Available online at www.sciencedirect.com
ScienceDirect
journal homepage: www.elsevier.com/locate/cose
Computers & Security

A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping

Rudresh Dwivedi *, *Somnath Dey*, *Ramveer Singh*, *Aditya Prasad*

Discipline of Computer Science & Engineering, Indian Institute of Technology Indore, Indore, India

ARTICLE INFO

Article history:
Received 23 November 2015
Received in revised form 20 September 2016
Accepted 17 October 2016
Available online

Keywords:
Biometrics
Iris biometric
Cancelable biometrics
Security
Privacy

ABSTRACT

Biometric-based recognition systems have overcome passive issues of traditional human authentication systems. However, security theft and privacy invasion are two passive issues that still persist in the effective deployment of biometric-based authentication systems. Compromise of biometric data can potentially lead to serious security violation as the user's biometric trait cannot be changed. In order to prevent the invasion of biometric templates, it is desired to morph the original biometric template through non-invertible or irreversible transformation function. This transformed template is referred to as cancelable template and can be replaced or reissued in case of compromise. In this paper, we propose a novel cancelable iris template generation technique based on randomized look-up table mapping. The technique utilizes a decimal vector generated from a rotation-invariant feature vector. The feature vector is generated using 1-D Log Gabor filter applied to the iris image. Experiments carried out on various iris databases confirm the efficacy of the proposed approach. After applying the template protection mechanism, we have achieved Equal Error Rate (EER) of 0.37%, 0.43% and 0.79% for CASIA-V 1.0, CASIA-V3-Interval and ICE 2005 iris databases, respectively. Moreover, the transformation preserves the irreversibility, revocability and diversity properties of the concealable iris templates.

1. Introduction

Over the last decade, biometric authentication has gained much public attention as compared to traditional knowledge (password, key) or token-based authentication systems and is widely deployed to identify/verify users firmly in several domains. However, biometric-based authentication systems suffer from security and privacy invasion challenges as their compromise may expose sensitive and ancillary information about a user. Further, if the biometric template gets compromised, it results in permanent identity theft as biometric data are intrinsically linked to the user. This introduces the research question "how do we replace the biometric data which is permanent and limited for a user without affecting the accuracy of the system?". The different attacks such as hill-climbing, correlation or stolen-token attacks (Jain et al., 2008) can be launched for illicit use of biometric data which reduce the reliability of the system. In correlation attack, the attacker intercepts multiple protected templates of the same user from different applications and tries to find out the correlation between these protected templates to retrieve the original template (Rathgeb and Uhl, 2011). The hill-climbing attack is launched to maximize the matching score by iteratively and incrementally modifying the biometric input (Rathgeb and Uhl, 2011). In case of the stolen token attack, the imposter captures the genuine

* *Corresponding author.*
E-mail addresses: phd1301201006@iiti.ac.in (R. Dwivedi), somnathd@iiti.ac.in (S. Dey).

http://dx.doi.org/10.1016/j.cose.2016.10.004
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

token of a user and combines this with his own biometric to enter the system (Rathgeb and Uhl, 2011).

To address these issues, there is a demand of designing a robust biometric system with substantial template protection mechanism which will be able to generate a new transformed template in case of compromise or generate distinct templates for the different applications to prevent cross-matching. Moreover, the biometric system should meet four design criteria to allow utmost template protection: irreversibility, revocability, diversity and accuracy (Rathgeb and Uhl, 2011). Irreversibility implies that it should be infeasible or computationally hard to reconstruct the original template from the transformed template (Ouda et al., 2010). Revocability means that if the transformed biometric template has been stolen or compromised, the verification system should be able to generate another unique template, or generate different unique templates from the original template and replaced in case of compromise (Khan et al., 2015) to prevent cross-matching in the different applications. Diversity ensures the generation of distinct protected templates from the same unprotected template so that the different templates can be used in various applications for the same identity to ensure the privacy (Ouda et al., 2010; Rathgeb and Uhl, 2011). Finally, the degradation in the recognition performance should be preserved over the accuracy obtained in the original biometric system (Ouda et al., 2010).

Several approaches have been proposed to obtain a secure biometric template. These approaches try to encounter the above mentioned privacy and security issues taking into account the practical biometric design criteria. "Cancelable biometrics" (Ratha et al., 2001) is one of them, which employs a key-dependent transformation to the raw biometric data. The transformation is irreversible such that the original biometric template cannot be revealed from the stored transformed template (Hammerle-Uhl et al., 2009). Biohashing based cancelable approaches proposed in Jin et al. (2014), Nanni et al. (2011), and Teoh et al. (2008) derive a uniformly distributed random sequence using a hash key. These approaches perform well if tokens used for verification are different for each user. However, the performance degrades in case of stolen-token scenario. Pillai et al (2010) divide the iris into different sectors and apply a random projection on each sector. They concatenate the random projections of all sectors to derive a secure cancelable template. In this approach, the matching accuracy gets retained if subject-specific projections are applied. Du et al (2011) propose a non-invertible transformation based on Gabor features. The radial position information (*r*) is combined with 64-bit Gabor descriptor to derive a cancelable template. Ouda et al (2010) incorporate the verification of a user based on grouping blocks of consistent bits in the IrisCode. Both these approaches are vulnerable to correlation attacks for small block sizes (Ouda et al., 2011).

Another way to achieve template security is through the use of cryptographic construct. Duagman et al (Duagman et al., 2006) derive a cryptographic key from 2048-bit IrisCode using the fuzzy commitment scheme. This utilizes Hadamard and Reed-Solomon error correcting codes to correct bit errors. The two schemes, fuzzy commitment and fuzzy vault, are introduced by Juels and Wattenberg (1999) and Juels and Sudan (2002), respectively. These approaches involve the exploitation of a biometric template into an error-correcting codeword with the addition of check bits. The main drawback of such schemes (Duagman et al., 2006; Juels and Sudan, 2002; Juels and Wattenberg, 1999) lies in the difficulty of generating exact error-free identifiers from noisy biometric features with high key entropy (Jain et al., 2008). In contrast, Dodis et al (2004) proposed secure sketch and fuzzy extractor schemes. These schemes use error tolerant key generation methods. Although, these schemes provide security against privacy invasion, they do not aim to provide revocability (Jain et al., 2008).

To satisfy the four defined criteria for an ideal biometric system, this paper presents a novel cancelable iris template generation method which employs a mapping between a decimal vector and a randomized binary look-up table. The decimal vector is obtained from the consistent bit vector partitioned into a number of fixed size blocks. The proposed method derives the protected template using check bits which are extracted from the mapped entries of the look-up table. The generated iris template is utilized for identity verification instead of true IrisCode. The method involves a randomized look-up table mapping to achieve irreversibility. Moreover, different values of block size and check bits are used to fulfill the requirements of diversity and revocability. The method involves a consistent-bit vector considering rotation-invariance into account to preserve the performance.

This paper is an extension of our earlier work (Dwivedi and Dey, 2015). In the earlier work, we proposed a technique for generation of cancelable iris template. However, the limitations of our earlier work lie in aspects of accuracy, security and attack analysis. In a nutshell, we extend this work in the following aspects as compared to our previous work:

(i) Consistent bit vector is used to generate decimal vector instead of original row vector that results in performance improvement over the original IrisCodes.
(ii) In the earlier work, the fixed values of parameters are utilized to evaluate the performance. Here, we have performed exhaustive evaluation with the different values of parameters such as block size and check bits on CASIA IrisV3-Interval dataset.
(iii) The earlier method was tested with only CASIA IrisV3-Interval. In this work, experiments have been carried out with CASIA-V 1.0, CASIA IrisV3-Interval and ICE 2005 (Phillips et al., 2008) datasets and experimental results are compared with existing approaches to determine the robustness of the proposed method.
(iv) We have performed a rigorous security analysis with respect to revocability, irreversibility and diversity, and also tested our method against possible attacks such as correlation, hill-climbing and stolen-token attack in this work.
(v) Finally, we have enhanced our literature review by adding descriptions of few more relevant existing approaches.

The rest of the paper is organized as follows. In Section 2, we briefly summarize existing methods related to the cancelable iris template. Section 3 describes our proposed method in detail. The experimental results and comparison with the existing approaches are presented in Section 4. The security analysis of our method is discussed in Section 5. Finally, Section 6 summarizes our findings and concludes the paper.

Please cite this article in press as: Rudresh Dwivedi, Somnath Dey, Ramveer Singh, Aditya Prasad, A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping, computers & security (2016), doi: 10.1016/j.cose.2016.10.004

2. Related work

In the last few years, several approaches have been proposed to address various issues of protecting biometric templates by the biometric research community. The approaches related to biometric template security presented in the literature can be widely categorized into two types namely, biometric cryptosystem and feature transformation (or cancelable biometrics) techniques (Jain et al., 2008). In the following, we shall discuss the existing techniques of both these two categories.

