Bloom filtered IrisCode, $\boldsymbol{B}$ through Bloom_filter $(W,\ L,\ \boldsymbol{I})$. Suppose we define W and L as the number of columns and rows, respectively. The matrix of IrisCode is first split into $l_1 \cdot\ l_2$ blocks with a size $L \times W$ each, where $l_1 = \frac{n_1}{L}$ and $l_2 = \frac{n_2}{W}$. Each block constitutes the formation of a Bloom filter with values within $b \in \{0,1\}^{2^L}$. All elements of b are initially zeros and element '1' is added to b based on the decimal position calculated from the column codeword, $x_j \in \{1,0\}^L \Big| j = 1,2,\ldots,W$ in each block. In the scenario where the same x_j is being mapped multiple times within a Bloom filter, b thus results in a many-to-one mapping and loss of information. Hence, the reconstruction of the original IrisCode can be prevented with this feature of non-invertibility. The collection of every Bloom filter b_i of each block (for $i = 1,2,\ldots,l_1{\cdot}l_2$) in an input matrix constitutes the final matrix of Bloom filtered IrisCode, $\boldsymbol{B} \in \{0,\ 1\}^{l_1\cdot l_2\times 2^L}$.

IFO hashing scheme [55] is adopted to achieve cancelable template protection and flexibility in system storage. First, any arbitrary binary input of IrisCode with a dimension $n_1 \times n_2$ is permuted with p number of random permutation sequences in a column-wise manner. All the randomly permuted IrisCodes are multiplied to generate a p-ordered Hadamard product code. Utilizing the concept of min-hashing, select the first '1' among the first κ elements for each row of the product code. The index value of the first occurrence of '1' is then recorded. The concept is further extended by imposing a modulo thresholding function. The imposed security threshold value τ can be used to regulate the security leakage while inducing a many-to-one mapping in strengthening the non-invertibility properties of this scheme. An $n_1 \times m$ matrix of IFO hashed codes $\boldsymbol{C} \in \mathbb{Z}_{\kappa-\tau}^{n_1\times m}$ is obtained by repeating these steps with m independent hash functions.

2.4. Motivation and Contribution

As highlighted in the previous section, there are limitations in both biometric cryptosystems and cancelable biometrics. ECC is often limited by its error correcting capacity and feasibility when it comes to practical implementation in biometrics. It is susceptible to attacks such as statistical attacks and trade-offs between performance and security. The performance of biometrics such as iris and fingerprint are always affected by an alignment issue, and the processes to reduce this effect are often tedious and time consuming.

The proposed design is leveraging on both biometric systems to tackle this open problem. In this paper, we proposed an alignment free iris key binding scheme with cancelable transform without depending on ECC. This idea is another approach based on chaffing and winnowing similar to Jin's approach [57]. This concept is often used in cryptology for data encryption when transferring through an insecure channel where direct application to biometrics is inappropriate due to the randomness and variability nature of the data. Our work adopted IFO hashing to achieve non-invertible and cancelable transformation for biometrics and the cryptographic key binding process under the proposed scheme. The contributions of this work are presented as follows:

Key regeneration: A new formulation to measure the success rate for key retrieval under genuine query is proposed and defined as Key Retrieval Rate (*KRR*). Thorough analysis was conducted to prove that *KRR* is in relation to Jaccard similarity. We demonstrated the calculation of *KRR* under certain configurations and its implementation in security analysis for indistinguishability game as well as false accept attacks.

Cancelability and renewal: A fast and simple method for key renewal is proposed. The proposed method requires neither re-enrollment of biometrics nor constant storage for seeds. This can be achieved by reshuffling the hashing functions randomly.

Security analysis: We performed in-depth analysis on the indistinguishability between synthetic and genuine biometric templates under the proposed scheme. The adversary's advantages in distinguishing the genuine and synthetic templates were evaluated through our proposed indistinguishability game. Besides that, potential brute force attacks and false accept attacks were investigated in detail.

Feature representation and *storage*: In this non-hierarchical key binding design, biometric template size and key length have critical effects on the storage space and computation power. The proposed format for biometric template in [57] is not directly applicable for all types of biometrics, especially iris. Thus, we induced the scheme with more flexibility through tuneable storage. This is achievable via controllable hash code length.

Performance discrepancy: The key binding approach in [57] reported FAR more than zero in their implementation on fingerprint. This implies the potential of this scheme to be compromised through FAR related attacks. This can lead to significant reduction in security and severe privacy leakage. Thus, there is a need to conduct in-depth analysis on security and privacy leakage to understand the full potential and the bottleneck of the chaffing and winnowing based key binding scheme.

3. Methodology

Our proposed scheme is based on the Chaffing and Winnowing concept in cryptosystem [58]. The idea is to bind a random binary cryptographic key by using a set of protected iris templates named as "cancelable" iris templates. Particularly, given a random cryptographic key, which is represented in binary form, e.g., $[1, 0, 1, 1]$, the proposed method enables the binding of different cancelable iris templates according to a randomly generated sequence of '1' and '0'. As a result, a cryptographic key can now be represented by a sequence of cancelable templates, which can be stored into a database for future authentication.

For key regeneration process, the genuine cancelable template is matched and authenticated with the formerly stored cancelable templates. For every matched instance, it enables the regeneration of partial information of the bound cryptographic key. If a binary bit '1' represents an anticipated match, this outcome eventually allows the regeneration of the entire key (retrieval) when all the stored templates are authenticated successfully. The design of the proposed key binding scheme is illustrated in Figure 1 to give a clear overview for all the processes involved. The original iris template is Bloom filtered first, followed by IFO hashing before entering the proposed key binding scheme.

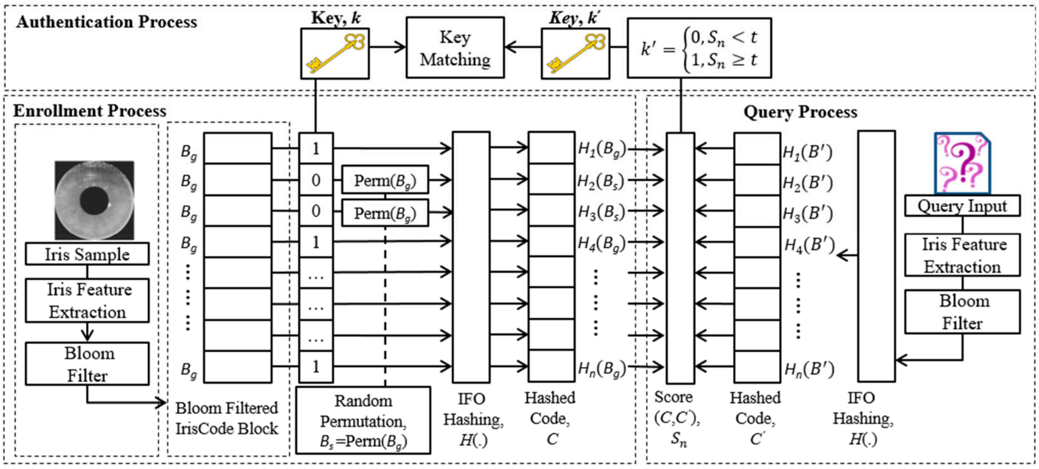


Figure 1. Overview of the design for the proposed key binding scheme.

3.1. Key Binding

To further explain the methodology of our proposed key binding scheme, let the input IrisCode denote $\boldsymbol{I}$, a random permutation function denotes Perm(.), and $\boldsymbol{B}_g$ is the Bloom filtered IrisCode. Our proposed key binding scheme can be divided into several steps:

1. Cryptographic key generation: A random binary cryptographic key $\boldsymbol{K} = \{k_j\}_{j=1}^{n}$ is generated where $k_j \in \{0,1\}$ and n is the input parameter determining the cryptographic key length.
2. Genuine and synthetic template generation: IrisCode $\boldsymbol{I}$ goes through feature transformation to generate a genuine iris template (Bloom filtered IrisCode) $\boldsymbol{B}_g$ while a synthetic iris template can be generated through permutation as $\boldsymbol{B}_s \leftarrow \text{Perm}\left(\boldsymbol{B}_g\right)$.
3. Key binding: Given a key, $\boldsymbol{K} \in \{0,1\}^n$, we can define n number of IFO hash groups $\{H_1, \ldots, H_n\}$. Each hash group H_j (for $j = 1 : n$) is used to generate the j-th IFO hashed code $\boldsymbol{C}_j$ based on the input matrix of either genuine or synthetic Bloom filtered IrisCode. For example, if $k_j = 1$, the j-th hashed code can be described as $\boldsymbol{C}_j \leftarrow H_j\left(\boldsymbol{B}_g\right)$, where $H_j\left(\boldsymbol{B}_g\right) = \left\{h_{i(j)}\left(\boldsymbol{B}_g\right)\middle| i = 1, \ \ldots, \ m \ hash \ functions\right\}$; otherwise (if $k_j = 0$), the j-th hashed code is described as $\boldsymbol{C}_j \leftarrow H_j(\boldsymbol{B}_s)$.
4. Hashed code generation: n number of hashed codes are constructed $[\boldsymbol{C}_1, \boldsymbol{C}_2, \ldots, \boldsymbol{C}_n]$ and stored in the database instead of the corresponding cryptographic key $\boldsymbol{K}$.
5. Storage: The collection of output IFO hashed codes $[\boldsymbol{C}_1, \boldsymbol{C}_2, \ldots, \boldsymbol{C}_n]$ are then stored together with the collection of IFO hash groups $\{H_1, \ldots, H_n\}$ used in the process of key binding.

