International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 12, No.1 (Dec-2022)

https://dx.doi.org/10.12785/ijcds/1201110

Multimodal Biometric Watermarking-based Transfer Learning Authentication

Sanaa Ghouzali

Department of Information Technology, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia

Received 7 Nov. 2021, Revised 1 Dec. 2022, Accepted 4 Dec. 2022, Published 8 Dec. 2022

Abstract: Though biometric-based authentication systems have inherent advantages over conventional authentication systems, which use passwords and ID cards, these systems cannot ensure the security and privacy of biometric data stored in their databases. Recently, several watermarking-based algorithms have been efficiently used to protect biometric templates. However, these methods also require storing the watermarked biometrics for the matching purpose of the query during the authentication phase. The paper aims to develop an approach for authenticating watermarked biometrics using transfer learning without the need to store biometric data. Benchmark face and fingerprint databases are employed to conduct the experimentation. The obtained results validated the proposed approach's ability to discriminate between different users with a performance accuracy rate achieving 99.17% while protecting the user's biometrics.

Keywords: Watermarking, Biometrics, Multimodal, Deep learning, Transfer learning

1. Introduction

Virtual communications are exponentially growing, both in volume and diversity; Henceforth, the threats of identity theft, financial fraud, and cybercrime are giving rise to international concerns about security. Secure and reliable identification and authentication systems are of a high importance in various fields such as banking transactions and public services. However, traditional personal authentication systems which are based on passwords or tokens are vulnerable to multiple attacks. By contrast, biometrics-based authentication systems which employ the physiological characteristics (iris, face, etc.) or the behavioral characteristics (gait, voice, etc.) have proved their priority compared to the traditional systems because biometrics cannot be stolen or guessed. The aim of a biometric system is to simulate the human recognition system by the machine and to automate applications such as remote monitoring and access control. A typical and simple biometric authentication system employs single biometric modality, called unimodal biometric systems. However, these systems have several drawbacks such as accuracy, non- universality, reliability and security (vulnerability to spoofing attacks). Multimodal biometric authentication systems which employ more than one biometric modality have been shown to effectively overcome these drawbacks.

Yet while biometrics provide secure authentication in a multitude of applications, they also suffer from different vulnerabilities. Among the main issues of biometrics authentication systems is the irrevocability of the biometric templates [1]. In traditional authentication systems, if a password is compromised, it is easy to create a new password and dismiss the former to the database by creating a revocation list. But if a biometric template is compromised, the model cannot be easily changed because the biometric features are unique. Henceforth, care is needed to safeguard the biometric templates storage in the system's database. In the literature, two major categories of methods have been proposed for biometric template protection [2]: Transformation methods and biometric cryptosystems.

Digital watermarking approaches are considered among the prominent biometric templates' protection approaches that have been effectively and widely employed in literature [3]. However, when developing a biometric information hiding approach, attention should be given to feature discriminability of the biometric host data rather than visual quality and the size of the generated biometric watermark concerning the limited capacity [4]. Various approaches exist in the literature to protect the biometric features using watermarking schemes (e.g., [5]–[14]). Furthermore, multimodal biometric watermarking approaches have offered a high level of security since the embedded biometric data would only be retrieved by a secret key. However, previous multimodal biometric watermarking works in literature usually relied on a multi-factor authentication technique by

E-mail address: sghouzali@ksu.edu.sa

matching the raw biometrics after extracting the watermark, which requires more processing. Additionally, specialized feature extraction methods are required to extract pertinent features from the raw biometrics data depending on the biometric modality. These methods can be very complex and do not always provide the most important set of features to achieve higher classification rates.

Recently, deep learning has shown effectiveness in extracting pertinent features for biometrics recognition technology [15]–[25]. When using the deep learning approach, the features are extracted automatically from the images contrary to most common biometrics matching methods. Nonetheless, deep learning is very time-consuming and computationally expensive [15]. Several studies showed that using pre-trained models, while originally trained for classifying generic objects, can effectively extract discriminative image characteristics and achieve promising results for the biometrics recognition (e.g., [20]–[23]).

In this paper, a novel transfer learning-based authentication of watermarked biometrics is presented. The proposed scheme employs fingerprint and face biometric modalities aiming to protect the authentication system while providing a high performance. The user's fingerprint and face biometrics are first captured before using the watermarking algorithm which employs the Dual-Tree Complex Wavelet Transform (DTCWT) and the Discrete Cosine Transform (DCT) to entrench the fingerprint features within the face image, resulting in a multi-biometric fusion scheme. The essential concept of the watermarking technique is that the inserted watermark data are held interconnected to the host image and therefore no supplementary transmission or storage means are required. Subsequently, this paper examines the effectiveness of using transfer learning from the pre-trained convolutional neural network (CNN) model for the recognition of watermarked face images. For security measure, the watermarked face images are only used in the training stage of the pre-trained CNN and then discarded along with the original raw biometrics. Henceforth, the proposed approach prevents illegal accessing or tampering with the biometric data.

