Multimedia Tools and Applications
https://doi.org/10.1007/s11042-020-09319-1

Cancellable face template algorithm based on speeded-up robust features and winner-takes-all

Hiba Basim Alwan[1] · Ku Ruhana Ku-Mahamud[2]

Received: 10 September 2019 / Revised: 9 June 2020 / Accepted: 9 July 2020
Published online: 06 August 2020

Abstract

Features such as face, fingerprint, and iris imprints have been used for authentication in biometric system. The toughest feature amongst these is the face. Extracting a region with the most potential face features from an image for biometric identification followed by illumination enhancement is a commonly used method. However, the region of interest extraction followed by illumination enhancement is sensitive to image face feature displacement, skewed image, and bad illumination. This research presents a cancellable face image algorithm built upon the speeded-up robust features method to extract and select features. A speeded-up robust feature approach is utilised for the image's features extraction, while Winner-Takes-All hashing is utilised for match-seeking. Finally, the features vectors are projected by utilising a random form of binary orthogonal matrice. Experiments were conducted on Yale and ORL datasets which provide grayscale images of sizes 168×192 and 112×92 pixels, respectively. The execution of the proposed algorithm was measured against several algorithms using equal error rate metric. It is found that the proposed algorithm produced an acceptable performance which indicates that this algorithm can be used in biometric security applications.

Keywords Feature selection. Speeded-up robust feature. Winner-takes-all. Hash function. Cancellable biometric

✉ Hiba Basim Alwan
hiba81basim@yahoo.com

Ku Ruhana Ku-Mahamud
ruhana@uum.edu.my

[1] Ministry of Finance, National Board of Pensions, Centre of Information and Computer Systems, Baghdad, Iraq

[2] School of Computing, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia

1 Introduction

Biometrics is an individual authentication and identification method that utilises many organs. The identification stage implements the verification and validation of users in a dataset while the authentication stage implements acceptance of users [6].

Biometric systems were proposed to mitigate the many challenges that were found in traditional authentication systems. Though many of the problems were solved or mitigated by biometric systems, there remain two major issues of security theft and privacy invasion in current biometric systems. These two problems hinder achieving optimality in biometric systems' development. This happens due to the magnitude of the security violation involved in biometric identity breach because individual biometric data cannot be changed [10].

Due to the promising nature of biometric authentication systems, substantial adoption has been witnessed in comparison to basic authentication techniques like username-password and token-based methods which are found in different domains of application. However, two key challenges in biometric-based authentication systems exist - security and privacy inversion. Breach of either of the two mentioned challenges can lead to two permanent loss of personal identity due to the permanency and intrinsic nature of the data involved. This leads to research the question of "How compromised biometric data can be replaced without sacrificing the accuracy of the system?". This necessitates the need to provide a robust biometric system that can withstand, protect, and in case of successful compromise, be capable of creating a different unique biometric template regardless of application type and domain, through a well-designed protection mechanism to disable chances of cross-matching. This mechanism should contain four established design criteria to meet the required protection capability as suggested in [1, 10]. These criteria are Irreversibility, Revocability, Unlinkability (Diversity) and Degradation. Only two criteria were suggested in [12, 13] to meet the required protection capability. These criteria are Irreversibility and Unlinkability.

Irreversibility simply means the ability of the system to make it extremely difficult, if not impossible, to regenerate the initially captured biometric data regardless of the computing power. In the case of revocability, one needs to understand that biometric data has to undergo some encryption before being stored. Thus, in the case of it being stolen, the system's ability to generate an entirely different encrypted template from the original to prevent cross-matching in another application is known as revocability. Diversity refers to the ability of the system, during regeneration of other templates from the original template, to generate a template that is different from any others that were previously generated, as in the case of system compromise or for utilisation in other systems to ensure maximum privacy protection. Degradation, in this context, implies that the recognition accuracy of the system should be preserved regardless of the time stretch [1, 10].

Two major approaches can be found in the researches in securing a biometric pattern. The first approach is a biometric cryptosystem which can be further sub-categorised into two schemes, i.e., create a key and bind-key structure [4]. The second approach is a feature transformation approach which is often referred to as the cancellable biometric. This approach can also be partitioned into non-invertible transformation and biometric salting [1, 4, 10]. In biometric salting, a unique, distorted biometric template is produced by merging the user's biometric data, a secret key and an input factor which is independent of the first two inputs. This method can be likened to password salting that can be found in cryptography [10, 25]. Bio-hashing is a well-known method used to achieve reliable biometric salting. Bio-hashing employs the method of mixing the initial biometric data with a token before converting it into a

discrete binary format to produce a uniformly random sequence of a hashed key. For the non-invertible transformation situation, the initial biometric data is encrypted in such a way that it cannot be reconstructed before it is being stored in a database. The approach is meant to provide maximum protection and privacy to the original biometric data [10]. This is achieved by passing the biometric data through a one-way function. The function uses, as part of its parameter, an externally generated specific range of values that serve as a secret key, obtained from the user, to generate the main template that has been saved in the database. This makes it easy for any generated template to be revoked if compromised. It allows another different and distinctive template to be generated from the initial template by changing the obtained secret key [25].

The biometric cryptosystem (or helper data method) is based on acquiring biometric information which, though not concealed, does not in any way reveal the actual biometric template. The method determines the validity of either generated or retrieved keys through a comparison based on the procedure adopted for generating the helper data. The key generation scheme generates the required encryption keys directly from the person's biometric information. The key binding method's main aim is to provide mapping between encryption keys and the person's biometric information so that it will be impossible to regenerate the encryption keys without having access to the original template at the time of authentication. It is worth mentioning that there is observed performance degradation in the key binding method when compared with the key generation method due to the effect of error correction in the key binding method. However, the basic goal of the two methods is to supply a secured biometric-based encryption key [10].

It is of great importance to point out the major distinction between creating the key method and bind-key method. Key binding and key creation operate differently on how the helper data are being extracted. In the key generation method, all helper data come from the original biometric pattern before the key is created from the combination of the biometric characteristics obtained from the query and the helper information. In the case of the key binding method, the initial biometric pattern is interfaced by a cryptographic key through mapping. The combination of both the cryptographic key and biometric data is stored as the helper information, for which an access key can only be issued if a similarity to a certain threshold has been reached [20].