The binary key binding processes of our proposed method are defined in Algorithm 1 as shown in Figure 2.

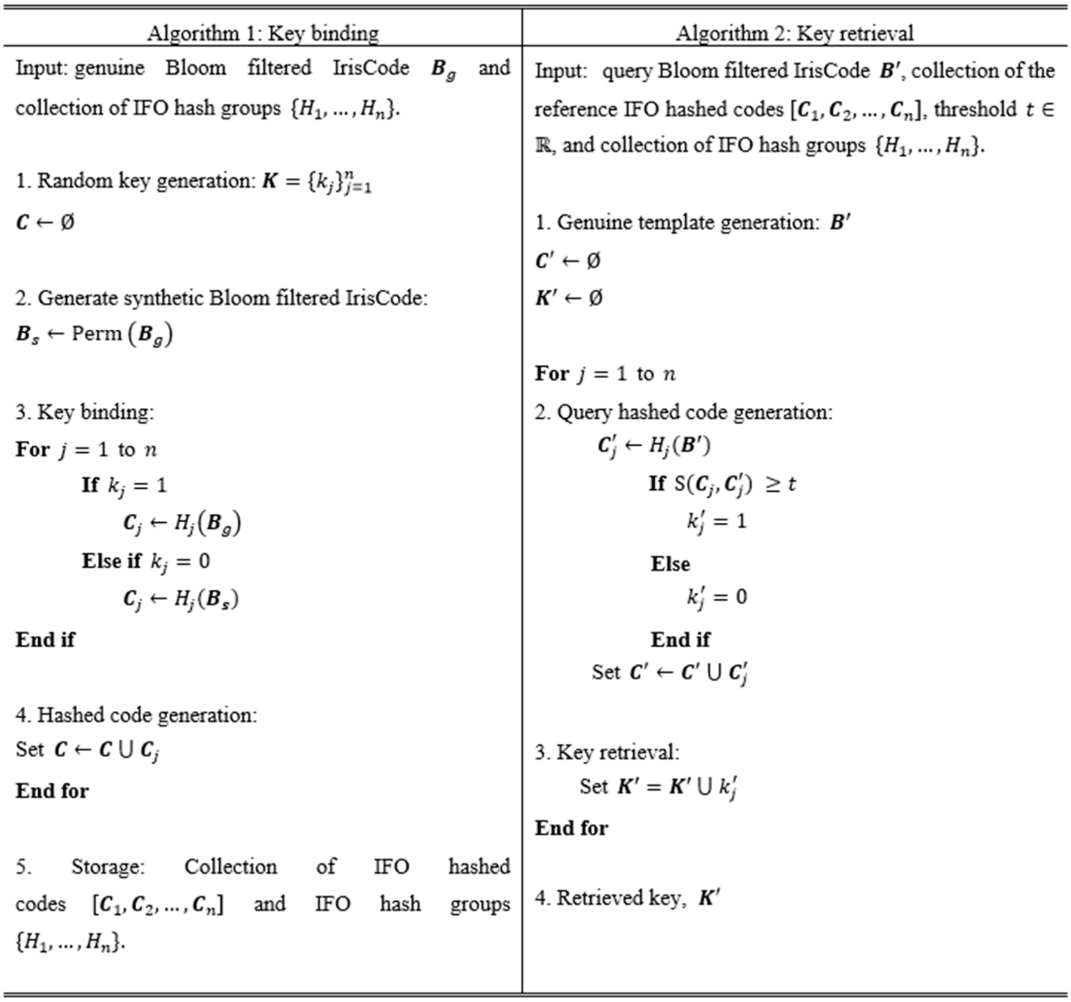
3.2. Key Retrieval

Let $S\left(\boldsymbol{C}, \boldsymbol{C}'\right)$ denote a matching score between a reference (stored) IFO hashed code $\boldsymbol{C}$ and a query hashed code $\boldsymbol{C}'$. Given a query IrisCode as the input denoted as $\boldsymbol{I}'$, our proposed key retrieval scheme can be divided into several steps as follows:

1. Genuine template generation: $\boldsymbol{I}'$ has to go through a similar transformation to first generate a query Bloom filtered IrisCode matrix, which can then be described as $\boldsymbol{B}' \leftarrow \text{Bloom\_filter}\left(W, \ L, \ \boldsymbol{I}'\right)$.
2. Query hashed code generation: By using the same IFO hash groups $[H_1(\boldsymbol{B}'), \ldots, H_n(\boldsymbol{B}')]$ with their respective permutations, n number of query hashed codes $\left[\boldsymbol{C}_1', \boldsymbol{C}_2', \ldots, \boldsymbol{C}_n'\right]$ can be generated.

3. Key retrieval: To prepare for key retrieval, we first generate an empty array denoted as $\boldsymbol{K}' = \{k_j{}'\}_{j=1}^{n}$ where $k_j{}' \in \{0,1\}$ and n is the cryptographic key length generated via the matching between the query and the reference hashed codes. Given any pre-defined threshold t, matching can be carried out by calculating the similarity score $\mathrm{S}(\boldsymbol{C}_j, \boldsymbol{C}'_j)$ between the reference hashed code $\boldsymbol{C}_j$ and the query hashed code $\boldsymbol{C}'_j$. If $\mathrm{S}(\boldsymbol{C}_j, \boldsymbol{C}'_j) \geq \mathrm{t}$, set $k_j{}' = 1$, otherwise, $k_j{}' = 0$.
4. Eventually, a final key $\boldsymbol{K}' = \{0,1\}^{\mathrm{n}}$ can be retrieved.

The matching score $S(\boldsymbol{C}_j, \boldsymbol{C}'_j)$ can be measured by finding the number of agreed positions between $\boldsymbol{C}_j$ and $\boldsymbol{C}'_j$, for example, $\frac{\text{No. of agreed positions}}{m\cdot\, l_1\cdot\, l_2}$. The whole process of key retrieval is outlined in Algorithm 2 as shown in Figure 2.



```
Algorithm 1: Key binding
Input: genuine Bloom filtered IrisCode $\boldsymbol{B}_g$ and collection of IFO hash groups $\{H_1, \dots, H_n\}$.

1. Random key generation: $\boldsymbol{K} = \{k_j\}_{j=1}^{n}$
$\boldsymbol{C} \leftarrow \emptyset$

2. Generate synthetic Bloom filtered IrisCode:
$\boldsymbol{B}_s \leftarrow \mathrm{Perm}(\boldsymbol{B}_g)$

3. Key binding:
For $j = 1$ to $n$
    If $k_j = 1$
        $\boldsymbol{C}_j \leftarrow H_j(\boldsymbol{B}_g)$
    Else if $k_j = 0$
        $\boldsymbol{C}_j \leftarrow H_j(\boldsymbol{B}_s)$
End if

4. Hashed code generation:
Set $\boldsymbol{C} \leftarrow \boldsymbol{C} \cup \boldsymbol{C}_j$
End for

5. Storage: Collection of IFO hashed codes $[\boldsymbol{C}_1, \boldsymbol{C}_2, \dots, \boldsymbol{C}_n]$ and IFO hash groups $\{H_1, \dots, H_n\}$.
```

```
Algorithm 2: Key retrieval
Input: query Bloom filtered IrisCode $\boldsymbol{B}'$, collection of the reference IFO hashed codes $[\boldsymbol{C}_1, \boldsymbol{C}_2, \dots, \boldsymbol{C}_n]$, threshold $t \in \mathbb{R}$, and collection of IFO hash groups $\{H_1, \dots, H_n\}$.

1. Genuine template generation: $\boldsymbol{B}'$
$\boldsymbol{C}' \leftarrow \emptyset$
$\boldsymbol{K}' \leftarrow \emptyset$

For $j = 1$ to $n$
2. Query hashed code generation:
    $\boldsymbol{C}'_j \leftarrow H_j(\boldsymbol{B}')$
        If $\mathrm{S}(\boldsymbol{C}_j, \boldsymbol{C}'_j) \geq t$
            $k'_j = 1$
        Else
            $k'_j = 0$
        End if
    Set $\boldsymbol{C}' \leftarrow \boldsymbol{C}' \cup \boldsymbol{C}'_j$

3. Key retrieval:
    Set $\boldsymbol{K}' = \boldsymbol{K}' \cup k'_j$
End for

4. Retrieved key, $\boldsymbol{K}'$
```

Figure 2. Algorithm 1: key binding process (**left**) and Algorithm 2: key retrieval process (**right**).