The structure of the paper is given as follows. In Section 2, recent studies about watermarking-based multimodal biometrics and deep learning-based face recognition are overviewed. The key concepts of the proposed transfer learning approach for multimodal biometric watermarking-based authentication are provided in Section 3. In Section 4, the results of the experimentation are explained and discussed in detail. Section 5 provides the conclusion and future work.

2. Related Work

Previous multimodal biometric watermarking works have been proposed in the literature and have demonstrated high recognition performance.

In [5], the author implemented a multi-biometric fusion approach based on watermarking to embed fingerprint features in face images. A DCT-based watermarking technique is developed to combine the face DCT coefficients and the fingerprint minutia bit-stream. In the authentication phase, the author employed Orthogonal Locality Preserving Projection (OLPP) algorithm to extract pertinent features from the watermarked face images. In [7], the features of face and fingerprint are first fused using a watermarking approach based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). Then the watermarked face image is manipulated using a shuffling process before XORing it with a Hadamard code and a chaotic map to attain both the orthogonality and randomization of the protected biometric templates. In [8], the authors implemented a watermarking technique based on DTCWT-DCT to insert the fingerprint minutia in the face image. The watermarked face images are then kept in the storage. The authentication relies on extracting the watermark and fusing the matching scores of the biometric templates of the query.

Several works have been suggested in the literature using CNN models for face recognition and have shown promising results without requiring complex feature extraction or classification methods. In [16], a face recognition algorithm uses local binary patterns (LBP) to extract face features and subsequently feeds them to a deep CNN. The SoftMax regression method is applied for classification. The experimental results obtained using the ORL dataset validated the method's effectiveness regardless of the small training dataset. In [17], the authors used the Convolution Architecture For Feature Extraction framework (Caffe) to build a nine-layer CNN model for face recognition. In the training phase, the stochastic gradient descent algorithm is employed to extract the face features and classify them automatically. This approach has shown high recognition accuracy using ORL and AR face databases. In [22], transfer learning from AlexNet is employed to construct a face recognition model. The authors implemented another face recognition model by extracting the features using the pre-trained AlexNet and performing the classification with the support vector machine (SVM). The obtained results using ORL dataset showed similar recognition accuracy of both approaches. Another work using transfer learning for face recognition is presented in [23]. The authors used transfer learning from the pre-trained CNN model VGG-16. First, the face features are extracted and used as input to the fully-connected layer followed by the SoftMax function for the classification task. This approach yielded high accuracy on the ORL dataset compared to other methods. In [25], the training of an inception-based CNN model was achieved by independently parsing the images of each person in the training dataset. For authentication, the distance between the test image and the average of the training images of each person is calculated. The corresponding class of the person providing the closest distance is attributed to the test image, and a match is found. Experimentation conducted using the ORL face dataset has shown promising results outperforming other state-of-the-art methods.

3. Methodology

The proposed scheme uses watermarking algorithm to fuse the fingerprint features in the face image. The watermarked face images are then entered as input to the pre-trained CNN model for both extracting the feature and classifying the extracted features. This section provides the key elements of the proposed approach.

A. Watermark Embedding

In this study, the watermarking algorithm uses the Dual-Tree Complex Wavelet Transform and the Discrete Cosine Transform. This algorithm aims at minimizing the distortion of the cover (face image) when embedding the watermark (fingerprint features). The DTCWT-based watermarking algorithm is established to provide consistency with the Human visual system using directional selectivity.

The embedding of the watermark can be explained as follows. First, the watermark is generated by extracting the fingerprint minutia and selecting the most relevant features by means of the spectral minutiae representation technique. The watermark consists of a 10240-bits binary stream. Next, the host face image is decomposed using DTCWT and subsequently, three high-frequency sub-bands of the first level decomposition are randomly selected and divided into non-overlapping 4x4 blocks. The DCT is then used to transform each block, and the watermark bits are inserted using the DCT coefficients using two generated pseudorandom sequences PN_0 and PN_1 for the watermark bits 0 and 1, respectively. Lastly, both the inverse DCT and DTCWT are used to create the watermarked face image.

DTCWT-based watermarking aims to protect the watermarked images by using the real values of the selected sub-bands (i.e., high-frequency) in the process of inserting the watermark bits. Unlike imaginary values, the real values of the sub-bands comprise less-sensitive data, which helps to detect illegitimate watermark manipulation. Furthermore, the watermark is entrenched by only changing the mid-frequency DCT coefficients to avoid affecting the perceptibility of the watermarked face image and resist compression attacks.

The scheme of the watermark embedding is illustrated in Figure 1 The detailed information about this watermarking algorithm is found in [8].

B. Transfer learning-based biometrics recognition

Deep learning approaches, particularly the convolutional neural network, have shown effectiveness and better performance in biometrics recognition technology. However, building the CNN model from scratch is a lengthy process that requires a large labelled dataset and enormous computing power. Instead, transfer learning could be used to accelerate the training and solve the problem of small training datasets.

