ORIGINAL RESEARCH PAPER

Generation of cancellable locality sampled codes from facial images

Debanjan Sadhya | Utkarsh Utsav | Zahid Akhtar

Abstract
Face is arguably the most common biometric trait that has been extensively utilised and thoroughly studied. Since this unimodal feature visually represents the identity of an individual, preserving the security of face-based authentication models is a prime concern. This work proposes a framework for generating cancellable templates from raw facial images. Our scheme is essentially based upon the notion of locality sensitive hashing (LSH), specifically on its locality sampled code (LSC) realisation. Facial features are initially extracted using the binarized statistical image features (BSIF) descriptor. These binary features are subsequently hashed using the random bit sampling mechanism of LSC. Finally, these local hashes are permanently stored in a non-invertible manner. We have empirically analysed the security requirements of unlinkability, non-invertibility, and revocability in our model. We have also validated our work over the benchmark AR, ORL, Yale, and CASIA-Face5 databases under multiple scenarios. Among all the resulting cases, the best performance of our model was noted at a minimum EER of 2.69%, 4.45%, 1.2%, and 2.66% for the four data sets, respectively.

1 | INTRODUCTION

Biometrics has become a convenient way of authenticating the identity of an individual. Conventional identifiers such as a personal identification number (PIN), passwords or tokens use knowledge-based information. However, tokens need to be carried along and consequently cause inconvenience to the user. Furthermore, PIN and tokens can easily be stolen or damaged. As an alternative, biometric systems have steadily gained popularity due to their usability and incurred performance gains. These automated mechanisms allow the identification or verification of individuals based on unique physiological and behavioural characteristics [1]. One of the most common biometric traits which is used for identification at a distance is the face. With the increase in computational resources, facial recognition technology has become effective in both indoor and outdoor environments. Its usage has become ubiquitous across multiple domains including law enforcement, forensics, home entertainment, and large-scale surveillance systems [2].

From a security perspective, the existing biometric systems can be subjected to a wide range of attacks such as hill-climbing [3], privacy invasion [4], and spoofing [5]. The stored biometric templates could get stolen by an adversary and subsequently utilised to gain access to other applications. Biometric template protection (BTP) schemes are designed to provide robust security guarantees against various biometric threat models. The ISO/IEC Standard 24745 on biometric information protection defines two major components for any BTP scheme: pseudonymous identifier and auxiliary data [6]. Based upon the generation technique of these two pieces of information, BTP schemes are broadly categorised as either cancellable biometrics [7] or biometric cryptosystems [8]. Our work is related to the later notion in which the biometric features are encoded using one-way transformation functions. However, it should also be ensured that these functions should be distance preserving in the transformed domain. This requirement is particularly imperative to mitigate the performance loss of the model. The matching process in any cancellable biometric scheme is usually performed in the transformed domain, rather than in the feature domain.

In this work, we have proposed a framework for generating cancellable biometric templates from face features. The transformed templates maintain the privacy of the user biometric data by guaranteeing non-invertibility, revocability, and
unlinkability [7]. Non-invertibility states that the original biometric features cannot be extracted from the stored template. From the adversarial perspective, the recovered data can be either complete or partial. Revocability ensures that a new transformed template can be created from the base features if they get stolen. Finally, unlinkability states that different templates that are generated from the same base features are indistinguishable from each other. This guarantee is required for eliminating any possibilities of cross-matching or linking attacks involving biometric databases. Most importantly, the template itself would not degrade the performance of the system. Alternatively stating, the recognition accuracy on the cancellable features must be close to that of the base features.

The central idea of this study is based on the principle of locality sensitive hashing (LSH), which maps similar inputs to identical positions. Unlike cryptographic hash functions (hi), LSH tries to increase the probability of collision for similar inputs. This study is essentially an extension of ref. [9], wherein cancellable features for iris were generated. In their work, the authors utilised a random bit sampling-based technique for creating a cancellable locality sampled code (LSC) from binary IrisCodes. The LSC hashing technique benefits from strong theoretical guarantees of performance preservation in the transformed domain. However, this mechanism cannot be directly extended to facial templates because the features extracted from the face are not generally represented in a binary format. This problem is addressed in our work using the binarized statistical image features (BSIF) descriptor [10]. In BSIF, a binary feature vector is constructed by linearly projecting patches onto a subspace, followed by a basis computation. The value is then binarized using a thresholding-based technique. Essentially, our work serves a dual purpose. It investigates the feasibility of creating LSC from the face, along with providing a holistic framework for generating cancellable templates from facial images. As an additional contribution, we have analysed reduction in the size of the LSC templates with regard to the original BSIF features.

The remaining sections are organised as follows. Section 2 presents some past studies related to our work. The notion of LSH is discussed in Section 3. We extensively present our proposed methodology in Section 4. Section 5 is our empirical part, wherein we present various relevant results. The security guarantees of our framework are discussed in Section 6. Finally, Section 7 concludes our study.

2 | RELATED WORK

In this section, we discuss some studies which deal only with generating cancellable templates from the human face. For similar works involving other biometric traits, the readers are referred to refs. [7, 11]. Savvides et al. [12] generated cancellable facial templates using user-specific random convolution kernels. The kernels were generated using a seed value, with which the images were subsequently convolved. The minimum average correlation energy (MACE) filter was generated and stored using the convolved images. However, it is proved that the performance of such systems deteriorates if the same matrix is applied to different enrolled users [13, 14].