Biometric cryptosystems may be further divided into two subcategories: key generation and key binding schemes. Key generation schemes (Chang and Roy, 2007; Dodis et al., 2004) are used to derive cryptographic keys from user's biometric features directly. On the other hand, the goal of key binding schemes (Duagman et al., 2006; Juels and Wattenberg, 1999) is to bind cryptographic keys with biometric features in such a way that it makes impossible to recover the key unless the true template is presented during authentication. However, the performance of key binding schemes may be affected due to the introduction of error correction schemes, which are necessary for key retrieval. It is obvious that although both key binding and key generation schemes offer protection to biometric templates; their main objective is to secure cryptographic keys using biometric features. Dodis et al (2004) applied a hash function on error-tolerant biometric input to attain non-invertibility. In this approach, two functions are proposed, namely fuzzy extractor and secure sketches. Fuzzy extractor applies a hash function on biometric input to generate a random string. This random string is utilized as a key. In contrast, secure sketch uses this random string to reconstruct the original template. Chang and Roy (2007) utilized this method on the fingerprint biometric. Another scheme for biometric cryptosystem proposed by Juels and Wattenberg (Juels and Wattenberg, 1999) is fuzzy commitment. This approach applies a function on the codeword and binary biometric input to generate the template. The codeword is prepared with error-correcting codes to eliminate bit-errors. At the time of verification, the codeword is evaluated for the query biometric data and matched using error-correcting codes. Bringer et al (2008) applied fuzzy commitment scheme (Juels and Wattenberg, 1999) with an improved error-correcting mechanism. In this approach, a matrix is formed with two different binary Reed–Muller codes. Next, a 2-D iterative min-sum decoding is performed to retrieve a 40-bit cryptographic key. Wu et al (2008) proposed an iris cryptosystem based on key generation. The iris feature vector is corrected with Reed–Solomon codes. Then, a hash function is applied to generate a cipher key. Reddy and Babu (2008) derived a key using password based transformation to encrypt the fuzzy vault (Juels and Sudan, 2002).

In contrast, the primary objective of the cancelable biometrics is to generate several revocable templates from the original biometric template. The different approaches for cancelable biometric introduced in the literature can be broadly categorized into two major primitives, namely biometric salting and non-invertible transforms (Rathgeb and Uhl, 2011). Biometric salting associates user-specific auxiliary information with biometric data to generate a "distorted" variant of biometric template as similar to password salting (hardening) in cryptography. A well-known approach for biometric salting is biohashing which derives a uniformly distributed random sequence using a hash key (Jin and Connie, 2006; Nanni et al., 2011; Teoh et al., 2008). In biohashing, biometric input is mixed with token and discretized in binary. The performance of the methods described in Jin and Connie (2006), Nanni et al. (2011), and Teoh et al. (2008) degrades in case of stolen-token scenario. In non-invertible transform based approach, instead of storing the original biometric, the biometric data are modified using a one-way function and stored into the database to ensure security and privacy of the actual biometric trait. Ratha et al (2001) focused on different irreversible methods of generating cancelable template such as grid morphing, block scrambling, Cartesian, polar and surface folding transformation. The transformations can be applied in either the signal domain or the feature domain to achieve distortion to attain irreversibility, revocability and to avoid cross-matching in stored biometric data among the different databases.

Du et al (2011) applied a key on the original iris template which rearranges the bit positions to achieve irreversibility. Zuo et al (2008) proposed four different non-invertible transforms namely GRAY-COMBO, BIN-COMBO, GRAY-SALT and BIN-SALT. GRAY-COMBO method performs circular shift operation on Gabor features and random addition of rows. BIN-COMBO utilizes similar transformation on the iris codes with random shifting and XOR operation. Random patterns are added to the Gabor features in GRAY-SALT method and XORed with original iris code in BIN-SALT method. Ouda et al (2010) derived BioCode by mapping randomly generated seed with biometric features evaluated using biohashing algorithm (Teoh et al., 2008). These transformations produce lower recognition performance for noisy biometric data. Hammerle-Uhl et al (2009; 2013) applied mapping of permuted blocks with the source texture obtained using wavelet transform. The method (Hammerle-Uhl et al., 2009) was reported with significant performance degradation. Rathgeb et al (2013) proposed block permutation on iris textures to protect the iris template. However, they improved the performance by applying bloom filter to generate an alignment-free cancelable iris template (Rathgeb and Busch, 2014). The method (Rathgeb and Busch, 2014) suffers against the claim of unlinkability.

3. Proposed method

In this section, we present the proposed method for generation of secure cancelable iris template. Our work consists of a number of tasks as shown in Fig. 1. First, iris images are preprocessed using Masek's (2003) and Daugman's (2002) techniques. Then, IrisCode features are extracted in form of

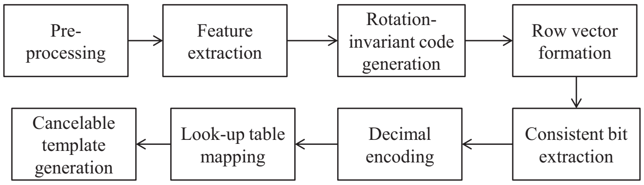

Pre-processing
Feature extraction
Rotation-invariant code generation
Row vector formation
Consistent bit extraction
Decimal encoding
Look-up table mapping
Cancelable template generation

Fig. 1 – Block diagram of the proposed method.

Fig. 2 – Enhanced image after normalization.

0–1 matrix using 1-D Log-Gabor filter (Masek, 2003) with phase quantization from the pre-processed iris images. Thereafter, rotation-invariant IrisCode is generated from the original IrisCodes and the rotation invariant IrisCode is transformed into a row vector. In the next step, we find the consistent bits from the row vectors and generate the consistent bit vector which is used in decimal encoding. Finally, a look-up table is created to map the decimal encoded vector and to generate the cancelable template. These steps are discussed in the following subsections.

3.1. *Pre-processing*

The pre-processing includes iris segmentation followed by iris normalization and image enhancement. Segmentation is performed to extract the iris region and to remove the eyelids, eyelashes and other noises from the eye image to avoid performance degradation. In our approach, circular Hough transformation (Masek, 2003) is applied to detect the iris and pupil circles using the parameters: radius and center coordinates. First, iris boundary is detected from the eye image and then pupil boundary is located from the detected iris region instead of the whole eye image, since the pupil is always within the iris region. Eyelids are detected from the image using parabolic curve parameter instead of the circle parameters (Masek, 2003). Due to illumination variations and the different imaging conditions, the radial size of the pupil may change accordingly. Therefore, the iris region is normalized using Daugman's rubber sheet model (Daugman, 2002; Masek, 2003) to compensate for these variations. Normalization process maps each point in the iris region to a polar coordinate. Thereafter, local histogram analysis based enhancement technique (Masek, 2003) is applied to the normalized iris image. This reduces the effect of non-uniform illumination and produces a well-distributed texture image. Reflection regions are characterized by high intensity values close to 255 to avoid low contrast. A simple thresholding operation (Masek, 2003) is performed to remove the reflection noise. The details of techniques involved in preprocessing can be found in the report of Masek (2003). Fig. 2 shows the enhanced normalized iris image.

3.2. *Feature extraction*

Normalized iris image is transformed into a 0–1 form of binary matrix by convolving 1-D Log-Gabor filter (Masek, 2003) to the normalized image. Each row in the normalized iris image is considered as a 1-D signal for convolution. The frequency response of 1-D Log-Gabor function is represented in Eq. (1).

$$G(f) = \exp\left(\frac{-\left(\log\left(\frac{f}{f_0}\right)\right)^2}{2\left(\log\left(\frac{\sigma}{f_0}\right)\right)^2}\right) \tag{1}$$

Table 1 – Performance comparison of original IrisCodes and rotation-invariant IrisCodes.

EER	Original IrisCdoes	Rotation-invariant IrisCodes
Without cancelable Transformation	4.11	0.39
With cancelable transformation	5.23	0.43

where f_0 and σ represent center frequency and bandwidth of the filters, respectively. The function produces real and imaginary components which are phase quantized to get IrisCode in the form of 0–1.

3.3. *Rotation-invariant code generation*

It is quite difficult to match iris image with rotational inconsistencies caused by tilt head while capturing the image. Even for genuine subject, it may result in poor intra-class Hamming distance (Daugman, 1985) causing performance degradation. We have measured the performance for original IrisCodes which shows an EER of 4.11 and 5.23 without applying cancelable transformation and after applying cancelable transformation, respectively as listed in Table 1. Therefore, rotation invariance mechanism needs to be employed. The whole circular iris pattern is considered to have 512 columns. Therefore, shifting of one column is equivalent to 360/512 = 0.703125 degree to a maximum of 8 columns (Daugman, 2002) generating 5.625 degree rotation. We consider 8-bit left as well as right rotations for each IrisCode of a particular subject. In order to achieve rotation invariance, we consider "*V*" number of IrisCodes per subject. The value of V is determined empirically (for details see Section 4.3). We randomly choose one IrisCode as reference from all V IrisCodes. Hamming distances are calculated between the reference IrisCode and 17 other IrisCodes which are derived from each remaining IrisCode by shifting 8 columns in both directions one at a time. The IrisCode having minimum Hamming distance is further utilized to form row vector and consistent bit extraction.