Transfer learning consists of reusing a CNN model previously trained on other large datasets for a different task, by modifying the weights and the nodes' number in the last fully-connected layers. Recently, pre-trained CNN models such as AlexNet, GoogleNet, VGG, and ResNet have been successfully and commonly used in different pattern recognition tasks (e.g., [20]–[23]). In this study, AlexNet is applied to extract suitable image features for the classification stage.

AlexNet was originally trained using ImageNet dataset which contains over a million images and thousand objects (mug, keyboard, pencil, etc.) [26]. It has a less complex architecture, compared to other pre-trained CNN models, with sufficient width and depth to ensure the generality and universality of the extracted features [27]. It has a small number of layers and a large number of parameters. AlexNet takes as an input a [2272273] image and comprises five convolutional layers, three max-pooling layers, and three fully-connected layers followed by the SoftMax function for the classification layer with 1000 output nodes corresponding to the ImageNet categories (objects).

In the proposed study, the pre-trained CNN model uses the watermarked images as input to obtain the features and perform the classification. For security measure, the watermarked face images are only used in the training stage of the pre-trained CNN and then discarded along with the original raw biometrics. Figure 2 provides an illustration of the transfer learning process.

4. EXPERIMENTS AND RESULTS

A. Experimental setting

The suggested scheme using transfer learning for multimodal biometric watermarking-based authentication is validated using benchmark face and fingerprint databases. The face images are acquired from ORL database counting for 400 images of size 92112 pixels for 40 users [28]. The fingerprint images are acquired from the FVC2002 DB1 database counting for 800 fingerprint images of size 374388 pixels for 100 users [29]. In this experiment, we used eight face images and eight fingerprints per user. The dataset of the watermarked images is gone through an augmentation process to increase the size and then randomly divided into 70% for training and 30% for validation. Both the biometric watermarking algorithm and the transfer learning authentication are implemented in MATLAB version 2020b. The computer CPU is Intel Core i9, clocked at 2.3 GHz 8-Core, and the memory size is 16 GB.

B. Results and Discussions

The different results obtained in these experiments are analyzed to assess the effectiveness of the proposed scheme. First, the fingerprint image is manipulated to generate the watermark bits which are subsequently inserted in the face images using the DTCWT-based watermarking algorithm, explained in the previous section. Figure 3 shows the histograms of an original face image and its watermarked version in order to compare the distribution of the image pixels at each gray-scale level with and without embedding

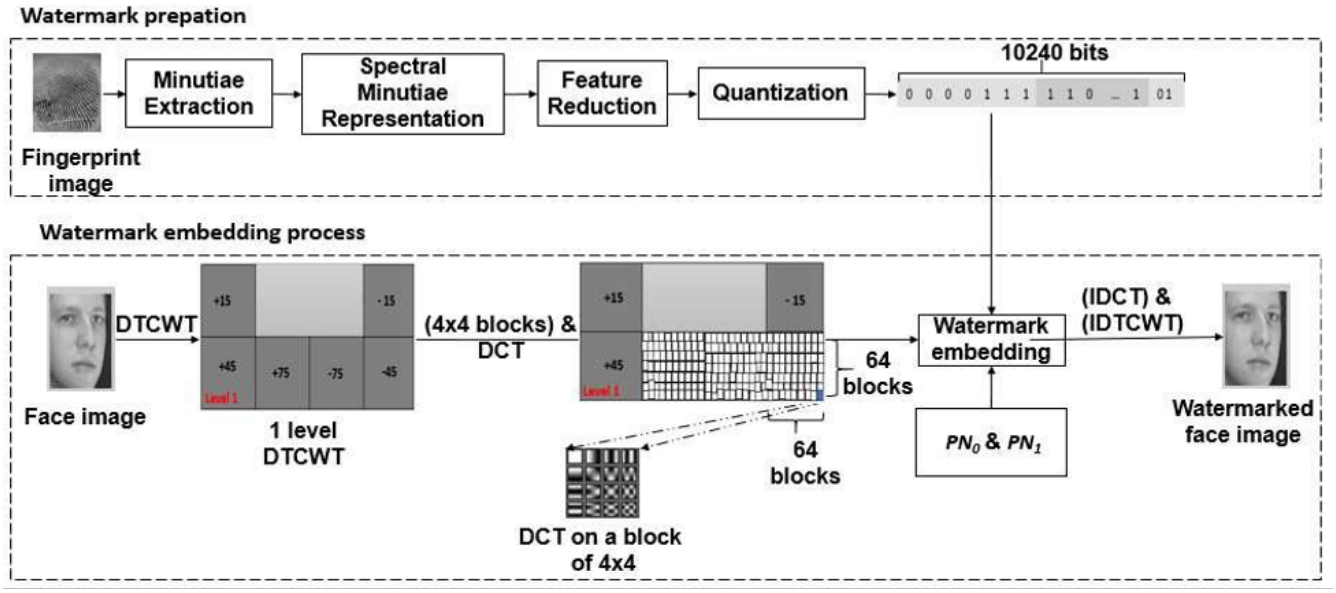

Figure 1. Watermark embedding process [8]