The idea of utilising modified bloom filters for generating cancellable biometric templates was initially proposed by Rathgeb et al. [15]. Later on, Gomez-Barrero et al. [16] extended this work for face templates. It has been shown that this mechanism can be used for generating an irreversible template without the degradation of the performance. Although the original work claimed to provide unlinkability and non-invertibility, Hermans et al. [17] proved that this method was susceptible to cross-matching-based attacks. Later on, Bringer et al. [18] also discussed the security limitations of bloom filters and demonstrated how to circumvent them.

Jeong et al. [19] extracted face features using ICA and PCA, and subsequently randomly scrambled them to produce the face templates. Wang et al. [20] proposed a partial face feature extraction process for generating cancellable biometric templates using two-dimensional projections. In their work, the authors extracted the vertical and horizontal face feature separately. The partial features were averaged over a Z number of transformations for incorporating the security objectives. In another work, Kim and Toh [21] used sparse random projections for generating cancellable templates from face images. Random matrices with values in \{0, 1, -1\} were utilised for this particular process.

The use of non-invertible transformations is a common approach for constructing cancellable features. Sutcu et al. [22] initially proposed a non-invertible transformation method for face images. The authors utilised a one-to-many transformation scheme over the biometric features for preserving their privacy. Cho and Teoh [23] used random permutation maxout (RPM) transformations to design face templates. The RPM transforms real-valued face features into a discrete index for providing security to the templates. In another work, Saito et al. [24] utilised the combination of random permutation and unitary matrices for generating cancellable face templates. Most recently, Kaur and Khanna [25] proposed a random distance-based model that generates privacy-preserving and revocable biometric identities along with 50% reduction in size.

3 | LOCALITY SENSITIVE HASHING

The LSH procedure maps similar input features into the same location with very high probability. Since LSH is essentially a hashing technique, the size of the input features is much larger than the number of locations. The LSH family is theoretically described as:

**Definition 1 (LSH [26]).** LSH is a hashing technique that tries to increase the probability of collision for similar inputs. Since it is a hash-based mapping, the size of the output range is much smaller than the input domain. Formally stating, an LSH is a probability distribution on a family of \( H \) of hash functions \( h \) such that \( \Pr_{h \in H}[h(x) = h(y)] = d(x, y) \) where \( d \) is a distance function defined on the collection of object \( X \) and \( Y \).
The core of the LSH scheme comprises of several local $b_i$. The utilization of these functions enables in an accurate estimation of the pairwise distance of the input items in the hashed domain. In this way, the LSH ascertains that the collision probability between the hashes of two similar items remains comparatively higher, and vice-versa. Theoretically stating,

$$P_{b \in H}(b_i(X) = b_j(Y)) \geq P_1, \quad \text{if} \quad d(X, Y) < R$$
$$P_{b \in H}(b_i(X) = b_j(Y)) \leq P_2, \quad \text{if} \quad d(X, Y) > cR$$

where $P_1 > P_2$.

In Equation (1), $P_1$ and $P_2$ are two probabilistic collision bounds of $b_i$, $X, Y \in \mathbb{R}^d$, $H = \{b : \mathbb{R}^d \rightarrow U\}$, $d(\cdot, \cdot)$ is the distance function and $U$ is the hashed space. Furthermore, $R$ is the distance threshold and $c$ is an approximation factor which is always greater than 1. This notion of LSH was recently used by Sadhya and Raman [9] for developing cancellable templates from iris features. In their work, the authors randomly sampled bits from the iris feature for generating the local hashes. One of the major features of this scheme is the collision probabilities for intra-class and inter-class sample points. These probabilistic bounds are represented as [9]:

$$P_1 = \left[ \left(1 - \frac{0.5}{c}\right)^k + \left(1 - \left(1 - \frac{0.5}{c}\right)^k\right) \times P_c \right]^n$$
$$P_2 = \left\{ 0.5^k + (1 - 0.5^k) \times P_c \right\}^n$$

where $P_c = \frac{(\log_{2}^2) \times \epsilon}{c \times C_i}$. The two bounds in Equation (2) implicitly determine the recognition accuracy of the biometric recognition model. A higher difference between $P_1$ and $P_2$ indicates that the intra-class samples map to the same locations, whereas the inter-class data map to different places. The overall performance of the biometric recognition system consequently increases. It is noticeable that $P_1 > P_2$ since $c > 1$.

4 | PROPOSED METHODOLOGY

The proposed cancellable template generation and authentication process has three phases: feature extraction, LSC generation and matching. A schematic illustration of generating LSC templates from an input face image is shown in Figure 1.

4.1 | Feature extraction

The features from a face image are extracted using the binarized statistical image features (BSIF) [10], which result in a binary string. Each bit of the binary string is generated by thresholding the response of the linear filter at zero. The filter is learned by maximizing the statistical independence of the filter response on training image patches. Given an image $X(u, v)$ and a linear filter $W_i(u, v)$ of the same size, the filter response $s_i$ is obtained by:

$$s_i = \sum_{u,v} X(u, v) W_i(u, v)$$

where $u, v$ denotes the size of the filter and $i$ denotes the $i$th filter. The binary matrix $b_i$ is subsequently obtained by thresholding the filter response $s_i$ at 0.

$$b_i = \begin{cases} 1, & \text{if } s_i > 0 \\ 0, & \text{otherwise} \end{cases}$$

The size of the binary string at each pixel $b_i(u, v)$ depends upon the number of filters used. The binary filter responses of $n$ filters are stacked together as each pixel is represented by $n$ bits. The input image is initially divided into $11 \times 11$ non-overlapping rectangular regions. The descriptors are then computed locally from each region and concatenated together to form the global descriptor. Since we used a single filter in this work, we converted
each pixel of the image into a binary bit. The final lengths of the BSIF code for the AR, ORL, Yale, and CASIA-Facev5 data sets were 442,368, 123,648, 480,000, and 480,000, respectively.

