CONVOLUTIONAL NEURAL NETWORK ALGORITHM FOR CANCELLABLE FACE TEMPLATE

Hiba Basim ALWAN[1], Ku Ruhana KU-MAHAMUD[2]

Biometrics systems utilizing hand geometry, fingerprint, iris, face, palm print, voice, gesture, and palm print have been utilised for authentication purposes. Through these templates, the face template is suggested as the strongest. However, problems still exist in face-matching implementation which affects biometric security. Thus, in this paper, a new cancellable face image algorithm using the Convolution Neural Network (CNN) feature extraction technique and Winner-Takes-All hashing method is proposed. The algorithm is to overcome the problem of matching which will enhance its security. ORL and Yale datasets were utilized in the evaluation of the proposed algorithm. Several common algorithms were utilised in the comparison based on Equal Error Ratio (ERR) measurement. The outcomes displayed the verification performance of the unimportant differences with EER = 0.95% and 3.25% for the extended version of the face dataset for the Yale and ORL face datasets, respectively. The acceptable implementation of the proposed algorithm demonstrates that it can be used for the security purpose of biometric trait tasks.

Keywords: Convolutional neural network; ResNet-50; Cancellable biometric; Winner-takes-all hashing

1. Introduction

Machine Learning (ML) is also related to the utilization of data and algorithms to mimic the manner of humans to learn, expect or classify. Precision in prediction can be enhanced because of its capability to mine, translate, and analyse huge data. ML approaches have been implemented in different areas involving biometrics and image processing. Matching is the basis of every biometric approach which is classified as one-to-one verification and one-to-many identification processes. ML approaches have proved to enhance the execution of biometrics systems; however, their full possibility in assisting biometrics to accomplish 100% execution has not been investigated satisfactorily [1]. Convolution Neural Network (CNN) and Deep Learning (DL) are among the ML approaches that have been extensively utilised to extract/select worthy information from data [2].

[1] PhD Eng., Dept. of Computer Science, University of Technology, Iraq, e-mail: 110154@uotechnology.edu.iq
[2] Prof., School of Computing, Universiti Utara Malaysia, Malaysia, e-mail: ruhana@uum.edu.my

Deep learning has been extensively utilised for feature extraction/selection, segmentation and classification with suitable execution and detection [3]. The fundamental of DL is a learning procedure that utilises deep neural networks to resolve the difficulties of feature depiction/illustration. DL contains several layers and has been utilised in several biometrics uses. DL approaches show the capability to generate strong and dependable verification prototypes that outperform standard methods like support vector machine and neural networks [1]. CNN is a type of network structural design for DL algorithms and is particularly utilised for image recognition, classification, and image processing. CNN includes convolutional layers of network, which implies its name. Within layers of convolution, it generates a pyramid of spatial features. Initially, CNN have produced significant achievements when employed with image. The layers in CNN are input, dimensionality decreasing, which is typically performed after the convolutional layers, and output layers [4].

The biometric system is a pattern recognition system that needs biometric information from persons built on their behavioural and (or) physical characters like iris, fingerprint, voice, electrocardiogram or face pattern. In contrast to classical approaches like token and passwords, biometrics cannot be shared, forgotten, copied, lost, or manipulated. Biometrics are not limited to criminal law implementation, several businesses also utilise biometrics to regulate entry to information systems and buildings [5, 6].

Biometric verification systems include the enrolment and identification stages. Through the enrolment stage, the biometric feature is present as input to the system to create the biometric pattern which is kept in the record beside other people's data. Through the identification stage, the biometric data of the person is present as input to the system to create the biometric pattern which is compared to the kept pattern in the record. The comparison procedure counts on statistical approaches and is not 100% precise. Several biometric information sources give various levels of precision. The face-established verification system is assumed to be extra precise as matched to other biometric systems [7].