It may be noted that we are not storing any reference IrisCode as this would cause a direct leakage of target IrisCode if the database has been compromised. In the verification stage, the verifiable template is exploited with 8-bit left and right rotations. The minimum distance is calculated using Eq. (2).

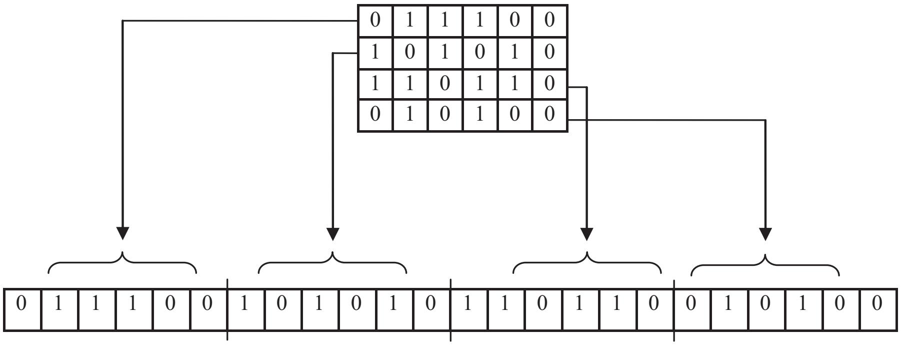
$$min\_dist = \min_k \{Icode(r) \oplus shift(Icode(q), k)\} \tag{2}$$

where *min_dist* represents the Hamming distance between reference IrisCode (*Icode*(*r*)) and the given Iriscode (*Icode*(*q*)) with *k* number of shifts. Here, *k* varies from −8 to 8. *k* = −8 represents 8 bits left shift and *k* = 8 represents 8 bits shift to right direction.

3.4. *Row vector formation*

The rotation free templates are shift invariant in comparison to original IrisCodes. We have evaluated the performance for

Please cite this article in press as: Rudresh Dwivedi, Somnath Dey, Ramveer Singh, Aditya Prasad, A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping, computers & security (2016), doi: 10.1016/j.cose.2016.10.004



0	1	1	1	0	0
1	0	1	0	1	0
1	1	0	1	1	0
0	1	0	1	0	0

0	1	1	1	0	0	1	0	1	0	1	0	1	1	0	1	1	0	0	1	0	1	0	0

Fig. 3 – Example of creating row vector.

rotationally aligned IrisCodes which shows an EER of 0.39 and 0.43 without applying cancelable transformation and after applying cancelable transformation, respectively as described in Table 1. Therefore, if we calculate Hamming distance between verifiable and the stored templates of the same subject, the performance degradation is 0.04% which is very low. It is easy to apply any transformation on 1-D vector instead of 2-D matrix because we need to traverse in one direction only in the case of 1-D vector. For easier implementation, rotation-free iris samples are stored in row vectors by merging the next row to the previous one. The row vector (R_v) is formed as:

$$R_v[j + i \times col\_dim] = Icode(i, j) \quad (3)$$

where col_dim is the width of column and R_v is the output row vector for IrisCode (Icode). For example, a row vector of 1 × 24, which is obtained from the IrisCode of 4 × 6 is shown in Fig. 3. Furthermore, any transformation can be implemented on the row vector.

3.5. *Consistent bit extraction*

After generating the row vector from all rotation-invariant IrisCodes, the consistent bits are extracted by considering significant bits in the row vector. Consistent bits are those bits in IrisCodes which are less likely to change. The consistent bit vector (C_b) is derived after aligning and summing up V IrisCodes in order to examine the occurrence of corresponding bits. The consistent bit vector contains same number of bits as in row vector. Hollingsworth et al (2009) presented a mathematical proof for inconsistent bits and its impact on performance. The model observed that the probability (p) of a bit flip does not affect the False Accept Rate (FAR). However, bit flip rate affects the False Reject Rate (FRR) performance. Hence, we empirically tested our approach with different values of p to improve the FRR. The bit indices that have higher probability of occurrence across various samples of the same IrisCodes are collected in C_b. Moreover, the bits in the original IrisCodes are protected using probability constraint.

In this work, a bit is taken into account if the probability of occurrences is greater than or equal to the threshold p_{th}, across the "V" row vectors as defined in Eq. (4) and Eq. (5):

$$C_b(i) = \begin{cases} 1 & for \quad p(i) \geqslant p_{th} \\ 0 & elsewhere \end{cases} \quad (4)$$

$$p(i) = \frac{\sum_{v=1}^{V} R_v(i)}{V} \quad (5)$$

where V is total number of samples of a subject and $p(i)$ is the probability of i^{th} bit in the samples of a particular subject. We have chosen the value of V empirically and results are reported in Section 4.3. To test the effect of p_{th} on FRR, we have considered four samples per subject ($V = 4$) in our experiment and results are shown in Table 2. The results reported in Table 2 show that FRR decreases gradually for $p = 0.25$, 0.5 and 0.75. However, FRR increases when we consider $p = 1$, that means all bits of a particular position in four row vectors are same. The reason of getting higher FRR is that number of consistent bits are less for $p = 1$. Therefore, it has been concluded that masking out inconsistent bits using $p = 0.75$ improves the recognition accuracy firmly.

3.6. *Decimal encoding*

It is difficult to apply any transformation function into the entire consistent bit vector as it comprises of 32,768 bits. Therefore, consistent bit vector is partitioned into fixed size blocks. The value of block-size (m) is considered as multiple of 2 to the power to get the consistent words of m bits. If it is not then the partition will not be perfect and some bits will be left over.

The decimal vector is derived from the partitioned consistent bit vector. The conversion of a word from binary to positive integer seizes the right most bit as the least significant bit. For example, we consider the value of $m = 4$ for a given row vector

Table 2 – FRR for different values of p.

p_{th}	FRR	FAR
0	2.38	0.1
0.25	1.57	0.1
0.50	0.83	0.1
0.75	0.43	0.1
1	0.73	0.1

Please cite this article in press as: Rudresh Dwivedi, Somnath Dey, Ramveer Singh, Aditya Prasad, A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping, computers & security (2016), doi: 10.1016/j.cose.2016.10.004

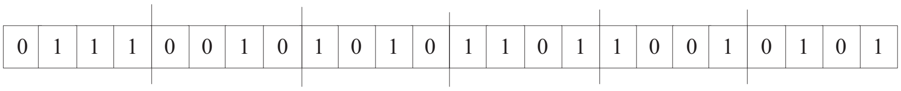


Fig. 4 – Partitioned vector.

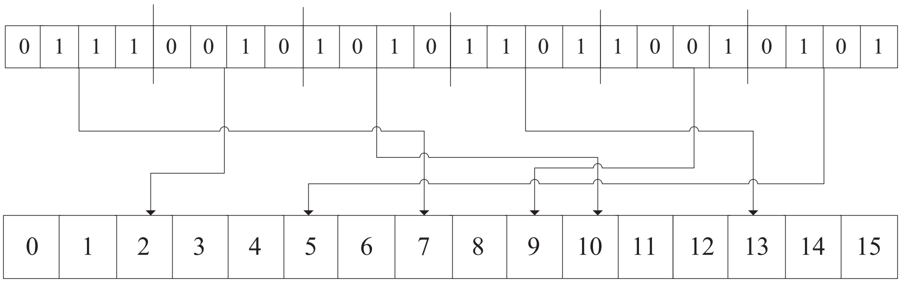


Fig. 5 – Mapping of word to decimal vector.

of size 24 bits. Therefore, the row vector is divided into 6 words, each having 4 bits as shown in Fig. 4. The size of decimal vector will be 2^m including positive integers in the range of 0 to $2^m - 1$.

The decimal vector will comprise large values of positive integers corresponding to large value of m. The words in the consistent bit vector are mapped to the corresponding decimal values. The mapping for given consistent bit vector is illustrated in Fig. 5.

3.7. *Look-up table mapping*

A binary look-up table (*LUT*) of size R × C is generated with random values 0 and 1 for each user. Here, *R* and *C* represent the size of the decimal vector and the size of each word, respectively. The size of the table depends on the value of m. The *LUT* consists $R = 2^m$ and $C = m$ number of rows and columns, respectively. The *LUT* is filled randomly as defined here:

$$LUT(i, j) = rand(0, 1), \quad \text{for } i = 0, 1, \ldots, 2^m - 1 \text{ and } j = 0, 1, \ldots, (m-1) \tag{6}$$

where *LUT*(i, *j*) represents the (i, *j*) position in the look-up table. For example, if we have word length 4, then the table must have at least 16 rows. To differentiate among the different words, we map the decimal vector to a corresponding word utilizing a look-up table. Fig. 6 illustrates the mapping procedure.