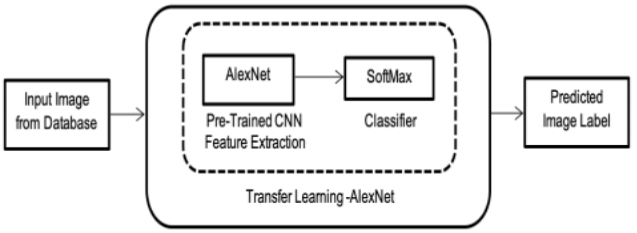

Figure 2. Transfer learning process for the authentication of the watermarked face images

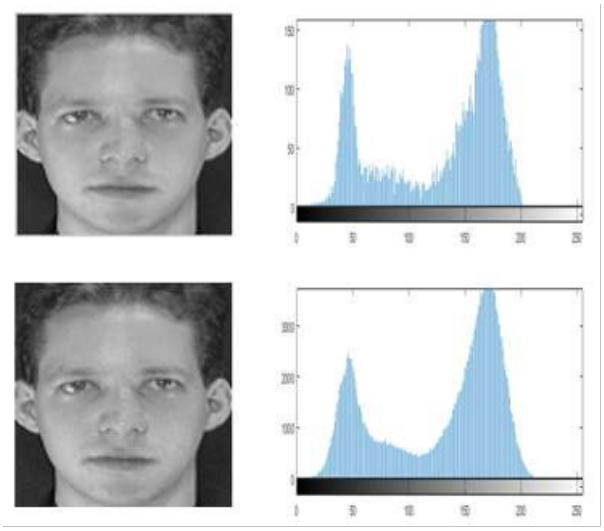

Figure 3. The histograms of an original image (above) and its corresponding watermarked image (below) [8]

the watermarking. It can be shown in the figure that the DTCWT-based watermarking algorithm did not deteriorate the perception quality of the face image. Moreover, it was demonstrated in [8] that DTCWT-based watermarking algorithm is resistant to most common image watermarking attacks including Gaussian noise, additive white noise, salt and pepper noise, median filter, and JPEG compression.

The pre-trained CNN model AlexNet is used to conduct different tests using the watermarked and the original face images. These images are gone through the preprocessing stage including image resizing. The images were resized to make them suitable for the pre-trained model AlexNet (i.e., $[227x227x3]$). Furthermore, data augmentation is performed on the training images to avoid the model from overfitting which occurs when the training dataset is small. AlexNet model is then employed to extract suitable features for the new classification task using the transfer learning.

As shown in Figure 4, AlexNet consists of 25 layers; feature extraction is achieved through the first 23 layers, whereas the feature classification is performed with the last 3 layers using the number of classes in the database. Using transfer learning in this study, only 40 nodes are included in the last fully-connected layer, which is similar to the number of users in the ORL dataset.

In this experiment, the proposed model has been tested using diverse numbers of epochs and iterations. The experiment results are shown in Figure 5 and Figure 6. The best accuracy was achieved with six epochs and 144 iterations, which shows the well convergence of the model. The mini-batch size is fixed to 10 and the validation frequency of

1	'data'	Image Input	227×227×3 images with 'zerocenter' normalization
2	'conv1'	Convolution	96 11×11×3 convolutions with stride [4 4] and padding [0 0 0 0]
3	'relu1'	ReLU	ReLU
4	'norm1'	Cross Channel Normalization	cross channel normalization with 5 channels per element
5	'pool1'	Max Pooling	3×3 max pooling with stride [2 2] and padding [0 0 0 0]
6	'conv2'	Grouped Convolution	2 groups of 128 5×5×48 convolutions with stride [1 1] and padding [2 2 2 2]
7	'relu2'	ReLU	ReLU
8	'norm2'	Cross Channel Normalization	cross channel normalization with 5 channels per element
9	'pool2'	Max Pooling	3×3 max pooling with stride [2 2] and padding [0 0 0 0]
10	'conv3'	Convolution	384 3×3×256 convolutions with stride [1 1] and padding [1 1 1 1]
11	'relu3'	ReLU	ReLU
12	'conv4'	Grouped Convolution	2 groups of 192 3×3×192 convolutions with stride [1 1] and padding [1 1 1 1]
13	'relu4'	ReLU	ReLU
14	'conv5'	Grouped Convolution	2 groups of 128 3×3×192 convolutions with stride [1 1] and padding [1 1 1 1]
15	'relu5'	ReLU	ReLU
16	'pool5'	Max Pooling	3×3 max pooling with stride [2 2] and padding [0 0 0 0]
17	'fc6'	Fully Connected	4096 fully connected layer
18	'relu6'	ReLU	ReLU
19	'drop6'	Dropout	50% dropout
20	'fc7'	Fully Connected	4096 fully connected layer
21	'relu7'	ReLU	ReLU
22	'drop7'	Dropout	50% dropout
23	''	Fully Connected	40 fully connected layer
24	''	Softmax	softmax
25	''	Classification Output	crossentropyex

Figure 4. AlexNet Architecture

the network is equal to 3 during the training. As shown in Figure 5 and Figure 6, after the training phase, the best validation accuracy attained 100% on the original face dataset and 99.17% on the watermarked face dataset.

