symmetry

Article

Towards Better Performance for Protected Iris Biometric System with Confidence Matrix

Tong-Yuen Chai *, **Bok-Min Goi** and **Wun-She Yap**

Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Bandar Sungai Long, Kajang 43000, Malaysia; goibm@utar.edu.my (B.-M.G.); yapws@utar.edu.my (W.-S.Y.)
* Correspondence: chaity@utar.edu.my; Tel.: +60-16781-1880

Abstract: Biometric template protection (BTP) schemes are implemented to increase public confidence in biometric systems regarding data privacy and security in recent years. The introduction of BTP has naturally incurred loss of information for security, which leads to performance degradation at the matching stage. Although efforts are shown in the extended work of some iris BTP schemes to improve their recognition performance, there is still a lack of a generalized solution for this problem. In this paper, a trainable approach that requires no further modification on the protected iris biometric templates has been proposed. This approach consists of two strategies to generate a confidence matrix to reduce the performance degradation of iris BTP schemes. The proposed binary confidence matrix showed better performance in noisy iris data, whereas the probability confidence matrix showed better performance in iris databases with better image quality. In addition, our proposed scheme has also taken into consideration the potential effects in recognition performance, which are caused by the database-associated noise masks and the variation in biometric data types produced by different iris BTP schemes. The proposed scheme has reported remarkable improvement in our experiments with various publicly available iris research databases being tested.

Keywords: template protection; biometric system; iris recognition; confidence matrix; recognition performance

Citation: Chai, T.-Y.; Goi, B.-M.; Yap, W.-S. Towards Better Performance for Protected Iris Biometric System with Confidence Matrix. *Symmetry* **2021**, *13*, 910. https://doi.org/10.3390/sym13050910

Academic Editors: Kuo-Hui Yeh and Sergei D. Odintsov

Received: 15 February 2021
Accepted: 6 May 2021
Published: 20 May 2021

1. Introduction

Biometrics authentication has been widely deployed in our daily lives. Identity verification based on behavioral and physiological characteristics such as iris, signatures, face, fingerprint, and palm-print can be conducted through biometric systems. Traditional password-based systems have been replaced gradually by biometric systems due to high recognition accuracy [1] and convenience. However, biometric systems are unsecured due to security threats such as misuse of biometric data and data management [2]. This is an important concern that needs to be addressed as the compromised biometric traits will become useless in all the involved applications.

The biometric template protection (BTP) scheme serves as a protection step in securing the biometric system by repeatedly distorting the biometric data through different transformations. This scheme transforms the biometric templates and enables the authentication process to be conducted in a secured domain [3]. The transformed templates under BTP scheme are irreversible and non-decryptable to protect the privacy and security of the original biometric data. Thus, it is more secure to store the transformed templates into the database rather than the original biometric templates [4]. Since the matching stage can be held in a transformed domain, original biometric data will not be exposed to any potential threat. A standard secured biometric system has been constructed with the integration of BTP scheme into a biometric recognition system. There are 3 main criteria to be fulfilled for a good BTP scheme [5]:

1. Irreversibility [6]: It should be computationally infeasible for a wrongdoer to reconstruct the original biometric data from multiple protected biometric templates.

2. Unlinkability [7]: It should be computationally hard to determine whether the protected biometric templates originate from the same biometric instance or not to avoid cross-matching across different applications.
3. Performance: The recognition performance should be approximately preserved with respect to the performance of its original biometric templates.

While the BTP schemes which fulfill the requirements above can secure a biometric system, there are still drawbacks and remaining issues in the search for optimum balance between the system's performance and security. BTP schemes that emphasize more on security protection most often distort the biometric data severely via different transformations in order to achieve better entropy, irreversibility, and unlinkability. These processes inevitably cause higher loss of useful information and thus performance degradation in exchange for better security. In other words, most of the good iris BTP schemes which provide stronger security features will expect weaker performance as the main drawback. Knowing the effect of this tradeoff, there are also efforts by respective iris BTP schemes [8,9] to introduce remedies such as optimizing the selection of parameters and some of the steps to mitigate the performance degradation. It is a non-trivial task to offer a security guaranty to a biometric template while preserving the recognition rate, which is viewed as one of the major requirements in designing an iris BTP scheme. Some works have been done (see [10–13] for complete surveys) to support the security of a biometric template without severely deteriorating the system performance. Nevertheless, since there is a plethora of iris BTP schemes being proposed, it introduces another issue on how to determine and select the best iris BTP scheme.

Our approach contributes to tackling the above question via confidence matrix generation that can be generally adopted for different iris biometric templates generated from different BTP schemes. In addition, our generalized solution can further improve the recognition performance of the protected (hashed) iris templates in biometric systems. Firstly, the proposed approach requires no modification to the original algorithms in iris BTP schemes. The design of this approach is kept simple and implementable onto protected iris templates generated by any BTP schemes. One important feature contributed by our proposed approach is the ability to improve the iris recognition performance further through training samples. Apart from this, the potential security threat of using confidence matrix is analyzed, for instance, information leakage and security attacks through irreversibility and unlinkability studies.

In different to the treatment of fragile bits, the proposed confidence matrix is not restricted to only binary iris feature representation but also accepts integer iris feature representation. As pointed out in [14,15], bit fragility generally occurs when the inner product between a filter and a region of the examined image produces a value with a small magnitude. Hence, the fragility of each bit in a code map depends on a combination of the biometric structure at that particular location, the filter adopted by the coding scheme and the quantization method for the filter response. However, our works focus more on the protected template generated from the iris BTP scheme. Since different schemes shall act as different functions $F(.)$ for the input iris features, the intrinsic biometric structure, for example, the distribution of genuine and imposter matching scores will thus, behave differently depending upon the designed iris BTP scheme. Therefore, the fragility of the generated iris template (after BTP is applied) is random for any random function $F(.)$. Thus, our proposed approaches enable confidence bits to be applied onto arbitrary hashed iris template protection schemes through collision theory while fragile bits focused on iris code instead.

Two reputed BTP schemes in the field of iris recognition, Bloom filter [16] and enhanced Indexing-First-One (IFO) hashing [17], are adopted in our experiments on publicly available research databases. Both methods incur transformation processes such as modulo function and many-to-one mapping function to increase the strength of security and privacy protection. These methods have good overall recognition performance and resistance from attacks such as cross-matching attacks and statistical attacks. Some publicly available iris research databases come with noise masks. This is another potential factor affecting the recognition performance of a protected iris biometric system especially when this additional feature cannot be utilized in the matching stage.

In view of this shortage, our proposed scheme has incorporated the information from the noise masks in the generation of our confidence matrices in the matching stage. This allows our proposed scheme to work on any iris database that comes with or without noise masks. In this paper, our proposed scheme is able to improve the recognition performance involving binary, and integer hashed values in the matching stage. Two unique strategies are proposed to accelerate the recognition performance of protected iris templates from iris databases with different image quality. In a nutshell, the proposed scheme has shown great flexibility in dealing with the iris template protection scheme, different hashed iris data types, and iris databases with varying image quality. The proposed method showed high adaptability on iris databases with or without noise masks while having good potential further to improve its recognition performance via its trainable capability.

The paper is organized as follows. Previous work-related to iris template protection schemes and their recognition performance is described in Section 2. The presentation of our proposed scheme and its implementation are shown in Section 3. The experimental results, discussion and security analysis are provided in Sections 4 and 5. Finally, concluding remarks are given in Section 6.

2. Related Work

Problem Definition

Iris recognition is first introduced by John Daugman [1]. The author encoded the iris features using quadrature 2-D Gabor wavelet demodulation. The complexity of the phase information across different persons spans about 249 degrees of freedom and discrimination entropy of about 3.2 $\mathrm{b/mm^2}$. It was also proven improbable that two different irises might disagree by chance in fewer than at least one-third of their bits. The probability of such an event is approximated to be 1 in 16 million with 9.1 million comparisons. In this method, fractional Hamming Distance (HD) was used as the measure of dissimilarity between two irises for iris recognition. Statistical analysis was then conducted by Kong [18] on the risk associated with two patented template protection schemes deployed for producing application-specific iris code is analyzed. The study has shown that the iris code can be unlocked and the key can be retrieved through statistical dependence detected. The security risk in these schemes, as well as the iris code, might endanger numerous people and organizations due to its wide deployment in commercial systems.

The initial work from Ratha et al. [3] had introduced the concept of a cancellable BTP scheme. Non-invertible geometric transformations consisting block permutation and feature folding were applied on biometric template. Random projections of discriminative features were used for cancelability in face biometrics in [19]. Pioneering work in the field of iris biometric was proposed in [20]. There are 4 non-invertible and revocable transformations. The first method, GRAY-COMBO transforms Gabor features by circular shifting followed by random rows addition. Similar transformations on iris codes are performed in the second method, BIN-COMBO but the combination is conducted through XOR operation. These methods reduce the amount of information available for recognition for better security. However, the global linear transformation includes outliers which can degrade the performance. The other two methods can be referred as biometric salting, namely GRAY-SALT and BIN-SALT where random patterns can be added to the real-valued or binarized iris features. It is found to be difficult in determining the relative strength of the noise patterns to be added to gain the balance between recognition performance and security. If the added patterns are weak and compromised, original iris pattern can be obtained by a simple subtraction operation.

Another salting method by Chong et al. [21] proposed S-iris code encoding, which combined iris features and secret random numbers through iterated inner-product and thresholding to produce a set of cancellable binary codes per person. Noise mask is developed to eliminate the weaker inner-product and improve the accuracy in matching. Another idea of iris template protection is based on the sectored random projections [22]. Random projections are applied to sectored iris features via user-specific Gaussian matrix. The random matrices are then concatenated to form new cancellable iris template. This method limits the effect of outliers but reduces the size of useful information. The author pointed out that direct projection of the entire image might lead to performance degradation due to the effects of external noises such as specular reflections and eyelashes. Further research [18,23] found that the performance of this method was degraded when the same random matrix was being applied to different users. In addition, the protected template is likely to be inverted when the user-specific random matrices are disclosed or the adversary possesses the secret token. Thus, biometric salting is feasible for template protection only if the auxiliary data are kept secret.