In this paper, the two-dimensional Winner-Takes-All (WTA) [4] hashing will be used to develop a cancellable transformation algorithm called Speeded-up Robust Features-Winner-Takes-All (SURF-WTA). The proposed algorithm is based on Random Binary Orthogonal Matrices Projection [4] to protect speech biometric information. Investigation on different biometric traits such as fingerprint and face has been suggested in [4]. This was part of the motivation of this work to investigate on face biometric modalities. Moreover, this study has also been motivated since there are many challenges in the present face image template security as reported in [4]. Some of these challenges are [4]:

i Most of the image pattern protection methods have been reported to be vulnerable to various malicious attacks such as stolen token, and attacks through record multiplicity because of the strong relationships amongst the patterns created through utilising the same biometric feature. Therefore, the opponent can obtain the original template by analysing many compromised templates.
ii The biometric feature is also transformed from one location to another which results in the loss of distinct features while increasing the intra-class variation. The accuracy of matching

will be negatively affected. Thus, it is crucial to create templates that are not dependent on each other but fulfilling the unlinkability and revocability criteria.

In contrast to the work in [4], the proposed SURF-WTA algorithm combines four methods which are SURF, random binary orthogonal matrices, permutated feature, and WTA non-invertible transformation. These methods have not been previously combined, especially in the subject of cancellable face biometric pattern. The combination of the four methods to form an algorithm is considered as the key contribution of this study. These methods are employed to form the proposed SURF-WTA algorithm because:

i. SURF is an excellent feature selection method and it is utilised within the proposed algorithm to produce a more robust and faster feature extraction/selection process.
ii. The feature extraction and selection activities using the SURF method are permutated to produce robustness of the proposed algorithm.
iii. The permutated features are projected with random generated binary orthogonal matrix to enhance the strength of the proposed algorithm.
iv. Prime factorisation is used to improve the security and privacy.

The organisation of this paper is as follows: The related work on cancellable biometrics and biometrics cryptosystems in security is explained in Section 2. Section 3 describes the methods and materials that have been used in the proposed SURF-WTA algorithm. Experiments and results are discussed in Section 4 while Section 5 presents the conclusion and future work.

2 Related work

This section will focus on the image template protection schema. A cancellable biometric is a method focused on distorting and varying of obtained biometric features to produce various forms of biometric patterns. A cancellable template simply means a template generated from a transformation, through an encryption function of the original biometric data to prevent access by malicious intruders. The transformation or encryption process must ensure that the transformed data possess the ability of not being recovered. The transformed template generated is often referred to as a cancellable biometric template, as described in [10]. There are four basic criteria that a cancellable template must possess:

i. It must not be revocable in a situation where the generated template is compromised.
ii. Diversity in terms of generating transformed templates from the original.
iii. It must be able to preserve the integrity of the original biometric data after transformation for accuracy recognition, and
iv. The original data must not be reversed or regenerated from any compromised template.

Cancellable biometrics has been studied by [10, 15, 19, 23, 25, 26, 29, 33, 35, 40, 42, 44]. The first use of cancellable biometrics was proposed by the authors of [40]. The authors studied several non-invertible transformations like functional transformation, polar, and Cartesian in the construction of characteristics of a fingerprint pattern. The fundamental minutiae characteristics are employed in the fingerprint pattern. Original minutiae features are not stored. Minutiae orientations and locations that are kept are converted irreversibly. The authors

concluded that a cancellable transformation in a feature domain can be an alternative approach to produce acceptable performance. Besides [40], the authors in [19] propose a method to facilitate the implementation of a Fuzzy Commitment Scheme (FCS). The major obstacle against the implementation of the proposed method was the difficulty of FCS to efficiently capture the minutiae in its most detailed format. Hence, the authors employed the effective binarisation method which emphasises on capturing the most discriminatory features of the captured fingerprint using Gabor filters, local binary pattern and local direction pattern. A method meant to serve as a template in creating an alignment-free cancellable fingerprint pattern was put forward by Wang, Yang, and Hu [44]. The proposed method built local minutia via zoning pairs of minutia. Panchal and Samanta [35] employed a support vector machine ranking mechanism, a statistical-based technique, to extract biomedical features to generate a hashed code by using the Reed-Solomon encoding technique. The hashed code is then used to generate a secret key for biometric authentication.

The Gabor filtering technique was also utilised in [10] as a novel cancellable iris template generation approach to generate invariant feature vectors. The method in [10] was able to regenerate a different pattern built on the initial pattern kept in the database. This cancellable iris pattern generation approach was based on a randomised look-up table with the ability to shield the original captured biometric information, in case the hashed template gets stolen. Harkeerat and Pritee in [23] proposed a new cancellable biometric pattern creation approach utilising Gaussian arbitrary vectors and a one- path modulus hashing. As an alternative to utilising the initial pattern, the suggested approach utilises converted pattern forms for keeping and matching. The main goal of this work was to generate a cancellable biometric pattern that is non-invertible and produce an improved function. Cancellability is obtained through a projection of biometric pattern on an arbitrary array. This array has columns that are generally distributed (Gaussian) vectors where the values of mean and variance are recorded. Another work for Harkeerat and Pritee was proposed in [26] where a smart card built on biometric authentication structure utilising cancellable fake biometrics identities is used. They also developed a confidential sharing system to focus on protection and privacy concerns in a distant multi-server nature appropriate for either cloud or network where many applications are put on many servers. Cross-matching and any additional database attacks can be avoided through creation of many fake identities from the initial user biometric. Thus, this will enable the user to work securely on different applications. The authors used an arbitrary distance approach to create revocable, different and non-invertible fake identities. This creation is done by reducing pattern size to 50% of its original size. So as to create sharing, confidential sharing ideas are used over transformed identities and user-specific keys. These sharings are kept on distributed databases. Multiple servers can be accessed through the smart card that transmits only several sharings. The authors of [15] proposed a new effective approach to accomplish privacy sustaining face recognition in the cloud. Diffusion, permutation, and shift transformation methods are combined to create a new transformation. This new transformation is utilised to secure the privacy of faces. The projection and recognition techniques are implemented in the encoded field with no interaction. The authors also proposed an optimisation approach to maximise the productivity of encoding.

Random slop has been proposed as a new cancellable biometric approach in [25]. This approach creates protect revocable, and non-invertible patterns. In this approach, the biometric characteristics, and some arbitrary individual-specific information are mapped as dots on the Cartesian plane. The slopes, and the intersection of lines across the arbitrary dots are computed to create transformed characteristics. RS-V1 and RS-V2 approaches have been suggested

within the proposed idea to create a reduction in dimensionality and to fulfil the necessary cancellability principles. A lightweight face recognition system that depends on depthwise separable convolution has been proposed in [29]. The triplet loss approach is utilised to optimise the training light face model. The light face needs a huge quantity of training data and parameters and this will keep the information of an individual, which can be recovered by attackers. Thus, to solve this issue, the authors proposed a lightweight face recognition system called 'LightFace' that can be used for robust privacy security. In the proposed system, the information generated from biometric data and noise data is integrated with the initial biometric data to make it more secure. This will enhance the confidence in using the system. The ensemble learning is also used to maximise the arbitrariness of the initial information distribution and improve the strength of the system.