The existing biometric pattern protection approaches can be classified into biometric cryptosystems, watermarking and cancellable pattern [6]. Biometric cryptosystems mix cryptography and biometrics to benefit from the powers of both areas. The information kept is independent of initial patterns and does not expose any data about the initial biometric pattern. The watermarking approach is difficult for a hacker to build as the watermarking data must be recognised by the hacker. In the cancellable pattern approach, the biometric characteristics obtained are planned to a pre-known multidimensional array that plans the character vector. By crossing the array, a binary chain is created and is then transformed. This approach is further protected and matched to the approaches reviewed above.

Cancellable biometrics is presented to create a confident and personal system which allows the renewal of the initial biometric characteristics. Biometric non-invertible and salting approaches are the two methods used to design cancellable biometrics. A transformation that will be non-invertible is a personal-saving biometric verification approach through utilizing a single-path transformation to hide the initial biometric. Alternatively, biometric salting uses the external feature to obtain a transformation array that can be utilised to fuse with biometric patterns. Cancellable biometrics is developed to hide the individual's real template by utilising a calculatedly converted pattern that should fulfil the non-invertibility, unlinkability, performance, and revocability criteria [8]. In unlinkability, the infeasibility of discriminating is related to whether several transformed examples are obtained from the same trait. This criterion avoids cross-matching among several databases while the revocability means the elimination of the transformation and re-release of another one if it has been compromised. The single-path transformation of the pattern to avoid calculation recovery of trait information is the non-invertibility criterion. Finally, the performance means the identification precision of the cancellable patterns must be kept or enhanced when matched to their unsecured counterparts.

In this paper, a new cancellable algorithm involving CNN has been proposed to satisfy most of the above criteria. The proposed algorithm is centred on face biometric representation where the random binary orthogonal matrices, permutation feature, ResNet-50 CNN and winner-takes-all (WTA) non-invertible transformation techniques are fused. The benefit of fusing is to improve the strength of the proposed algorithm for face attacks. The ResNet-50 CNN is considered as one of the most excellent feature extraction techniques. This technique is used in the proposed algorithm to make it more robust and to accelerate the process of extracting/selecting features. The permutation technique is used to permute the selected features to boost the robustness of the proposed algorithm. An arbitrary generated binary orthogonal array that stores the permutated features is used in the projection process to increase robustness. Finally, the WTA technique is used as a non-invertible transformation technique. The prime factorisation characteristics are used to improve privacy and security, particularly for the many-to-one task. The outline of this paper is as follows: Section 2 presents the literature review. The proposed algorithm is described in Section 3 while Section 4 presents the results of the experiment. The conclusion and suggestions for future works are demonstrated in Section 5.

2. Biometric approaches

A token less cancellable biometric approach named Multimodal Extended Feature Vector (MFEV) hashing that utilizes an enhanced XOR

encoding/decoding method to implement on the transformed parameter has been proposed in [5]. The actual value fingerprint and face vectors are mixed and inserted into a binarized cancellable pattern. The approach includes three steps of transformation. The first step is normalisation and biometric fixing. The second step is arbitrary and binarization. Finally, the third step is cancellable pattern creation. Many datasets for fingerprint and face have been used to assess the approach. The authentication implementation was proven through embedding FVC comparison method. Several attacks were mimicked and examined to illustrate the robustness of the proposed approach. The experiment results show a good result for the proposed approach. The proposed approach needs to be examined on a wide-ranging biometric verification to test the protection and effectiveness of the cancellable indexing and its application accuracy.

A new algorithm based on a deep learning and cancellable biometric approach for face verification has been reported in [6]. The deep rank hashing network is used for cancellable face identification. In this paper, the authors used one-to-several comparison approaches to verify the face which include two elements; the Deep Rank Hashing (DRH) network and cancellable verification. The DRH net converts an original face photograph to recognisable, compressed face hash codes built on the nonlinear subspace rank concept. The DRH net is trained for both verification and hashing aims. An enhanced softmax function is used to improve the hashing quantisation mistake and a regularisation concept is generated to assist hash code stability. The hash code is binarized, compacted, and protected with the randomised lookup table operation. The algorithm requires only the face photograph for verification. The face pattern is replaceable when required built on a one-time XOR code concept. The proposed algorithm is examined on different benchmark datasets and the experiment illustrates a good result. The proposed algorithm is required to improve the training competence and generalisation execution.