The analysis of the model performance was conducted using the most common evaluation measures: Accuracy (A), precision (P), recall (R), and F1_score. Accuracy is the proportion of correctly classified images to the total number of images. Precision is the capacity of a classification model to correctly recognize positive instances. However, recall, also known as sensitivity, is the ability of a classification model to identify all positive instances within the whole dataset. Thus, the precision identifies the purity of the results while the recall identifies the completeness of the results. In order to find an optimal blend of these two metrics, F1_score is a useful measure, which is the weighted mean of the precision and recall. Expressions of these metrics are given as:

$$A = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$P = \frac{TP}{TP + FP} \tag{2}$$

$$R = \frac{TP}{TP + FN} \tag{3}$$

$$F1 = 2 * \frac{P * R}{P + R} \tag{4}$$

where TP is the rate of true positives, FP is the rate of false positives, TN is the rate of true negatives, and FN is the rate of false negatives.

The proposed model using transfer learning from AlexNet has shown comparable performance for the original face dataset and the watermarked face dataset, as illustrated in Table I. These results revealed that transfer learning from AlexNet is effective in the authentication of the watermarked images and does not deteriorate the recognition rate of the original images

C. Comparisons with Related Models

In Table II, we summarized the results obtained by related biometric authentication algorithms in the literature which apply watermarking and deep learning techniques. However, a valid and fair comparison of these approaches cannot take place since experiments are conducted using different biometric modalities and databases.

In [5], the authors used watermarking to entrench fingerprint features in face images. The user's watermarked face image is then authenticated using Laplacianface features extracted by OLPP method. Nevertheless, this method did not achieve high accuracy because the training dataset was very small. Other multimodal biometric watermarking works in literature such as [7], [8] have demonstrated high recognition performance. However, these methods usually rely on a multi-factor authentication technique after extracting the watermark; the authentication is attained by fusing the matching scores of the raw biometrics, which requires more processing.

Several works have been offered in the literature using CNN models for face recognition. In [16], the authors claimed the algorithm has strong generalization ability and excellent performance, regardless of using a small training dataset. In [17], the ORL face database was employed in the experimentation using 90% of the images for training and 10% for testing. This model achieved 99.82% accuracy rate. In [25], the inception-based CNN model has yielded