3.3. The Relation of Key Retrieval Rate to Jaccard Similarity

For an efficient biometric cryptosystem, it ensures the regeneration of an exact key given a similar (genuine) query Bloom filtered IrisCode during key retrieval. In our case, the success rate of the key retrieval attempt under genuine query can be measured through our proposed key retrieval rate (*KRR*). In this section, we briefly discuss the relation of *KRR* to the Jaccard similarity between the enrolled and query Bloom filtered IrisCodes, which are denoted as $\mathrm{JA}(\boldsymbol{B}_g, \boldsymbol{B}')$. For the ease of understanding, given a threshold t, suppose that we are now considering only single binary bit, k'_j where $(j = 1)$ of a cryptographic key. Let us consider a single bit of the key as $k'_{j=1} \in \{0,1\}$, which is retrieved by matching a query hashed code $\boldsymbol{C}'_{j=1}$ against a reference hashed code $\boldsymbol{C}_{j=1}$. The correctness of the regenerated key $k'_{j=1}$ can be described as follows:

$$k'_{j=1} = \begin{cases} 1, & S\left(\boldsymbol{C}, \boldsymbol{C}'\right) \ \geq t \\ 0, & S\left(\boldsymbol{C}, \boldsymbol{C}'\right) \ < t \end{cases} . \tag{1}$$

Referring to the procedures under the IFO hashing scheme, hashing of Bloom filtered IrisCode $H_{j=1}\left(\boldsymbol{B}_g\right)$ is conducted through independently and randomly generated permutation seeds $\{\boldsymbol{N}_1, \ldots, \boldsymbol{N}_m\}_{j=1}$. Treating each bloom filter b_i as independent, the number of agreed positions (collisions) between query and reference hashed codes can be defined as $z = \sum_{i=1}^{m\cdot l_1\cdot\ l_2} \chi_i$, where χ_i refers to a Bernoulli variable of $X_i = 1$ (if $\boldsymbol{C}_{j=1} = \boldsymbol{C}'_{j=1}$) or $\chi_i = 0$ (if $\boldsymbol{C}_{j=1} \neq \boldsymbol{C}'_{j=1}$). Thus, each element of $\boldsymbol{C}_{j=1}/\boldsymbol{C}'_{j=1}$ can then be treated as independent to each other. The independency of different bloom filters can be further strengthened by applying different public random permutations on the bloom filters. Therefore, $z \sim \mathrm{B}(M, P)$ follows a binomial distribution of probability of success $P = S\left(\boldsymbol{B}_g, \boldsymbol{B}'\right)$, where $M = m\cdot l_1\cdot\ l_2$ denotes the total number of elements $\left\{c_{i=1}, \ldots, c_{i=m\cdot l_1\cdot\ l_2}\right\}_j$ in $\boldsymbol{C}_j/\boldsymbol{C}'_j$ (for $j = 1,\ 2, \ldots, n$). This probability provides a similarity measurement between $\boldsymbol{B}_g$ and $\boldsymbol{B}'$ through $S\left(\boldsymbol{B}_g, \boldsymbol{B}'\right)$.

Since the publicly known random permutations are merely applied to strengthen independency, we therefore highlight only the resultant effect on the independency of the bloom filters here. This helps to simplify the computation of the expected value $\mathbf{E}(z) = MP$. Particularly, referring to the convention of IFO as an instance of min hash [55], one has $P = \mathbb{P}\left[c_i = c'_i \middle| i = 1, 2, \ldots, M\right] = S\left(\boldsymbol{B}_g, \boldsymbol{B}'\right) = \mathrm{JA}\left(\boldsymbol{B}_g, \boldsymbol{B}'\right)$, which corresponds to the Jaccard similarity of $\boldsymbol{B}_g$ and $\boldsymbol{B}'$. Thus, we can infer that $S\left(\boldsymbol{C}_j, \boldsymbol{C}'_j\right) = \frac{z}{M}$, while the probability of success P is M dependent. Therefore, the *KRR* for a single binary bit cryptographic key can be described as the probability:

$$\begin{aligned} KRR &= \mathbb{P}\left(k'_{\mathrm{j}} = k_{\mathrm{j}}\right) \\ &= \mathbb{P}\left(S\left(\boldsymbol{C}_j, \boldsymbol{C}'_j\right) \geq t\right) \\ &= \mathbb{P}\left(\frac{1}{M}\ \sum_{i=1}^{M} \chi_i \geq t\right) = \mathbb{P}(z \geq tM). \end{aligned} \tag{2}$$

The definition of the probability in (2) can be further extended for longer key length with n^* denoted as the number of binary bit '1' (successful genuine matching) in a cryptography key. Thus, *KRR* can be redefined again as:

$$KRR = \mathbb{P}\left[k'_j = k_j = 1 \middle| j = 1, 2, \ldots, n\right] = \left(\mathbb{P}(z \geq tM)\right)^{n^*}. \tag{3}$$

Theoretically, $n^* \approx \frac{n}{2}$ is the approximation for maximum key entropy [59]. Nevertheless, one can easily notice from the equation that as long as the probability $\mathbb{P}(z \geq tM)$ comes close or equal to 1, n can be further increased. This allows the flexibility to bind even longer cryptographic keys in such a way that $KRR = (\approx 1)^{n^*} \approx 1$ maintains the optimum success rate for key retrieval. This implies that the exact cryptographic key can be retrieved as long as $\mathbb{P}(z \geq tM) \approx 1$ for a selected threshold t. The selection of t affects the *KRR* significantly in two ways: (1) Given a fixed value of P, decreasing the value of threshold t increases $\mathbb{P}(z \geq tM)$ as well as *KRR* and vice versa. In contrary, the failure rate of a genuine query can also be computed using our proposed method through *KRR*; (2) Lower *KRR* is expected from the equation if we increase the value of n^* further and vice versa. This is another highlight of *KRR* through its amplification factor contributed by n^*, which always ensures that an imposter query will have way lower *KRR* compared to a genuine query.

3.4. Example

For better illustration, we hereby give an example to calculate KRR under certain configurations. Suppose we set $M = 200$, $n = 40$ $n^* \approx 20$, and $t = 0.75$, given $\boldsymbol{B}_g$ and $\boldsymbol{B}\prime$ such that $P = S(\boldsymbol{B}_g, \boldsymbol{B}') = 0.85$ (e.g., 85% similar in terms of the Jaccard similarity between the enrolled and query iris templates), we can then calculate the $KRR = (\mathbb{P}(z \geq 150))^{20} = 0.9985$ that is close to 1 with $\mathbb{P}(z \geq 150) = 0.9999$. For higher similarity, for instance, $S(\boldsymbol{B}_g, \boldsymbol{B}') = 0.9$, we can obtain optimum $KRR = (\mathbb{P}(z \geq 150))^{20} = 1$.

4. Performance Evaluation

A thorough analysis of the performance and security of our proposed key binding scheme was conducted on a public iris database CASIA v3-interval [29]. This dataset contains 2639 iris images from 396 different classes (eyes). In our experiments, left eye images were chosen since the patterns of genetically identical eyes appeared to be uncorrelated, as they were among imposters' eyes statistically [1]. To standardize the matching from all the left eye images, we selected any subset that contained at least seven iris samples per class. This resulted in a total of 124 classes with 868 iris images. Each iris image went through IrisCode generation [1] to generate IrisCode $\boldsymbol{I} \in \{0,1\}^{n_1 \times n_2}$ of dimension $n_1 = 20, n_2 = 512$ with a total of 10,240 bits.

The experiments were designed with the purpose of emphasizing the implementation and security analysis. The proposed key binding scheme here was not addressed or analyzed thoroughly to provide insights regarding its potential, limitation, and tradeoff in iris biometric. Firstly, the performance tradeoff upon introducing an alignment-free cancelable IrisCode was presented. IFO hashing showed its ability in preserving the system's performance in the following section. Next, an overview of the performance of the proposed key binding scheme was presented through standard metrics evaluation. The inter-relation of the main parameters—similarity threshold (t), cryptographic key length (n), and IFO hashed code length (m)—were tested and examined. In addition, we demonstrated the flexibility of our proposed scheme in managing inherent storage problems due to the nature of the cryptographic key binding's design without sacrificing security strength via reducing key length. All the experiments were conducted under a PC with processor core i7- 2.60 GHz, 8GB RAM and with MATLAB R2013b.

4.1. Performance of Original IrisCode and Bloom Filter IrisCode

We first carried out experimental testing on the original IrisCode $\boldsymbol{I} \in \{0,1\}^{20 \times 512}$ and Bloom filtered IrisCode, respectively. The parameters used for Bloom filter generation [49] were fixed as $W = 7$ and $L = 20$, yielding $l_1 \cdot l_2 = 50$ blocks and Bloom filtered IrisCode $\boldsymbol{B}_g \in \{0,1\}^{50 \times 128}$ as the outputs. This testing covered different matching protocols, such as genuine matching and imposter matching. For genuine matching, all iris images were used to generate IrisCodes. The matching was done by calculating the hamming distance between different IrisCodes of the same user, which then yielded $\frac{7 \times 6 \times 124}{2} = 2604$ genuine matching scores in total. The same genuine matching protocol was implemented in all the respective Bloom filtered IrisCodes. For imposter matching, the matching was done by calculating the hamming distance between IrisCodes of different users—interclass matching, in this case. Each user came with seven IrisCodes, which yielded a total of $\frac{7 \times 123 \times 7 \times 124}{2} = 373674$ imposter matching scores. The same imposter matching protocol was implemented as the Bloom filtered IrisCodes. We also tested the performance of Bloom filtered IrisCodes after applying IFO hashing in [55] $(m = 200,\ p = 3,\ \kappa = 64,\ \tau = 30)$ by using the same genuine and imposter protocols.