A novel face biometric system which depends on optical transformation has been proposed for protection and authentication [42]. To make the suggested system non-invertible, the face biometric is transmuted by utilising the stage retrieval method. Optimum biometric characteristics are selected by a sparse cover and linked with the chaotic technique which is kept for purpose of verification. The chaotic variables are joined like a pin variable to the registered individual in the enrolment stage. The proposed system is useful to improve the protect technique through the use of a two-variable authentication approach. The authors in [33] have proposed a novel face encoding system built on fuzzy commitment, chaos characteristic permutation, and binarisation transformation approach. To improve discriminability, actual valued patterns are encoded to their binary forms through novel special binarisation transformation count on the output correcting code. The chaos characteristic permutation is then utilised to maximise the protection as well as privacy of binary patterns in securing the fuzzy dedication approach versus cross-matching attacks.

Cryptosystem biometric has also been studied apart from cancellable biometric [2, 30, 32]. Mai, Lim and Yuen [30] proposed a binary feature fusion technique based not only on its discrimination ability, but also overall system security. The authors considered the degree of variation that can be found between binarised extracted features which can be differentiated based on the dependency of sources. Each distinct feature is extracted forming a group of features from a unimodal source. The extracted features of each group are fused through mapping. The mapping process minimises the variations of intra-user and increases the variations of inter-user. A framework that has the capability of integrating many biometric cryptosystems with a high degree of reliable security to the template model has been proposed by Murakami, Ohki, and Takahashi [32]. This framework was built on the concept of a minimum number of extracted input characteristics. The proposed method performs its computational process at feature level by sequencing and fusion of the on-the-spot extracted features each time a user tries to access the system; it determines the authenticity of the input value based on the stored hashed template. Barman, Chattopadhyay, Samanta and Panchal [2] proposed a technique based on a key regeneration FCS that ensures secured communication of encrypted data between users and efficient preservation of biometric data privacy. A two-stage protocol operation is necessary to produce the technique. In the first stage, a locker-to-locker exchange of the extracted key is performed using the secured information kept in the database. The second protocol is to create a key process of FCS and use it to exchange the secret key from the locker through the recipient-based personalised locker.

Accuracy, security and privacy are major shortcomings of cancellable biometrics and key binding approaches. So, Jin, Goi, and Tay [20] proposed a scheme that bridges existing cancellable biometrics and biometric cryptosystems. The achieved biometric template is

protected by creating a cancellable transformation from randomised graphic-based hamming embedding. Their method proved to be effective for template protection. A multi-biometric protection method, proposed by Gomez-Barrero, Maiorana, Galbally, Campisi, and Fierrez [13], is based on bloom filter and designed in such a way that both biometric and multi-biometric templates are protected from malicious attacks. The authors have tested their proposed method on different multi-sources of biometric data ranging from iris, facial and fingerprints of individuals.

3 Methods and materials

This section is meant to provide the methods and materials of the proposed SURF-WTA algorithm. Descriptions on the SURF and WTA hash functions which provide- the foundation of the work are provided. This is followed by the details of the proposed SURF-WTA algorithm.

3.1 Speeded-up robust features

One of the commonly utilised methods to identify significant features is the Feature Selection (FS) method [16]. Nevertheless, identifying these significant features in huge dimensional data is usually a difficult task [28]. So, FS method is a necessary step and it is utilised to minimise dimensionality, unrelated data, and data redundancy [9, 38]. FS is a procedure to minimise the number of characteristics. Moreover, FS includes a select subset of features from the initial features set. The core aim of FS is to minimise data dimensionality and to improve performance [38]. Investigating strong, adaptable, and effective FS methods to manage the growth of big data is yet an exciting issue. Lately, investigating effective FS methods to manage big data with high-dimensional challenges as well as to enhance the execution of the algorithms has been one of the necessary research areas in the different application fields [9]. Chi-squared, mutual information, a random forest of decision trees, SURF, etc. are all methods for FS [41].

The Speeded-Up Robust Feature is a novel descriptor and detector method that has proved to be excellent in detecting points of interest in a given region. The method is scale, rotation and illumination invariant [48]. It is considered as a faster feature extraction and selection method than other methods. SURF utilises a descriptor built on specific characteristics, the difficulties of which are reduced when compared with other methods [14]. SURF is derived from the scale-invariant feature transform [18]. The SURF method uses two distinctive processing steps. In the first stage, the detector assigns a base orientation to a given key point with an identified circular boundary. Then, in the second stage, the circular region is projected onto a squared region from which the descriptor of SURF is extracted based on Haar wavelet reactions. Improvements recorded on SURF were based on utilising the Hessian detector. The improvements were noticed on the accommodation of various lighting changes, different image compression, and intensity of image blurring and image rotation. SURF gives an output of 64-dimensional data [22]. This enables SURF to be used in various domains ranging from computer vision in object recognition and image reconstruction which is usually in three dimensions [11, 21].

Speed and simultaneous processing are the key characteristics of SURF which has the functions of recurrence, uniqueness, scale and rotation invariance, and robustness [17, 34, 39, 49]. Generally, SURF contains four stages: keypoint detection or interest point detection, an

optional step of orientation assignment, local descriptor, and keypoint matching (utilising its descriptor) [31, 37]. There are many reasons to use the SURF method. SURF which has been established on the theory of multi-scale space also has a valuable implementation in obtaining distinct characteristics from the images. It will not change upon orientation, scaling, as well as being partially invariant to affine distortion or different brightness. SURF is also significantly faster than Laplacian of Gaussian kernel because it utilises the Fast-Hessian detector. Finally, the SURF detector can detect tiny objects and points of interest of isotropic possessions [48].

3.2 Winner-takes-all hash

Winner-Takes-All hash is an advanced method used by Google due to its effectiveness in enabling fast similarity searches. The method can be used to generate different sequences based on the number of permutations. It utilises the rank of association measures and records the position of the highest value of biometric features. This happens after the application of random permutations [4]. Every hash function of WTA describes an embedding of digits and a related rank that measures the similarity of correlation. An invariance rank will be offered related to disorder in numeric rates and is suited, perfectly, as a foundation for sensitive hashing of the locality. The WTA hash functions are decisive, non-linear and yield insufficient descriptors. WTA hash has also yielded significant improvement using simple linear classifiers which take a shorter time to train. The WTA hash that contains any data will permit the coefficient to be restructured in the hashed vector, even though it is a partial organisation [8].