More than one word can be mapped to the same positive integer which prevents the attacker to employ reverse mapping. There is a possibility that all entries of a particular row or more than one row are 0. In this situation, the use of these entries is vulnerable to privacy invasion attacks, as this makes imposter's task easy. Therefore, look-up table should maintain approximately same number of 0s and 1s in a randomized manner.

3.8. *Cancelable template generation*

The mapping is performed between the decimal vector and the corresponding row of the *LUT*. Each row in *LUT* consists of m bits. We can choose d bits ($\leq m$) to generate the final template. These bits are referred to as check bits. For example, if $d = 2$ as shown in Fig. 6, then 2 bits from the 2nd and 3rd positions are selected from the mapped entries in the *LUT*. It may be noted that these 2 bits can be chosen from any position in the *LUT*. Therefore, the final template consists of 12 bits if we choose 2 bits from each word as depicted in Fig. 7.

Different templates can be derived using different values of m, but look-up table is kept fixed for every m. If we select all bits from each block i.e. $d = m$, the number of matching will be less across all bits in the stored and verifiable templates. Hence, performance will degrade. We have evaluated our method with different values of d for a fixed value of m (please see Section 4.3, Table 4) and observed that performance

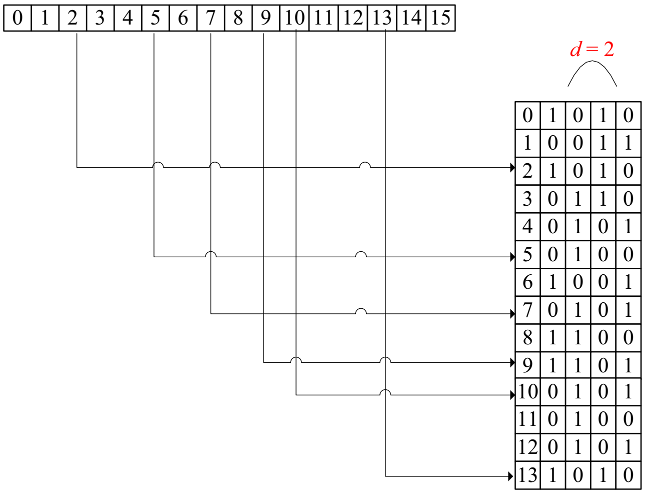


Fig. 6 – Mapping from decimal vector to look-up table.

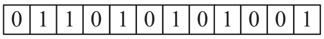


Fig. 7 – Final template.

degrades when $m = d$. Finally, matching is performed in the transformed domain by measuring the dissimilarity between two templates. We have computed Hamming distance between two templates to measure the dissimilarity. Hamming distance (HD) is sum of non-equivalent bits (exclusive-OR) between stored and query templates as defined in Eq. (7):

$$\textit{Hamming Distance (HD)} = \frac{1}{N}\sum_{i}^{N} S_i \oplus Q_i \tag{7}$$

where, Q_i and S_i are the i^{th} bits of the query and stored templates, respectively. N is the total number of bits in the template.

4. Experimental results and comparisons

In this section, we present the details of experimental design and results to illustrate performance of the proposed method and the effect of the different parameters as well as comparison with the existing approaches.

4.1. *Database*

We have chosen three widely used iris databases (CASIA-V 1.0, CASIA IrisV3-Interval, and ICE 2005) for evaluation of our proposed method. The CASIA-V 1.0 database consists of 756 images of 108 eyes. Each subject has 7 images captured in two sessions; 3 in the first session and 4 in the second. The CASIA-iris V3 Interval database includes 2639 images captured from 249 different subjects. The prime motive behind using these datasets is to compare our proposed method with the existing approaches in Du et al. (2011), Hammerle-Uhl et al. (2009, 2013), and Ouda et al. (2010) since their results are reported on the same dataset. The ICE 2005 Database (Phillips et al., 2008) from the National Institute of Standards and Technology (NIST) consists of 2953 images composed of 244 subjects. The results obtained from this database are compared with Du et al. (2011).

4.2. *Experimental design*

In our experiments, we have considered left and right eyes as different subjects because iris pattern is different for left and right eyes. We require 4 images per subject to create rotation invariant template at the time of enrollment and 1 image for verification. Hence, we consider the subjects which have at least 5 images. The experiment is performed on 348 subjects containing 177 subjects of left eye and 171 subjects of right eye iris patterns for CASIA-V3-Interval dataset. To evaluate imposter score, iris template of each subject is matched against the corresponding templates of other subjects, yielding 1,197,019 different inter-class comparisons. To evaluate genuine score, each iris pattern is matched with other iris patterns of the same subject resulting to a total of 7223 different intra-class comparisons. For ICE 2005 dataset (Phillips et al., 2008), the experiment is performed on 210 subjects containing 109 subjects of left eye and 101 subjects of right eye iris patterns resulting into 6560 intra-class comparison and 1,386,127 inter-class comparison. The experiment performed on CASIA-V 1.0 database outputs a total of 432 genuine comparisons and 80,892 imposter comparisons.

To evaluate our method, each database is randomly divided into two partitions, keeping 4 samples in the first partition and the rest in the second partition. The first partition is utilized for enrollment and the second partition for verification. We have conducted a number of experiments using different parameter values. We repeatedly perform each experiment 10 times as the enrollment and test samples are chosen randomly. The average performance for 10 trials is reported in the paper. We have used CASIA-V3-Interval database to choose the values of different parameters. We have also evaluated our method with CASIA-V 1.0 and ICE 2005 (Phillips et al., 2008) databases using the chosen parameter values.

The efficiency of the proposed method is evaluated by different performance measures such as FAR, FRR and EER. FRR measures the probability of falsely rejecting an iris as an imposter iris pattern and FAR measures the probability of falsely accepting an imposter iris pattern as genuine iris pattern. EER denotes the error rate where the FAR and FRR hold equality. Genuine Accept Rate (GAR) can be calculated using GAR = 1-FRR. The values of these performance metrics are evaluated from the genuine and imposter scores. Genuine score refers to matching an iris pattern of a subject with other patterns of the same subject, whereas imposter score is derived by comparing an iris pattern of each subject against the iris patterns of all other subjects. The effectiveness of a biometric system can be illustrated graphically by plotting a Receiver Operating Characteristic (ROC) curve with GAR against the FAR.

4.3. *Validation of parameters*

The proposed method uses four parameters to generate the different cancelable templates. These parameters are: number of samples used for rotation-invariance (V), block-size (m), number of check bits (d) and different look-up tables. In this section, we highlight the impact of the different parameters on the performance of our approach. We have validated all these parameters with respect to CASIA-V3-Interval dataset.

4.3.1. *Number of samples (V) used for rotation-invariance*

Before the formation of row vector, the derived IrisCodes are aligned to eliminate rotational deviation caused due to head tilt while acquisition. We consider "V" number of samples of the same user to achieve rotation-invariance. From the rotation-invariant IrisCode, we generate row vector followed by consistent bit vector, which considers the different probability values (p). To validate the parameter V and p, we have conducted a number of experiments with different values of $V = 2, 3\ldots, 6$ and $p = 0.33, 0.4, \ldots, 0.83$. The performance is measured with respect to EER and results are reported in Table 3. It has been observed experimentally that EER reduces for $V > 3$. For high values of V, the EER does not deviate much. Therefore, we have considered $V = 4$. The consistent bits are determined with different values of p.

4.3.2. *Block size (m)*

The row vector is divided into fixed size blocks of size m. The different values of m produce different Hamming distances for

Table 3 – Number of samples used for aligning IrisCodes.

V	EER								
	$p = 0.33$	$p = 0.4$	$p = 0.5$	$p = 0.6$	$p = 0.66$	$p = 0.75$	$p = 0.8$	$p = 0.83$	$p = 1$
2	-	-	-	-	-	-	-	-	3.12
3	-	-	-	-	2.03	-	-	-	2.89
4	-		1.93			0.43			2.03
5	-	0.82	-	0.48	-	-	0.57	-	2.18
6	1.73	-	1.04	-	0.43	-	-	0.73	3.03

Table 4 – EER for different values of *m* and *d*.

Block size(m)	Number of check bits(d)	EER
2	2	2.08
4	2	1.73
	4	1.01
8	2	1.49
	4	0.91
	8	1.09
16	2	1.47
	4	0.43
	8	0.82
	16	1.04
32	2	1.47
	4	0.44
	8	0.80
	16	1.03
	32	1.09

the same subject; therefore, the parameter m has an impact on the efficiency of the proposed method. Moreover, a change in m may result in the generation of the different biometric templates. To validate the parameter m, we have evaluated the proposed method with $m = 2, 4, 8, 16$ and 32, and measure the performance with respect to ERR. We can also choose different values of d for each m. Table 4 shows the EER for the different values of m and d.