In biometric systems, EER has been widely used for performance evaluation by calculating the False Acceptant Rate (FAR) and False Rejection Rate (FRR) between the collected genuine and imposter scores, where lower EER implies higher performance. In our context, EER was approximated as $\text{EER} \approx (\text{FAR} + \text{FRR})/2$. The result is tabulated in Table 1 shown below:

Table 1. System performance for the original alignment-free and hashed IrisCodes.

CASIA v3 Database [29]	Equal Error Rate (EER %)
IrisCode	0.38
Bloom filtered IrisCode	0.50
Bloom filtered IrisCode (IFO applied)	0.58

The result from Table 1 indicates that the system performance did not experience significant deterioration after applying Bloom filter to resolve the alignment issues originated from IrisCode's generation process (rotational inconsistency due to head tilt during eye image acquisition). Moreover, IFO hashing, which inherited properties such as distance and similarity preservation from the Jaccard similarity and min hashing, showed compatible performance after the application of IFO hashing.

4.2. Performance of the Proposed Key Binding Method

This section provides the evaluation and overview of the performance of our proposed key binding method. For performance evaluation, intensive experiments were carried out under different parameter configurations. The metrics used for performance evaluation were FAR and FRR, as discussed earlier. Lower FAR and FRR values implied a higher system performance.

In order to measure the system's performance, similar protocols were applied in the following experiments. The first one referred to the genuine matching protocol where the first Bloom filtered IrisCode was used for the key binding (enrollment) purpose and the remaining Bloom filtered IrisCodes from the same class was used for key retrieval (query). Thus, this protocol yielded a total of 2604 testing results. The genuine matching protocol was then used to calculate the system's FRR $= \frac{\text{No. of wrongly retrieved key}}{2604} \times 100\%$. The second protocol referred to the imposter matching protocol where the first Bloom filtered IrisCode of each class was used for key binding (enrollment). The key retrieval (query) was then conducted over the second Bloom filtered IrisCodes of all the classes, excluding the samples from the enrolled class, and yielded a total of $(124 \times 123)/2 = 7626$ testing results. The imposter matching protocol was then used to calculate the FAR $= \frac{\text{No. correctly retrieved key}}{7626} \times 100\%$.

4.3. Evaluation on Similarity Score Threshold, t

As mentioned in our proposed method, there were three main parameters (t, n, m) in our proposed scheme. Several tests were carried out to study the relation of these important parameters to the system performance. By using the same parameter setting for IFO as in the previous section, the evaluation for the similarity score threshold t was carried out by fixing the parameters $m = 100$ and $n = 10$. The genuine matching and imposter matching protocols were performed under a range of values $t = [0.16,\ 0.17, \ldots, 0.25]$. The results of FAR and FRR for every t, given the parameter set $(t, 10, 100)]$ were recorded. Meanwhile, we also calculated their corresponding EERs, as tabulated in Table 2.

Table 2. System performance for parameter set $(t, 10, 100)$.

t	FRR (%)	FAR (%)	EER (%)
0.16	0.15	12.14	6.97
0.17	0.31	3.23	1.77
0.18	0.62	0.62	0.62
0.19	1.65	0.05	0.85
0.20	2.65	0.00	1.33
0.21	3.80	0.00	1.90
0.22	5.61	0.00	2.81
0.23	8.26	0.00	4.13
0.24	11.56	0.00	5.78
0.25	15.40	0.00	7.70

From the result in Table 2, it was not surprising that the best EER (0.62%) obtained was close to the original Bloom Filtered IrisCode's performance (0.58%) in Table 1 under a slightly different setting. This was mainly attributed to the Jaccard similarity's preserving property, which allowed us to measure the similarity between different Bloom filtered IrisCodes under IFO's hashed domain.

The matching scores between each IFO hashed code $j = 1, 2, \ldots, n$ under genuine matching and imposter matching were plotted and are depicted in Figure 3. It showed an overlapped region between genuine and imposter matching scores. This scenario was mainly due to the imposed synthetic Bloom filtered IrisCodes. The matching between a hashed synthetic Bloom filtered IrisCode and the query hashed code always resulted in a smaller matching score. This observation further supports our earlier claim that the synthetic template indeed acts like an imposter template to be used for the chaffing and winnowing process in concealing the genuine IFO hashed code in our proposed method.

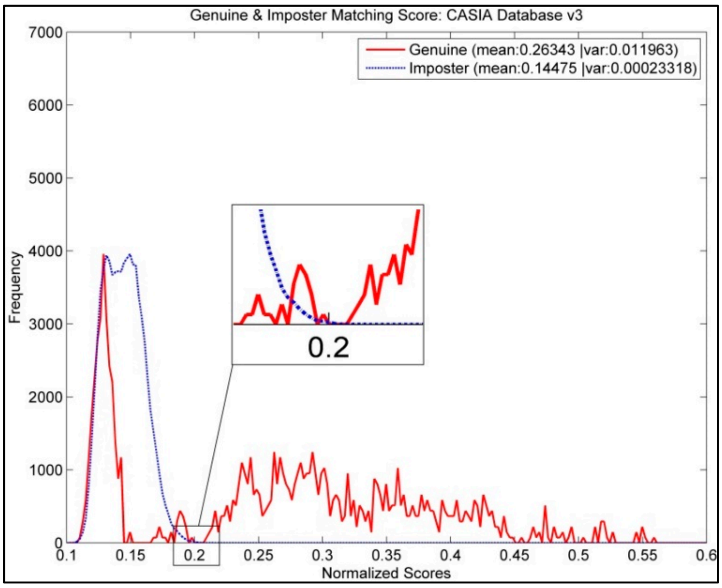


Figure 3. Graph for the genuine and imposter matching score.

Moreover, with the zoomed region in Figure 3, the best threshold value for t to avoid any imposter in potentially getting access into the system with FAR equals to zero would be around $t = 0.2$. In fact, this was justified by our results in Table 2, where the system reported an EER of 1.33% when FAR was 0 at $t = 0.2$. From the table, we can easily observe a trend that an increase in t resulted in a higher FRR but a lower FAR and vice versa.

For a cryptosystem to be useful, it is normally suggested that the FAR should be zero, thus any imposter or adversary can certainly be rejected by our proposed system for higher level of system security. Therefore, our analysis suggests that the optimal value of t lies under the range of $t \geq 0.2$.

4.4. Evaluation on Cryptographic Key Length, *n*

The evaluation of the effect of cryptographic key length n on system performance was carried out by fixing the values for parameters t and m. The genuine and imposter matching protocols were performed by setting different key lengths where $n = [10,\ 20,\ 40,\ 60,\ 80, 100,\ 150,\ 200]$. As a result, FAR and FRR for every n given $t = 0.2$ and $m = 100$ were recorded. Meanwhile, their corresponding Genuine Acceptance Rate, $GAR = 100 - FRR$ and EER were also calculated and are tabulated in Table 3.

Table 3. System performance for parameter set (0.2, n, 100).

n	GAR (%)	FAR (%)	EER (%)
10	97.35	0.00	1.33
20	96.67	0.00	1.67
40	96.67	0.00	1.67
60	96.37	0.00	1.82
80	96.37	0.00	1.82
100	96.37	0.00	1.82
150	96.37	0.00	1.82
200	96.37	0.00	1.82

From Figure 4, an EER as low as 1.33% was observed when shorter key length $(n = 10)$ was used. The EER gradually increased when the key length became longer and remained stagnant at 1.82% even though the key length increased further from 60 to 200. In contrast, GAR showed a slight reduction of 0.98% when the key length increased from 10 to 200. Besides that, the result in Table 3 shows that the increase in key length n reduced the FAR, as emphasized earlier in our proposed KRR. Given $t = 0.2$, the system performance was preserved even though the key length n increased up to 200. This implies that the binding of a long cryptographic key with a bit length as long as 200 bits is feasible while maintaining the same KRR and system performance captured by GAR.

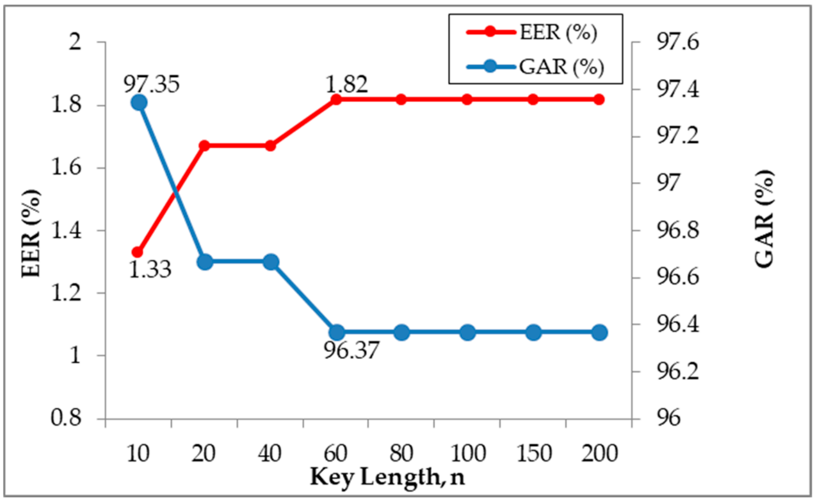


Figure 4. Graph for the evaluation on cryptographic key length.