The algorithm for obtaining the position vector for the WTA hash is explained with an example as shown in Table 1. Assume there are four features with five items each. The first step is to input several sets of feature x. Randomly change the position of the item in each set and permute x'. Assume the first four items are selected from each x'. Determine the maximum value amongst the four selected items. Then, determine the position (index) of this maximum value. The hashed code is placed to be equivalent to the position of these maximum values [45].

4 Proposed SURF-WTA algorithm

The SURF-WTA algorithm has been proposed to protect the face template in this research. Features were extracted and selected from the face image using SURF and then permutated to obtain a robust non-invertible characteristic. This will make it difficult for an attacker to access the original template and retrieve the original feature value. WTA hashing has been utilised after the permutation process. This hash function is also used in the Google image retrieval domain to prepare the hash code matrix. Due to the non-linearity properties of hash functions, it is expected for them to be non-invertible. Furthermore, a hashed datum is not expected to be

Table 1 WTA example

Feature x	10, 5, 6, 12, 3	4, 5, 10, 2, 3, 1	22, 12, 6, 14, 26, 8	11, 4, 3, 7, 13, 2
Permuted feature x'	5, 3, 10, 6, 12	10, 5, 3, 1, 4, 2	12, 8, 6, 26, 22, 14	4, 13, 3, 2, 11, 7
Select first four items	5, 3, 10, 6	10, 5, 3, 1	12, 8, 6, 26	4, 13, 3, 2
Identify position of highest item	2	0	3	1
Hashed code	2, 0, 3, 1			

regenerated to its original form after being hashed unless considerable computing time has been spent. The resultant hashed code should be able to withstand invertibility attack on a template. This needs the hash function to be conflict-resistant. Thus, it is extremely difficult to obtain information that will create the exact hash value. Conflict resistance is achieved in portion, through creating extremely big hash values. The proposed algorithm will take in the image set and will output the Equal Error Rate (EER). Amongst the calculation that will be performed are the Permuted Feature (PF), hash code, similarity score, False Rejection Rate (FRR) and False Acceptance Rate (FAR). The pseudo algorithm is shown as follows:

Pseudo algorithm of the proposed SURF-WTA
Input: image set, no. of strongest extracted feature, first members (window size), no. of the hash function
Output: EER
//for each user
Read image set
y = no. of images in image set
For x = 1 to y
    Read image (x)
    Extract image feature using SURF
    Select the strongest extracted feature
    Permute the strongest selected feature
    For i = 1 to no. of the hash function
        Create orthogonal matrices
        Project the permuted strongest selected feature with orthogonal matrix
        Select first members
        Find position of highest no. amongst the first selected members
        Calculate *PF*
        Compute prime factorisation for *PF*
        Hash code (i) = total count of prime numbers
Compute similarity score
Compute FAR, FRR, and EER

Figure 1 shows a one-round graphical implementation of the proposed algorithm. For every image, the SURF algorithm will extract important characteristics and multiply them by the first

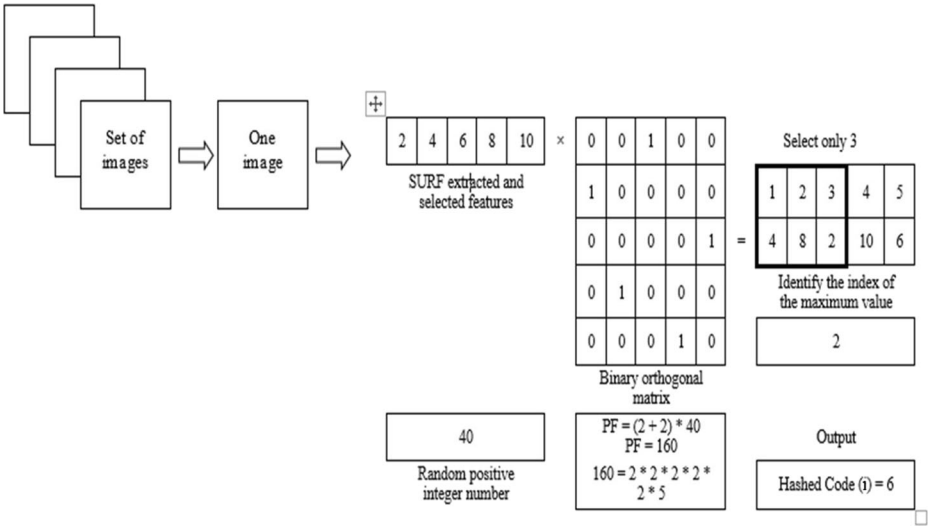

Fig. 1 A one-round implementation of the SURF-WTA algorithm

generated binary orthogonal matrix. Several of the first generated feature members are then selected. For example, only the first three members are selected. The position of the maximum number (PMN) is identified and a random number is generated to calculate the PF. The calculation of PF is done using Eq. 1 [4]:

$$PF = (\mathrm{PMN} + 2) \times \text{random number} \tag{1}$$

Thus, if a generated random positive number is 40, the permutated feature will be 160. The prime factorisation of 160 is then computed. In other words, 160 will be represented as multiplication of prime numbers. The benefit of using such a random positive number is to strengthen the robustness of the proposed algorithm and enable the template to remain intact. Finally, the total count of prime numbers (which is 6) is assigned as the first digit of the hashed code. The second and consecutive digits of the hashed code will be obtained from the second and consecutive rounds of implementation of the SURF-WTA algorithm.

The SURF-WTA algorithm is simple and less complex compared with other algorithms such as the region of interest or Hill cypher algorithms. The main limitation of the Hill cypher method is that it encrypts the same plaintext blocks to the same encrypted plaintext block. Thus, image features that reveal patterns in the plaintext can be obtained. Furthermore, it can be simply destroyed with an acknowledged plaintext attack that exposes vulnerable protection through solving a system of linear formulas to discover the decoding matrix. The region of interest extracting method followed by illumination enhancement is sensitive to image feature displacement, skewed image, and bad illumination. So, detecting the skew angle of the image, correcting the skewed image based on a skewed angle, and enhanced illumination must first be implemented before using the region of interest algorithm. This will lead to an increase in computational complexity as a result of matrix multiplication operations. In the proposed algorithm, there is no need to hide image features as required in the Hill cypher. Furthermore, the proposed algorithm is not affected by image displacement, skewed image, and bad illumination as in the region of interest method.

