Journal of Ambient Intelligence and Humanized Computing (2022) 13:2177–2189
https://doi.org/10.1007/s12652-021-03513-1

ORIGINAL RESEARCH

An efficient multi-biometric cancellable biometric scheme based on deep fusion and deep dream

Basma Abd El-Rahiem[1] · Mohamed Amin[1] · Ahmed Sedik[2] · Fathi E. Abd El Samie[3] · Abdullah M. Iliyasu[4,5,6]

Received: 1 October 2020 / Accepted: 13 September 2021 / Published online: 1 November 2021

Abstract
Today, biometrics are the preferred technologies for person identification, authentication, and verification cutting across different applications and industries. Sadly, this ubiquity has invigorated criminal efforts aimed at violating the integrity of these modalities. Our study presents a multi-biometric cancellable scheme (MBCS) that exploits the proven utility of deep learning models to fuse multi-exposure fingerprint, finger vein, and iris biometrics by using an Inspection V3 pre-trained model to generate an aggregate tamper-proof cancellable template. To validate our MBCS, we employed an extensive evaluation including visual, quantitative, and qualitative assessments as well as complexity analysis where average outcomes of 99.158%, 24.523 dB, 0.079, 0.909, 59.582 and 23.627 were recorded for NPCR, PSNR, SSIM, UIQ, SD and UACI respectively. These quantitative outcomes indicate that the proposed scheme compares favourably against state-of-the-art methods reported in the literature. To further improve the utility of the proposed MBCS, we are exploring its refinement to facilitate generation of cancellable templates for real-time biometric applications in person authentication at airports, banks, etc.

Keywords Multi-biometrics · Cancellable biometric system · Deep learning model · Fusion · Deep dream

1 Introduction

Human biometrics in the form of signals and images are widely used in several applications such as human recognition, identification, and authentication. Among them, the most extensively used biometrics employed in various applications are fingerprint, iris, finger vein, and facial images. Today, these traits are ubiquitous for human identification in banks, airports, hospitals, and applications ranging from banking, surveillance, litigation, education, electronic healthcare, and many other areas. Furthermore, more recently, human biometrics are assuming important roles in engineering technology and security including blockchains, Internet of things (IoT) and cloud computing (Gudeme et al. 2020). The preponderance and ubiquity of human biometric information make it imperative to invest in securing such biometric data. This is the primary objective for this study, which presents a scheme to generate and evaluate cancellable biometric templates. Our choice of cancellable biometric systems (CBS) is motivated by its proven capability to facilitate the required updates to biometric information whenever needed without affecting the rest of the system (Gudeme et al. 2020; Peng et al. 2021; Kaur and Khanna 2020; Wang et al. 2017; Akdogan et al. 2018). This makes CBS attractive for deployment in different advanced biometric identification and authentication frameworks, especially in platforms of emerging technologies such as cloud services and Internet of Things (IoT). To deliver on our outlined contribution, the rest of the study is organised as follows. Section 2 presents an overview of the work related to contributions emanating

✉ Basma Abd El-Rahiem
basma.rahiem@gmail.com

Abdullah M. Iliyasu
a.iliyasu@psau.edu.sa

[1] Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin El-Koom, Egypt

[2] Department of the Robotics and Intelligent Machines, Kafrelsheikh University, Kafrelsheikh 33511, Egypt

[3] Department of Electronics and Electrical Communications Engineering, Menoufia University, Menouf, Egypt

[4] Electrical Engineering Department, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia

[5] School of Computing, Tokyo Institute of Technology, Yokohama 226-8502, Japan

[6] School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China

from the study. Section 3 presents an overview of cancellable biometric systems as the foundation for our proposed multi-biometric cancellable scheme (MBCS) that is presented in later parts of the same section. Section 4 is devoted to presenting extensive performance evaluation in terms simulation results reporting visual, quantitative, qualitative, and complexity analyses of our proposed MBCS relative to similar state-of-the-art methods reported in the literature.

2 Related work

Cancellable biometric templates provide frameworks to safeguard biometric information where different inputs can be revised or updated without affecting the rest of the system (Peng et al. 2021). Furthermore, CBS systems are known to have low storage demands (Kaur and Khanna 2020), which has led to their consideration in different applications and domains. For example, a bi-level biometric system employing secure key arrangement (i.e., SKA) conventions was proposed by Kaur et al. in Kaur and Khanna (2020). Therein, the first convention utilised unadulterated biometric SKA arrangement (i.e., SKA-PB) while the second one utilises a cancellable biometric arrangement (i.e., SKA-CB). Both conventions use biometrics with unordered highlights, but SKA-PB uses symmetric cryptographic key arrangement between client and worker. Therefore, its resulting key is composed of irregular or arbitrary information. Unlike SKA-PB, dropped biometrics of the client are associated with SKA-CB instead of the unadulterated biometrics and the ability to generate cancellable templates is acquired by a two-fold string technique. As an insurance to layout bargain, which, in the SKA-CB convention, biometric formats can be dropped at any time. The conventions were validated using two fingerprints in applications demonstrating multi-standards security and examination of unpredictability.