From Table 4, we observe that the EER is high for $m = 2$ because of less variation in bits of different words. This leads to very low separability in intra-class comparisons. For $m = 4$, less value of EER is obtained as variability in bits increases for the different words. We also observe that for higher values of m, ERR is less as the bit difference is more.

The ROC curves for different values of m with $d = 2$ are shown in Fig. 8. Fig. 8 shows that the EER obtained for $d = 2$ are 2.08%, 1.73%, 1.49%, 1.47%, 1.47% for $m = 2, 4, 8, 16$ and 32 respectively on CASIA-V3-Interval dataset. It has been observed that there is not much difference in EER for $m = 16$ and $m = 32$ respectively. Therefore, we conclude that $m = 16$ is the best value to preserve the performance.

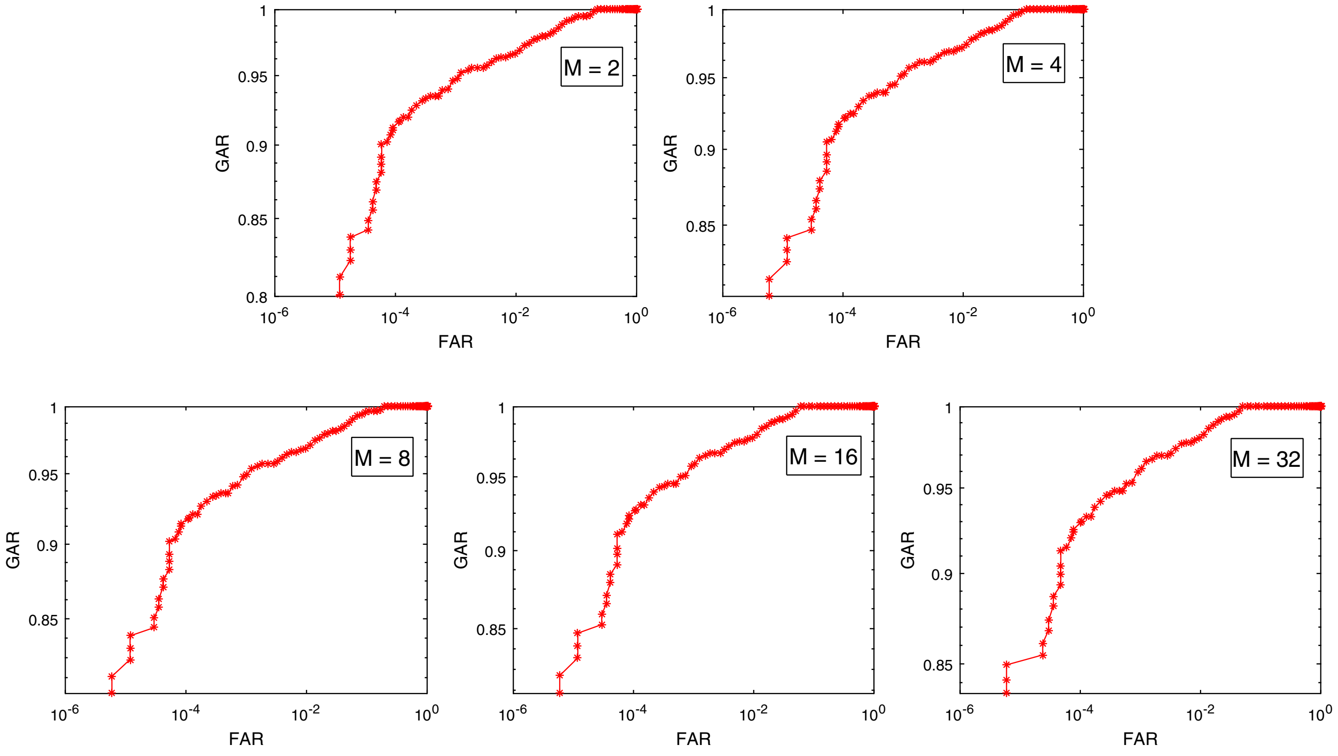


Fig. 8 – ROC curves for $m = 2, 4, 8, 16$ and 32 respectively.

Please cite this article in press as: Rudresh Dwivedi, Somnath Dey, Ramveer Singh, Aditya Prasad, A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping, computers & security (2016), doi: 10.1016/j.cose.2016.10.004

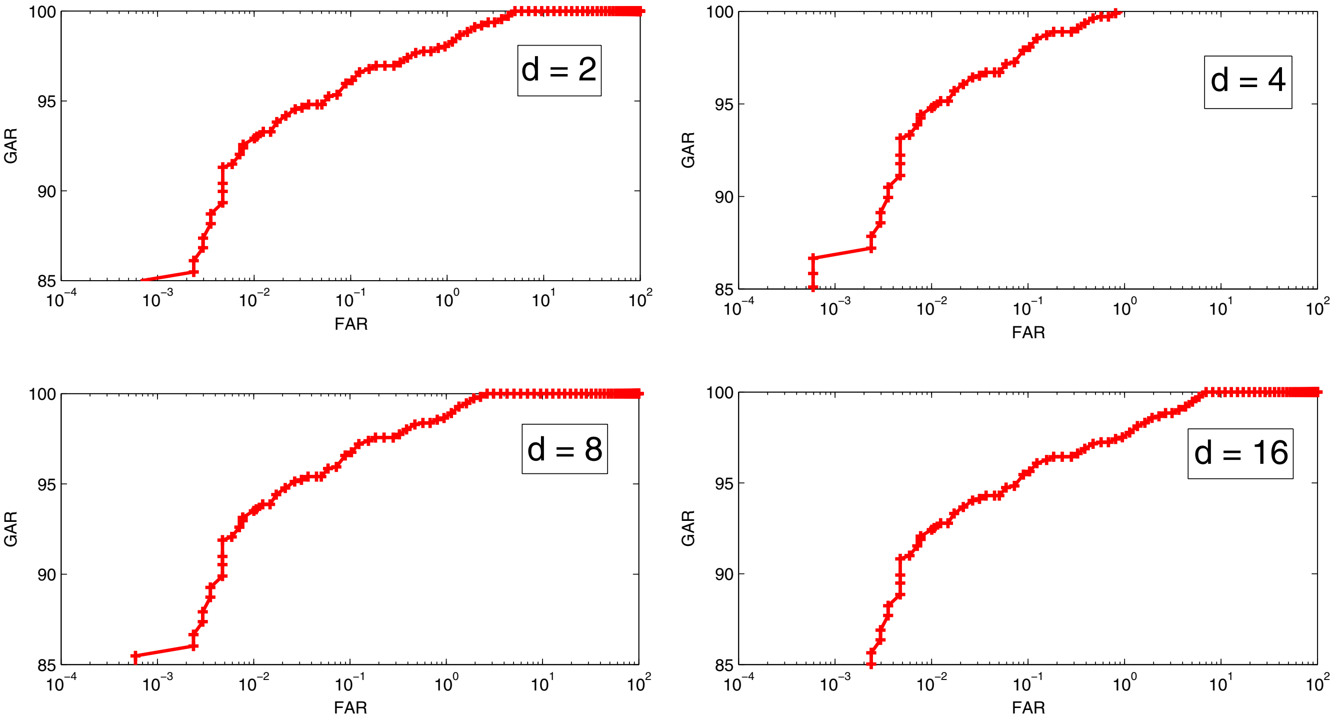


Fig. 9 – ROC curves for $m = 16$ and $d = 2$, 4, 8 and 16 respectively.

4.3.3. *Check bits (d)*

Final cancelable template is generated by selecting d bits from the mapped entries of the look-up table. The parameter d is responsible for security and revocability as various cancelable templates can be generated by varying the value of d (see Table 8). The ROC curves for different values of d with $m = 16$ are shown in Fig. 9. The EER obtained for $m = 16$ are 1.47%, 0.43%, 0.82% and 1.04% for $d = 2$, 4, 8 and 16 on CASIA-V3-Interval dataset, respectively. It has been observed from Fig. 9 that $d = 4$ is the best value to preserve the performance. Therefore, it can be concluded that the best recognition accuracy is obtained for $m = 16$ and $d = 4$.

4.3.4. *Effect of different look-up table*

The look-up tables are constructed using randomly generated 0–1 values. Sometimes it may happen that a table is biased for either 0 or 1 that makes the proposed approach non-revocable. A modification in the look-up table leads to alter the random bits for deriving a new template. We have chosen two sets of different look-up tables. Both sets contains different look-up tables for different subjects, however the look-up table of a subject in the first set is different from the look-up table of the same subject in other set. First, we have evaluated the performance with the $m = 16$ and $d = 4$ using first set of look-up tables. Then, we perform the same experiment using second set of look-up tables. The ROC curves for the two experiments are shown in Fig. 10a,b. We observe EER of 0.43 and 0.46 with the first and second set of look-up tables, respectively. Therefore, it is clear that change in the look-up table will less affect the overall performance.