Besides cancellable biometrics, a biometric cryptosystem is another alternative to BTP aiming at generating cryptographic keys out of or with biometric traits. Generally, key generation schemes require exact recovery of the input biometric feature via error tolerance, for instance, error correction code (ECC). This is to ensure that the same key can be regenerated from the varying biometric feature for authentication. Using error correction code in biometric system introduces high tension between error-correcting capability and security [24]. In particular, there is an existing tradeoff in between the error-correcting capability of an ECC and the system security (in terms of false acceptance), duped as the granular effect, where it is crucial to know the genuine and imposter distribution before designing a biometric system with ECC. Analysis has been done in [25,26] and reported that correcting the large number of errors in the input feature imposes high information loss, further leads to low attack complexity. It is still an open problem on how to choose the best ECC for BCS.

There is an attempt made to introduce iris fuzzy vault system [27] based on local iris features. The circular shape of iris is considered rotational symmetry. The shape of iris is iden-tical to origin under different angles of head orientation. However, the alignment issue occurs and affects the matching performance between rotated irises as the pattern of iris features is not rotational symmetry. Thus, iris features are extracted from multiple regions with shift-matching applied to solve the alignment issue in this system. Reed-Solomon (RS) coding scheme is then used for error correction. The best Genuine Acceptance Rate (GAR) reported was 83.4% and 91.1% respectively for CASIAv1 and CASIAv3 iris databases (Center for Biometrics and Security Research, Beijing, China) under adequate system security. Rathgeb et al. [28] have proposed an iris key generation scheme based on interval mapping for iris features in real values. The highest key generation rate reported on CASIAv3 was 95.09% for five enrollment samples. However, our approach do not require exact recovery of the input biometric. Authentication is done by computing the similarity score between two biometric templates. This is to avoid the usage of ECC that lead to another code selection problem.

Hamerle-Uhl et al. [29] proposed a BTP scheme that incorporates block-remapping and image warping to prevent non-invertible transformation. The normalized iris image is first partitioned into blocks which will be mapped randomly to blocks from the source texture. Then, a key is used as a seed to represent one particular distortion on the remapped image to prevent reconstruction of the original iris data. Jenisch and Uhl [30] highlighted the vulnerability of the remapping process in the scenario of coalition attack presuming that single or multiple templates are available to an attacker. Increasing the security to the recommended level will sacrifice the performance of the system with more than 100% of EER degradation from 1.244 to 2.846. Ouda et al. [31] proposed a tokenless cancelable biometrics scheme, BioCode. First, consistent bits of several iris codes of the same iris with lower probability of flipping are extracted. The bits are then grouped into m binary codewords in each block. Each block is mapped to a single bit of a random binary sequence with length $l = 2^m$ where the location is determined by the decimal value of that specific block. The mapped binary values are then arranged according to the associated positions of the blocks to form the BioCodes. The many-to-one mapping used in the generation of BioCode fulfils the non-invertibility requirement by making the recovery of original iris code computationally infeasible. However, BioEncoding scheme recorded the best EER of 6.27% for CASIAv3. Larcharme [32] revisited bioencoding and regarded the scheme as a simple application of random Boolean function on the original iris code which is invertible.

Cancellable iris biometric without tedious alignment steps was introduced by Rathgeb et al. [16] using an adaptive Bloom filter. This representation allows biometric templates such as iris codes to have an alignment-invariant comparison at the matching stage without degrading the performance of the iris recognition system. In other words, Bloom filtered iris features have become rotational symmetry in matching. The best EER reported was 1.49% for CASIAv3. The many-to-one mapping of biometric features to form a Bloom filter is non-invertible. An application-specific secret bit vector is XORed with each codeword prior to mapping to provide unlinkability between multiple cancelable templates of a subject. The scheme has reported a comparable accuracy performance to its original counterparts. Undesirably low attack complexities of 2^{25} for false positives generation and between 2^2–2^8 for key recovery are then reported by [33]. It is proved that this method was susceptible to cross-matching attack. Bringer et al. [34] successfully performed brute force attack on each block of the codewords by analyzing the cancelable templates generated from two different intra-class iris codes. However, [35,36] have demonstrated the solutions to circumvent the security limitations of the Bloom filter. Sadhya et. al. [37] has recently proposed a cancelable iris code based on Locality Sensitive Hashing (LSH) with the best EER 0.105% for CASIAv3. Random bits sampling strategy was implemented by using an arbitrary number of hash functions, $h_{1, \dots,}$ h_n to sample n random binary string from the iris code. Under this framework, intra-class samples are expected to be close to each other and thus, they will be hashed to the same location. In contrary, inter-class samples are dissimilar and consequently hashed to different locations. Low EER was reported due to the collision guarantees from bit sampling based LSH.

Dwivedi et al. [38] proposed a cancellable template protection scheme based on randomized look-up table mapping. The iris codes are divided into groups of binary codewords. The corresponding decimal value of each group will be mapped to a look-up table with random binary bits equivalent to the length of the codewords in each group. A degradation of 10% to 49% in EER performance reported. A recent research proposed an iris protection scheme by ranking the decimal value of each group of codewords locally [39]. The highest degradation experienced was 5% compared to a traditional iris recognition system with EER reported at 1.32% for CASIAv3. Another chaos-based cancelable scheme encrypted iris features by using a modified Logistic map. The best performance of this scheme is still inevitably suffered from a 41% of degradation compared to its original system. Indexing-first-one (IFO) hashing [17] is able to create strong resistance against numerous privacy attacks with its non-invertible formulations such as Hadamard Product and Modulo Threshold functions. This protected scheme is able to achieve low EER of 0.54% with the corresponding degradation of 42.10% in performance. Despite the significant improvement in performance and security of recent iris template protection schemes, degradation in performance is still observable when comparing against unsecured iris recognition system. Besides that, there is also lack of a generalized approach which can improve the performance of these reputed BTP schemes.

3. Methodology

3.1. Problem Definition

From the previous section of this article, we observed that performance degradation in terms of accuracy and error rate was inevitable after the implementation of BTP scheme. This swas due to the fact that intentional matrix distortion, random permutation and remapping are among the techniques used to achieve irreversibility and unlinkability in most of the BTP schemes. This implies loss and distortion of biometric information in this process. In the methodology of Bloom filter [16], binary to decimal value function is used along with index remapping technique. Therefore, certain degrees of information loss can be expected through this mapping. For instance, using a word size of 5 for the Bloom filter, five neighboring binary bits in a column will be converted to a decimal value. The decimal value will then be remapped into its respective index position in the Bloom filter. In this process, part of the information of these binary bits is lost in exchange for a decimal value as the final outcome. Referring to the recommended level of information for better security [30] against coalition attack, an information loss of 80% can be anticipated through block remapping. If we consider this on a decimal value '1' which is produced by every '5' binary values, the total information loss can be higher for a longer word size. This improves the strength of the system, but the false non-match rate will increase as well. Hence, there is always a tradeoff between the security and usability of a system.

In a separate example, another type of information loss can be anticipated in the process of Hadamard multiplication between permuted iris codes in BTP scheme such as IFO hashing [17]. In Figure 1b, there are 3 permuted iris codes. Hadamard multiplication process of IFO hashing can be represented by AND-operation between the permuted iris codes. The new iris code is now '01000', which has experienced information loss through AND-operation as illustrated. This is a common methodology in designing BTP scheme because the anticipated information loss is to prevent the restoration of biometric data. The scheme has experienced loss of information through the product codes generated from the permuted biometric data instead of value remapping as shown in Figure 1a like in Bloom filter. These two methodologies are commonly introduced in BTP schemes with the purpose of strengthening the privacy or security protection through loss of information.

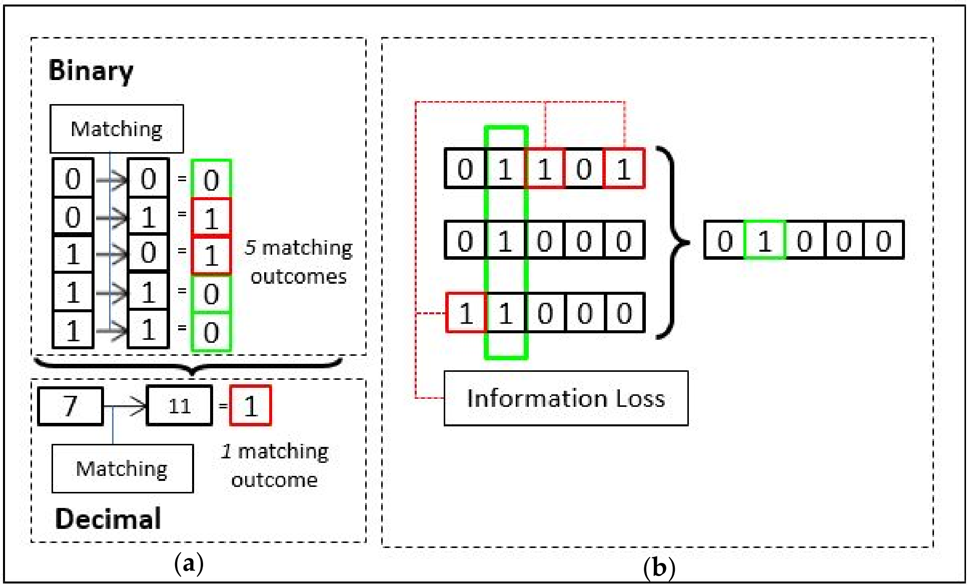


Figure 1. The difference in the number of matching outcomes before/after binary-to-decimal transformation (**a**) and the loss of information through the product of binary codes (**b**).

The purpose of stating the examples above is not to point out the degree of information loss nor the weakness of the BTP systems. In fact, information loss can happen in almost every BTP scheme. It serves as a double edge sword in a BTP scheme. The more information we lose in the process of template protection, the harder it is for others to reconstruct the raw biometric features. On the contrary, this also means that information loss will inevitably cause performance degradation.