5 Experimental result

Experiments were performed on two datasets to assess the SURF-WTA algorithm. Comparisons were made with Principle Component Analysis (PCA), Linear Discriminant Analysis (LDA) [23], optical transformation, digital holographic built on cancellable biometric for personal authentication, also cancellable face verification using optical encryption and authentication [42], Hill cypher [24], Random Permutation Maxout (RPM) [7], Deep Convolution Neural Network (Deep CNN) [36], and Hybrid Gabor Principle Component Analysis (HGPCA) [27]. An EER metric, which is considered the standard measurement utilised to measure the execution of the cancellable biometric algorithm, is used. EER computes the probability of false acceptance and false rejection. A smaller EER value means good performance [24]. Results of the experiments are presented and discussed based on seven (7) items: i) face datasets, ii) similarity score, iii) FAR and FRR, iv) effect on EER with different window sizes, v) effect on EER with different hash functions, vi) performance comparison with other algorithms and vii) revocability criteria of cancellable biometric.

5.1 Face dataset

The datasets utilised in the experiments are the Olivetti Research Laboratory (ORL) face dataset and Extended Yale face dataset. The ORL is a publicly available face dataset that includes groups of faces acquired from April 1992 to April 1994 at the ORL in Cambridge, United Kingdom. This dataset contains 400 images of 40 persons taken against a dark background at various times of the day, and slightly varied lighting settings and facial gestures. The images were acquired while the owners were facing front (though tolerance of slight side movement was given) and all are in the upright position. Also, all images were greyed to a value of 256 levels per pixel at a size of 112 × 92 pixels for each; it includes 40 persons' face images with ten images each per person [3]. In conducting the experiments, the first image of each user was employed as the base pattern while the remaining nine images of the exact user were considered as the query images employed to compute the FRR. The FAR was also computed using the same method as FRR. In that manner, 1800 genuine matching tests and 78,000 imposter matching tests were obtained based on the above rule.

Similarly, the extended Yale face dataset B used in the experiment has the same data format as the previous Yale face dataset. The extended dataset includes images of 38 individuals (unlike the first Yale face dataset with only ten individuals) is made up of 1128 different images which were taken under nine different poses and 64 various illumination conditions. The images used in the experiment were pre-processed by converting each image into 168 × 192 pixels size and were all properly aligned and cropped [46]. In computing the FRR, the first image of each user was employed as the base pattern while the balance of 63 images were considered as the input query. As for the computation of FAR, the first image of each user was selected as the base pattern and the remaining images were treated as input queries. Based on the described rule, the yielded result showed 76,608 genuine match tests and 2,879,488 for the imposter matching tests.

5.2 Similarity score

To ensure the protection of the initial biometric information, the matching function in the SURF-WTA algorithm was conducted in a transformed domain. The two phases of enrolment and verification were included in the algorithm. The features of the target image were extracted, and only significant features were then selected by using the SURF method. The selected features were converted into vectors of integers which were then projected with orthogonal matrices based upon non-invertible transformation and continued with the other steps of the SURF-WTA algorithm, as included in Algorithm 2. The result of transformation was then hashed and stored in a database from which comparison and verification were performed at later stages. At the verification stage, the database was queried based on a hashed query that was transformed with an exact procedure employed during the transformation of the original biometric data to the hashed feature vector as described above. The similarity value was then computed to determine the existing matching, or otherwise, amongst the two characteristic vectors. The similarity score is calculated using Eq. 2 [4]:

$$\text{Similarity score} = \frac{\text{number of zeros}}{\text{length of hashed code}} \tag{2}$$

Table 2 Computation of similarity score

Step 1	Enrolled hashed code, S_x	6	10	1	4	7
	Query hashed code, S_x	5	10	2	4	7
	Compute the difference between enrolled hashed code (S_x) and query hashed code (S_x)	1	0	−1	0	0
	S_x - S_x					
Step 2	Compute number of 0's in S_x - S_x					
	no. of 0's = 3					
Step 3	Compute the similarity score between enrolled hashed code (S_x) and query hashed code (S_x) using Eq. 2					
	Similarity score = 0.6					

The procedure to calculate the similarity score is as follows:

i. Determine the difference between stored hashed code denoted as S_x and hashed code used as query denoted as S_x, (i.e. S_x - S_x).
ii. The number of zeros "0" in the resultant vectors are determined. Existence of zero "0" indicates that there is a match between the enrolled hashed code and the hashed code in the query.
iii. Determine the value of similarity score by computing the total count of zeros "0" over the total length of the hashed codes.

Table 2 illustrates an example of a matching value calculation.

The similarity score calculated using Eq. 1 is within 0 to 1. A small score indicates less similarity amongst vectors of the pattern and query [47].

5.3 Computation of FAR, FRR, and EER

A genuine attempt can be described as a single attempt by the user to match the user preserved pattern/template. The imposter attempt is when the individual's pattern/template matched another individual's template. Many genuine and impostor attempts are made in the system and all similarity scores are saved if the system's performance were to be measured. Both FAR

Table 3 Effect of window size

Window size	EER %	
	ORL face dataset	Extended Yale face dataset B
5	9.09	1.54
10	9.09	1.44
15	9.02	1.43
20	8.85	1.42
25	8.67	1.42
30	8.41	1.38
35	8.28	1.36
40	8.23	1.35
45	7.96	1.30
50	5.68	1.17

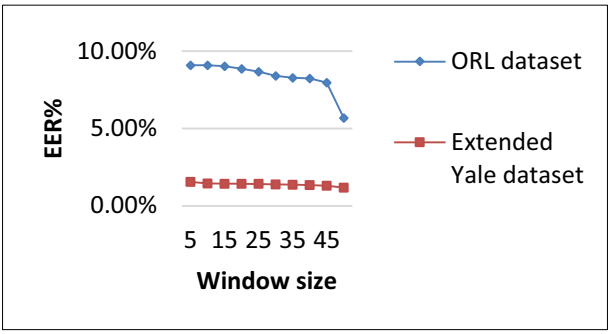

Fig. 2 Effect of window size

and FRR are used in computing EER as performance metrics and values which can be calculated using Eqs. 3 and 4 [5]:

$$FAR = \frac{\text{number of impostors that have been authenticated}}{\text{number of impostor users}} \tag{3}$$

$$FRR = \frac{\text{number of users that have been correctly authenticated}}{\text{number of genuine users}} \tag{4}$$