4.2 | LSC generation

In our work, the binarized face data is divided into \( n \) non-overlapping blocks, represented by the set \( B \). For each block \( B_i \), \( k \) random bits are sampled \( l \) times. Thus, \( l \) is the number of hash function and \( k \) is the size of each hash function. Each hash function is independent of the remaining \((l - 1)\) hashes since they are randomly sampled. As discussed during security analysis, a high value of \( k \) is desirable for minimising the adversarial probability in guessing all the bits of the hash function. On the other hand, increasing the value of \( l \) is beneficial only in multi-hash attack (MHA) where the adversary possesses multiple LSC instances of a single feature vector. However, increasing the number of local hashes simultaneously increments the overall computation time.

All the sampled BSIF indices as termed as marked positions (denoted by \([B]\)) and the remaining indices as the unmarked positions. The set \([B]\) is essentially a permutation set on the input feature indices. These user-specific tokens get stored in the database along with the protected templates. For each block \( B_i \), the set of hash function is represented by \( H(B_i) \) and the decimal equivalents of the sampled bits are denoted by \( c_{i,j} \) where \( j \epsilon [1, \ l] \). For incorporating the property of non-invertibility, these decimal values are reduced in a modular way by the factor \((t \times 2^k)\), where \( t \) is a security parameter such that \( 0 < t < 1 \). A higher value of \( t \) decreases the number of possible multi-mappings from the input to the output domain, thereby
**Figure 3**  Similarity score generation between two LSC templates. The hashing parameters are $l = 3$ and $k = 3$.

**Figure 4**  Sample images from the AR face database exhibiting variations in expression, illumination, and occlusion.
increasing the security of the framework. This conversion is formally represented as:

\[ c'_{ij} = c_{ij} \mod \lfloor t \times 2^k \rfloor \]  

(4)

In Equation (4), \( c'_{ij} \) represents the non-invertible decimal equivalents, which are subsequently stored in the form of Map \( (b_j) \). This step concludes the creation of the LSCs. Figure 2 demonstrates the process of generating LSC templates from an input BSIF feature vector.

The size of the LSC template is determined by several model parameters, specifically \( n, k, l, \) and \( t \). Since the non-invertible components solely constitute the LSC maps, the size of each component can be bounded by the number of bits required to represent it. As described through Equation (4), the mod function limits the permissible range for the non-invertible components within \( t \times 2^k \). The number of bits that characterise this quantity is always less than \( k \) as \( t < 1 \). Considering that there exists a total of \( n \) such components within an LSC map, each map size becomes \( n \times k \) bits. Since an LSC template comprises of \( l \) independent LSC maps, its maximum size can be represented by \( n \times k \times l \) bits. If we take into account the optimum empirical values of these parameters (details are presented in Section 5.3), 27000 and 9000 bits are required for storing each LSC template corresponding to the AR and ORL data sets, respectively. Thus, we obtain a size reduction of \( \approx 93.89\% \) and \( 92.72\% \) with respect to the original BSIF features in these two data sets.

4.3 | Similarity score generation

The authentication decision of a biometric system is based on the similarity between a query sample and the template stored during
TABLE 1 Effects of the number of blocks on the performance of the recognition system over the AR data set

| # of Blocks (n) | EER (%) | d’ | Time (s) |
|-----------------|---------|----|---------|
| 6               | 2.69    | 3.11 | 0.01842 |
| 12              | 4.53    | 3.05 | 0.02082 |

The other system parameters \(l = 150, k = 5\), and \(t = 0.5\) have been fixed for this simulation.

TABLE 2 Effects of the number of blocks on the performance of the recognition system over the ORL data set

| # of Blocks (n) | EER (%) | d’ | Time (s) |
|-----------------|---------|----|---------|
| 3               | 11.24   | 1.62 | 0.00329 |
| 6               | 6.74    | 1.71 | 0.00341 |
| 12              | 4.62    | 1.76 | 0.00529 |
| 16              | 4.75    | 1.72 | 0.00894 |

The other system parameters \(l = 150, k = 5\), and \(t = 0.5\) have been fixed for this simulation.

FIGURE 8 ROC curves while varying the number of blocks (n) over the AR data set

FIGURE 9 ROC curves while varying the number of blocks (n) over the ORL data set

FIGURE 10 ROC curves while varying the number of blocks (n) over the Yale data set

5 | EMPIRICAL RESULT AND ANALYSIS

In this section, we investigate the performance of our cancellable model with reference to its recognition accuracy. All the simulations were performed in MATLAB over a Core i7-8565U CPU @ 1.8 GHz with 64 GB of RAM.

5.1 | Database

All the results were validated on four publicly available data sets—AR Face [27], ORL (https://cam-orl.co.uk/facedatabase).


| # of blocks ($n$) | EER (%) | $d'$  | Time (s) |
|-------------------|---------|-------|---------|
| 16                | 3.89    | 1.74  | 0.00049 |
| 20                | 3.6     | 1.74  | 0.00063 |
| 24                | 3.54    | 1.72  | 0.00041 |
| 30                | 2.83    | 1.74  | 0.00053 |
| 32                | 3.03    | 1.73  | 0.00067 |

The other system parameters $l = 150$, $k = 5$, and $t = 0.5$ have been fixed for this simulation.