A new cancellable face identification algorithm depends on face photograph coding and fractional order Lorenz chaotic system was developed by [7]. The basic concept of the algorithm is to create certain arbitrary person elements to be XORed with RGB elements of colour face photograph. These elements are created through the fractional order Lorenz chaotic system. In this proposed algorithm, a rotation and transposition operation are performed as a post-processing step on the encoded colour elements of the face photo. To create a single cancellable pattern for every colour face photo, a wavelet mix operation is implemented directly after the post-processing step on the encoded and processed face photo elements. This acts as the guide to improve the diffusion in the encoded face pattern. The experiment results showed that the EER ratio is near to zero. The proposed algorithm needs to be applied with other fractional-order chaotic systems to obtain full encrypted faces because the proposed algorithm

obtained partially encrypted faces. Also, the non-linearity of the proposed algorithm requires improvement to provide a better algorithm.

A feature-adaptive random projection-based method had been proposed in [8]. The main idea of the method focuses on the projection arrays which were created from the single main array with a combination of local characteristic slots. The created projection arrays are deleted after utilisation, which means it would hard for the attacker to make their attack. The algorithm can simplify the undesirable effect of biometric uncertainty on identification precision because it bounds the mistakes to portions of the transformed characteristics vector instead of the whole vector. The experiment results illustrate the authority of the proposed algorithm. The proposed method requires a long time to be trained and tested because it uses a huge number of features to be optimized. The proposed method needs to be examined on bigger datasets.

An encoding method has been proposed in [9] to create a cancellable face pattern built on quantum image Hilbert permutation. This method aims to supply the necessary distortion of the person's face biometrics to be kept in a database for verification necessities via encoding. The power of the method is to ensure, via the capability, creation of cancellable face patterns through implementing the mixing process of the face biometric after adding a noise mask alongside pre-identified alterations of an initial seed. The method includes three steps: initialization, even and odd modules. Results show that this method provides high identification rates count on area under the receiver operating characteristic curve.

A summary of recent (2021 and 2022) face biometric methods is presented in Table 1.

Table 1

Biometric approaches

Studies	Method used	Biometric trait
[5]	Multimodal extended feature vector hashing	Face and Fingerprint
[6]	Deep rank hashing network	Face
[7]	Fractional order Lorenz chaotic system	Face
[8]	Feature adaptive random projection	Face
[9]	Quantum image Hilbert permutation	Face

3. The proposed algorithm

Any biometric identification algorithm involves two phases, enrolment and identification, as illustrated in Fig. 1.

In the enrolment phase of the proposed algorithm, the biometric trait will be enrolled by the individual and the important features will be extracted by ResNet-50 and kept in the database. The selected features will be permuted to increase the robustness of the proposed algorithm and projected with binary orthogonal matrices that are randomly generated. Then WTA will be applied to

generate a non-invertible transformation and the trait will be transformed and become a cancellable trait. The verification phase is the same as the enrolment phase except that the biometric trait is queried from the individual rather than being provided by him/her.

After the enrolment and verification phases have been completed, a matching process is made between the cancellable traits from the enrolment and verification phases. If the result of matching is one, this implies that the individual from the enrolment and verification phases is the same. However, if the result of matching is zero, the enrolment and verification phases comprise two different individuals.