4.4. *Comparison of with and without transformation*

In this experiment, first we computed the genuine and imposter score using consistent bit vector of the original IrisCodes. Then, we apply the proposed approach to derive cancelable template. Matching between query and stored template is performed in the transformed domain. Table 5 shows the EER obtained from the original (unprotected) IrisCode and cancelable template for different datasets. The reported results in Table 5 shows that performance is degraded by 0.09%, 0.093% and 0.329% for CASIA-V 1.0, CASIA-V3-Interval and ICE 2005 datasets, respectively. Therefore, we conclude that performance degradation produced by the transformation is very low.

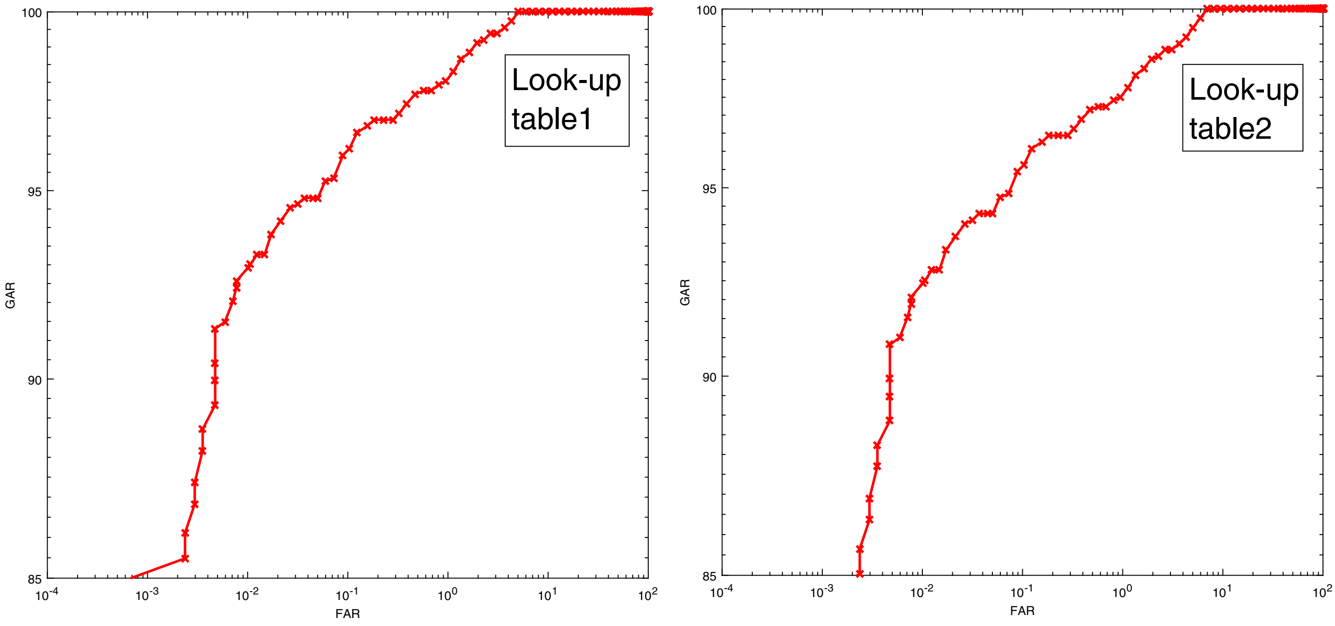
4.5. *Comparison with existing approaches*

We have analyzed the performance of proposed method for different values of parameters and observed that the best accuracy of EER = 0.43% is achieved corresponding to the parameter values $m = 16$ and $d = 4$. The objective of the approaches reported in Bringer et al. (2008), Du et al. (2011),

Table 5 – Baseline comparison.

Dataset	EER	
	Without cancelable transformation	With cancelable transformation
CASIA-V 1.0	0.28	0.37
CASIA-V3-Interval	0.39	0.43
ICE 2005	0.53	0.79

Please cite this article in press as: Rudresh Dwivedi, Somnath Dey, Ramveer Singh, Aditya Prasad, A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping, computers & security (2016), doi: 10.1016/j.cose.2016.10.004



(a) ROC for LUT set 1

(b) ROC for LUT set 2

Fig. 10 – ROC curves for $m = 16$ and $d = 8$ for two different look-up tables.

Hammerle-Uhl et al. (2009, 2013), Ouda et al. (2010), Rathgeb and Busch (2014), Reddy and Ramesh Babu (2008), and Wu et al. (2008) is same with our work. Hence, we compare our work with these approaches only.

The approaches in Bringer et al. (2008) and Wu et al. (2008) used CASIA-V 1.0, and the approaches in Hammerle-Uhl et al. (2009, 2013), Ouda et al. (2010), Rathgeb and Busch (2014), and Reddy and Ramesh Babu (2008) used CASIA-V3-Interval. ICE 2005 (Phillips et al., 2008) dataset is used by Du et al (2011). The summary of the results of the existing approaches and our proposed approach are reported in Table 6. Form Table 6, we observe that the best result reported in existing literature is EER = 0.84 and EER = 1.06 for CASIA-V3-Interval and ICE 2005 (Phillips et al., 2008) dataset, respectively, whereas our approach gives EER of 0.37, 0.43 and 0.79 for CASIA-V1.0, CASIA-V3-Interval, and ICE 2005 (Phillips et al., 2008) databases, respectively. From the reported result, it is evident that our approach performs better for CASIA-V3-Interval and ICE 2005 (Phillips et al., 2008) dataset, respectively, over the existing approaches.

5. Security analysis

A cancelable biometrics system needs to satisfy the security constraints as described in Section 1. In this section, analysis of revocability, irreversibility and diversity of our method are discussed to show that our approach fulfills the criteria for template protection schemes by preserving the recognition accuracy. The analysis of the different well known attacks against templates generated by our algorithm is also presented in this section.

5.1. *Revocability analysis*

It is necessary that a new template must be issued if the stored template is stolen. The new template should be uncorrelated

Table 6 – Performance comparison between proposed method and existing method for cancelable iris template generation.

Methods	EER			Remarks
	CASIA-V 1.0	CASIA-V3-Interval	ICE 2005	
(Bringer et al., 2008).	6.65/0 FRR/FAR	–	–	Fuzzy commitment scheme, EER very high
(Wu et al., 2008).	5.55/0 FRR/FAR	–	–	BC (Hash encoding with error-correcting codes)
(Reddy and Ramesh Babu, 2008).	–	9.8/0 FRR/FAR	–	Hardened fuzzy vault
(Hammerle-Uhl et al., 2009).	–	1.3	–	Block transformation
(Ouda et al., 2010).	–	1.3	–	Non-invertible transformation
(Du et al., 2011).	–	–	1.06	For IUPUI database 2.95 EER
(Hammerle-Uhl et al., 2013).	–	0.84	–	EER 0.76 for partial dataset
(Rathgeb and Busch, 2014).	–	2.6	–	Non-invertible transformation
Proposed method	0.37	0.43	0.79	Non-invertible transformation

Please cite this article in press as: Rudresh Dwivedi, Somnath Dey, Ramveer Singh, Aditya Prasad, A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping, computers & security (2016), doi: 10.1016/j.cose.2016.10.004

Table 7 – Mean and variance of imposter (μ_i & σ_i), pseudo-imposter (μ_{pi} & σ_{pi}) and genuine distributions (μ_g & σ_g) for different values of *m*.

Block size(*m*)	μ_i	σ_i	μ_{pi}	σ_{pi}	μ_g	σ_g
2	0.4834	0.0019	0.3980	0.02783	0.1132	0.0043
4	0.4802	0.0018	0.3893	0.02871	0.1241	0.0052
8	0.4789	0.0016	0.3741	0.02889	0.1534	0.0059
16	0.4770	0.0015	0.3692	0.03112	0.1784	0.0072
32	0.4698	0.0013	0.3591	0.03156	0.1837	0.0080

to the previously compromised templates though they are derived from the same biometric data. It is a necessary requirement for a biometric template protection scheme to generate numerous transformed templates from the same iris and they should differ with other templates to prevent cross-mating of templates across various applications.

1820 templates can be generated for the same sample of each subject corresponding to $m = 16$ and $d = 4$. We have selected 100 different templates randomly from this combination and matched with the original enrolled templates to obtain pseudo-imposter distribution. The mean and variance of genuine, imposter and pseudo-imposter distribution for different values of m is shown in Table 7. Table 7 indicates that mean and variance for pseudo-imposter distribution is near to the imposter distribution and far from genuine distribution. This signifies that the derived templates are dissimilar to enrolled templates for the same iris pattern. Although the templates are generated from same iris pattern, they are uncorrelated with each other. Therefore, claim of revocability is preserved.