### Table 5

| Size of hash Fn. ($k$) | EER (%) | $d'$  |
|------------------------|---------|-------|
| 15                     | 4.23    | 3.16  |
| 20                     | 3.26    | 3.19  |
| 30                     | 2.69    | 3.11  |

The other system parameters $n = 6$, $l = 150$, and $t = 0.5$ have been fixed for this simulation.

### Table 6

| Size of hash Fn. ($k$) | EER (%) | $d'$  | Time (s) |
|------------------------|---------|-------|---------|
| 3                      | 4.78    | 2.11  | 0.00341 |
| 5                      | 4.62    | 1.76  | 0.00529 |
| 7                      | 6.23    | 1.39  | 0.00535 |

The other system parameters $n = 12$, $l = 150$, and $t = 0.5$ have been fixed for this simulation.

html] Yale Face [28], and CASIA-Facev5 (CASIA-FaceV5, http://biometrics.idealtest.org/). In the AR data set, 13 different instances of 74 male and 60 female subjects were used for evaluation. The covariates of this facial database include neutral expression, wearing scarf, smile, anger, scream, all side light on, left side light on, right side light on, wearing sun glasses, all side light on with wearing scarf, left side light on with wearing scarf and right side light on with wearing scarf. In total, the AR data set contains more than 4000 sample images of dimension $768 \times 576$. Some sample images from the AR data set are presented in Figure 4.

The ORL data set (currently known as The Database of Faces) comprises of 10 different images of 40 subjects. For some subjects, the images were taken at different times with varying illumination and facial expressions. All the images were taken against a dark homogenous background with the subjects in an upright, frontal position. The dimension of each image is $92 \times 112$, with 256 grey levels per pixel. Some samples are presented in Figure 5.

The Yale Faces data set comprises of 165 facial images of 15 subjects. There are 11 images for each subject exhibiting the following facial expressions or configurations: centre-light, w/glasses, happy, left-light, w/no glasses, normal, right-light, sad, sleepy, surprised, and wink. Although the AR, ORL, and Yale datasets are relatively old, we used them in our work since they have been thoroughly analysed and utilised in other related works. Some instances from this data set are illustrated in Figure 6.

The CASIA-Facev5 data set is a comparatively large data set which contains 2500 colour facial images of 500 subjects.
 TABLE 7 Effects of the size of hash functions on the performance of the recognition system over the Yale data set

| Size of hash Fn. (k) | EER (%) | $d'$ | Time (s) |
|----------------------|---------|------|----------|
| 3                    | 1.74    | 2.03 | 0.03387  |
| 5                    | 1.2     | 1.36 | 0.03159  |
| 7                    | 2.16    | 0.82 | 0.02065  |

The other system parameters $n = 12, l = 150$, and $t = 0.5$ have been fixed for this simulation.

 FIGURE 14 ROC curves while varying the size of hash functions (k) over the Yale data set

 TABLE 8 Effects of the size of hash functions on the performance of the recognition system over the CASIA-Facev5 data set

| Size of hash Fn. (k) | EER (%) | $d'$ | Time (s) |
|----------------------|---------|------|----------|
| 3                    | 3.01    | 2.14 | 0.00051  |
| 5                    | 2.83    | 1.74 | 0.00053  |
| 7                    | 3.53    | 1.3  | 0.00076  |
| 10                   | 7.31    | 0.66 | 0.00092  |

The other system parameters $n = 30, l = 150$, and $t = 0.5$ have been fixed for this simulation.

(i.e. five samples per person). It is characterised by a large variation in illumination, pose, expression, eye-glasses, and imaging distance. All the facial images are 16-bit colour BMP files with a resolution of 640 × 480. We used the cropped version of this data set in our simulations. Some samples are shown in Figure 7.

5.2 Comparison protocol and metrics

In the comparison protocol, the impostor scores were calculated by matching the first sample of every class with the first sample of the remaining classes. Alternatively, the genuine scores were calculated by matching every intra-class sample with each other (for every class). It is noticeable that this protocol is analogous to the standard FVC protocol for fingerprints (http://bias.csr.unibo.it/fvc2002/perfeval.asp).

 FIGURE 15 ROC curves while varying the size of hash functions (k) over the CASIA-Facev5 data set

 TABLE 9 Effects of the security threshold on the performance of the recognition system over the AR data set

| Security threshold (t) | EER (%) | $d'$ |
|------------------------|---------|------|
| 0.25                   | 2.71    | 3.11 |
| 0.5                    | 2.69    | 3.11 |
| 0.75                   | 2.7     | 3.08 |

The other system parameters $n = 6, l = 150$, and $k = 30$ have been optimally fixed for this simulation.

 FIGURE 16 ROC curves while varying the security threshold (t) over the AR data set

The equal error rate (EER) and decidability index ($d'$) are used for quantitatively evaluating the performance of the recognition system. The EER is defined as the point where the FAR and FRR are identical, whereas the $d'$ value indicates the degree of separation between the genuine and imposter score distributions. For the ORL, Yale, and CASIA-Facev5 data sets, the time required to generate the LSC templates are also included (measured in seconds).

5.3 Performance evaluation

We analysed our model on the following system parameters: size of the hash function (k), security threshold (t), and the
number of blocks \( (n) \). Following previous studies, we do not vary the number of local hash functions \( (l) \) since it does not affect the overall system performance \cite{9}. For all cases, we fixed an average value of \( l = 150 \).