4.5. Evaluation on Hashed Code Length, m

The evaluation of the effect of the IFO hashed code length m on system performance was conducted by fixing the parameters t and n. The genuine and imposter matching protocols were performed through different $m = [10, 50, 100, 150, 200, 250, 300]$ for this study. The tested results of FAR and FRR for every value of m given $t = 0.2$ and $n = 10$ in the parameter set $(0.2, 10, m)$ were recorded. Meanwhile, their corresponding GAR, EER, and storage per bit kB$/n$ were computed and are tabulated in Table 4. The unit of storage per bit was measured in kilobytes (kB), indicating the space required (for single bit of key binding, $n = 1$) for different m used in IFO hashed code generation.

Table 4. System performance for parameter set (0.2, 10, m).

m	GAR (%)	FAR (%)	EER (%)	Storage/bit (kB/n)
10	89.51	0	5.25	0.19
50	95.97	0	2.02	0.94
100	96.37	0	1.82	1.90
150	96.37	0	1.82	2.81
200	96.37	0	1.82	3.75
250	96.37	0	1.82	4.69
300	96.37	0	1.82	5.63

The IFO hashed code length played a critical role in terms of system storage, as the proposed method bound the key by using the IFO hashed code. In order to serve as an efficient biometric cryptosystem, the storage requirement for storing the helper data must be kept within an acceptable limit apart from high system security and performance. A system can become infeasible in actual implementation if it requires infinite storage for helper data to facilitate the key retrieval process despite high performance and security.

On the other hand, our proposed method offers flexibility in handling a system's storage limits. In our scheme, the IFO hashing provided a flexible and controllable code length (regulated by parameter m). This feature allowed us to keep our storage at a minimum while maintaining high system performance. As shown in Table 4, our proposed method achieved high GAR around 95–96% with storage records equal to 0.94–1.90 kB. The form of storage offered by our proposed scheme is more compact than the records generated by other schemes such as [60]. It was also demonstrated that the system's storage requirement could be decreased further with a shorter hashed code length (e.g., decreasing from $m = 300$ to 100) while maintaining the same system performance, as shown in Figure 5. Therefore, the system storage requirement for our proposed method is indeed controllable with respect to m. Figure 5 shows that EER reduced sharply from 5.25% ($m = 10$) to 1.82% ($m = 100$) and remained stable even with the further increment of hashed code length until $m = 300$. Thus, our proposed key binding method achieved its optimum performance (GAR of 96.37%) at $m = 100$, which required a storage space of 1.90 kB per bit through the evaluation of the three main parameters in our scheme, a similarity score threshold (t), a key length (n), and a hashed code length (m).

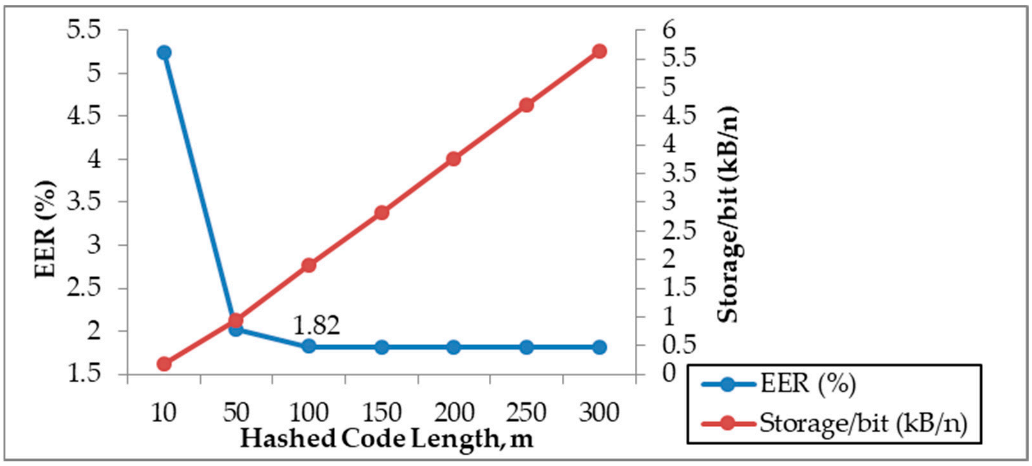


Figure 5. Graph for the evaluation on hashed code length.

5. Security Analysis

As our proposed method utilizes synthetic templates to conceal the genuine templates (with IFO hashing applied), it is important to examine the indistinguishability property in such a way that any attacker cannot gain advantages in distinguishing whether the stored IFO hashed code is generated from genuine or synthetic Bloom filtered IrisCode. We examined the security of our proposed method in the aspect of indistinguishability between genuine and synthetic templates. We also extended our analysis to potential security attacks on the proposed system, such as brute force attacks and false accept attacks.

5.1. Indistinguishability Between Genuine and Synthetic Templates

The indistinguishability property is examined in such a way that an attacker is allowed to accumulate certain information during a matching process and gain advantages that may be useful to retrieve the secret key. In this case, we characterized the indistinguishability between genuine and synthetic templates in an indistinguishability game between a challenger and an adversary to achieve the objective. The proposed indistinguishability game was designed as follows:

1. To start the game, given a group IFO hash function H, the challenger allows the adversary to choose any class/individual from the database.
2. After a class is chosen by the adversary, the challenger selects a random Bloom filtered IrisCode of that individual and generates $\boldsymbol{B}_g \leftarrow \text{Bloom\_filter}(W = 7,\ L = 20,\ \boldsymbol{I})$.
3. The challenger can then produce the IFO hashed code $\boldsymbol{C}_g \leftarrow H(\boldsymbol{B}_g)$ and give $\boldsymbol{C}_g$ to the adversary.
4. After that, the challenger flips a fair coin $b \in \{0, 1\}$. If $b = 1$, the challenger selects another Bloom filtered IrisCode of the selected person $\boldsymbol{B}_g{}'$ with a threshold $t' \in [0, 1]$, such that $\text{JA}(\boldsymbol{B}_g, \boldsymbol{B}_g{}') \le t'$ and generates $\boldsymbol{C} \leftarrow H(\boldsymbol{B}_g{}')$. In addition, hashed code $\boldsymbol{B}_g{}'$. can also be generated by adding random noise to the filtered IrisCode as long as $\text{JA}(\boldsymbol{B}_g, \boldsymbol{B}_g{}') \le t\prime$. If $b = 0$, the challenger permutes the Bloom filtered IrisCode $\boldsymbol{B}_s \leftarrow \text{Perm}\ (\boldsymbol{B}_g)$ and generates $\boldsymbol{C} \leftarrow H(\boldsymbol{B}_s)$. Then challenger gives $\boldsymbol{C}$ to the adversary.
5. The adversary outputs a word $\hat{k} \in \{0, 1\}$ and wins if $\hat{k} = k$.

Based on the game above, it is valid to say that if $\hat{k} = k$, then the adversary successfully retrieved a single bit of the cryptography key. It is important to note that the adversary does not know whether $\boldsymbol{C}$ is generated from genuine $\boldsymbol{B}_g$ or synthetic $\boldsymbol{B}_s$ Bloom filtered iris templates. Therefore, the adversary is required to find out the answer by matching the hashed codes and getting $S(\boldsymbol{C}, \boldsymbol{C}_g)$. We hereby describe the adversary in this game as $\text{Adv}_{\text{Gen}-\text{Syn}}$ for advantages gained in retrieving a single bit of the cryptographic key successfully. When $\text{Adv}_{\text{Gen}-\text{Syn}} = 0$, we say that the scheme is perfectly indistinguishable between genuine and synthetic templates. The advantages gained by $\text{Adv}_{\text{Gen}-\text{Syn}}$ can be described as follows:

$$\text{Adv}_{\text{Gen}-\text{Syn}} = \left| \mathbb{P}[\hat{k} = k] - \frac{1}{2} \right|, \tag{4}$$

given that:

$$\mathbb{P}[\hat{\boldsymbol{k}} = \boldsymbol{k}] == \frac{\boldsymbol{1}}{\boldsymbol{2}}\mathbb{P}\left[\boldsymbol{S}(\boldsymbol{C}, \boldsymbol{C}_g)\ \ge \boldsymbol{t} | \boldsymbol{k} = \boldsymbol{0}\right] + \frac{\boldsymbol{1}}{\boldsymbol{2}}\mathbb{P}\left[\boldsymbol{S}(\boldsymbol{C}, \boldsymbol{C}_g)\ \ge \boldsymbol{t} | \boldsymbol{k} = \boldsymbol{1}\right]$$