Ideally, an optimum BTP scheme will need to achieve extensive information loss while maintaining minimal performance degradation. However, the requirement of stronger security imposes a trade-off between information loss and recognition performance. Stronger security in protection scheme is likely to have more severe performance degradation [40] while schemes which maintain recognition accuracy are often left with unattended doubts in security.

3.2. Overview of the Proposed Method

To mitigate the problems outlined in the previous section, confidence matrix generation scheme is proposed to improve the performance of protected biometric systems. The proposed method relaxes the tradeoff suffered by most of the BTP schemes in finding a balance between security strength and recognition performance. In other words, our proposed method enables BTP schemes to gain adequate security strength without worrying about its drawback in recognition performance. Preliminary work regarding confidence bits was tested on one BTP scheme in [41]. In this paper, we have proposed a more comprehensive scheme for confidence matrix generation with thorough experiments and analysis on various publicly available iris databases.

Our proposed method, confidence matrix generation, will take place only after BTP scheme. Figure 2 shows the basic design of a protected biometric system with and without confidence matrix generation scheme. A standard system will first acquire, process, and extract pertinent features given raw iris data. The extracted iris features will then undergo BTP in order to conduct matching in a more secured domain during the authentication stage. Our proposed design consists of a confidence matrix generation stage and the authentication stage. After BTP, a confidence matrix can be generated directly with at least two protected biometric samples from each enrolled personnel. When arbitrary iris data are being tested against another biometric sample, authentication can be carried out in a secured domain between hashed templates based on our proposed confidence scoring system.

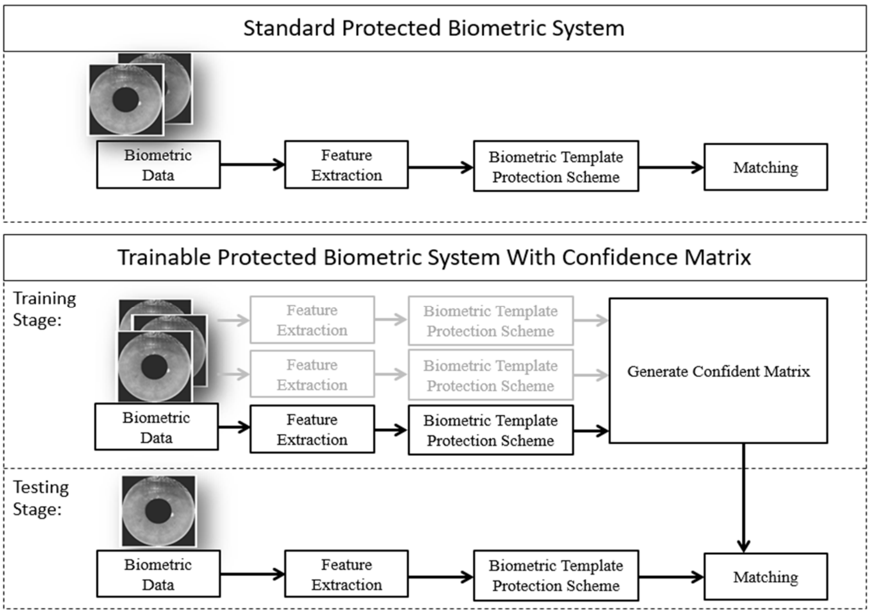

Standard Protected Biometric System
Biometric Data
Feature Extraction
Biometric Template Protection Scheme
Matching
Trainable Protected Biometric System With Confidence Matrix
Training Stage:
Feature Extraction
Biometric Template Protection Scheme
Feature Extraction
Biometric Template Protection Scheme
Biometric Data
Feature Extraction
Biometric Template Protection Scheme
Generate Confident Matrix
Testing Stage:
Biometric Data
Feature Extraction
Biometric Template Protection Scheme
Matching

Figure 2. Overview of the standard protected biometrics system and our proposed system.

3.3. Generation Stage

The main concept of the confidence matrix is to identify the confidence locations in the matrix, verify the results of a collision between two hashed templates and authenticate based on the final confidence score. The proposed method is flexible in the sense that there are no limitations in terms of ways to construct the confidence matrix and its properties. In this work, we have also proposed methods to construct confidence matrix into binary and fraction forms with their corresponding computation for confidence scores.

3.3.1. Generation Method for Binary Confidence Matrix

In the confidence matrix generation stage, multiple hashed templates can be used to generate a consolidated confidence matrix. The process of generating a confidence matrix is shown in Figure 3.

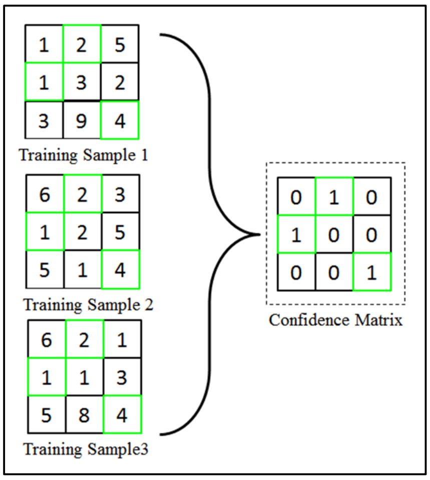


Figure 3. Process of generating binary confidence matrix.

From this illustrated example, three samples are selected randomly. For the generation of confidence matrix, element-based collision matching can be carried out between hashed samples:

$$N = {}^{n}C_{r} = \frac{n!}{r!(n-r)!} \tag{1}$$

where N denotes the maximum possible combinations, n is the number of training samples to choose from and r is the number of selected samples.

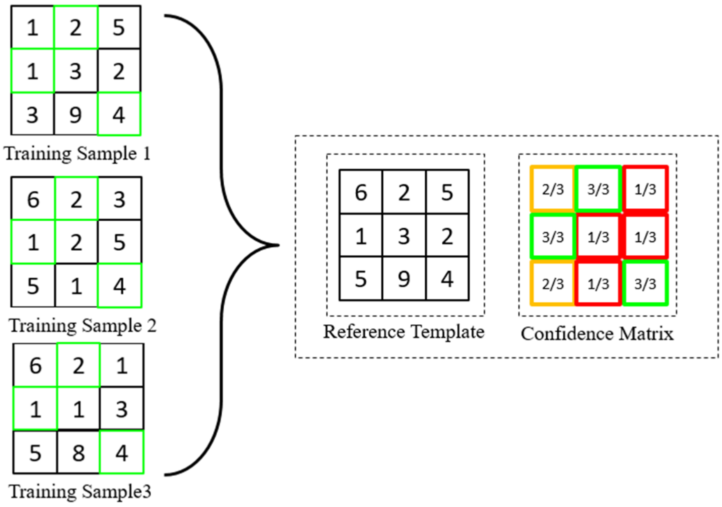
For this example, the number of combinations, N will equal to 3 when $r = 2$ and $n = 3$. Therefore, 3 sets of collision matching outcomes R_n will be obtained. Element-wise product rule is then used to obtain the collision matching outcomes to form the final confidence matrix, M as shown below:

$$M(x,y) = \begin{cases} 1, \; if \; \prod_{n=1}^{N} R_n(x,y) = 1 \\ 0, \; otherwise \end{cases} \tag{2}$$

The construction phase starts by creating a zero matrix with the same size as the hashed samples. Our proposed scheme will cross-match every element within the selected hashed training samples. The collision formula in the equation above is mainly indicating the confidence locations across multiple hashed samples by fusing all the outcomes of a collision via the product rule. The main purpose of the confidence matrix here is to identify hashed bits, which can be categorized as confidence bits. When all the paired training samples gives the same value in a particular location, a matched collision is fulfilled and this is defined as the confidence bit location. For instance, if the same value is found in all the hashed training samples at the same respective location (x,y) as in Figure 3, the value "1" will be assigned to that confidence location (x,y). If this condition is not fulfilled, the particular bit location will be labeled as "0" under "no confidence" location. Finally, a binary confidence matrix will be generated.

3.3.2. Generation Method for Probability Confidence Matrix

In this section, we would like to show the flexibility of our proposed concept by constructing the confidence matrix alternatively. We determine a confidence location in this matrix based on the frequency of matched collisions to have the final form in fraction instead of a binary bit this round. Note that our proposed method is different than fragile bits method [14]. First, the fragile bits method identifies bits, which have flipped more than a preset threshold to determine inconsistent bits. In our proposed method, we do not set any threshold and fraction is being used to represent the frequency of collisions as the main idea to construct the proposed confidence matrix for authentication. The method of generating a probability confidence matrix is different compared to binary confidence matrix. Instead of using the product rule to combine all the collision results, probability confidence matrix captures the frequency of matched collisions over the total number of collisions in a particular location. In binary confidence matrix, confidence location exists only if all the collisions at this particular location are matched collisions while disabling other locations, which do not fulfil this criteria. On the contrary, the probability confidence matrix takes every location in its matrix into account by calculating its respective frequency of matched collisions. The process of generating a probability confidence matrix is shown in Figure 4.



1	2	5
1	3	2
3	9	4

Training Sample 1

6	2	3
1	2	5
5	1	4

Training Sample 2

6	2	1
1	1	3
5	8	4

Training Sample3

6	2	5
1	3	2
5	9	4

Reference Template

2/3	3/3	1/3
3/3	1/3	1/3
2/3	1/3	3/3

Confidence Matrix

Figure 4. Process of generating probability confidence matrix.

Referring to the visual aid above, a reference template and a fraction matrix need to be generated. The value of the reference template, $R(x, y)$ is generated based on the value, which appears the most on coordinate (x, y) across the hashed samples. Otherwise, the default value at sample 1 will be taken. As information from multiple hashed samples are utilized in this formation, the reference template has higher reliability in representing the characteristic of a class. This is because a portion of noise can already be filtered through the process of template generation. The fraction matrix tabulates the corresponding percentage of matched collisions in each location of the reference template. This matrix is very important to determine the degree of confidence in each location. For instance, $R(1, 1)$ in Figure 4 indicates a confidence of $2/3$, which is equivalent to 66.7%. The confidence in probability is calculated based on the matched collisions for value '6' in 2 out of 3 hashed samples. Taking $R(3, 3)$ as another example, the corresponding confidence is $3/3$ (100%) indicating that 3 matched collisions out of 3 hashed samples. As a result, the location at $R(3, 3)$ of the reference template has higher confidence compared to the location at $R(1, 1)$. Thus, the generation of a reference template and its corresponding fraction matrix will form the final probability confidence matrix.