### 5.3.1 Effect of \# blocks

Since the total size of the binary feature vector in the AR data set is 442,368 bits, we performed experiments on \( n = \{6, 12, 16\} \) with block size \( = \{73,728, 36,864\} \). The resulting EER values are presented in Table 1, wherein it can be noted that increasing the number of blocks decreases the performance of our model. The corresponding ROC curves are illustrated in Figure 8. We did not reduce the number of blocks further from six since the security of the framework would have considerably decreased in those cases (later analysed in Section 6.1). For average values of \( t = 0.5 \), \( l = 150 \) and \( k = 30 \), we get the best ERR = 2.69% corresponding to \( n = 6 \). We would consequently fix this value in further experiments.

For the ORL data set, we performed simulations with \( n = \{3, 6, 12, 16\} \) and resulting block size \( = \{41,216, 20,608, 10,304, 7728\} \). The results of these scenarios are presented in Table 2, in which we get the lowest EER = 4.62% corresponding to \( n = 12 \). The accompanying ROC curves are presented in Figure 9. Since a total of \( k \times l \) indices are sampled from every distinct block, the overall operational time for generating the LSC templates increases with the number of blocks. It is also noticeable that the effects of any model parameter on the performance of the biometric model are

### Table 10 Effects of the security threshold on the performance of the recognition system over the ORL data set

| Security threshold \( (t) \) | EER \( (%) \) | \( d' \) | Time \( (s) \) |
|-------------------------------|-------------|---------|---------|
| 0.15                          | 5.28        | 2.11    | 0.00497 |
| 0.25                          | 4.45        | 1.95    | 0.00521 |
| 0.5                           | 4.62        | 1.76    | 0.00529 |
| 0.75                          | 5.61        | 1.62    | 0.00725 |

The other system parameters \( n = 12, l = 150, \) and \( k = 5 \) have been optimally fixed for this simulation.

### Table 11 Effects of the security threshold on the performance of the recognition system over the Yale data set

| Security threshold \( (t) \) | EER \( (%) \) | \( d' \) | Time \( (s) \) |
|-------------------------------|-------------|---------|---------|
| 0.15                          | 2.82        | 2.07    | 0.0305  |
| 0.25                          | 2.82        | 1.67    | 0.03231 |
| 0.5                           | 1.2         | 1.36    | 0.03159 |
| 0.75                          | 1.86        | 1.09    | 0.03848 |

The other system parameters \( n = 12, l = 150, \) and \( k = 5 \) have been optimally fixed for this simulation.

### Table 12 Effects of the security threshold on the performance of the recognition system over the CASIA-FaceV5 data set

| Security threshold \( (t) \) | EER \( (%) \) | \( d' \) | Time \( (s) \) |
|-------------------------------|-------------|---------|---------|
| 0.15                          | 2.81        | 2.14    | 0.0006  |
| 0.25                          | 2.66        | 1.96    | 0.00063 |
| 0.5                           | 2.83        | 1.74    | 0.00076 |
| 0.75                          | 3.54        | 1.57    | 0.00054 |

The other system parameters \( n = 30, l = 150, \) and \( k = 5 \) have been optimally fixed for this simulation.

### Figure 17 ROC curves while varying the security threshold \( (t) \) over the ORL data set

### Figure 18 ROC curves while varying the security threshold \( (t) \) over the Yale data set

### Figure 19 ROC curves while varying the security threshold \( (t) \) over the CASIA-FaceV5 data set
5.3.2 Effect of hash size

We performed the experiment while varying the hash size \( k = \{15, 20, 30\} \) on the AR data set. We made a conscious effort not to decrease the value of \( k \) less than 15 since decrementing \( k \) increases the adversarial success probability in inverting the protected LSC templates [9]. The resulting EER and \( d' \) values are presented in Table 5, and the ROC curves are shown in Figure 12. It can be distinctly observed that increasing the size of \( h \) results in a better model performance, which can be again attributed to the collision probabilities stated in Equation (2). A higher value of \( k \) increases the interval between the intra-class and inter-class collision probabilities, thereby resulting in a better model performance. However, a large value of \( k \) simultaneously increases the computation cost for generating the LSC templates since more indices get sampled for every hash function. We did not perform simulations for \( k > 30 \) due to a long operational time. The minimum EER was noted to be 2.69% for \( k = 30 \).

For the ORL data set, we varied the size of the hash function as \( k = \{3, 5, 7\} \). All the relevant results are presented in Table 6 and the associated ROC curves are illustrated in Figure 13. The effect on the performance metrics was noted to be opposite in trend when compared to the AR data set. Specifically, the lowest EER = 4.62% corresponded to a small value of \( k = 5 \). This discrepancy can be attributed mainly to the distribution of consistent bits (viz., the specific bits which do not change across intra-class samples) in the ORL data set. The EER significantly degrades for higher values of \( k \) due to the sparse distribution of the consistent bits in the BSIF features of this particular data set. Although it affects the security of the model, the time required to construct the local hashes was considerably faster since a lesser number of bits were sampled from each feature block.

The same values of \( k = \{3, 5, 7\} \) were also considered for the Yale data set. As noticeable in Table 7 and Figure 14, the optimum size of the hash function was observed to be \( k = 5 \). Under this configuration, the EER and operational time were noted to be 1.36% and 0.03159 s, respectively. Interestingly, these are the same set of values that we had already obtained while varying the number of blocks. The fast degradation of the recognition accuracy for higher values of \( k \) can be again attributed to the sparse distribution of intra-class consistent bits in this data set.