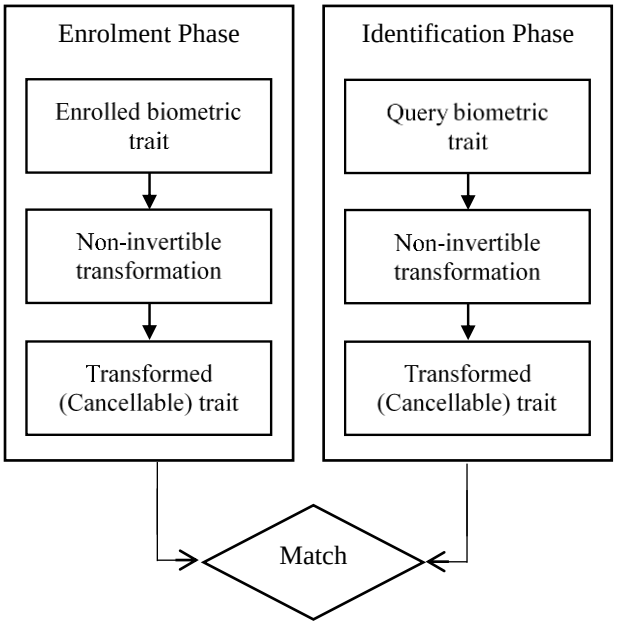

Fig. 1. Biometric identification algorithm

Useful features are extracted and selected in the enrolment phase to differentiate between various individuals. To extract/select features, ResNet-50 has been used. ResNet is considered as a new kind of CNN. In order to accelerate the performance speed, ResNet presents the residual component into the DNN and cancels the repeated network construction. This will also remove the gradient problems and degradation of classical CNN. The inside residual component in ResNet adopts the shortest linking to directly transfer the x-input which is the initial result to output, and this guarantees the integrity of the data [10]. The ResNet-50 is an alternative to the ResNet structure with 50 deep layers. The ResNet-50 structure includes a series of convolution blocks besides average pooling. Softmax is utilised to be the final classification layer. ResNet-50 involves five convolutional layers [11].

The extracted features are permutated to increase the robustness of the non-invertible characteristic of the algorithm. Subsequently, this non-invertible characteristic will make the process of obtaining the initial characteristic of the secured pattern very difficult to the attacker. Every selected feature will be permuted and projected with an arbitrary binary orthogonal array. After the projection process is made, a number of feature items will be selected based on the user specific number called window size. The position of the maximum selected features' items will be recorded, and the prime factorisation will be computed.

The WTA hash is an approach implemented to accelerate the matching and seeking process. WTA utilises a grade relationship scale to preserve the biggest value address of the biometric characteristic. This is performed after the arbitrary transformations. Various position vectors can be created by countless transformation orders [12]. Every WTA hash procedure introduces ordinal insertion as well as a related grade relationship matching measure. This provides a quantity of invariance regarding perturbations in numeric values, in addition to the fact that it is acceptable when investigating as a foundation for locality sensitive hashing. These deterministic procedures are nonlinear and generate sparse identifiers that have been illustrated to guide necessary enhancements through utilising easy linear classifiers that can be trained immediately. Intuitively, the data kept in a WTA hash permit a single aspect to rebuild a fractional sequence of the factors in the hashed vector [13].

The hash algorithm to address the position vector of WTA is as follows [12, 14]:

Algorithm 1: WTA Hash

1 Random Permutation: Compute a permuted feature vector X^p by subjecting feature vector X to the random permutation process.

2 Reduce the characteristics vector length by choosing the first K-items from the permuted feature vector X^p obtained at stage 1. The selected values are usually between the range of $2 \leq K \leq n-1$. However, this usually results in information loss.

3 The index of the K-item with the highest value is determined and recorded as C.

4 Steps (1) through (3) are repeated by applying different H permutation arrangements. A sequence of C_i determined indices are created.

where $i's \in [1, H]$. S is the set containing the created C_i (i.e., $S = \{C_1, C_2, \ldots, C_H\}$). For each image, the ResNet-50 CNN will select important features then multiply by the initial created binary orthogonal array. The numbers of initial created characteristic elements are then chosen. This number is specified by the user. As an example, the first three elements are chosen. The index of the largest

number is determined and an arbitrary number is created to compute the prime factorisation. If a created arbitrary non-negative number is 30, the permutated feature is equal to 90. The advantage of utilising such an arbitrary non-negative number is to improve the strength of the suggested algorithm, which enables the pattern to stay in one piece. Lastly, the final number of prime numbers (equal to 4) is designated as the first digit of the hashed code. The remaining digits of the hashed code is gained from the successive loops of execution of the proposed algorithm.