5.2. *Irreversibility analysis*

The term, irreversibility refers to the computational hardness in recovering the true IrisCodes. Recall that a randomized look-up table is maintained to map decimal entries and certain digits are selected from the mapped entries to generate a cancelable template. Moreover, our approach does not allow the storage of any parameter except the look-up table for each subject. Therefore, an imposter would need to learn the entire procedure to have any chance of compromising the security of the iris template. From the security frame of reference, acquiring the consistent bit vector of an IrisCode is as severe as recovering the true IrisCode itself since it contains the most significant bit information. Therefore, we apply a probability constraint for the evaluation of the consistent bit vector from the IrisCode. In addition to this, utilization of the different values of m, different look-up tables and selection of different d bits ensure robustness of the approach. In this section, we analyze three different scenarios to test the irreversibility of the method.

5.2.1. *Compromised look-up table and protected template*

In this case, we assume that an attacker is able to reveal the stored look-up table and protected template of a user. From the size of the look-up table and protected template, the value of m and d may be computed. Now, to reconstruct the original IrisCode, the attacker has to compute the mapped locations in the look-up table from the protected template. For this purpose, first attacker will divide the protected template (PT) into L number of bit sequences of the length of d bits where $L = Len_{PT}/d$ as shown in Fig. 11. Len_{PT} is the length of the protected template. Next, each bit sequence would be searched in each row of the look-up table to find the mapped location. The number of attempts required to find a match corresponding to a bit sequence in a single row is ${}^mC_d$ and ${}^mP_d$ when d bits are taken from the look-up table to generate the protected template in order and without any order, respectively. We denote this number of attempts as M_r. There are 2^d possible bit sequences in the protected template and 2^m number of rows in the look-up table. Hence, the attacker requires $2^d \times 2^m \times M_r$ number of attempts to find mapped locations for all bit sequences of the protected template from all rows of the look-up table. It may be noted that the substring matching cannot be utilized as the positions of d bits may not necessarily be consecutive. For example, if the length of the original template is 32,768; the value of m and d are 16 and 4, respectively, then the size of the protected template is 8192, and the number of attempts to find possible mapped locations for all bit sequences of the protected template is 1908 million and 45,801 million when d bits are selected in order and without any order, respectively, to generate the protected template. Further, each bit sequence of the protected template can be found in multiple rows of the look-up table which could be considered as a set of possible mapped entries of that bit sequence. Fig. 11 shows that the set of possible mapped locations is $\{1, 3, 7\}$ as the 2nd bit sequence is found in the 1st, 3rd and 7th rows in the look-up table. Similarly, the attacker can generate L number of sets of possible mapped locations corresponding to all bit sequences of the protected template. We assume that the number of possible mapped locations for the i^{th} bit sequence is N_i. Hence, the total number of attempts to generate the original decimal vector from the sets of possible mapped locations is

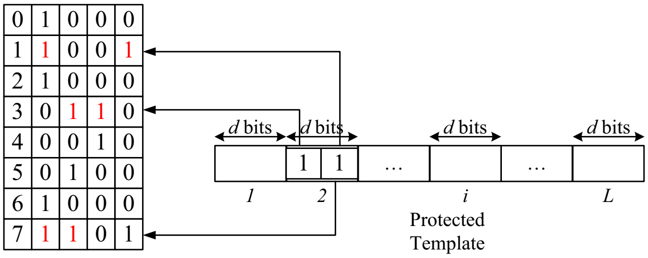


Fig. 11 – Mapping from protected template to look-up table.

Please cite this article in press as: Rudresh Dwivedi, Somnath Dey, Ramveer Singh, Aditya Prasad, A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping, computers & security (2016), doi: 10.1016/j.cose.2016.10.004

$N_{MT} = N_1 \times N_2 \times \cdots \times N_i \times \cdots \times N_L$. As a result, the number of computations required to derive the decimal vector from the compromised look-up table and protected template is $2^d \times 2^m \times M_r + N_{MT}$. Moreover, even if the attacker derives the consistent-bit vector from the computed decimal vector; it would be hard to retrieve the original template as the attacker does not know the positions of consistent bits out of 32,768 bits.

5.2.2. *Compromised protected template and value of m*

Assume that an attacker infiltrates the protected template and the value of *m*. In this scenario, an attacker has to reconstruct the look-up table and derive the decimal vector to obtain the original IrisCode. The reconstruction of the look-up table is computationally hard as the number of attempts required to reconstruct the original look-up table is $2^{2^m \times m}$ because there are $2^m \times m$ number of cells in the look-up table and the value of each cell is either 0 or 1. The reconstruction of look-up table is computationally hard as the number of attempts required to reconstruct original look-up table is $2^{2^m \times m}$ for a look-up table of size $2^m \times m$. Now, there are $2^{2^m \times m}$ possible look-up tables and the attacker has to derive the decimal vector corresponding to each look-up table. The number of computations required to generate decimal vector for single look-up table is $2^d \times 2^m \times M_r + N_{MT}$ as discussed in Section 5.2.1. Therefore, the total number of computations required to derive the decimal vector from the compromised protected template and value of *m* is $2^{2^m \times m} \times (2^d \times 2^m \times M_r + N_{MT})$. For example, we assume that the size of the look-up table is 16×4 and 2 bits are selected in order as well as without any order from the look-up table to generate the protected template. We also assume that the size of the protected template is 8 bits which contains 4 mapped locations and each set has 2 entries. The number of attempts required to generate the decimal vector is 7.4×10^{21} when the bits are selected in order and 1.4×10^{22} when the bits are not selected in any particular order. These values are comparable with those of Du et al (2011) and Hammerle-Uhl et al (2009) methods.

5.2.3. *Compromised look-up table*

In this case, we assume that an attacker reveals the stored look-up table but no information about the protected template. In this situation, the value of *m* is known to the attacker. However, the attacker would not be able to reconstruct the original template as the look-up table comprises random 0–1 entries. From random 0–1 entries, it is impossible to retrieve any information about the true IrisCode.

5.3. *Diversity analysis*

It is essential for a template protection mechanism that numerous derived templates should not match over various applications to avoid cross-matching. To evaluate this criterion, we employ different combination of *m* and *d* from the mapped row of the look-up table. The selection of *d* bits from the mapped instances in the look-up table can derive many templates for a particular subject. Table 8 shows the possible number of templates generated using different values of *d*. Further, we can also generate different templates by choosing different look-up tables.

Table 8 – Total number of possible templates.

Block-size(*m*)	Possible templates		
	$d = 2$	$d = 3$	$d = 4$
2	${}^{2}C_2 = 1$	-	-
4	${}^{4}C_2 = 6$	${}^{4}C_3 = 4$	-
8	${}^{8}C_2 = 28$	${}^{8}C_3 = 56$	${}^{8}C_4 = 70$
16	${}^{16}C_2 = 120$	${}^{16}C_3 = 560$	${}^{16}C_4 = 1820$
32	${}^{32}C_2 = 496$	${}^{32}C_3 = 4960$	${}^{32}C_4 = 35,960$

The parameters illustrated in Section 4 shows that multiple templates can be generated for a single subject; they can still significantly be distinguished from the original template which means an individual can enroll different templates of the same subject at different physical applications without cross-matching. Therefore, the experiments validate the property of diversity.

5.4. *Correlation attack*

To avoid correlation attack, the proposed approach uses different values of *m* and *d* to derive multiple templates across various applications. If an imposter is able to reveal the two templates of the same user, it would not be possible to link the i^{th} bit in two templates derived using different values of *m* and *d*. It is also possible to permute the bits in derived template or it can be XORed with a random sequence before deploying it to a new application. This random sequence will be dependent on the value of *m*. For example, if $m = 4$, random sequence will have 8192 bits, which is computationally hard to invent for an imposter.

5.5. *Hill-climbing attack*

The primary idea behind hill climbing attack is to consecutively modify a biometric input to verification system in order to reconstruct the original IrisCode. The attacker observes the matching score returned by the system at each attempt and tries to maximize the matching score. The process of attempts with modified input continues until no significant improvement in matching score is observed. In our approach, we are considering consistent bit vector after aligning the different IrisCodes. The bits which are less likely to change across the different IrisCodes of the same subject are treated as consistent bits. For example if we have four IrisCodes 0110, 0010, 0101 and 0100, then the consistent bit vector we consider is 0100. Here, the attacker needs to know the position of consistent bits to launch the hill-climbing attack. The consistent bits are selected based on probability constraint. Hence, the attacker has to match all possible bit vectors to obtain the desired score for verification. Moreover, the attacker has to apply all possible combination of parameters (*m* and *d*) to derive the cancelable template which is hard to invent.