3.4. Authentication Stage

The authentication stage takes place after the confidence matrix of each class is successfully constructed. The proposed strategy is different from the traditional method where two hashed templates are directly compared to produce the matching result. Instead, the confidence matrix serves as the reference in validating matching (collisions) outcomes to improve the recognition performance. Note that our focus in this paper is to have a generalized solution to improve the performance of BTP schemes without any modification. Knowing the information from the confidence mask would imply that the attacker has succeeded in performing the frequency analysis based attack on the protected template. In order to address the mentioned security threat, we propose to adopt AES [42] to encrypt the confidence mask. Thus, a decryption process is needed before authentication can be conducted.

3.4.1. Matching Strategy for Binary Confidence Matrix

In authentication, hashed template 1 will first undergo our proposed element-wise collision matching function with hashed template 2 to produce a collision result matrix as shown in Figure 4. After that, we can then apply AND logic function to validate the collision result with a class-specific confidence matrix. This authentication process can be carried out by determining the total number of matched collisions at the confidence locations. Finally, a proposed matching score can be formulated as follows:

$$Matching\ score = \frac{sum(Final\ Result == 1)}{sum(Confidence\ Matrix == 1)} \tag{3}$$

Referring to Figure 5 below, the matching score of this example is equal to 0.667 where there are two collided bits identified at the confidence bit locations over a total of 3 confidence bit-locations as indicated in the binary confidence matrix. The matching score of Equation (3) is also formulated mathematically in Equation (7).

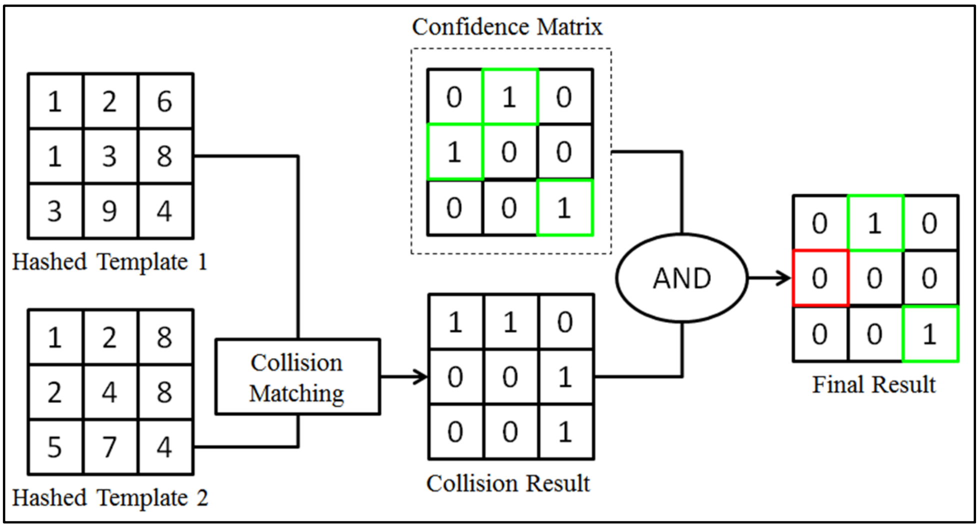


Figure 5. Proposed matching strategy for binary confidence matrix.

3.4.2. Matching Strategy for Probability Confidence Matrix

On the other hand, class-specific reference template generated at an earlier stage will be used to authenticate any query hashed template to produce the collision result matrix. This is then followed by the dot product between the probability confidence matrix and collision result matrix to obtain the final matrix. The proposed strategy not only determines the collided bits but also estimates the degree of confidence at the collided bit-locations. As a result, the final matching score can then be computed as follows:

$$Matching\ score = \frac{sum\ of\ fractions\ (Final\ Result)}{sum\ of\ fractions\ (Confidence\ matrix)} \tag{4}$$

From the Figure 6, the matching score is equal to 0.5291 (3.00/5.67).

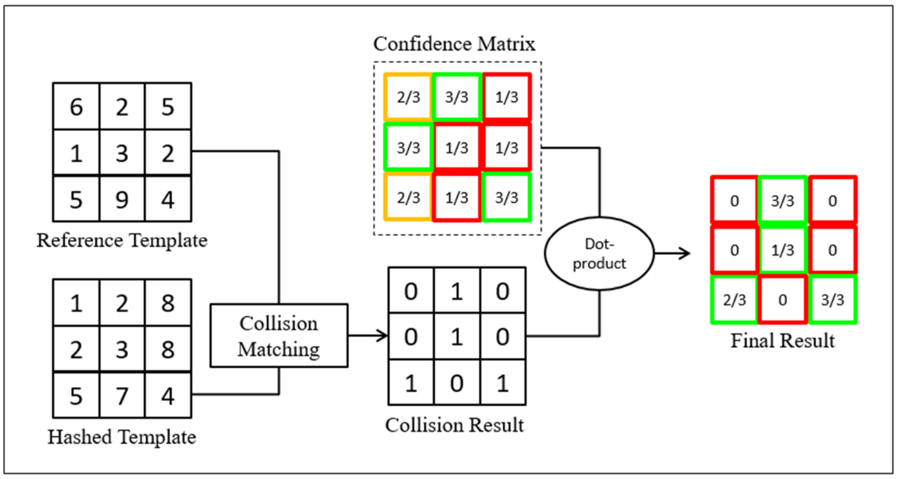


Figure 6. Proposed matching strategy for probability confidence matrix.

3.5. Iris Database with Noise-Mask

In order to increase the flexibility in implementing our proposed method, the existence of noise masks in several publicly available iris databases is worth to be considered in the experiments to improve the recognition performance. As one of the contributions in this paper, a solution is proposed to enable the integration of noise mask into popular BTP schemes, Bloom filter [16] and IFO [9] with no feature alignment process, will be used in our experiments. An example of noise mask is shown in Figure 7.

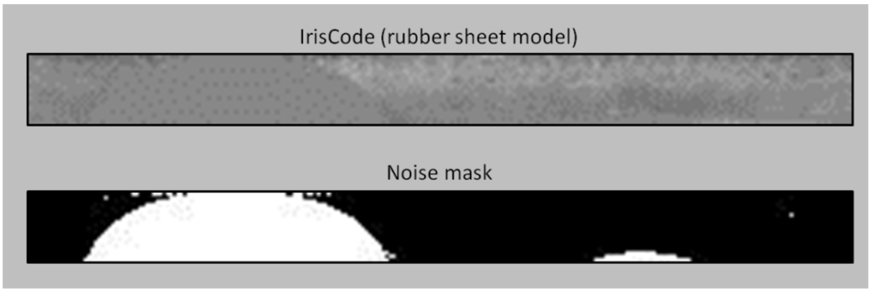


Figure 7. Visualization of iris code and noise mask (bottom).

First, a brief explanation on the methodology of Bloom filter is demonstrated in Figure 8 below. Any arbitrary matrix of iris code will be separated into multiple iris blocks according to the word size, w and number of codeword, n. In each iris block, a column-wise binary to decimal function is used to convert binary values into decimal values. The converted decimal values are then remapped into its associated index location (column) of a row matrix, R_n. The process will be repeated for the next iris block $(w \times n)$ and the converted decimal values will be remapped again according to the indices of the next row matrix, R_{n+1}.

In order to enable the implementation of Bloom filter onto database with noise mask, a threshold based approach is proposed to determine which iris block can be considered as "noisy block". By pre-setting a threshold T ($T = 0.1$ is used in our experiment), if the number of noisy bits in any iris block is more than the preset threshold, the corresponding row matrix R_n will be considered as 'null' row and excluded from the calculation of matching score as shown in Figure 9. The proposed approach is also applicable for IFO hashing with Bloom filter integration to solve alignment-issue when biometric template acquisition.

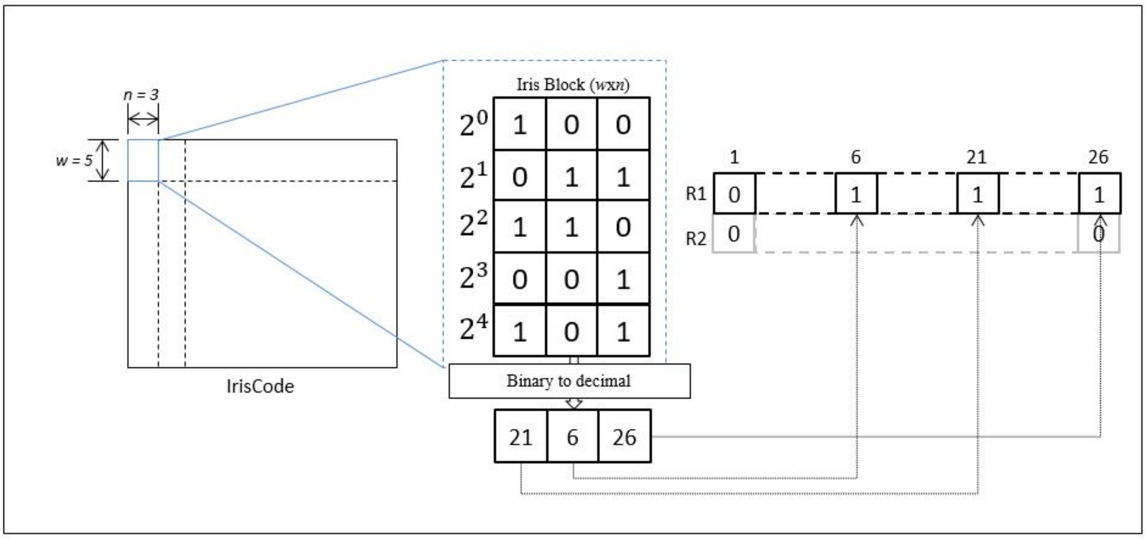


Figure 8. Overview of the methodology of Bloom filter.