4. Experimental results and analysis

The ORL [15] and the Yale [16] face datasets were utilised to examine the performance of the suggested algorithm. These are publicly available datasets meant for research purposes. The face images in these datasets are of varied quality with huge margins in most cases. The quality varies from good to poor in most cases. A description of each dataset is presented in Table 2.

Table 2

Features of the datasets

Feature	ORL dataset	Yale dataset
No. of individual	40	38
No. of images	400	16128
No. of images/individual	10	64
Resolution	256 grey levels per pixel	
Image size	92 × 112	168 × 192
Date	April 1992 & April 1994	
Place images taken	ORL in Cambridge, UK	Yale, USA
Time images taken	Different time	
Lighting quality	Light changing	64 illumination situations
Facial expressions	Slight open and closed eyes, smiling and non-smiling	
Facial specifies of facial	Glasses and no glasses	
Background	Dark homogeneous background	
Positions	Up-right, frontal position	9
Subject		10

The ORL and Yale dataset B are face datasets developed by ORL in Cambridge UK, and Yale University, respectively. These datasets contain the images of 40 and 38 persons with 10 and 64 images for each person, respectively. The ORL image size was 92 by 112 while the size was 168 by 192 for Yale dataset B. Both datasets images were grey imaging with two positions for the ORL dataset and nine positions for Yale dataset B.

Every user first image was utilised as the pattern while the rest of the images of the user were used to calculate the False Rejection Rate (FRR). The False Acceptance Rate (FAR) is calculated by using the first image of each user as

the template, whereas the rest of the images from the remaining users were used as the query. Therefore, for the ORL dataset, there are 1,800 genuine matching examinations and 78,000 imposter matching examinations because each user had ten images. Meanwhile, for the extended Yale B dataset, there are 76,608 genuine matching examinations and 2,879,488 imposter matching examinations because each user had 64 images. The similarity score was calculated using the following formula, which was exactly the same as that used in [12]:

$$Similarity\ score = \frac{number\ of\ zeros}{length\ of\ hashed\ code} \tag{1}$$

The similarity score results were in values with the range of zero to one. A higher similarity grade of the query characteristic vector with the feature vectors saved during the enrolment phase indicated close similarity among the two versions of feature vectors [17]. The similarity computation procedure could be described in three major steps: Computation of the difference between the stored hashed code (S_x) that was captured during enrolment and the query hash (S_x') code took place in the first stage, i.e., S_x - S_x'. If the resulting value evaluated to zero, it is an indication that there is a similarity among the supplied hashed code values from the query pattern vector and the kept hashed code in the template. Counting the number of zeroes was the process that took place at the second stage of the similarity score computation. Lastly, the similarity count was then calculated depending on the total count of resulting zeroes obtained from stage two. This process was executed over the total length of the hashed code as shown in [14].

The FAR, FRR, and EER rates were utilised as the performance measurements and were calculated using the following formulae [18]:

$$FAR = \frac{number\ of\ impostors\ that\ have\ been\ authenticated}{number\ of\ impostor\ users} \tag{2}$$

$$FRR = \frac{number\ of\ users\ that\ have\ been\ correctly\ authenticated}{number\ of\ genuine\ users} \tag{3}$$

$$EER = \frac{FAR+FRR}{2} \tag{4}$$

In the face pattern security studies, the number of face examples utilised in the experiments varied. No regular experimental procedure was utilised in the current face pattern security methods. Therefore, it was difficult to compare them reasonably. Nevertheless, it was important to demonstrate the implementation result of the suggested algorithm and standard algorithms for benchmarking purposes. The results are presented in Table 3. There are two and three different algorithms that were proposed in [24] and [25] respectively. The symbol 'N/A' indicates that no experiment was performed on the respective datasets. The result showed that the execution of the suggested algorithm was better than the

performance of other algorithms for the ORL and the Yale face datasets. The suggested algorithm was able to preserve the verification task concerning unimportant differences of EER = 0.95% and 3.25% for the extended version of the Yale face dataset B and ORL face datasets, respectively. This is because of the benefits of ResNet-50 which includes good architecture, robust learning capability, the ability to take complex characteristics, and the ability to avoid over fitting.