5.6. *Stolen-token scenario*

This is a scenario where the attacker has access to the genuine token. The stolen token, combined with his own biometric input is utilized for verification. If the attacker gets access to the block

Please cite this article in press as: Rudresh Dwivedi, Somnath Dey, Ramveer Singh, Aditya Prasad, A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping, computers & security (2016), doi: 10.1016/j.cose.2016.10.004

size (*m*) and check bits (*d*), it will be impossible to reconstruct the original template as the look-up table is comprised of random 0–1 entries. This will avoid the condition of stolen-token and aid more revocability to our approach. Under stolen-token (same key) scenario, the experimental results are provided in Section 4.3. Our method achieves an EER close to 0% in case of different-key scenario.

6. Conclusion

In this paper, we have proposed a novel cancelable iris template generation method which is able to derive a new and unique template from the original biometric template in case the stored transformed template is compromised. Further, the approach also satisfies the four design criteria of irreversibility, revocability, diversity and accuracy. The method utilizes the look-up table mapping to protect the original IrisCodes. Our approach uses 1-D Log-Gabor filter to generate iris code which is further partitioned into a number of fixed size words. The proposed method generates bit strings or cancelable templates by mapping the decimal vector into the look-up table. The significant performance improvement is achieved by our approach as it involves consistent-bit vector over rotation invariant IrisCodes for enrollment. We achieve 0.37%, 0.43% and 0.79% EER for CASIA-V1.0, CASIA V3-Interval and ICE 2005 databases, respectively, which indicates that our approach performs better than the existing approaches after applying the transformation. If the cancelable template is compromised, the parameters utilized in our experiment or the look-up table entries can be altered to derive another unique protected template. However, one limitation of our approach is that it requires 4 iris images per subject to generate rotation invariant template which can be captured at the time of enrollment. Further, the accuracy is affected by the preprocessing task as it cannot properly segment the iris region for poor quality images. Hence, there is a scope of improvement in the segmentation process. Although the proposed method outperforms against stolen-token scenario, there is need for secure look-up table generation. In future work, these limitations can be addressed. In addition, the template security mechanism for multimodal biometric systems can be looked into the future.

Acknowledgment

We would like to acknowledge the Indian Institute of Technology Indore for providing the laboratory support and research facilities to carry out this research.

REFERENCES

Bringer J, Chabanne H, Cohen G, Kindarji B, Zemor G. Theoretical and practical boundaries of binary secure sketches. IEEE Trans Inf Forensics Security 2008;3(4):673–83.

Casia Iris Image Database Version 3.0. http://biometrics.idealtest.org/dbDetailForUser.do?id=3. [Accessed 1 May 2014].

Casia Iris Image Database 1.0. http://biometrics.idealtest.org/dbDetailForUser.do?id=1. [Accessed 1 May 2014].

Chang E-C, Roy S. Robust extraction of secret bits from minutiae, in: Proceedings of the 2007 International Conference on Advances in Biometrics, ICB'07, Springer-Verlag, Berlin, Heidelberg, 2007, pp. 750–759.

Daugman J. How iris recognition works, in: International Conference on Image Processing, Vol. 1, 2002, pp. 33–36.

Daugman JG. Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters. J Opt Soc Am A 1985;2(7):1160–9.

Dodis Y, Reyzin L, Smith A. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, in: Advances in Cryptology – EUROCRYPT 2004, Vol. 3027 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2004, pp. 523–540.

Du EY, Yang K, Zhou Z. Key incorporation scheme for cancelable biometrics. J Inform Sec 2011;2(4):185–94.

Duagman J, Anderson R, Hao F. Combining crypto with biometrics effectively. IEEE Trans Comput 2006;55(9):1081–8.

Dwivedi R, Dey S. Cancelable iris template generation using look-up table mapping, in: 2nd International Conference on Signal Processing and Integrated Networks (SPIN), 2015, pp. 785–790.

Hammerle-Uhl J, Pschernig E, Uhl A. Cancelable iris biometrics using block re-mapping and image warping. In: Samarati P, Yung M, Martinelli F, Ardagna C, editors. Information security, vol. 5735 of lecture notes in computer science. Springer Berlin Heidelberg; 2009. p. 135–42.

Hammerle-Uhl J, Pschernig E, Uhl A. Cancelable iris-templates using key-dependent wavelet transforms, in: International Conference on Biometrics (ICB), 2013, pp. 1–8.

Hollingsworth K, Bowyer K, Flynn P. The best bits in an iris code. IEEE Trans Pattern Anal Mach Intell 2009;31(6):964–73.

Jain AK, Nandakumar K, Nagar A. Biometric template security. EURASIP J Adv Signal Process 2008;113:1–113:17.

Jin ATB, Connie T. Remarks on BioHashing based cancelable biometrics in verification system. Neurocomputing 2006;69(1618):2461–4.

Jin Z, Goi B-M, Teoh A, Tay YH. A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template. Security Commun Netw 2014;7(11):1691–701.

Juels A, Sudan M. A fuzzy vault scheme, in: IEEE International Symposium on Information Theory, 2002, pp. 408.

Juels A, Wattenberg M. A fuzzy commitment scheme, in: Proceedings of the 6th ACM Conference on Computer and Communications Security, ACM, New York, NY, 1999, pp. 28–36.

Khan SH, Akbar MA, Shahzad F, Farooq M, Khan Z. Secure biometric template generation for multi-factor authentication. Pattern Recognit 2015;48(2):458–72.

Masek L. Recognition of human iris patterns for biometric identification. Tech Rep Univ Western Australia 2003. http://www.peterkovesi.com/studentprojects/libor/LiborMasekThesis.pdf.

Nanni L, Brahnam S, Lumini A. Biohashing applied to orientation-based minutia descriptor for secure fingerprint authentication system. Electron Lett 2011;47(15):851–3.

Ouda O, Tsumura N, Nakaguchi T. Tokenless cancelable biometrics scheme for protecting iris codes, in: 20th International Conference on Pattern Recognition (ICPR), 2010, pp. 882–885.

Ouda O, Tusmura N, Nakaguchi T. Securing BioEncoded IrisCodes against Correlation Attacks, in: IEEE International Conference on Communications, 2011, pp. 1–5.

Phillips P, Bowyer K, Flynn P, Liu X, Scruggs W. The Iris Challenge Evaluation 2005, in: 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, 2008, pp. 1–8.

Pillai J, Patel V, Chellappa R, Ratha N. Sectored random projections for cancelable iris biometrics, in: IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), 2010, pp. 1838–1841.

Ratha N, Connell JH, Bolle R. Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 2001;40(3):614–34.

Rathgeb C, Busch C. Comparison score fusion towards an optimal alignment for enhancing cancelable iris biometrics, in: Fourth International Conference on Emerging Security Technologies (EST), 2013, pp. 51–54.

Rathgeb C, Busch C. Cancelable multi-biometrics: mixing iris-codes based on adaptive bloom filters. Comput Secur 2014;42:1–12.

Rathgeb C, Uhl A. A survey on biometric cryptosystems and cancelable biometrics. EURASIP J Inform Sec 2011;2011:3.

Reddy E, Ramesh Babu I. Performance of iris based hard fuzzy vault, in: 8th International Conference on Computer and Information Technology Workshops, 2008, pp. 248–253.

Teoh AB, Kuan YW, Lee S. Cancellable biometrics and annotations on BioHash. Pattern Recognit 2008;41(6):2034–44.

Wu X, Qi N, Wang K, Zhang D. A novel cryptosystem based on iris key generation, in: Fourth International Conference on Natural Computation, Vol. 4, 2008, pp. 53–56.

Zuo J, Ratha N, Connell J. Cancelable iris biometric, in: 19th International Conference on Pattern Recognition, 2008, pp. 1–4.

Rudresh Dwivedi received his M.Tech degree in computer technology from the National Institute of Technology, Raipur, in 2013. Presently, he is pursuing a Ph.D. degree in the Discipline of Computer Science and Engineering, Indian Institute of Technology, Indore. His research interests include biometrics, image processing, and pattern recognition.

Somnath Dey received his B.Tech degree in information technology from the University of Kalyani, in 2004 and the M.S. (by research) degree in information technology from the School of Information Technology, Indian Institute of Technology, Kharagpur, in 2008. Presently, he is Assistant Professor in the Discipline of Computer Science and Engineering, Indian Institute of Technology, Indore. His research interest includes biometrics, image processing, pattern recognition, and human computer interaction.

Ramveer Singh received his B.Tech in the Discipline of Computer Science and Engineering from Indian Institute of Technology (IIT), Indore in 2014. Currently, he is a Software Engineer in NTT DATA Bangalore. His research interests are mobile and biometric security, data base systems and software engineering.

Aditya Prasad received his B.Tech in the Discipline of Computer Science and Engineering from the Indian Institute of Technology (IIT), Indore in 2014. His research interests are mobile and biometric security, big-data analysis, cyber security and artificial intelligence.