Assuming that for the case where $S(\boldsymbol{C}, \boldsymbol{C}_g)\ \ge t$, the adversary can surely differentiate that $\boldsymbol{C}$ is generated by $\boldsymbol{B}_g$, we can therefore define $\mathbb{P}\left[S(\boldsymbol{C}, \boldsymbol{C}_g)\ \ge t | k = 1\right] = 1$ and yield the final formulation:

$$\begin{aligned} \text{Adv}_{\text{Gen}-\text{Syn}} &= \tfrac{1}{2} \left| \mathbb{P}\left[S(\boldsymbol{C}, \boldsymbol{C}_g) \ge t | k = 0\right] \right| \\ &= \tfrac{1}{2} \left| \mathbb{P}[\mathrm{z} \ge tM | k = 0] \right|. \end{aligned} \tag{5}$$

As mentioned in Section 4.3, $\mathbb{P}[\mathrm{z} \ge tM | k = 0]$ is highly dependent on $P = S(\boldsymbol{B}_g, \boldsymbol{B}')$. From our matching result depicted in Figure 3, we expect to gain zero FAR with a threshold $t = 0.2$ while $S(\boldsymbol{C}, \boldsymbol{C}_g) < 0.2$ indicates an imposter matching score (showed in red-blue overlapped imposter distribution region). Thus, we let $t = 0.2$ and calculate $\mathbb{P}[\mathrm{z} \ge tM | k = 0]$ to estimate the adversary advantages $S(\boldsymbol{B}_g, \boldsymbol{B}')$ in this analysis. For further estimation, let $\text{Adv}^{n}_{\text{Gen}-\text{Syn}} = n\text{Adv}_{\text{Gen}-\text{Syn}}$, which describes the total adversary advantages gained from n bits in the cryptographic key. The total advantages are estimated by running the indistinguishability game n times independently (repeating

Step 4 and 5 of the indistinguishability game). Table 5 shows the results with $S(\boldsymbol{B}_g, \boldsymbol{B}') = [0.16, 0.17, 0.18, 0.19]$ for $n = [1, 50, 100, 200]$ and $M = 10000$.

Table 5. Indistinguishability between genuine and synthetic iris templates.

$S(B_g, B^{'})$	$\mathbf{Adv}_{\mathbf{Gen-Syn}}$ (n=1)	$\mathbf{Adv}^{n}_{\mathbf{Gen-Syn}}$ (n=50)	$\mathbf{Adv}^{n}_{\mathbf{Gen-Syn}}$ (n=100)	$\mathbf{Adv}^{n}_{\mathbf{Gen-Syn}}$ (n=200)
0.16	2.0561×10^{-26}	1.0281×10^{-24}	2.0561×10^{-24}	4.1122×10^{-24}
0.17	3.0075×10^{-15}	1.5038×10^{-13}	3.0075×10^{-13}	6.015×10^{-13}
0.18	1.4936×10^{-7}	7.6480×10^{-6}	1.4936×10^{-5}	2.9872×10^{-5}
0.19	0.0058	0.29	0.58	1.16

From this table, the adversary's advantages in distinguishing the genuine and synthetic iris templates can be quantitatively estimated through our proposed indistinguishability game. It is important to take into consideration the level of similarity between synthetic and genuine templates for the chaffed key binding scheme to fairly evaluate the indistinguishability property in terms of security. For instance, the computed adversary's advantage is $\text{Adv}_{\text{Gen-Syn}} = 0.58$ with $S(\boldsymbol{B}_g, \boldsymbol{B}') = 0.19$ when $n = 100$. The total advantages go up to more than 1 when n is increased to 200. This is because more iris templates are needed in order to bind longer key length, thus there is greater information leakage. Particularly, with $\text{Adv}^{n}_{\text{Gen-Syn}} \geq 1$, one can expect weaker security due to excessive information leakage. Nevertheless, our results show that with $S(\boldsymbol{B}_g, \boldsymbol{B}') = 0.16,\ 0.17$ and 0.18, the total adversary advantages to learn a single bit of information at the key length of 200 bits are estimated to be 2^{-78}, 2^{-41}, and 2^{-15} bits, respectively (lower bounded at 2^{-11}). The security of this scheme is based upon the selected threshold value and the similarity score, which determine the amount of information leakage (i.e., mutual information) due to the linkability between $\boldsymbol{B}_g$ and $\boldsymbol{B}'$. To the best of our knowledge, there is still no known algorithm to extract this information for the purpose of full IrisCode reconstruction practically in relation to the similarity score.

5.2. Cancelability and Renewal

For the renewal process, a new key needs to be reissued when the current cryptographic key is compromised. Our proposed key binding method requires no re-enrollment in this scenario. Key update can be achieved by interchanging the positions of the genuine and synthetic iris templates randomly together with their corresponding hashing groups. Thus, a new binary key string can be updated automatically. Our proposed design aims to provide a simple and fast key renewal process. The proposed algorithm achieved a GAR of more than 96% at zero FAR with hashed code length m and key length n up to 300 and 200, respectively.

For cancelability, the regeneration of a cancelable template is guaranteed by the revocability and unlinkability of the IFO hashing scheme. It was verified through security analysis [55] that it is computationally infeasible to derive the original biometric information from the IFO hashed code. The revocability was evaluated thoroughly by analyzing the pseudo-imposter score distribution of the randomly generated hashed codes of multiple subjects. The refreshed hashed codes are distinctive and uncorrelated to the old hashed code, albeit they are generated from the same IrisCode. With rigorous analysis backed by empirical data, the IFO hashing scheme satisfied the revocability and unlinkability requirements, while users are not required to keep their permutation token in secret.

5.3. Potential Attacks

Besides the indistinguishability between genuine and synthetic templates, we extended our analysis into potential security attacks. In this section, the proposed method is evaluated against potential security attacks.

5.3.1. Brute Force Attack

For brute force attacks, it relies on randomly guessing the n bit cryptographic key without the need for actual interception between the adversaries and the cancelable templates' storage. Therefore, the complexity of this attack is merely dependent on the cryptographic key length, which is controlled by the parameter n in our proposed method. Straightforwardly, the brute force attack complexity can be described as follows:

$$\mathbf{Bf}_{\mathrm{n}} = 2^{\mathrm{n}}. \tag{6}$$

Higher n indicates higher attack complexity, which also requires more cancelable templates for the key binding process. For instance, with a key length of $n = 100$, the brute force attack complexity is measured as $\mathrm{Bf}_n = 2^{100}$. Our best performance was preserved even up to a cryptographic key length of 200, as shown in Table 3. This is equal to an upper bound brute force attack's complexity of 2^{200}, which is already sufficient in cryptography applications. The proposed method demonstrated the flexibility to allow a potential key length that is longer than 200 while preserving the acceptable performance when there is a need for higher attack complexity.

5.3.2. False Accept Attack

Apart from brute force attacks, another security attack that needs to be taken into consideration is the false accept attack. In conjunction to brute force attacks, this kind of attack requires the interception of the adversary with the cancelable storage. Instead of randomly guessing, the false accept attack relies on the continuous trials of an attacker through conventional matching between the stored cancelable templates and the imposter templates. In our context, an unlimited number of trials are allowed. Therefore, the false accept attack is not constrained to the usage of several imposter templates but uses an infinite number of artificial/synthetic templates instead.

Since the false accept attack relies on the conventional matching mechanism, the false accept attack complexity can be calculated based on our proposed key retrieval rate, KRR. To avoid confusion, we denote the key retrieval rate for false accept attack by arbitrary attacker as KRR_{imp}. Thus, false accept attack's complexity, $\mathbf{fa}_{KRR_{\mathrm{imp}}}$ can be described directly as:

$$\mathbf{fa}_{KRR_{\mathrm{imp}}} = \mathbb{P}\left[k_j' = k_j \middle| j = 1, 2, \ldots, n\right] = \left(\mathbb{P}(z \geq tM)\right)^{n^*}. \tag{7}$$

We can estimate the $\mathbf{fa}_{KRR_{\mathrm{imp}}}$ by assuming that the adversary is able to generate a cancelable template $\boldsymbol{C}_j'$ with $S(\boldsymbol{B}_g, \boldsymbol{B}') < 0.2$. In this experiment, the $\mathbf{fa}_{KRR_{\mathrm{imp}}}$ was estimated using synthetic templates, which showed high similarity score when compared with genuine template. Thus, $S(\boldsymbol{B}_g, \boldsymbol{B}') = [0.195, 0.196, 0.197, 0.198, 0.199, 0.20]$ are tested in Table 6 with the following parameters: $n^* = \frac{n}{2}$ for maximum key entropy, $m = 200$, and $t = 0.20$.

Table 6. Estimation of complexity for brute force and false accept attacks.