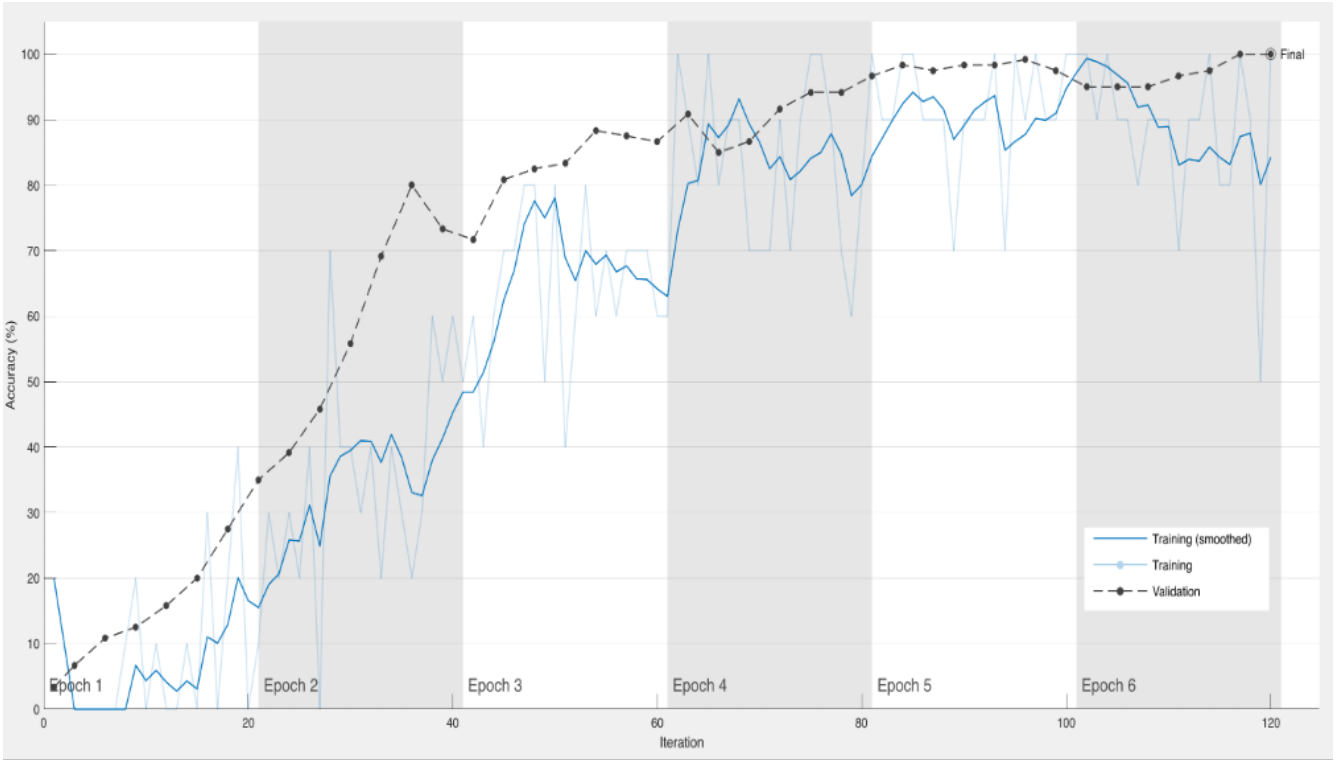

Figure 5. Accuracy for the transfer learning from AlexNet on the original face dataset

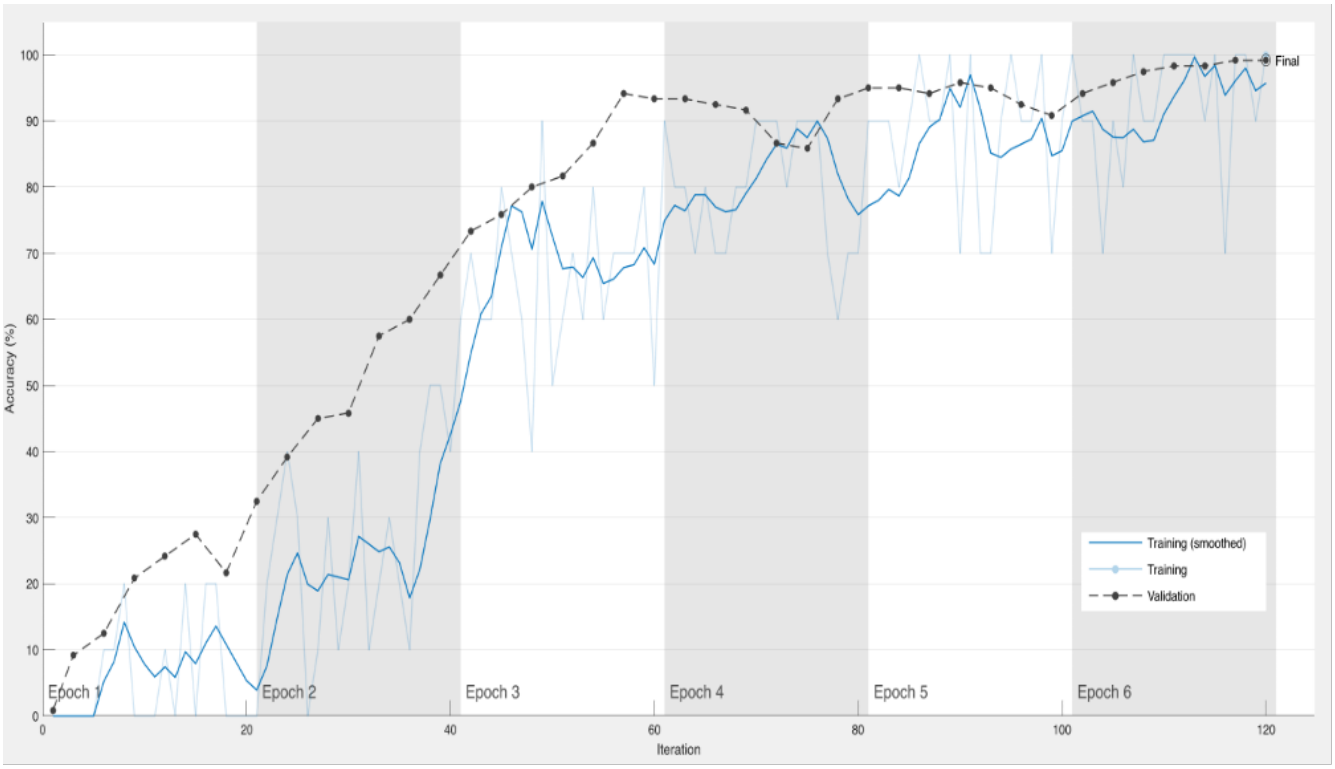

Figure 6. Accuracy of the transfer learning from AlexNet on the watermarked face dataset