Table 3

EER results for the proposed algorithm and state of the arts algorithms

Algorithm	EER %	
	ORL	**Yale**
Proposed algorithm	**3.25**	**0.95**
[19]	N/A	1.06
[20]	4.99	1.17
[21]	5.42	11.7
[22]	12.44	32.5
[23]	7.12	9.95
[24]	N/A	5.45
[24]	N/A	12.13
[25]	N/A	1.19
[25]	N/A	1.36
[25]	N/A	1.77
[26]	6.75	N/A

6. Conclusions and future work

A cancellable face image model protection algorithm utilising a CNN method has been presented in this paper. The proposed algorithm is the first algorithm that uses the combination of facial features and CNN for cancellable face biometrics. The proposed algorithm protects the biometric feature through utilising binary orthogonal arrays, which will prompt a robust non-invertible characteristic.

It was also proven that using the proposed algorithm, the user does not need to preserve the binary orthogonal array or arbitrary token in private. The proposed algorithm has the benefit of the WTA and is capable of accomplishing a robust non-invertible characteristic with the addition of user-specific arbitrary token, prime factorisation, and non-invertible function. As cancellable biometrics is a developed field, new ways to extract features from face image traits will be examined in the future. Moreover, it is necessary to propose efficient non-invertible transformation procedures for cancellable biometric methods.

REFERENCES

[1] Lina Chato and Shahram Latifi. Application of machine learning to biometric systems-A survey, Journal of physics: Conference Series 1098, 2018, https://doi.org/10.1088/1742-6596/1098/1/012017.

[2] Xindi Yu, Shusen Zhou, Hailin Zou, Qingjun Wang, Chanjuan Liu, Mujun Zang, Tong Liu. Survey of deep learning techniques for disease prediction based on omics data, Human Gene, vol 35, 2023, https://doi.org/10.1016/j.humgen.2022.201140.

[3] Solemane Coulibaly, Bernard Kamsu-Foguem, Dantouma Kamissoko, Daouda Traore. Deep Convolution Neural Network sharing for the multi-label images classification, Machine Learning with Applications, vol 10, 2022.

[4] Fabio R. Llorella, Eduardo Iáñez, José M. Azorín, Gustavo Patow, Classification of imagined geometric shapes using EEG signals and convolutional neural networks, Neuroscience Informatics, vol 1, 2021, https://doi.org/10.1016/j.neuri.2021.100029.

[5] Lee Jie Ming, Teoh Jin Beng Andrew, Uhl Andreas, Liang Shiuan-Ni, A Tokenless Cancellable Schema for Multimodal Biometric Systems, Computers & Security, vol 108, 2021.

[6] Ilaiah Kavati, A. Mallikarjuna Reddy, E. Suresh Babu, K. Sudheer Reddyc, Ramalinga Swamy Cheruku, Design of a fingerprint template protection scheme using elliptical structures, ICT Express, vol 7, 2021, https://doi.org/10.1016/j.icte.2021.04.001.

[7] Firdous Kausar, Iris based cancelable biometric cryptosystem for secure healthcare smart card, Egyptian Informatics Journal, vol 22, 2021, https://doi.org/10.1016/j.eij.2021.01.004.

[8] Ahmed S. Sakr, Paweł Pławiak, Ryszard Tadeusiewicz, Mohamed Hammad, Cancelable ECG biometric based on combination of deep transfer learning with DNA and amino acid approaches for human authentication, Information Sciences, vol 585, 2022, https://doi.org/10.1016/j.ins.2021.11.066.

[9] Hesham Alhumyani, Ghada M. El-Banby, Hala S. El-Sayed, Fathi E. Abd El-Samieand Osama S. Faragallah, Efficient Generation of Cancelable Face Templates Based on Quantum Image Hilbert Permutation, Electronics, vol 11, 2022, https://doi.org/10.3390/electronics11071040.