For the CASIA-Facev5 data set, we varied the values of \( k = \{3, 5, 7, 10\} \). As observed from Table 8 and Figure 15, the minimum EER = 2.83% corresponded to \( k = 5 \) with an operational time of 0.00053 s. Hence, the recognition accuracy over this dataset is maximised when five indices are sampled from each BSIF block.

5.3.3 Effect of security threshold

In the final experiment, we analysed the effect of the security threshold parameter \( t \) on the recognition accuracy of the model. To reiterate, the value of \( t \) lies in \([0, 1]\) so that the mapping between the invertible and non-invertible block components becomes a surjection. For the AR data set, we varied \( t = \{0.25, 0.50, 0.75\} \), for which the results are depicted in Table 9, and the ROC curves are presented in Figure 16. Since no significant deviations can be observed in the resulting EERs, no direct effects of the threshold value on the model performance could be established. It is noticeable that this trend is consistent with previous studies [9]. The minimum EER was noted to be 2.69% for \( t = 0.5 \).

The results associated with the ORL data set are presented in Table 10 along with the ROC curves in Figure 17. Among all the scenarios, the lowest EER = 4.45% was observed corresponding to \( t = 0.25 \). To summarise, the best model parameters were noted to be \( n = 12, k = 5, \) and \( t = 0.25 \), for which the interval between \( P_1 \) and \( P_2 \) in Equation (2) was maximised.

All the results for the Yale data set are shown in Table 11 and Figure 18. Among the different values of \( t \), the minimum EER = 1.2% was noted for \( t = 0.5 \). Since this is the same result which we had already obtained in our previous simulations, it can be concluded that the optimum parameter values for this particular data set are \( n = 12, k = 5, \) and \( t = 0.5 \).
| Database       | Reference                                      | Components               | Best EER (%) |
|----------------|-----------------------------------------------|--------------------------|--------------|
| AR Face        | Jeong et al. [19]                             | PCA + ICA                | 14.3         |
|                | Kim and Toh [21]                              | Random projection        | 8.01         |
|                | Rosenberger and Brun [29]                     | SIFT                     | 12           |
|                | Oh et al. [30]                                | Partial face feature     | 3            |
|                | Thamizharasi and Jayasudha [31]               | DCT coefficients         | 2.87         |
|                | Proposed                                      | BSIF + LSC               | 2.69         |
|                | ORL                                           | Partial face feature     | 14           |
|                | Proposed                                      | BSIF + LSC               | 4.45         |
| CASIA-Facev5   | Kaur and Khanna [25]                          | Random distance          | 2.6 ± 0.97   |
|                | Proposed                                      | BSIF + LSC               | 2.66         |

**Table 15** Adversarial success probabilities of non-invertibility for the LSC features [9]

| Scenario | Genuine token | Stolen token |
|----------|---------------|--------------|
| SHA      | \(\frac{1}{\varepsilon^l_2} \times \frac{1}{|R_s|^k} \times \frac{1}{n^{1-t}} \times \Pi_{i=1}^l \) | \(\frac{1}{\varepsilon^l_2} \times \Pi_{i=1}^l \) |
| MHA      | \(\frac{1}{\varepsilon^l_2} \times \frac{1}{|R_s|^k} \times \frac{1}{n^{1-t}} \times \Pi_{i=1}^l \) | \(\frac{1}{\varepsilon^l_2} \times \Pi_{i=1}^l \) |
| ARM      | \(\frac{1}{\varepsilon^l_2} \times \frac{1}{|R_s|^k} \times \frac{1}{n^{1-t}} \times \Pi_{i=1}^l \) | \(\frac{1}{\varepsilon^l_2} \times \Pi_{i=1}^l \) |

Our final simulation in this section was performed by altering the values of \(t = \{0.15, 0.25, 0.5, 0.75\}\) over the CASIA-Facev5 dataset. As presented in Table 12 and Figure 19, the best recognition rate was obtained for \(t = 0.25\). The EER and the operational time under this configuration was noted to be 2.66% and 0.00063, respectively. The optimum parameter values corresponding to all the four data sets are collectively presented in Table 13.

5.4 Comparative analysis

We have compared our obtained results with other facial recognition studies that reported their results on our utilised data sets (some of these works have an exclusive focus on generating cancellable templates). As noticeable in Table 14, the proposed scheme results in a significantly lower EER for the majority of the data sets. Our technique produced good recognition performance due to the strong intra-class collision properties of LSC [9]. Even for the challenging CASIA-Facev5 data set, our EER is comparable to the state-of-the-art work of Kaur and Khanna [25]. Although BSIF is a relatively constrained texture descriptor, these results demonstrate that our framework can simultaneously provide a satisfactory performance with strong security characteristics.

6 SECURITY ANALYSIS

In this section, we exclusively investigate the security parameters of our LSC model, specifically non-invertibility, revocation, and unlinkability.

6.1 Non-invertibility

Non-invertibility requires that it should be computationally infeasible to revert the LSC templates into their corresponding BSIF codes. The major parameters which affect the security of the framework are \(n, l, k, t,\) and \(x\). The security of the LSC-based technique has been analysed on the basis of three attack scenarios: single hash attack (SHA), multiple hash attack (MHA) and attack via record multiplicity (ARM). SHA refers to the scenario when an adversary generates the original feature code from a single LSC feature. In MHA, we assume that the adversary exploits information from all available LSC templates consisting of \(l\) base feature. Under the independence assumption of the bits in the feature code, the adversarial success bounds in performing such attacks are summarised in Table 15. To estimate a practical attack scenario, the parameters for the best EER in the AR data set are considered, that is \((n, l, k, t, x) = \{(6, 150, 30, 0.5, 69228, 2)\}. The adversarial success of SHA under the stolen-token scenario is computed as:

\[
P = \left(\frac{1}{r \times 2^n}\right)^n = \left(\frac{1}{2 \times 2^{69228}}\right)^6.
\] (6)