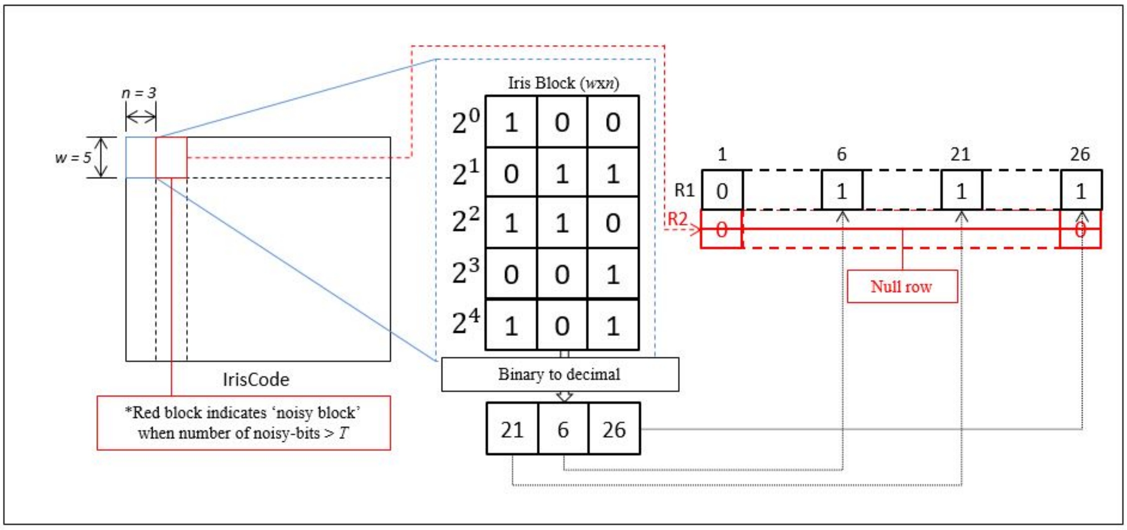


Figure 9. Overview of the methodology of Bloom filter with the proposed noise-mask solution.

4. Results

4.1. Iris Databases

In this project, four publicly available Near Infrared (NIR) iris databases, CASIAv1 [43], CASIAv3 Iris-Interval [44], CASIAv4 Iris-Thousand [45] and ND0405 [46] databases are used in the experiments. The information of these experimented databases are shown in Table 1.

Table 1. List of iris databases.

Database	Number of Eye Images	Number of Class	Wavelength	Noise Mask (Y/N)
CASIAv1	756	108	NIR	Yes
CASIAv3	868	124	NIR	No
CASIAv4	331	100	NIR	Yes
ND0405	784	100	NIR	Yes

CASIAv1 consists of iris images, which are captured in two sessions by a self-developed camera with 850 nm NIR illuminators. All images are stored in BMP format with resolution

320 × 280. The pupil region is automatically detected and specular reflections from the NIR illuminators are masked out by a circular region of constant intensity. CASIAv3 Iris-Interval (referred to as CASIAv3 in this paper) is another database constructed through two sessions by a close-up homemade iris camera. The 320 × 280 iris images have very clear iris texture details due to its circular NIR LED array with optimal luminous flux for iris imaging. Left eye images from CASIAv3 are chosen to form a subset of the database, which contains 7 eye images for each class in this project.

CASIAv4 Iris-Thousand (referred to as CASIAv4 in this paper) contains images collected using a dual-eye iris camera IKEMB-100. The high-quality iris images with resolution 640 × 480 are captured with optimal pose adjustment. The intra-class variation are mainly specular reflections and eyeglasses. ND0405 is a large-scale database captured in NIR wavelength at a close distance by a LG2200 iris imaging system. Many real-world conditions appear in this iris database, leading to degradations such as blurring, occlusion, specular reflection, off-angle, etc. Some subjects wore contact lenses, which cause distortion on iris textures. Same as CASIAv4, both databases have uneven number of images per class. Referring to a similar work [47], CASIAv3 has the highest image quality, followed by CASIAv4, CASIAv1, and ND0405. To have a compatible variability and reasonable benchmarking between the databases, the first 100 classes of CASIAv4 and ND0405 are selected for the following experiments in this project.

4.2. Design of Experiment

The experiment below aims to examine the proposed scheme's ability to improve the performance of the iris template protection scheme when tested against iris databases with and without noise masks. The state-of-the-art BTP schemes, Bloom filter [16], and enhanced IFO hashing [9] are selected for performance evaluation as these schemes have been experimented thoroughly and widely applied in this field. Both schemes are well known with their good recognition performance and resistance against multiple attacks. Note that, enhanced IFO has incorporated Bloom filter to solve its alignment issue. In this experiment, these schemes have been tested by the selected databases with their respective recognition performance. The results are tabulated in terms of equal error rate (EER) when the false acceptance rate (FAR) is equal to the false rejection rate (FRR).

Table 2 above shows the EER performance of the proposed confidence matrices for iris databases hashed by enhanced IFO. During the process of obtaining the best results of Bloom filter from different word size, minimum word size of 3 is set. Smaller word size is ignored as the security strength will reduce. Different ranges of parameters of enhanced IFO are tested by referring to the optimal setting published in [9,48]. In this experiment, a clear decrease in EER (%) is observed from 4 different sets of databases. For iris databases that come with noise mask (CASIAv1, CASIAv4, ND0405), performance improvement ranging from 17.38% to 68.68% is observed when using for binary confidence matrix. On the other hand, performance improvement ranging from 65.40% to 82.33% is achieved using the probability confidence matrix. For CASIAv3, the database without noise-mask had achieved a reasonable performance improvement of 26.09% (binary confidence matrix) and 92.75% (probability confidence matrix).

Table 2. Recognition performance of the proposed scheme and state-of-the-arts BTP schemes.

Database	Equal Error Rate, %			
	Bloom Filter	Enhanced IFO Hashing	Proposed Binary Confidence Matrix	Proposed Probability Confidence Matrix
CASIAv1	5.91	5.81	4.80	2.01
CASIAv3	1.14	0.69	0.51	0.05
CASIAv4	8.11	6.17	1.64	1.08
ND0405	10.74	7.28	2.28	2.48

As a result, both proposed confidence matrix generation methods have successfully improved the recognition performance of the BTP scheme. On top of that, the results also proved the reliability of this approach when dealing with noise-masks associated databases. In the upcoming experiment, we have evaluated the construction of confidence matrices by using different number of training samples as shown in Table 3. The probability confidence matrix is able to generate lowest EER with 3 training samples. For instance, EER as low as 1.08% is reported for CASIAv4 database. In terms of performance, the observed deviation of error rate using 2 to 4 samples is less than 2% and 3% for binary and probability confidence matrix, respectively.

Table 3. Recognition performance of the proposed scheme with a different number of training samples.

Iris Database	Training Sample	Equal Error Rate (%)	
		Binary Confidence Matrix	Probability Confidence Matrix
CASIAv1	2	4.80	4.40
	3	5.01	2.01
	4	4.67	2.17
	5	3.11	2.12
	6	2.10	2.05
CASIAv4	2	3.02	3.90
	3	1.64	1.08
	4	1.41	2.82
	5	0.97	2.99
	6	1.42	2.89
ND0405	2	3.43	4.27
	3	2.28	2.48
	4	2.34	3.12
	5	2.11	3.17
	6	2.71	3.80
CASIAv3	2	0.51	0.49
	3	0.20	0.20
	4	0.27	0.05
	5	0.76	0.03
	6	0.88	0.09

From Table 3, the probability confidence matrix has outperformed the binary confidence matrix in our experiments conducted on CASIAv1 and CASIAv3. The deviation in performance can range from 0.5 to 3%. Both methods have reported equally low EER for CASIAv4. Binary confidence matrix, which extracts only the exact collisions, has a slightly better performance compared to the probability confidence matrix for ND0405, which is noisier. This is expected as the former method tends to eliminate more noise where there is no collision within all the training samples used.

The upper row of Figure 10 has shown the normalized genuine-imposter matching scores for all the adopted iris databases. The score distributions generated by the confidence mask are shown in the left column, whereas the plots in the right column are generated without the implementation of the confidence matrix. We can see that the confidence matrix enables better spread between genuine and imposter distributions visually. The mean matching scores of genuine and imposter are separated in a wider manner. This phenomena has greatly reduced the area of the overlapped region between genuine and imposter while shifting the intersected matching score more to the right. Empirically, the decidability indices [49] between IFO and our proposed method are recorded in Table 4. According to John Daugman [49], "decidability" of a decision is determined by the degree of overlap between two distributions. A standard measure of decidability for genuine-imposter score distribution can be defined as follows if the means of the two distributions are μ_1 and μ_2 and their standard deviations are σ_1 and σ_2:

$$d = \frac{|\mu_1 - \mu_2|}{\sqrt{\frac{1}{2}(\sigma_1^2 + \sigma_2^2)}} \tag{5}$$