TABLE I. PERFORMANCE MEASURES OF THE PROPOSED MODEL FOR THE ORIGINAL AND WATERMARKED DATASETS

	Accuracy	Precision	Recall	F1_score
Original Face Dataset	100%	100%	100%	100%
Watermarked Face Dataset	99.17%	99.17%	99.38%	99.29%

TABLE II. COMPARATIVE RESULTS OF DIFFERENT FACE/FINGERPRINT RECOGNITION MODELS

Reference	Modalities	Approach	Accuracy
[5]	Face and Fingerprint	Multi-biometric fusion using DCT-based watermarking	91%
[7]	Face and Fingerprint	DWT-SVD-based watermarking approach	100%
[8]	Face and Fingerprint	Multimodal biometric protection using DTCWT-based watermarking	100%
[16]	Face	LBP feature extraction + deep CNN	96.6%
[17]	Face	Nine-layers CNN	99.82%
[22]	Face	Transfer learning from AlexNet	99.17%
[23]	Face	Transfer learning from VGG-16	100%
[25]	Face	Inception-based CNN	98.75%
Proposed	**Face and Fingerprint**	**DTCWT-based watermarking and Transfer learning from AlexNet**	**99.17%**

an average accuracy of 98.75% on ORL face dataset. In [22], the obtained results using ORL dataset showed a recognition accuracy of 99.17%. The approach in [23] yielded 100% accuracy on ORL dataset using SoftMax function for the classification. Although these approaches have shown promising results, they require storing biometric templates in the system's database which can be a threat to user's privacy.

In this paper, the proposed approach has shown promising results compared to related works. The principal gain of this approach is the ability to accurately identify the watermarked face without referring to a stored template due to the pre-trained CNN enhanced generalizability. Thus, biometric data is protected against illegal accessing or tampering with.

5. Conclusions and Future Work

In this paper, a novel authentication approach of watermarked multimodal biometrics using transfer learning is presented. The suggested approach aims at increasing biometric authentication security without decreasing the authentication accuracy. The watermarking algorithm is used to fuse the two biometric modalities by entrenching the fingerprint features in the face image. The watermarked face images are entered into the pre-trained CNN model to generate the features for the classification task. Experiments were conducted using AlexNet with benchmark face and fingerprint databases. The obtained results revealed the efficiency of the presented approach in the authentication task without degrading the recognition performance. Moreover, the user's biometric templates are protected since they are only used in the training stage of the model and they are not required in the authentication stage. In addition, the watermark data consisting of the fingerprint features can be employed as an additional layer of defense to guarantee the legitimacy of the face image.

Future work will aim at performing extensive experimentations with various biometric databases of different modalities (palmprint, iris, etc ...) and different pre-trained CNN models such as VGG-16 and ResNet-50. Moreover, one-way functions can be used in the watermarking process to make it impossible for a watermark to be removed from previously watermarked data which might allow an imposter to gain illegal access to the system.

References

[1] "Information technology — Security techniques — Biometric information protection," International Organization for Standardization, Standard, Jun. 2011.

[2] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 1, pp. 1–17, 2008.

[3] J. Hämmerle-Uhl, K. Raab, and A. Hämmerle-Uhl, "Watermarking as a means to enhance biometric systems: A critical survey," in *Information Hiding*, T. Filler, T. Pevny, S. Craver, and A. Ker, Eds. Springer, Heidelberg, 2011.

[4] B. Ma, C. Li, Z. Zhang, and Y. Wang, "Biometric information hiding: promoting multimedia security with content and identity authentication," in *IEEE China Summit and International Conference on Signal and Information Processing*, 2013, p. 442—446.

[5] S. Ghouzali, "Watermarking based multi-biometric fusion approach," in *Codes, Cryptology, and Information Security*, ser. Lecture Notes in Computer Science, S. ElHajji, A. Nitaj, C. Carlet, and E. Souidi, Eds. Springer, Cham, 2015, vol. 9084, p. 342–351.

[6] N. Bousnina, S. Ghouzali, M. Lafkih, O. Nafea, M. Mikram, and W. Abdul, "Watermarking for protected fingerprint authentication," in *12th International Conference on Innovations in Information Technology*, Al-Ain, United Arab Emirates, 2016, p. 1–5.

[7] O. Nafea, S. Ghouzali, W. Abdul, and E. H. Qazi, "Hybrid multi-biometric template protection using watermarking," *The Computer Journal*, vol. 59, p. 1392–1407, 2016.

[8] N. Bousnina, S. Ghouzali, M. Mikram, and W. Abdul, "Dtcwt-dct watermarking method for multimodal biometric authentication," in *2nd International Conference on Networking, Information Systems and Security*, Rabat, Morocco, 2019, p. 1–7.

[9] L. R. Haddada and N. E. Ben-Amara, "Double watermarking-based biometric access control for radio frequency identification card," *International Journal of RF and Microwave Computer-Aided Engineering*, vol. 29, no. 5, p. 1–11, 2019.