The EER is utilised to assess the execution of the SURF-WTA algorithm. EER is the functioning situation where FAR and FRR are equivalent. Calculation of EER was performed using Eq. 5 [43]:

$$EER = (FAR + FRR)/2 \tag{5}$$

5.4 Effect of window size

Optimum window size has been investigated based on EER. The window size varies from 5, 10, 15, 20, 25, 30, 35, 40, 45, and 50. From Table 3 and Fig. 2, when the window size is increased, the EER value decreases. The EER is sensitive to small window sizes. When the

Table 4 Effect of the hash function

No. of hash functions	EER %	
	ORL face dataset	Extended Yale face dataset B
10	9.59	1.47
20	9.09	1.45
30	8.84	1.44
40	7.92	1.41
50	7.62	1.39
100	6.56	1.37
200	6.11	1.33
300	5.68	1.22
400	4.99	1.17

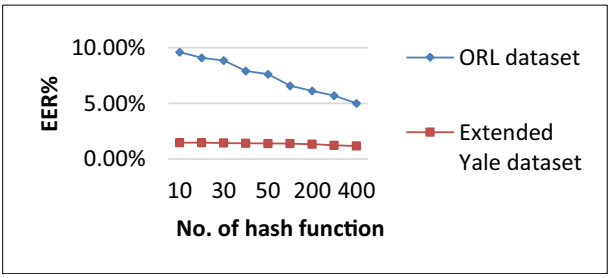

Fig. 3 Effect of the hash function

window size is small, there will be a chance to obtain fewer zeros and this will result in a low similarity score. Increasing the window size enables EER to capture more "0 s" which then enables the probability of capturing other values in the window to be reduced.

Conclusively, more bits are considered as the window size increases which, in turn, compensates for the effect of similarity score subtraction. However, the result shows that when a certain window size is reached, a decrease of EER level-off occurs which means there is a need for a much bigger window size to gain the lowest EER.

5.5 Effect of the hash function

The relationship between hash function values and verification performance is examined in this section. Different experiments were executed based on various hash function values of 10, 20, 30, 40, 50, 100, 200, 300, and 400 as illustrated in Table 4 and Fig. 3. Experimental outputs show an increment of better similarity score with an increase of hash function value subject to different window sizes. However, with a lowered hash function, there is a noticeable deterioration of the algorithm's verification performance which, in turn, results in EER increment.

5.6 Performance comparison

From previous studies on the facial-based template protection domain, the number of samples used for verification of different methods and techniques differ amongst researchers. However, in this study, the first image of each user is considered as a base pattern and the balance of the images were considered as the query used to determine the FRR. In computing FAR, each first image of every individual is placed as the base-template while all remaining images from the remaining users are set as the query. The comparison of SURF-WTA performance on ORL dataset with [7, 23, 24] has been provided in Table 5. Table 6 shows the performances of

Table 5 Performance of EER on ORL dataset

Algorithm	EER %
Proposed SURF-WTA	4.99
PCA [13]	12.44
LDA [13]	5.2
Hill cypher [41]	7.12
RPM [42]	6.75

Table 6 Performance for EER on extended Yale face dataset B

Algorithm	EER%
Proposed SURF-WTA	1.17
PCA [13]	32.5
LDA [13]	11.7
Digital holographic [17]	1.77
Optical encryption [17]	1.36
Optical transformation [17]	1.19
Hill cypher [41]	9.95
Deep CNN, scenario 1 [43]	5.45
Deep CNN, scenario 2 [43]	12.13
HGPCA [44]	1.065

SURF-WTA, [23, 24, 27, 36, 42] on the extended Yale dataset. PCA and LDA were used in [23]. The method used in [24] is a one-way hashing on the biometric template by making use of the non-invertibility of the Hill cypher algorithm while the method used in [7] is a cancellable algorithm that is based on RPM transform. [36] uses deep CNN. Two scenarios have been used in [36]. In scenario 1, the exact result of the deep CNN, i.e., with no hashing has been used while in scenario 2, the deep CNN result has been mapped and hashed to get high protection. Both scenarios used 128, 256, 512, 1024 bits of security. Their best results from these two scenarios were with 1024 bits of security as shown in Table 6. Finally, the method proposed in [27] utilised the HGPCA method to extract features. Then, the extracted features are transformed using wavelet transform and concatenated. Finally, scrambling is performed to the concatenated features utilising the arbitrary key given amongst the user.

It can be noted that the SURF-WTA algorithm is capable of preserving the verification performance with an insignificant deviation of EER = 1.17% and 4.99% for Yale and ORL face datasets, respectively.

5.7 Revocability

Revocability is regarded as one of the key elements required for a cancellable biometric system to be considered as an effective qualified system. The importance of revocability in a cancellable biometric system is to enable the system to have any compromised template to be rendered useless, while another new template for a user should be auto-generated without making the newly generated template share any similarities with the revoked template, hence enhancing security.

The Yale dataset was used in this experiment for testing the revocability effect of the proposed SURF-WTA algorithm. A hash code was generated and matched with different hash codes generated from binarised random matrices with orthogonality properties. In total, 200 hashed codes are obtained from the proposed algorithm amongst 200 various binary orthogonal arrays. Various hashed codes are compared with the first to calculate the total of pseudo-imposters. To generate an aggregation of $199 \times 2 \times 38 = 15{,}124$,[1] the procedure is reiterated for various face images users. A window size of 50 and round hash function of 200, as illustrated in Fig. 4, was utilised to aggregate the scores of the imposter spread, along with the scores of pseudo-imposters. It is possible to notice that the distribution of the imposter scores is similar to the distribution of pseudo-imposter scores. This ensures that although the recently produced

[1] Only 200 hashed codes were generated for the first two images of each user

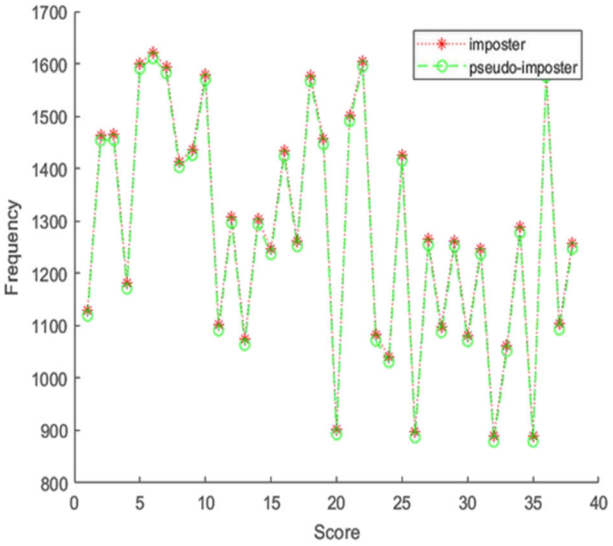

Fig. 4 Pseudo-imposter and imposter distribution on Yale dataset

hash codes originated from an identical characteristic of the face image, they are still unrecognisable to each other. As the old hashed code is unrelated to those recently produced, it can be justified that the presented algorithm achieved the criteria of revocability.