$S(\boldsymbol{B}_g,\boldsymbol{B}^{'})$	$\mathbf{Bf}_{n=100}$	$\mathbf{fa}_{KRR_{\mathrm{imp}}}$
0.195	2^{100}	2^{162}
0.196	2^{100}	2^{133}
0.197	2^{100}	2^{107}
0.198	2^{100}	2^{85}
0.199	2^{100}	2^{66}

The calculated result shows that the false accept attack's complexity is lower compared to the brute force attack, given that $S(\boldsymbol{B}_g, \boldsymbol{B}') > 0.198$. This indicates that if any attacker is able to generate hashed code with the similarity $S(\boldsymbol{B}_g, \boldsymbol{B}') > 0.198$, he/she can potentially get access to the system due to the lower attack complexity. Referring to Figure 3, the region where an imposter can launch a false accept attack is typically within the range of $0.1 - 0.2$ with the mean of the imposter matching distribution around 0.14. It is expected that any false accept attack at a similarity score around $S\left(\boldsymbol{B}_g, \boldsymbol{B}'\right) = 0.14$ or < 0.195 will likely be infeasible $\left(\mathbf{fa}_{KRR_{\text{imp}}} \gg 2^{162}\right)$ due to a much higher false accept attack's complexity.

In fact, we also took the worst case scenario into consideration by calculating the $\mathbf{fa}_{KRR_{\text{imp}}}$ according to a list of high similarity scores $S\left(\boldsymbol{B}_g, \boldsymbol{B}'\right)$ ranging from 0.195 to 0.199 according to the threshold set. The proposed method showed a false accept complexity of 2^{66} bits. It is important to note that the overlapped region from 0.1 to 0.15 in Figure 3 mainly was contributed to by the synthetic iris templates, which acted like imposter iris templates as an extra layer of protection to chaff the genuine iris templates.

5.4. Comparison

In reviewing the performance of the state-of-the-art method, Rathgeb and Uhl [61] conducted a compact survey compiling the key binding approaches in iris biometric cryptosystems. Representing one of the simplest key binding approaches, the fuzzy commitment scheme was successfully applied to iris. More significant performance evaluation on the iris based fuzzy commitment scheme [61] was applied after analyzing the error distribution of IrisCodes of different iris recognition algorithms. The method reported a GAR of 95.08% with 128-bit cryptography keys at zero FAR. In another extended work [62], the authors applied a context-based reliable component selection in order to extract cryptographic keys from IrisCodes, which were then bound to Hadamard code words, achieving a lower GAR of 93.47%. A most recent work aimed to improve the security and performance of the fuzzy vault scheme using multi-biometrics [63]. The best GAR of approximately 95% was achieved with security levels around 50 bits. As for the fuzzy vault using single iris, a lower GAR around 90% was reported with similar security levels. Summarized results of state-of-the-arts iris key binding methods are shown in Table 7 below.

Table 7. Summarized results of state-of-the-arts.

Methods	GAR (%)	FAR (%)	Keybits
Iris-based fuzzy commitment schemes [61]	95.08	0	128
Iris-biometric key generation [62]	93.47	0	128
Iris fuzzy vault [63]	92.10	0	51
Multi-iris fuzzy vault [63]	95.49	0	53
Proposed method	97.35	0	66

6. Conclusions

In this paper, we proposed a cancelable iris based key binding scheme that is freed from the limitation of error correcting capacity and tedious alignment process. The main reason for introducing IFO hashing as part of the proposed method is to enable efficient and tunable storage and fulfill the non-invertibility and unlinkability requirements. Storage (kB) per bit was proposed as the metric to vindicate the significant effect of controllable hashed code length in managing the storage space and preserving the accuracy performance. As a result, the highest GAR of 96.37% at zero FAR with storage record equal to 1.90 kB was achieved by our proposed scheme. A precise and useful key retrieval metric—*KRR*—was proposed and implemented for security analysis, such as false accept attacks and the indistinguishability game. In-depth security analysis emphasizing the adversary's advantages gained over the proposed key binding design was evaluated through an indistinguishability game. In addition, the complexity and the security level of the proposed method were also justified against potential attacks. For example, our proposed method showed a brute force attack complexity of 2^{100} and a sufficient false accept complexity of 2^{66} bits under the worst case scenario for a key length of 100 bits. The proposed method embraces the flexibility while maintaining significant accuracy performance and security level. The security-performance tradeoff was attended to through experiments where the optimum GAR ranged from 96.37% to 97.35%, and zero FAR remained stagnant, regardless of the increasing key length from 10 to 200 bits. This implies that the quality preservation of the accuracy performance at higher security levels is achievable through our proposed key binding scheme. Finally, the proposed method requires no re-enrollment and storage for seeds, making it more attractive for actual implementation compared to other methods. We hope that this work can evoke more thoughts and analysis towards higher flexibility and security for the iris key binding scheme in future.

Author Contributions: T.-Y.C. designed the overall system, performed experiments and wrote the paper; B.-M.G., Y.-H.T. and Z.J. supervised and reviewed the draft; Funding support, B.-M.G., T.-Y.C. and Z.J.

Funding: This research was funded by Fundamental Research Grant Schemes (FRGS) with grant numbers, FRGS/1/2016/ICT02/UTAR/03/1, FRGS/1/2016/ICT04/UTAR/01/1 and FRGS/1/2018/ICT02/MUSM/03/3.

Acknowledgments: The authors gratefully acknowledge the support from Ministry of Higher Education Malaysia for this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Daugman, J. How iris recognition works. *IEEE Trans. Circuits Syst. Video Technol.* **2004**, *14*, 21–30. [CrossRef]
2. Sasse, M.A. Red-eye blink, bendy shuffle, and the yuck factor: A user experience of biometric airport systems. *IEEE Secur. Priv.* **2007**, 5. [CrossRef]
3. Cimato, S.; Gamassi, M.; Piuri, V.; Sassi, R.; Scotti, F. Privacy in Biometrics. Available online: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=cimato+Privacy+in+biometrics&btnG= (accessed on 17 December 2018).
4. Klein, D.V. Foiling the cracker: A survey of, and improvements to, password security. In Proceedings of the 2nd USENIX Security Workshop, Boston, MA, USA, 6–10 August 1990; pp. 5–14.
5. Jain, A.K.; Ross, A.; Pankanti, S. Biometrics: A tool for information security. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 125–143. [CrossRef]
6. Juels, A.; Wattenberg, M. A fuzzy commitment scheme. In Proceedings of the 6th ACM conference on Computer and communications security, Singapore, 1–4 November 1999; pp. 28–36. [CrossRef]
7. Jain, A.K.; Nandakumar, K.; Nagar, A. Biometric template security. *Eurasip J. Adv. Signal Process.* **2008**, *2008*, 113. [CrossRef]
8. Jain, A.K.; Ross, A.; Prabhakar, S. An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Technol.* **2004**, *14*, 4–20. [CrossRef]
9. Dodis, Y.; Reyzin, L.; Smith, A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 523–540.
10. Verbitskiy, E.A.; Tuyls, P.; Obi, C.; Schoenmakers, B.; Skoric, B. Key extraction from general nondiscrete signals. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 269–279. [CrossRef]
11. Juels, A.; Sudan, M. A fuzzy vault scheme. *Des. Codes Cryptogr.* **2006**, *38*, 237–257. [CrossRef]
12. Ratha, N.K.; Chikkerur, S.; Connell, J.H.; Bolle, R.M. Generating cancelable fingerprint templates. *IEEE Trans. Pattern Anal. Mach. Intell.* **2007**, *29*, 561–572. [CrossRef]
13. Cavoukian, A.; Stoianov, A. Biometric encryption. In *Encyclopedia of Cryptography and Security*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 90–98.
14. Hao, F.; Anderson, R.; Daugman, J. Combining crypto with biometrics effectively. *IEEE Trans. Comput.* **2006**, *55*, 1081–1088.
15. Bringer, J.; Chabanne, H.; Cohen, G.; Kindarji, B.; Zemor, G. Theoretical and practical boundaries of binary secure sketches. *IEEE Trans. Inf. Forensics Secur.* **2008**, *3*, 673–683. [CrossRef]
16. Phillips, P.J.; Bowyer, K.W.; Flynn, P.J.; Liu, X.; Scruggs, W.T. The iris challenge evaluation 2005. In Proceedings of the 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, BTAS 2008, Arlington, VA, USA, 29 September–1 October 2008; pp. 1–8.
17. Rathgeb, C.; Uhl, A. Context-based biometric key generation for Iris. *IET Comput. Vis.* **2011**, *5*, 389–397. [CrossRef]