[10] W. Abdul, O. Nafea, and S. Ghouzali, "Combining watermarking and hyper-chaotic map to enhance the security of stored biometric templates," *The Computer Journal*, vol. 63, p. 479–493, 2020.

[11] N. Bousnina, S. Ghouzali, M. Mikram, M. Lafkih, O. Nafea, M. S. Alrazgan, and W. Abdul, "Hybrid multimodal biometric template protection," *Intelligent Automation Soft Computing*, vol. 27, no. 1, p. 35–51, 2021.

[12] C. Vensila and A. B. Wesley, "Template protection in multimodal biometric system using watermarking approach," in *Computer Networks, Big Data and IoT*, ser. Lecture Notes on Data Engineering and Communications Technologies, A. P. Pandian, X. Fernando, and W. Haoxiang, Eds. Springer Nature Singapore, 2022, vol. 117, p. 617–631.

[13] P. Garg and A. Jain, "A robust technique for biometric image authentication using invisible watermarking," *Multimedia Tools and Applications*, 2022.

[14] R. Thabit and B. E. Khoo, "Robust reversible watermarking application for fingerprint image security," *Advances in Systems Science and Applications*, vol. 22, no. 1, pp. 117–129, 2022.

[15] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "Deepface: Closing the gap to human-level performance in face verification," in *IEEE Conference on Computer Vision and Pattern Recognition*, Columbus, OH, USA, June 2014, p. 1701–1708.

[16] M. Wang, Z. Wang, and J. Li, "Deep convolutional neural network applies to face recognition in small and medium databases," in *4th International Conference on Systems and Informatics (ICSAI)*, 2017, pp. 1368–1372.

[17] K. Yan, S. Huang, Y. Song, W. Liu, and N. Fan, "Face recognition based on convolution neural network," in *36th Chinese Control Conference (CCC)*, 2017, pp. 4077–4081.

[18] C. Militello, L. Rundo, S. Vitabile, and V. Conti, "Fingerprint classification based on deep learning approaches: Experimental findings and comparisons," *Sensors*, vol. 13, no. 5, p. 750, 2021.

[19] Y. Wang, D. Shi, and W. Zhou, "Convolutional neural network approach based on multimodal biometric system with fusion of face and finger vein features," *Symmetry*, vol. 22, no. 5, p. 6039, 2022.

[20] H. Aung, C. Pluempitiwiriyawej, K. Hamamoto, and S. Wangsiripitak, "Multimodal biometrics recognition using a deep convolutional neural network with transfer learning in surveillance videos," *Computation*, vol. 10, no. 7, p. 127, 2022.

[21] K. Nguyen, C. Fookes, A. Ross, and S. Sridharan, "Iris recognition with off-the-shelf cnn features: A deep learning perspective," *IEEE Access*, vol. 6, pp. 18 848–18 855, 2018.

[22] S. Almabdy and L. Elrefaei, "Deep convolutional neural network-based approaches for face recognition," *Applied Sciences*, vol. 9, no. 20, p. 4397, 2019.

[23] R. M. Prakash, N. Thenmoezhi, and M. Gayathri, "Face recognition with convolutional neural network and transfer learning," in *International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2019, pp. 861–864.

[24] S. Almabdy and L. Elrefaei, "Feature extraction and fusion for face recognition systems using pre-trained convolutional neural networks," *International Journal of Computing and Digital Systems*, vol. 10, no. 1, pp. 455–461, 2021.

[25] L. Patil and V. D. Mytri, "Face recognition with inception-based cnn models," in *Algorithms for Intelligent Systems*, D. Goyal, P. Chaturvedi, A. K. Nagar, and S. Purohit, Eds. Springer, 2021.

[26] J. Deng, W. Dong, R. Socher, L. Li, K. Li, and L. Fei-Fei, "Imagenet: A large-scale hierarchical image database," in *IEEE Conference on Computer Vision and Pattern Recognition*. 248–255, June 2009.

[27] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *ACM Commun.*, vol. 60, no. 6, p. 84–90, May 2017.

[28] "Orl face database." [Online]. Available: https://cam-orl.co.uk/facedatabase.html

[29] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*, 2nd ed. Springer, 2009.

Sanaa Ghouzali is an Associate Professor in the College of Computer and Information Sciences at King Saud University (Riyadh, Saudi Arabia). She received her Ph.D. degree in computer science and telecommunications from the University of Mohammed V-Agdal (Rabat, Morocco) in 2009. In 2005, she received a Fulbright grant for a joint-supervision program at Cornell University (Ithaca, NY, USA). From 2009 to 2011, she held an Assistant Professor position in ENSA (the National School of Applied Sciences, Tetuan, Morocco) before joining King Saud University in 2012. Her research interests include Pattern Recognition, Biometrics, Biometric Template Protection, Information Security.