6 Conclusion

A cancellable face image template protection called SURF-WTA has been proposed for biometric recognition system. Comprehensive experimental results have shown that the proposed algorithm is capable of meeting the required conditions for a biometric algorithm. The proposed algorithm has also fulfilled the revocability and cancellability criteria of biometric algorithms. The experimental results show that when the number of hash functions and the window sizes increase, the EER values decrease and this indicates that the SURF-WTA algorithm is better than other compared algorithm. To test the revocability criteria of the proposed algorithm, experiments on the Yale dataset have shown that the proposed algorithm accomplished the revocability criteria. Furthermore, users are not required to keep track of any random symbol or binarised orthogonal matrix. The proposed algorithm has the advantage of a fast similarity searching mechanism from WTA and it also possesses the ability to exhibit both the strengths of non-invertible properties coupled with non-invertible functions in addition to the randomised user-specific generated token. However, there are several limitations to the proposed SURF-WTA algorithm. It cannot be applied to real-time face image dataset and the algorithm consists of complex mathematical formulation.

Cancellable biometrics is a promising area of research. Further research can focus on designing new feature extraction algorithms. Cancellable biometric systems also need to be designed based on non-invertible efficient functions which utilise other feature extracting methods with the use of deep learning method.

Acknowledgements This work was supported by the Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme [grant number 12490].

References

1. Alam B, Jin Z, Yap W-S, Goi B-M (2018) An alignment-free cancelable fingerprint template for bio-cryptosystems. J Netw Comput Appl 115(2018):20–32. https://doi.org/10.1016/j.jnca.2018.04.013
2. Barman S, Chattopadhyay S, Samanta D, Panchal G (2017) A novel secure key-exchange protocol using biometrics of the sender and reciever. Comput Electr Eng 64(2017):65–82. https://doi.org/10.1016/j.compeleceng.2016.11.017
3. Cambridge University Computer Laboratory http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html
4. Chee KY, Jin Z, Cai D, Li M, Yap WS, Lai YL (2018) Cancellable speech template via random binary orthogonal matrices projection hashing. Pattern Recogn 76(2018):273–287. https://doi.org/10.1016/j.patcog.2017.10.041
5. Cherifi F, Hemery B, Giot R, Pasquet M, Rosenberger C (2010). Performance evaluation of behavioral biometric systems, in behavioral biometrics for human identification: intelligent applications. IGI Global Disseminator of Knowledge. https://doi.org/10.4018/978-1-60566-725-6.ch003
6. Chesada K, Chidchanok L, Peraphon S (2017) High accuracy EEG biometrics identification using ICA and AR model. Journal of Information and Communication Technology 16(2):354–373
7. Cho S, Teoh AB (2017) Face template protection via random permutation maxout transform. Proceedings of 2017 ACM international conference on biometrics engineering and application, pp 21-27
8. Dean T, Ruzon MA, Segal M, Shlens J, Vijayanarasimhan S, Yagnik J (2013) Fast, accurate detection of 100000 object classes on a single machine. Proceedings of 2013 IEEE international conference on computer vision and pattern recognition, pp 1812-18121
9. Ding W, Lin CT, Prasad M (2018) Hierarchical co-evolutionary clustering tree-based rough feature game equilibrium selection and its application in neonatal cerebral cortex MRI. Expert Syst Appl 101(2018):243–257. https://doi.org/10.1016/j.eswa.2018.01.053
10. Dwivedi R, Dey S, Singh R, Prasad A (2017) A privacy-preserving cancelable iris generation schema using decimal encoding and look-up table mapping. Computers & Security 65(2017):373–386. https://doi.org/10.1016/j.cose.2016.10.004
11. Favorskaya M, Proskurin A (2015) Image categorization using color G-SURF invariant to light intensity. Procedia Computer Science 60(2015):681–690. https://doi.org/10.1016/j.procs.2015.08.208
12. Gomez-Barrero M, Maiorana E, Galbally J, Campisi P, Fierrez J (2017) Multi-biometric template protection based on homomorphic encryption. Pattern Recogn 67(2017):149–163. https://doi.org/10.1016/j.patcog.2017.01.024
13. Gomez-Barrero M, Rathgeb C, Li G, Ramachandra R, Galbally J, Busch C (2018) Multi-biometric template protection based on bloom filters. Information Fusion 42(2018):37–50. https://doi.org/10.1016/j.inffus.2017.10.003
14. Govindaraju S, Kumar GPR (2016) A novel content based medical image retrieval using SURF features. Indian journals of science and technology 9(20):1–8. https://doi.org/10.17485/ijst/2016/v9i20/89786
15. Guo S, Xiang T, Li X (2019) Towards efficient privacy-preserving face recognition in the cloud. Signal Process 164(2019):320–328. https://doi.org/10.1016/j.sigpro.2019.06.024
16. Gupta A, Agrawal RK, Kirar JS, Andreu-Perez J, Ding WP, Lin CT, Prasad M (2018) On the utility of power spectral techniques with feature selection techniques for effective mental task classification in non-invasive BCI. IEEE Trans Syst Man Cybern Syst Hum. https://doi.org/10.1109/TSMC.2019.2917599, 1, 13
17. Hebbar VAD, Shekhar VS, Murthy KNB, Natarajan S (2015) Two novel detector-descriptor based approaches for face recognition using SIFT and SURF. Procedia Computer Science 70(2015):185–197. https://doi.org/10.1016/j.procs.2015.10.070
18. Huang L, Chen C, Shen H, He B (2015) Adaptive registration algorithm of color images based on SURF. Measurement 66(2015):118–124. https://doi.org/10.1016/j.measurement.2015.01.011
19. Imamverdiyev Y, Teoh AB, Kim J (2016) Biometric cryptosystem based on discretized fingerprint texture descriptors. Expert Syst Appl 40(5):1888–1901. https://doi.org/10.1016/j.eswa.2012.10.009
20. Jin Z, Jin ATB, Goi BM, Tay YH (2016) Biometric cryptosystems: a new biometric key binding and its implementatio for fingerprint minutiae-based representation. Pattern Recogn 56(2016):50–62. https://doi.org/10.1016/j.patcog.2016.02.024