[10] Ziyun Yan, Honggao Liu, Tao Li, Jieqing Li, Yuanzhong Wang, Two dimensional correlation spectroscopy combined with ResNet: Efficient method to identify bolete species compared to traditional machine learning, LWT - Food Science and Technology, vol 162, 2022, https://doi.org/10.1016/j.lwt.2022.113490.

[11] A. Victor Ikechukwu, S. Murali, R. Deepu, R.C. Shivamurthy, ResNet-50 vs VGG-19 vs training from scratch: A comparative analysis of the segmentation and classification of Pneumonia from chest X-ray images, Global Transitions Proceedings, vol 2, 2021, https://doi.org/10.1016/j.gltp.2021.08.027.

[12] Chee, K. Y., Jin, Z., Cai, D., Li, M., Yap, W. S., Lai, Y. L.: Cancelable speech template via random binary orthogonal matrices projection hashing. Pattern Recognition 76(2018) 273-287.

[13] Dean, T., Ruzon, M. A., Segal, M., Shlens, J., Vijayanarasimhan, S., Yagnik, J.: Fast, accurate detection of 100000 object classes on a single machine. In: Computer Vision and Pattern Recognition Conference. IEEE. 1814-1821 (2013).

[14] Yagnik, J., Strelow, D., Ross, D. A., Lin, R. S.: The power of comparative reasoning. In: Computer Vision Conference. IEEE. 2431-2438 (2017).

[15] C.U.C. Laboratory, Cambridge University Computer Laboratory. http://www.cl.cam.ac.uk/research/dtg/attarchive/facedataset.html. (access 1 July 2018).

[16] Yale Laboratory, Yale University Computer Laboratory. http://vision.ucsd.edu/content/extended-yale-face-dataset-b-b. (access 1 July 2018).

[17] Yang, W., Wang, S., Hu, J., Zheng, G., Valli, C.: A fingerprint and finger-vein based cancelable multi-biometric system. Pattern Recognition 78(2018), 242-251 (2018).

[18] Cherifi, F., Hemery, B., Giot, R., Pasquet, M., Rosenberger, C.: Performance evaluation of behavioral biometric systems, behavioral biometrics for human identification: Intelligent applications. IGI Global Disseminator of Knowledge. 1-22 (2010).

[19] Wang, S., Yang, W., Hu, J.: Design of alignment-free cancelable fingerprint templates with zoned minutia pairs. Pattern Recognition. 66(2017) 295-301.

[20] Alwan, H. B., Ku-Mahamud, K. R.: Cancellable face template algorithm based on speeded-up robust features and winner-takes-all. Multimedia Tools Applications. 79(39) 28675-28693 (2020).

[21] Kaur, H., Khanna, P.: Non-invertible biometric encryption to generate cancelable biometric templates. In: Engineering and Computer Science (WCECS 2017) World Congress. 1-4 (2017).

[22] Kaur, H., Khanna, P.: Gaussian random projection based non-invertible cancelable biometric templates. Computer Science. 54(2015) 661-670.

[23] Urbanowicza, R. J., Olsona, R. S., Schmitta, P., Meekerb, M., Moorea, J. H.: Benchmarking relief-based feature selection methods for bioinformatics data mining. J Biomed Inform. 85(2018) 168–188.

[24] Wang, Y., Plataniotis, K. N.: Face based biometric authentication with changeable and privacy preservable templates. In: Biometrics International Symposium. IEEE. 1-6 (2007).

[25] Hebbar, V. A. D., Shekhar, V. S., Murthy, K. N. B., Natarajan, S.: Two novel detector-descriptor based approaches for face recognition using SIFT and SURF. Procedia Computer Science. 70(2015) 185–197.

[26] Verma, G., Liao, M., Lu, D., He, W., Peng, X.: A novel optical two-factor face authentication scheme. Opt Lasers Eng, 123(2019) 28–36.