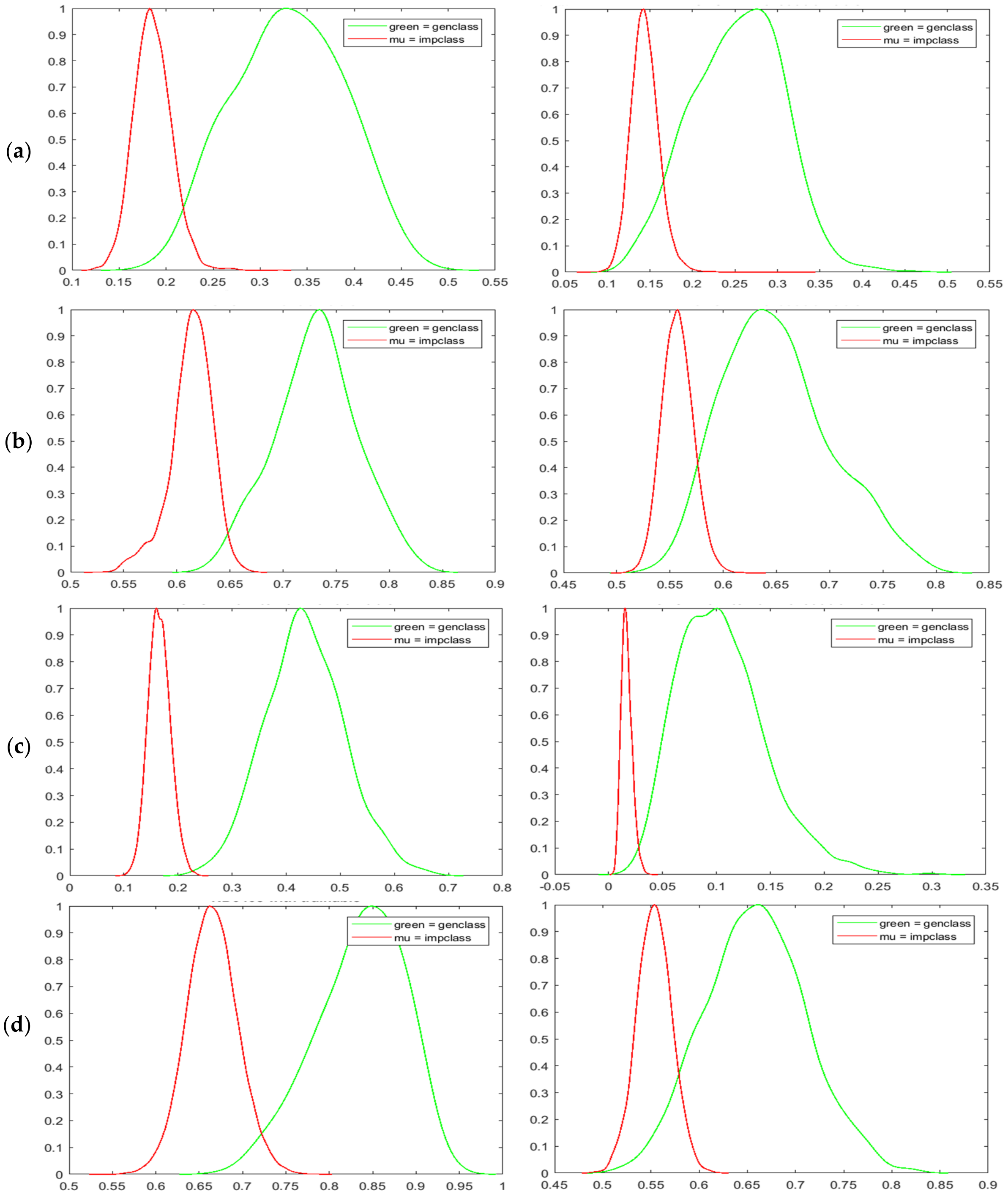


Figure 10. Genuine-imposter score distributions for (**a**) CASIAv1 (**b**) CASIAv4 (**c**) CASIAv3 (**d**) ND0405.

Table 4. Decidability measure for IFO and confidence matrix.

Methods	**Iris Databases**			
	CASIAv1	**CASIAv4**	**ND0405**	**CASIAV3**
Enhanced IFO	2.772	2.521	2.641	4.94
Confidence Matrix (binary/probability)	3.624/3.404	4.567/3.859	4.12/3.7064	5.92/4.91

Better decidability indices for genuine-imposter distributions are proven achievable through the implementation of our proposed scheme as shown in Table 4. As an additional reference, Receiver Operating Characteristic Curves (ROCs) are also plotted with True Positive Rate (TPR) against the False Positive Rate (FPR) to measure the separability of classes. The ROCs of binary confidence matrix in Figure 11a and probability confidence matrix in 11b are plotted against enhanced IFO for iris databases CASIAV1, CASIAV4, and ND0405 (arranged in rows). Improvement in recognition performance have been observed in all ROC graphs. In overall, all the statistical and empirical studies conducted on the proposed method have indicated an increase in recognition performance and decidability.

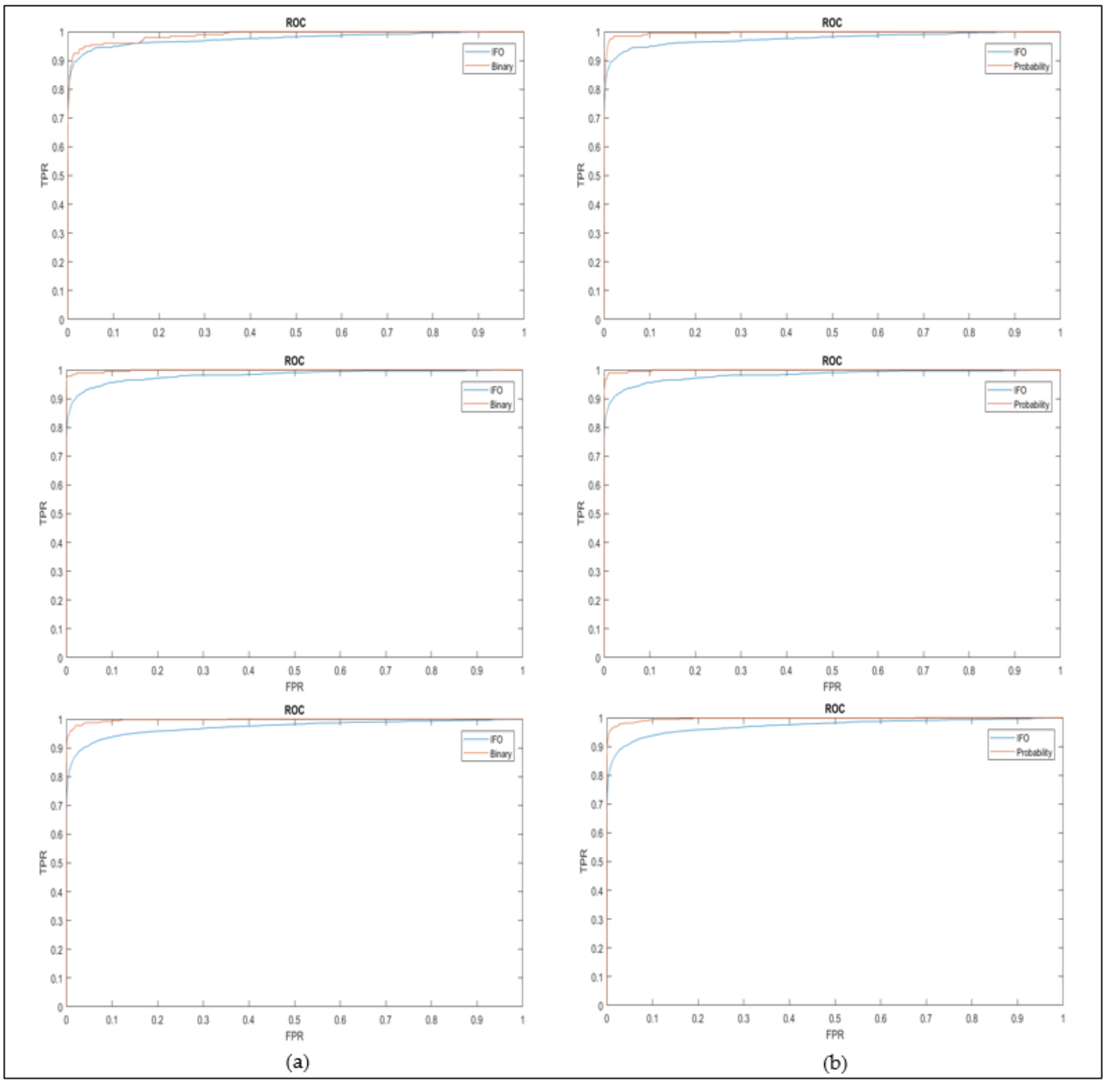


Figure 11. Example of ROC plots for the implementation of (**a**) binary and (**b**) probability confidence against enhanced IFO.

5. Security Model

The security model will be focused on the case when an attacker is trying to attack the reference template to get confidential information. If confidence information leaks, it leads to permanent identity loss as biometrics are individually associated. In view of this, frequency analysis-based attacks like Attack via Record Multiplicity (ARM) is the common threat for this approach.

Under binary confidence matrix, the reference template contains the locations of confidence bits. Compromising the reference template indeed enables the construction of binary mask. Thus, we would like to calculate the complexity in getting all ones in the mask. Randomly taking a hashed reference template of size 5940 × 50 from the databases, which is equivalent to $297,000$ elements with 143,038 confident bits. The complexity of this attack to be successful can be estimated as ${}^{297,000}\mathrm{C}_{143,038} \gg 6.39 \times 10^{89,315}$ combinations.

For the probability confidence matrix, non-binary values in each reference template are non-zero. The confidence values are calculated as a probability instead of binary. It is difficult for the attacker to know the exact confidence location where the perfect matched collision happens (i.e., confidence score of 3/3 if the same number occurs at the same position across 3 hashed samples). Given a more relaxing security situation by assuming that the system can be compromised with a success probability of 0.33 instead of 1, the complexity of this probability can be assessed. In other words, his scenario is equivalent to the probability of guessing the positions in the reference template with probability of $1/3$ (1 occurrence out of 3) correctly. The probability of the attacker in getting $\boldsymbol{k}$ positions among n tries given unlimited computation power can be estimated through:

$$p_X(k) = \mathbf{Pr}(X = k) = \frac{\begin{pmatrix} K \\ k \end{pmatrix}\begin{pmatrix} N-K \\ n-k \end{pmatrix}}{\begin{pmatrix} N \\ n \end{pmatrix}} \tag{6}$$

where N is the population size, $\boldsymbol{K}$ is the number of success states in the population, n is the number of draws, $\boldsymbol{k}$ is the number of observed successes and $\begin{pmatrix} a \\ b \end{pmatrix}$ is a binomial coefficient.