21. Kang T-K, Choi I-H, Lim M-T (2014) MDGHM-SURF: a robust local image descriptor based on modified discrete Gaussian-Hermite moment. Pattern Recogn 48(3):670–684. https://doi.org/10.1016/j.patcog.2014.06.022
22. Kashif M, Deserno TM, Haak D, Jonas S (2016) Feature description with SIFT, SURF, BRIEF, BRISK, or FREAK? Ageneral question answered for bone age assessment. Comput Biol Med 68(2016):67–75. https://doi.org/10.1016/j.compbiomed.2015.11.006
23. Kaur H, Khanna P (2015) Gaussian random projection based non-invertible cancelable biometric templates. Procedia Computer Science 54(2015):661–670. https://doi.org/10.1016/j.procs.2015.06.077
24. Kaur H, Khanna P (2017) Non-invertible biometric encryption to generate cancelable biometric templates. Proceedings of 2017 world congress on engineering and computer science, pp 432-435
25. Kaur H, Khanna P (2019) Random slope method for generation of cancelable biometric features. Pattern Recogn Lett 126(2019):31–40. https://doi.org/10.1016/j.patrec.2018.02.016
26. Kaur H, Khanna P (2020) Privacy preserving remote multi-server biometric authentication using cancellable biometrics and secret sharing. Futur Gener Comput Syst 102(2020):30–41. https://doi.org/10.1016/j.future.2019.07.023
27. Kausar F (2020) Cancelable face template protection using transform features for cyber world security. International Journal of Advanced Computer Science and Applications (IJACSA) 11(1):333–341
28. Li DL, Prasad M, Lin CT, Chang JY (2016) Self-adjusting feature maps network and its applications. Neurocomputing 207(2016):78–94. https://doi.org/10.1016/j.neucom.2016.03.067
29. Li Y, Wang Y, Li D (2019) Privacy-preserving lightweight face recognition. Neurocomputing 363(2019):212–222. https://doi.org/10.1016/j.neucom.2019.07.039
30. Mai G, Lim M-H, Yuen PC (2017) Binary feature fusion for discriminative and secure multi-biometric cryptosystems. Image Vis Comput 58(2017):254–265. https://doi.org/10.1016/j.imavis.2016.11.011
31. Mehrotra H, Sa PK, Majhi B (2012) Fast segmentation and adaptive SURF descriptor for iris recognition. Math Comput Model 58(1–2):132–146. https://doi.org/10.1016/j.mcm.2012.06.034
32. Murakami T, Ohki T, Takahashi K (2016) Optimal sequential fusion for multibiometric cryptosystems. Information fusion. 32(part B 2016):93–108. https://doi.org/10.1016/j.inffus.2016.02.002
33. Nazari S, Moin MS, Kanan HR (2018) Securing templates in a face recognition system using error-correcting output code and chaos theory. Comput Electr Eng 72(2018):644–659. https://doi.org/10.1016/j.compeleceng.2018.01.029
34. Oliveira SAF, Neto ARR, Bezerra FN (2016) Anovel genetic algorithms and SURF-based approach for image retargeting. Expert Syst Appl 44(2016):332–343. https://doi.org/10.1016/j.eswa.2015.09.015
35. Panchal G, Samanta D (2018) A novel approach to fingerprint biometric-based cryptographic key generation and its applications to storage security. Comput Electr Eng 69(2018):461–478. https://doi.org/10.1016/j.compeleceng.2018.01.028
36. Pandey R, Zhou Y, Govindaraju V (2015). Deep secure encoding: an application to face recognition. arxiv.org/pdf/1506.04340.pdf. Accessed 16 May 2020
37. Patel MI, Thakar VK, Shah SK (2016) Image registeration of satellite images with varying illumination level using HOG descriptor based SURF. Procedia Computer Science 93(2016):382–388. https://doi.org/10.1016/j.procs.2016.07.224
38. Rahman MA, Singh P, Muniyandi RC, Mery D, Prasad M (2019) Prostate cancer classification based on best first search and taguchi feature selection method. In: Lee C, Su Z, Sugimoto A (eds) Image and video technology, Lecture Notes in Computer Science. Springer, Cham, pp 325–336
39. Raj R, Joseph N (2016) Keypoint extraction using SURF algorithm for CMFD. Procedia Computer Science 93(2016):375–381. https://doi.org/10.1016/j.procs.2016.07.223
40. Ratha NK, Chikkerur S, Connell JH, Bolle RM (2007) Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intell 29(4):561–572. https://doi.org/10.1109/TPAMI.2007.1004
41. Urbanowicza RJ, Olsona RS, Schmitta P, Meekerb M, Moorea JH (2018) Benchmarking relief-based feature selection methods for bioinformatics data mining. J Biomed Inform 85(2018):168–188. https://doi.org/10.1016/j.jbi.2018.07.015
42. Verma G, Liao M, Lu D, He W, Peng X (2019) A novel optical two-factor face authentication scheme. Opt Lasers Eng 123(2019):28–36. https://doi.org/10.1016/j.optlaseng.2019.06.028
43. Wang Y, Plataniotis KN (2007). Face based biometric authentication with changeable and privacy preservable templates. 2007 IEEE international symposium on biometrics, pp. 1-6. https://doi.org/10.1109/BCC.2007.4430530
44. Wang S, Yang W, Hu J (2017) Design of alignment-free cancelable fingerprint templates with zoned minutia pairs. Pattern Recogn 66(2017):295–301. https://doi.org/10.1016/j.patcog.2017.01.019
45. Yagnik J, Strelow D, Ross DA, Lin RS (2011) The power of comparative reasoning. Proceedings of 2011 IEEE international conference on computer vision, pp 2431-2438
46. Yale University Computer Laboratory http://vision.ucsd.edu/content/extended-yale-face-database-b-b

47. Yang W, Wang S, Hu J, Zheng G, Valli C (2018) A fingerprint and finger-vein based cancelable multi-biometric system. Pattern Recogn 78(2018):242–251. https://doi.org/10.1016/j.patcog.2018.01.026
48. Zhang H, Bai J, Li Z, Liu Y, Liu K (2017) Scale invariant SURF detector and automatic clustering segmentation for infrared small targets detection. Infrared Phys Technol 83(2017):7–16. https://doi.org/10.1016/j.infrared.2017.04.001
49. Zhao D, Yang Y, Ji Z, Xiaopeng H (2014) Rapid multimodality registration based on MM-SURF. Neurocomputing 131(2014):87–97. https://doi.org/10.1016/j.neucom.2013.10.037