18. Maiorana, E.; Campisi, P.; Neri, A. IRIS template protection using a digital modulation paradigm. In Proceedings of the 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Florence, Italy, 4–9 May 2014; pp. 3759–3763.
19. Kelkboom, E.J.; Breebaart, J.; Kevenaar, T.A.; Buhan, I.; Veldhuis, R.N. Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 107–121. [CrossRef]
20. Teoh, A.B.J.; Kim, J. Secure biometric template protection in fuzzy commitment scheme. *IEICE Electron. Express* **2007**, *4*, 724–730. [CrossRef]
21. Zhang, L.; Sun, Z.; Tan, T.; Hu, S. Robust biometric key extraction based on iris cryptosystem. In *International Conference on Biometrics*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 1060–1069.
22. Zhou, X.; Kuijper, A.; Veldhuis, R.; Busch, C. Quantifying privacy and security of biometric fuzzy commitment. In Proceedings of the 2011 International Joint Conference on Biometrics (IJCB), Washington, DC, USA, 11–13 October 2011; pp. 1–8.
23. Rathgeb, C.; Uhl, A. Statistical attack against iris-biometric fuzzy commitment schemes. In Proceedings of the 2011 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Colorado Springs, CO, USA, 20–25 June 2011; pp. 23–30.
24. Scheirer, W.J.; Boult, T.E. Cracking fuzzy vaults and biometric encryption. In Proceedings of the Biometrics Symposium, Baltimore, MD, USA, 11–13 September 2007; pp. 1–6.
25. Carter, F.; Stoianov, A. Implications of biometric encryption on wide spread use of biometrics. In Proceedings of the EBF Biometric Encryption Seminar (June, 2008), Amsterdam, The Netherlands, 24 June 2008.
26. Ignatenko, T.; Willems, F.M. Information leakage in fuzzy commitment schemes. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 337–348. [CrossRef]
27. Kelkboom, E.J.; Breebaart, J.; Buhan, I.; Veldhuis, R.N. Maximum key size and classification performance of fuzzy commitment for gaussian modeled biometric sources. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1225–1241. [CrossRef]
28. Lee, Y.J.; Park, K.R.; Lee, S.J.; Bae, K.; Kim, J. A new method for generating an invariant iris private key based on the fuzzy vault system. *IEEE Trans. Syst. Man Cybern. Part B* **2008**, *38*, 1302–1313. [CrossRef]
29. Chinese Academy of Sciences' Institute of Automation: CASIA Iris Image Database V3.0—Interval. 2002. Available online: http://biometrics.idealtest.org (accessed on 8 September 2015).
30. Reddy, E.S.; Babu, I.R. Performance of iris based hard fuzzy vault. In Proceedings of the IEEE 8th International Conference on Computer and Information Technology Workshops, CIT Workshops 2008, Sydney, QLD, Australia, 8–11 July 2008; pp. 248–253. [CrossRef]
31. Chinese Academy of Sciences' Institute of Automation: CASIA Iris Image Database V1.0. 2002. Available online: http://biometrics.idealtest.org (accessed on 8 September 2015).
32. Multimedia University: MMU Iris Image Database. 2004. Available online: http://pesona.mmu.edu.my/ccteo (accessed on 8 September 2015).
33. Mariño, R.Á.; Alvarez, F.H.; Encinas, L.H. A crypto-biometric scheme based on iris-templates with fuzzy extractors. *Inf. Sci.* **2012**, *195*, 91–102. [CrossRef]
34. Fouad, M.; El Saddik, A.; Zhao, J.; Petriu, E. A fuzzy vault implementation for securing revocable iris templates. In Proceedings of the 2011 the IEEE International on Systems Conference (SysCon), Montreal, QC, Canada, 4–7 April 2011; pp. 491–494.
35. Kholmatov, A.; Yanikoglu, B. Realization of correlation attack against the fuzzy vault scheme. In Proceedings of the Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, San Jose, CA, USA, 27–31 January 2008; p. 68190O.
36. Tams, B.; Mihăilescu, P.; Munk, A. Security considerations in minutiae-based fuzzy vaults. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 985–998. [CrossRef]
37. Nandakumar, K.; Jain, A.K.; Pankanti, S. Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Trans. Inf. Forensics Secur.* **2007**, *2*, 744–757. [CrossRef]
38. Quan, F.; Fei, S.; Anni, C.; Feifei, Z. Cracking cancelable fingerprint template of Ratha. In Proceedings of the International Symposium on Computer Science and Computational Technology, ISCSCT'08, Shanghai, China, 20–22 December 2008; pp. 572–575.

39. Savvides, M.; Kumar, B.V.; Khosla, P.K. Cancelable biometric filters for face recognition. In Proceedings of the 17th International Conference on Pattern Recognition, ICPR 2004, 2004, Cambridge, UK, 26 August 2004; pp. 922–925.
40. Chin, C.S.; Jin, A.T.B.; Ling, D.N.C. High security iris verification system based on random secret integration. *Comput. Vis. Image Underst.* **2006**, *102*, 169–177. [CrossRef]
41. Zuo, J.; Ratha, N.K.; Connell, J.H. Cancelable iris biometric. In Proceedings of the 19th International Conference on Pattern Recognition, ICPR 2008, Tampa, FL, USA, 8–11 December 2008; pp. 1–4.
42. Pillai, J.K.; Patel, V.M.; Chellappa, R.; Ratha, N.K. Sectored random projections for cancelable iris biometrics. In Proceedings of the 2010 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), Dallas, TX, USA, 14–19 March 2010; pp. 1838–1841.
43. Kong, A.; Cheung, K.-H.; Zhang, D.; Kamel, M.; You, J. An analysis of BioHashing and its variants. *Pattern Recognit.* **2006**, *39*, 1359–1368. [CrossRef]
44. Lacharme, P.; Cherrier, E.; Rosenberger, C. Preimage attack on biohashing. In Proceedings of the 2013 International Conference on Security and Cryptography (SECRYPT), Reykjavik, Iceland, 29–31 July 2013; pp. 1–8.
45. Hämmerle-Uhl, J.; Pschernig, E.; Uhl, A. Cancelable Iris Biometrics Using Block Re-mapping and Image Warping. In Proceedings of the ISC, Pisa, Italy, 7–9 September 2009; pp. 135–142.
46. Jenisch, S.; Uhl, A. Security analysis of a cancelable iris recognition system based on block remapping. In Proceedings of the 2011 18th IEEE International Conference on Image Processing (ICIP), Brussels, Belgium, 11–14 September 2011; pp. 3213–3216.
47. Ouda, O.; Tsumura, N.; Nakaguchi, T. On the security of bioencoding based cancelable biometrics. *IEICE Trans. Inf. Syst.* **2011**, *94*, 1768–1777. [CrossRef]
48. Lacharme, P. Analysis of the iriscodes bioencoding scheme. *Int. J. Comput. Sci. Softw. Eng.* **2012**, *6*, 315–321.
49. Rathgeb, C.; Breitinger, F.; Busch, C. Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013; pp. 1–8.
50. Hermans, J.; Mennink, B.; Peeters, R. When a bloom filter is a doom filter: Security assessment of a novel iris biometric template protection system. In Proceedings of the 2014 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 10–12 September 2014; pp. 1–6.
51. Bringer, J.; Morel, C.; Rathgeb, C. Security analysis of bloom filter-based iris biometric template protection. In Proceedings of the 2015 International Conference on Biometrics (ICB), Phuket, Thailand, 19–22 May 2015; pp. 527–534.
52. Gomez-Barrero, M.; Rathgeb, C.; Galbally, J.; Busch, C.; Fierrez, J. Unlinkable and irreversible biometric template protection based on bloom filters. *Inf. Sci.* **2016**, *370*, 18–32. [CrossRef]
53. Dwivedi, R.; Dey, S. Cancelable iris template generation using look-up table mapping. In Proceedings of the 2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 19–20 February 2015; pp. 785–790.
54. Umer, S.; Dhara, B.C.; Chanda, B. A novel cancelable iris recognition system based on feature learning techniques. *Inf. Sci.* **2017**, *406*, 102–118. [CrossRef]
55. Lai, Y.-L.; Jin, Z.; Teoh, A.B.J.; Goi, B.-M.; Yap, W.-S.; Chai, T.-Y.; Rathgeb, C. Cancellable iris template generation based on Indexing-First-One hashing. *Pattern Recognit.* **2017**, *64*, 105–117. [CrossRef]
56. Lai, Y.-L.; Goi, B.-M.; Chai, T.-Y. Alignment-free indexing-first-one hashing with bloom filter integration. In Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, China, 22–24 July 2017; pp. 78–82.
57. Jin, Z.; Teoh, A.B.J.; Goi, B.-M.; Tay, Y.-H. Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation. *Pattern Recognit.* **2016**, *56*, 50–62. [CrossRef]
58. Rivest, R.L. Chaffing and winnowing: Confidentiality without encryption. *Cryptobytes* **1998**, *4*, 12–17.
59. Gács, P.; Körner, J. Common information is far less than mutual information. *Probl. Control Inf. Theory* **1973**, *2*, 149–162.
60. Li, P.; Yang, X.; Cao, K.; Tao, X.; Wang, R.; Tian, J. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. *J. Netw. Comput. Appl.* **2010**, *33*, 207–220. [CrossRef]

61. Rathgeb, C.; Uhl, A. The State-of-the-Art in Iris Biometric Cryptosystems. Available online: http://cdn.intechopen.com/pdfs/16590/InTech-The_state_of_the_art_in_iris_biometric_cryptosystems.pdf (accessed on 17 December 2018).
62. Rathgeb, C.; Uhl, A. Context-based texture analysis for secure revocable iris-biometric key generation. In Proceedings of the 3rd International Conference on Imaging for Crime Detection and Prevention (ICDP 2009), London, UK, 3 December 2009.
63. Rathgeb, C.; Tams, B.; Wagner, J.; Busch, C. Unlinkable improved multi-biometric iris fuzzy vault. *Eurasip J. Inf. Secur.* **2016**, *2016*, 26. [CrossRef]