Since \(P \approx 0\), the chances of inverting the LSC templates can be considered computationally infeasible. Consequently, we can claim that the non-invertibility property is fulfilled in our model. It is noticeable that this estimate is only a
the theoretical bound of non-invertibility when considered for the whole template. Extracting partial information from the stored templates would significantly increase the adversarial success rates. For instance, an adversary can accurately recover all the bits in a single block with probability:

\[
P = \frac{1}{r \times 2^x} = \frac{1}{2 \times 69228}.
\] (7)

In general, the adversarial success chance increases by a factor of \( n \) while reconstructing a single block. This constraint is enforced in the LSC scheme since the blocks are formed in a non-overlapping manner. The non-invertibility guarantee can be more granularly examined if we analyse the unmarked position bits. The value of \( x \) is implicitly dependent on the hash function parameters (viz. \( l \) and \( k \)). For instance, marking more indices per block decreases the number of unmarked position bits. The term \( \frac{1}{r} \) in Equation (6) would consequently increase, thereby indicating more success for the adversary. Another important factor which dictates the non-invertibility bounds is the size of the feature code. Specifically speaking, a large input feature would naturally result in increased block sizes. The adversary would subsequently require to invert more bits from the LSC templates for either full or partial data recovery. One of the primary reasons that we obtained the bound of Equation (6) is due to the BSIF code being considerably long. As such, it is recommended to utilise long binary feature vectors as the input for the LSC-based mechanism.

### 6.2 | Revocability

Revocability states that distinct LSC templates should be created from the same BSIF feature vector. To demonstrate this property, the distributions of the genuine, imposter, and

| Database  | Genuine/impostor | Genuine/pseudo-impostor | Impostor Pseudo-impostor |
|-----------|------------------|------------------------|--------------------------|
| AR        | 3.11             | 3.03                   | 0.18                     |
| ORL       | 1.95             | 1.94                   | 0.06                     |
| Yale      | 1.36             | 1.34                   | 0.23                     |
| CASIA-Facev5 | 1.96         | 1.84                   | 0.65                     |

*TABLE 16* Decidability index \( (d^p) \) values among the three score distributions.

![Graphs showing revocability analysis of the LSC templates over different datasets](image-url)
pseudo-imposter scores are considered. For estimating the pseudo-imposter scores, 100 different keys were used for creating 100 separate LSCs. This process was repeated for all the samples present in the databases. For each sample, the first LSC was matched with the remaining 99 LSCs, thereby generating the pseudo-imposter scores. As observed in Figure 20, the distributions of genuine and imposter scores are separated, whereas the same for pseudo-imposter and imposter scores overlap. The distances between the various distributions are quantitatively presented in Table 16 through their $d'$ values. This pattern subsequently signifies that different random keys which can be utilised without having any distinguishing properties. Alternatively stating, the matching scores would exhibit no differences between the LSC templates generated from either different or the same individuals. Hence, the requirement of revocability is satisfied in our model.

6.3 Unlinkability

Unlinkability dictates that different LSC templates generated from the same base feature should be indistinguishable. One way to verify this requirement is to analyse the mated ($H_m$) and non-mated ($H_{nm}$) score distributions. The $H_m$ scores are computed by comparing the intra-class LSC templates generated using the same key, whereas the $H_{nm}$ scores correspond to LSC templates arising from different face images using different keys. Ideally, the mated and non-mated score distributions should be identical. Unlinkability can also be quantitatively estimated by the corresponding Local measure $D_{lm}(s)$, and Global measure $D^{2*}_{lm}$ [32]. Both these metrics have values in $[0, 1]$, with zero denoting complete unlinkability and unity indicating no unlinkability. Figure 21 portrays that the $H_m$ and $H_{nm}$ scores significantly overlap with each other, which is the definite sign of unlinkability. The $D_{lm}(s)$ values are also displayed in the same figure. The corresponding global measure was estimated to be $D^{2*}_{lm} = \{0.0051, 0.0017, 0.0077, 0.0081\}$ for the AR, ORL, Yale, and CASIA-Facev5 data sets, respectively. Since these values approximate zero, we can validate the claim of unlinkability.

7 CONCLUSION

Preserving the security of face-based biometric identification systems is a critical task. In this work, we have proposed a framework for generating cancellable and secure templates from face images. Our model is composed of two central techniques, namely BSIF and LSC. The BSIF descriptor is used to extract binary feature vectors from the input image. Subsequently, cancellable LSCs are created from them by utilising the random sampling mechanism. Since LSC is a particular realisation of the LSH principle, the corresponding transformation function does not degrade the original utility of the model. Extensive empirical analysis on four benchmark facial databases vindicates our claim of providing satisfactory recognition rates in comparison to
other state-of-the-art works. Furthermore, important security requirements such as non-invertibility, revocability, and unlinkability are also rigorously examined and empirically established. Examining the adaptability of this framework for multimodal biometric characteristics would be undertaken as the future extension of this work.

ACKNOWLEDGEMENTS

Portions of the research in this article use the CASIA-FaceV5 collected by the Chinese Academy of Sciences’ Institute of Automation (CASIA).