The success probability of attacker $\boldsymbol{p_X(k)}$ in this case is equivalent to the matching score of our probability confidence matrix as shown in Equation (4) since $\frac{\boldsymbol{(\#1/3)}}{\boldsymbol{sum\ of\ probabilities\ from\ all\ positions}}$. In another words, the attacker can only achieve the matching score if he can get k positions with probability $1/3$. Same scenario is applicable to obtain positions for other probabilities such $2/3$ or $3/3$. If an attacker is able to get most of the positions of a probability, other probabilities can be revealed. Using the same random protected template, the number of positions with probability $1/3$ are found to be $\boldsymbol{K} = 25,543$ from a template size of $N = 297,000$. Referring to Rathgeb et al. [50], it is acceptable that 2^{200} can be considered as computationally infeasible for an attack on arbitrary secure iris template. Thus, this is approximately ${}^{297,000}\mathrm{C}_{13}$ for our case where the number of trials allowed are only as low as $n = 13$. Using the determined parameter, the success probability for an attack can then be estimated at:

$$p_X(k) = \mathbf{Pr}(X = k) = \frac{\begin{pmatrix} 25,543 \\ k \end{pmatrix}\begin{pmatrix} 297,000 - 25,543 \\ \mathbf{13} - k \end{pmatrix}}{\begin{pmatrix} 297,000 \\ \mathbf{13} \end{pmatrix}} = \frac{\begin{pmatrix} 25,543 \\ k \end{pmatrix}\begin{pmatrix} 271,457 \\ \mathbf{13} - k \end{pmatrix}}{\begin{pmatrix} 297,000 \\ \mathbf{13} \end{pmatrix}} \tag{7}$$

The success probability in Equation (7) is positive when $0 \le \boldsymbol{k} \le 13$. Theoretically, $\boldsymbol{k} \approx \frac{n}{2}$ can be the approximation for the lower bound of the observed success, while the highest observed success can be 12 out of 13 draws. As a result, the success probability of an attack is estimated to be within the range of $1.92 \times 10^{-12} \le \mathbf{Pr}(X = k) \le 3.48 \times 10^{-5}$. An attacker needs to go through a computation complexity of 2^{200} steps before he can achieve a low success probability of 1.92×10^{-12}. In view of this, the attack becomes highly complicated. This is because more n positions are needed to increase the matching score in real case scenario and this will extensively increase the computation complexity of $^{\mathrm{N}}\mathrm{C}_{\mathrm{n}}$ before obtaining the low success probability. In addition, note that the increase of template size, N will increase the complexity exponentially. Using the example above, the matching score of the confidence matrix can be further expressed as:

$$\boldsymbol{Matching\ score} = \frac{\boldsymbol{k_1}\left(\frac{1}{t}\right) + \boldsymbol{k_2}\left(\frac{2}{t}\right) + \boldsymbol{k_3}\left(\frac{3}{t}\right)}{\boldsymbol{n_1}\left(\frac{1}{t}\right) + \boldsymbol{n_2}\left(\frac{2}{t}\right) + \boldsymbol{n_3}\left(\frac{3}{t}\right)} = \left(\frac{\boldsymbol{k_i}}{\sum_{i=1}^{t} \boldsymbol{n_i}}\right) \tag{8}$$

where $i = 1, 2, \ldots,\ \boldsymbol{t}$ is the $i - th$ number of training samples used for the construction of confidence matrix ($\boldsymbol{t} = 3$ is used for the example above). Theoretically, the higher the expected number of collisions $\boldsymbol{k}_i$, the higher is the matching score. However, the increase of $\boldsymbol{k}_1$ will inevitably reduce the success probability of an attacker, as shown in Equation (7). Hence, we can fairly say that it is computationally infeasible by looking at the large amount of steps incurred even before achieving the success probability, which can be negligible. This is because the computation will also become infeasible if a larger template size is used due to the asymptotic behavior caused by the increase of N or $\boldsymbol{k}$. Thus, the requirement of irreversibility for our proposed scheme has been fulfilled.

Unlinkability emphasizes that multiple protected templates generated from the same Iriscode should be indistinguishable from each other. To evaluate the unlinkability of our proposed scheme, the method proposed by Gomez et al. [7] is adopted. The unlinkability can be evaluated by the mated and non-mated score distributions. The mated scores are generated by matching between protected templates of the same subject using different sets of hashing functions, h while non-mated scores refer to the matching of protected templates belonged to different subjects using different sets of h. The unlinkability property of a biometric system is fulfilled if there is an overlap between the score distributions of mated and non-mated distributions [7].

Let $P(s|M_s)$ be the conditional probability of a similarity score $s \in [0, 1]$ that belongs to the mated matching group M_s and $P(s|M_s')$ denotes the conditional probability of a similarity score s that belongs to the non-mated group M_s'. Two protected templates are said to have linkage if it is more likely that both templates are mated samples (M_s) rather than non-mated samples (M_s') given a score s: $P(M_s|s) > P(M_s'|s)$. The unlinkability property is characterized by the local linkability:

$$D(s) = 2\frac{\omega LR(s)}{1 + \omega LR(s)} - 1 \tag{9}$$

Given that $\omega LR(s) = \frac{P(s|M_s)}{P(s|M_s')} > 1$ where $LR(s)$ is the likelihood ratio between the known probabilities $P(s|M_s)/P(s|M_s')$ and $\omega = P(M_s)/P(M_s')$ denotes the ratio between the unknown probabilities of the *mated samples* and *non-mated samples* distributions. We can assume that $P(M_s) = P(M_s')$, thus set $\omega = 1$. The system's overall linkability can be further defined as:

$$D_{sys} = \int D(s) \cdot P(s|M_s) ds \tag{10}$$

This measure is within the range of $D_{sys} \in [0, 1]$ with zero represents full unlinkability and unity for system, which is completely linkable. Therefore, to attain the unlinkability of a BTP scheme, it is desirable to show that D_{sys} is negligibly small.

Figure 12 depicted three different graphs of CASIAv1, CASIAv4 and ND0405 generated using our proposed binary (first row) and probability (second row) confidence matrices using the same parameter settings with 3 training samples. All the mated and non-mated score distributions showed significant overlapping and negligibly small value of $D_{sys\ (binary)} = 0.008, 0.014, 0.05$; $D_{sys\ (probability)} = 0.005, 0.01, 0.009$ respectively. Therefore, we assert that the proposed scheme fulfills the criteria on unlinkability.

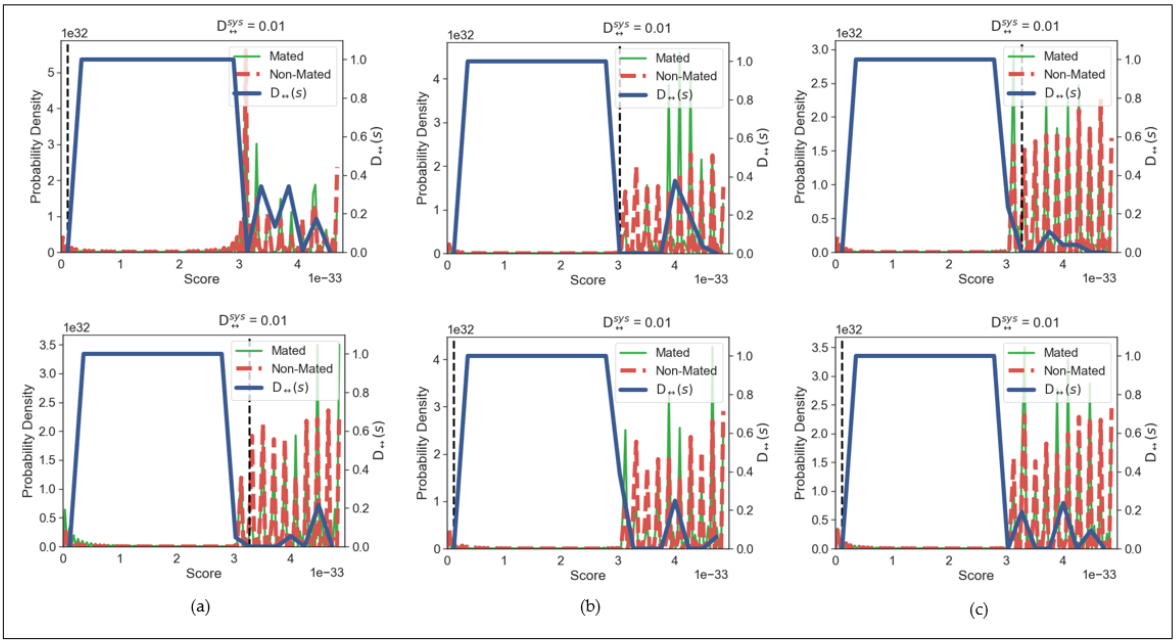


Figure 12. Unlinkability analysis of the proposed binary (first row) and probability (second row) confidence matrices for databases (**a**) CASIAv1, (**b**) CASIAv4, (**c**) ND0405.

6. Discussion

From the result obtained in the previous section, improvement in performance has been proven on all four different publicly available iris databases using our proposed methods. The proposed scheme is able to mitigate the performance degradation caused by BTP scheme in existing biometrics recognition system. However, there are still several key points, which are worth to be discussed. First, a solution has to be formulated to overcome the implementation problem since most of the publicly available databases come with noise masks. The conventional Bloom filter and Indexing-first-one hashing scheme did not attempt to solve this problem, which can potentially be a roadblock in mitigating performance degradation.

A noise mask serves as an aid to determine the noisy pixels within the biometric template. These pixels will be excluded at the matching stage of protected biometric templates. The enhanced IFO hashing scheme, which does not require alignment, will first divide the iris data into different blocks of Bloom filters. Our proposed solution is to first determine the acceptable noise level of a protected iris recognition system through a noise threshold. When a Bloom filter block has exceeded the acceptable noise level, the corresponding row of hashed data will be considered as null and thus excluded during the matching stage in the secure domain. This approach enables our proposed method to work with any iris database with associated noise masks. However, note that higher requirement on the noise level of your protected iris recognition system might cause a larger amount of null rows. This can lead to unnecessary information loss and greatly reduce the amount of information available for confidence matrix generation. Therefore, our proposed probability confidence matrix is useful in optimizing the matching accuracy through probabilities of collision in this situation.

On the other hand, experiments between the two proposed methods have been carried out in this research. Firstly, we studied the relationship between the number of training samples and the performance of our proposed methods. The generated results have indicated that 3 training samples have the optimum performance in most of the tested databases. Our proposed binary confidence matrix has shown better performance when it is tested with lower quality iris images, while the probability confidence matrix performs better when dealing with better quality iris images. In a nutshell, the proposed binary confidence matrix has a higher tolerance to noise because of its nature in eliminating noise via the implementation of AND logic operation. Thus, this approach is more suitable to improve the performance of protected biometric templates, which are captured under challenging and non-cooperative environments.

7. Conclusions

In this paper, we have proposed two methods to mitigate the performance degradation in a protected iris recognition system due to the implementation of a BTP scheme. The reported EER is as low as 0.05% for higher quality iris images, around 1% for moderately good quality iris images, and less than 2.5% for the lowest quality iris images tested on the publicly available iris databases. As shown in Table 2, the proposed methods have successfully improved the performance of state-of-the-art BTP in our experiments by 68.68% in the best scenario. Our proposed binary-based confidence matrix is capable of mitigating the performance degradation of noisy protected biometric templates, whereas the proposed probability-based approach performs better with higher quality iris images captured under a more controlled environment. In addition, our proposed confidence matrix has also taken into consideration the existence of a noise mask in this implementation. In this case, our design provides flexibility with no modification required on BTP schemes while reducing performance degradation at the secured matching stage.

Author Contributions: Methodology, T.-Y.C.; Supervision, B.-M.G. and W.-S.Y.; Writing—original draft, T.-Y.C.; Writing—review & editing, B.-M.G. and W.-S.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Fundamental Research Grant Schemes (FRGS) with grant number, FRGS/1/2016/ICT02/UTAR/03/1.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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. Cimato, S.; Gamassi, M.; Piuri, V.; Sassi, R.; Scotti, F. Privacy in biometrics. In Proceedings of the Biometrics: Fundamentals, Theory, and Systems, Anaheim, CA, USA, 8–12 December 2008.
3. 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] [PubMed]
4. Cavoukian, A.; Stoianov, A. Biometric encryption. In *Encyclopedia of Cryptography and Security*; Springer: Boston, MA, USA, 2011. [CrossRef]
5. Simoens, K.; Yang, B.; Zhou, X.; Beato, F.; Busch, C.; Newton, E.M.; Preneel, B. Criteria towards metrics for benchmarking template protection algorithms. In Proceedings of the 2012 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, 29 March–1 April 2012; pp. 498–505.
6. Inuma, M. A relation between irreversibility and unlinkability for biometric template protection algorithms. *Josai Math. Monogr.* **2014**, *7*, 55–65.
7. Gomez-Barrero, M.; Galbally, J.; Rathgeb, C.; Busch, C. General framework to evaluate unlinkability in biometric template protection systems. *IEEE Trans. Inf. Forensics Secur.* **2017**, *13*, 1406–1420. [CrossRef]
8. Mitzenmacher, M. Compressed bloom filters. *IEEE/ACM Trans. Netw.* **2002**, *10*, 604–612. [CrossRef]
9. 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.
10. Prabhakar, S.; Pankanti, S.; Jain, A.K. Biometric recognition: Security and privacy concerns. *IEEE Secur. Priv.* **2003**, *1*, 33–42. [CrossRef]
11. Rathgeb, C.; Uhl, A. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J. Inf. Secur.* **2011**, *2011*, 1–25. [CrossRef]

12. Patel, V.M.; Ratha, N.K.; Chellappa, R. Cancelable biometrics: A review. *IEEE Signal Process. Mag.* **2015**, *32*, 54–65. [CrossRef]
13. Natgunanathan, I.; Mehmood, A.; Xiang, Y.; Beliakov, G.; Yearwood, J. Protection of privacy in biometric data. *IEEE Access* **2016**, *4*, 880–892. [CrossRef]
14. Hollingsworth, K.P.; Bowyer, K.W.; Flynn, P.J. The best bits in an iris code. *IEEE Trans. Pattern Anal. Mach. Intell.* **2009**, *31*, 964–973. [CrossRef]
15. Hollingsworth, K.P.; Bowyer, K.W.; Flynn, P.J. Improved iris recognition through fusion of hamming distance and fragile bit distance. *IEEE Trans. Pattern Anal. Mach. Intell.* **2011**, *33*, 2465–2476. [CrossRef] [PubMed]
16. 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.
17. 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]
18. 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]
19. Teoh, A.B.; Kuan, Y.W.; Lee, S. Cancellable biometrics and annotations on biohash. *Pattern Recognit.* **2008**, *41*, 2034–2044. [CrossRef]
20. Zuo, J.; Ratha, N.K.; Connell, J.H. Cancelable iris biometric. In Proceedings of the ICPR 2008 19th International Conference on Pattern Recognition, Tampa, FL, USA, 8–11 December 2008; pp. 1–4.
21. 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]
22. 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.
23. 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.
24. Noto, S.; Correia, P.L.; Soares, L.D. Analysis of error correcting codes for the secure storage of biometric templates. In Proceedings of the 2011 IEEE EUROCON-International Conference on Computer as a Tool, Lisbon, Portugal, 27–29 April 2011; pp. 1–4.
25. Merkle, J.; Niesing, M.; Schwaiger, M.; Ihmor, H.; Korte, U. Security capacity of the fuzzy fingerprint vault. *Int. J. Adv. Secur.* **2010**, *3*, 146–168.
26. Tams, B. Attacks and countermeasures in fingerprint based biometric cryptosystems. *arXiv* **2013**, arXiv:1304.7386.
27. 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. Manand Cybern. Part B (Cybern.)* **2008**, *38*, 1302–1313. [CrossRef]
28. Rathgeb, C.; Uhl, A. Privacy preserving key generation for iris biometrics. In Proceedings of the2010 IFIP International Conference on Communications and Multimedia Security, Linz, Austria, 31 May–2 June 2010; pp. 191–200.
29. Hämmerle-Uhl, J.; Pschernig, E.; Uhl, A. Cancelable Iris Biometrics Using Block Re-mapping and Image Warping. In Proceedings of the 2009 ISC, Pisa, Italy, 7–9 September 2009; pp. 135–142.
30. 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.
31. Ouda, O.; Tsumura, N.; Nakaguchi, T. On the security of bioencoding based cancelable biometrics. *IEICE Trans. Inf. Syst.* **2011**, *94*, 1768–1777. [CrossRef]
32. Lacharme, P. Analysis of the iriscodes bioencoding scheme. *Int. J. Comput. Sci. Softw. Eng. (IJCSSE 2012)* **2012**, *6*, 315–321.
33. 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, 18–20 September 2019; pp. 1–6.
34. 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.
35. 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]
36. Gomez-Barrero, M.; Rathgeb, C.; Li, G.; Ramachandra, R.; Galbally, J.; Busch, C. Multi-biometric template protection based on bloom filters. *Inf. Fusion* **2018**, *42*, 37–50. [CrossRef]
37. Sadhya, D.; Raman, B. Generation of cancelable iris templates via randomized bit sampling. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2972–2986. [CrossRef]
38. 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), New Delhi, India, 19–20 February 2015; pp. 785–790.
39. Zhao, D.; Fang, S.; Xiang, J.; Tian, J.; Xiong, S. Iris template protection based on local ranking. *Secur. Commun. Netw.* **2018**, *2018*, 1–9. [CrossRef]
40. Nandakumar, K.; Jain, A.K. Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Process. Mag.* **2015**, *32*, 88–100. [CrossRef]
41. Chai, T.-Y.; Goi, B.-M.; Tay, Y.-H. The Construction of Confidence Bits to Improve Protected Iris Recognition System. *Int. J. Adv. Soft Compu. Appl* **2019**, *11*, 81–93.

42. Hao, F.; Anderson, R.; Daugman, J. *Combining Cryptography with Biometrics Effectively*; Computer Laboratory, University of Cambridge: Cambridge, UK, 2005.
43. Chinese Academy of Sciences. CASIA Iris Image Database V1.0. 2003. Available online: http://biometrics.idealtest.org/dbDetailForUser.do?id=1 (accessed on 2 April 2021).
44. Chinese Academy of Sciences. CASIA Iris Image Database V3.0-Interval. Available online: http://biometrics.idealtest.org (accessed on 2 April 2021).
45. Biometrics Ideal Test. CASIA Iris Thousand Database V4.0. 2014. Available online: http://biometrics.idealtest.org/dbDetailForUser.do?id=4 (accessed on 2 April 2021).
46. Phillips, P.J.; Scruggs, W.T.; O'Toole, A.J.; Flynn, P.J.; Bowyer, K.W.; Schott, C.L.; Sharpe, M. FRVT 2006 and ICE 2006 large-scale experimental results. *IEEE Trans. Pattern Anal. Mach. Intell.* **2009**, *32*, 831–846. [CrossRef] [PubMed]
47. Hu, Y.; Sirlantzis, K.; Howells, G. Optimal generation of iris codes for iris recognition. *IEEE Trans. Inf. Forensics Secur.* **2016**, *12*, 157–171. [CrossRef]
48. Lai, Y.-L.; Jin, Z.; Goi, B.-M.; Chai, T.-Y.; Yap, W.-S. Iris Cancellable Template Generation Based on Indexing-First-One Hashing. In Proceedings of the 2016 International Conference on Network and System Security, Taipei, Taiwan, 28–30 September 2016; pp. 450–463.
49. Daugman, J. *Biometric Decision Landscapes*; Computer Laboratory, University of Cambridge: Cambridge, UK, 2000.
50. Rathgeb, C.; Uhl, A. Secure iris recognition based on local intensity variations. In Proceedings of the 2010 International Conference Image Analysis and Recognition, Póvoa de Varzim, Portugal, 21–23 June 2010; pp. 266–275.