ORCID

Debanjan Sadhya  
https://orcid.org/0000-0002-9989-3464

Zabid Akhtar  
https://orcid.org/0000-0002-5026-5416

REFERENCES

1. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. Circ. Syst. Video Technol. 14(1), 4–20 (2004)
2. Zhao, W., et al.: Face recognition: a literature survey. ACM Comput. Surv. 35, 399–458 (2003)
3. Maiorana, E., Hine, G.E., Campisi, P.: Hill-climbing attacks on multi-biometrics recognition systems. IEEE Trans. Inf. Forensics Secur. 10(5), 900–915 (2014)
4. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security. EURASIP J. Adv. Signal Process. (2008)
5. Biggio, B., et al.: Security evaluation of biometric authentication systems under real spoofing attacks. IET Biom. 1(1), 11–24 (2012)
6. Natgananthan, I., et al.: Protection of privacy in biometric data. IEEE Access. 4, 880–892 (2016)
7. Patel, V.M., Ratha, N.K., Chellappa, R.: Cancelable biometrics: a review. IEEE Signal Process. Mag. 32(5), 54–65 (2015)
8. Sadhya, D., Singh, S.K., Chakraborty, B.: Review of key-binding-based biometric data protection schemes. IET Biom. 5(4), 263–275 (2016)
9. Sadhya, D., Raman, B.: Generation of cancelable iris templates via randomized bit sampling. IEEE Trans. Inf. Forensics Secur. (2019)
10. Kannala, J., Rautu, E.: Bif: binarized statistical image features. In Proceedings of the 21st international conference on pattern recognition (ICPR2012), pp. 1363–1366 (2012).
11. Manisha, Kumar, N.: Cancelable biometrics: a comprehensive survey. Artif. Intell. Rev. pp. 1–44 (2019)
12. Savvides, M., Kumar, B.V., Khosla, P.K.: Cancelable biometric filters for face recognition. In Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICCPR 2004, vol. 3, pp. 922–925 (2004).
13. Kong, A.W-K., et al.: An analysis of biohashing and its variants. Pattern Recognit. 39, 1359–1368 (2006)
14. Lacharme, P., Cherrier, E., Rosenberger, C.: Preimage attack on biohashing. In 2013 International Conference on Security and Cryptography (SECRYPT), pp. 1–8 (2013).
15. Rathgeb, C., Breitinger, P., Busch, C.: Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In 2013 International Conference on Biometrics (ICB), pp. 1–8 (2013).
16. Gomez-Barrero, M., et al.: Protected facial biometric templates based on local gabor patterns and adaptive bloom filters. In 2014 22nd International Conference on Pattern Recognition, pp. 4483–4488 (2014).
17. 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 2014 International Conference of the Biometrics Special Interest Group (BIOSIG), pp. I–6 (2014).
18. Bringer, J., Morel, C., Rathegel, C.: Security analysis of bloom filter-based iris biometric template protectionin 2015 International Conference on Biometrics (ICB), pp. 527–534 (2015).
19. Jeong, M., et al.: Changeable biometrics for appearance based face recognition. In 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, pp. 1–5 (2006).
20. Wang, S., Hu, J.: A blind system identification approach to cancelable fingerprint templates. Pattern Recogn. 54, 14–22 (2016)
21. Kim, Y., Toh, K.-A.: A method to enhance face biometric security. In 2007 First IEEE International Conference on Biometrics: Theory, Applications, and Systems, pp. 1–6 (2007).
22. Suteu, Y., Sencar, H.T., Meton, N.: A secure biometric authentication scheme based on robust hashing. In Proceedings of the 7th workshop on Multimedia and security, pp. 111–116 (2005).
23. Cho, S., Teoh, A.B.J.: Face template protection via random permutation maxout transform. In Proceedings of the 2017 International Conference on Biometrics Engineering and Application, pp. 21–27 (2017)
24. Saito, Y., et al.: An efficient random unitary matrix for biometric template protection. In 2016 Joint 8th International Conference on Soft Computing and Intelligent Systems (SCIS) and 17th International Symposium on Advanced Intelligent Systems (ISIS), pp. 366–370 (2016).
25. Kaur, H., Khanna, P.: Random distance method for generating unimodal and multimodal cancelable biometric features. IEEE Trans. Inf. Forensics Secur. 14(3), 709–719 (2019)
26. Charikar, M.S.: Similarity estimation techniques from rounding algorithms. In Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing, STOC ’02, pp. 380–388. Association for Computing Machinery, New York, NY, USA) (2002)
27. Martinez, A. M.: The AR face database. CVC Technical Report 24 (1998)
28. Bellumcure, P.N., Hespangha, J.P., Kriegman, D.J.: Eigenfaces vs. fisherfaces: recognition using class specific linear projection. IEEE Trans. Pattern Anal. Mach. Intell. 19(7), 711–720 (1997)
29. Rosenberger, C., Brun, L.: Similarity-based matching for face authentication. In 2008 19th International Conference on Pattern Recognition, pp. 1–4 (2008).
30. Oh, B-S., et al.: Extraction and fusion of partial face features for cancelable identity verification. Pattern Recogn. 45(9), 3288–3303 (2012).
31. Thamizharasi, A., Jayasudha, J.: An illumination invariant face recognition by selection of DCT coefficients. Int. J. Image Process. 10(1), 14 (2016).
32. Gomez-Barrero, M., et al.: General framework to evaluate unlinkability in biometric template protection systems. IEEE Trans. Inf. Forensics Secur. 13(6), 1406–1420 (2018).

How to cite this article: Sadhya D, Utsav U, Akhtar Z. Generation of cancellable locality sampled codes from facial images. IET Biome 2021;10:260–274. https://doi.org/10.1049/bmc2.12016