Similar to Kaur and Khanna (2020), Akdogan et al. (2018) proposed a CBS-based connection invariant irregular separation (CIRF) convention. Their scheme is considered a promising assurance format that depends on the representation of the element of a certain biometric using 2D number threshold transform (NTT) and arbitrary sifting. However, despite its utility, CIRF is known to have image related computational demands that are attributed to the reverse 2D NTT used in the coordinating stage. This makes its development as a biometric ID system very costly. Consequently, in Akdogan et al. (2018), the concept of cancellable ordering was proposed to circumvent issues around CIRF. The resulting protocol utilises low-position estimates of biometric traits as a minimum spanning tree representation. Therefore, Akdogan et al.'s CIRF is a two-stage score level combination approach that associates the acquired scores from cancellable layouts of different biometric modalities. At the first level, scores from different matchers are combined using a mean-conclusion weighting (MCW) strategy. Subsequently, at the second level, scores from various modalities that utilise a rectangular territory weighting (RAW) technique are used.

Elsewhere in Murakami et al. (2019), a cancellable biometric approach dependent on Gaussian random vectors (GRV) and hashing was proposed by Murakami et al. The proposed framework applies variants of the first biometrics as opposed to the first biometric itself for storage and authentication. The study reports assessments in exhibition, non-invertibility and uniqueness, while validation was accomplished using face and palmprint biometric modalities.

In their contribution, Yang et al. proposed a CBS based on a random slope strategy in Yang et al. (2018). This technique reportedly creates a safe and revocable system with non-invertible cancelled templates. Structurally, the technique consists of two stages: random slope version one (RS-V1) and version two (RS-V2), which provide secured layouts manifesting two-thirds decrease in measurements. The technique was validated using different biometric modalities including noticeable and warm faces, print, palm vein, and finger vein.

CBS techniques have also been used to secure access to cloud-based platforms where biometric authentication is used to safeguard different levels of cloud resources (Gudeme et al. 2020). Among others, pseudo biometric characters of cancellable biometrics have been used to circumvent unauthorised access (Peng et al. 2021) where the cancelled biometric identities are generated using a random distance method. Additionally, the generated biometrics exhibited properties of revocability, diversity, and security for the user in diverse applications. Similarly, in Rathgeb and Busch (2014), Rathgeb and Busch proposed a cancellable biometric approach based on adaptive Bloom filter-based transforms. This technique integrates features of binary iris biometric templates to generate an irreversible fused template that obscures the information of both iris templates. The framework is implemented on Iris Database version 1.0 (Rathgeb and Busch 2014. In Trivedi et al. (2020), a CBS was proposed for fingerprint biometrics based on information extracted from the Delaunay triangulation of minutiae points. Further, to generate a user-specific cancellable biometric, a key of a random binary string is generated for each user. As with other highlighted CBS methods, the generated cancellable template exhibits properties of revocability, diversity, and security.

Meanwhile, in their contribution in Dwivedi and Dey (2019), Dwivedi and Dey proposed a non-invertible cancellable biometric technique based on partial Hadamard transform. To address the security issue, the proposed transformation is carried out on the DFT transformed biometric instead of the original biometric, specifically a set of fingerprint biometrics where the generated cancellable templates are required to satisfy revocability, diversity, non-invertibility and performance. Similarly, Kaur and Khana proposed a multi-biometric CBS system based on both fingerprint and finger vein modalities in Kaur and Khanna (2015). The focus of that study was aimed at meeting the protection and revocability requirements of the generated templates which combine minutia-based fingerprint feature set and image-based finger-vein feature set. Subsequently, a fusion process is carried out on both sets and the proposed approach was evaluated and analysed prior to matching and security. After that, they compared their proposed method alongside the original partial discrete Fourier transform (P-DFT). In Kaur and Khanna (2019), Kaur and Khana also proposed Random Slope concept to generate the cancelable features. They designed two biometric template protection methods based on this concept for various biometric modalities to observe efficacy and the security of the approaches.

Recently, however, the potency of deep learning models (DLM) has led to its emergence as the go-to strategy in different applications across wide ranging domains, including self-driving cars, natural language processing, entertainment, visual recognition, fraud detection and healthcare. In healthcare, recent applications of DLM have been reported in COVID-19 detection (Sedik et al. 2020b), e-healthcare for smart cities (Alghamdi et al. 2020), security (Al-Azrak et al. 2020; Elaskily et al. 2020; Sallam et al. 2019), biometric recognition (El-Rahiem et al. 2020; El-Moneim et al. 2019) and wireless communication (El-Ashkar et al. 2019).

Building on the highlighted contributions, in this study, we explore utilising the practicality of DLMs to generate secure and efficient cancellable biometric templates for iris, fingerprint, and finger vein modalities. Specifically, our proposed strategy is to generate a unique template that suffuses these modalities into an efficient multi-biometric CBS.

Consequently, the main contributions of our proposed study include:

1. Building a multi-exposure deep fusion module to generate a fused aggregate of different input biometric modalities.
2. Deploying a deep dream module to generate a cancellable template from the fused biometric image modalities.
3. Utilising standard metrics and techniques to evaluate the performance of the generated cancellable template relative to available state-of-the-art methods.

3 Proposed multi-biometric cancellable scheme

Cancellable biometric systems (CBS) are used to safeguard biometrics by generating an alternative encrypted template and storing it instead of the original biometric images where the generated cancellable templates are considered secure and unique for each identity.

Our proposed multi-biometric cancellable scheme (MBCS) is based on multi-exposure biometric fusion using deep dream. To elaborate, we employ a deep learning strategy to fuse the multi-exposure biometric modalities from iris, fingerprint, and finger vein biometrics that are subsequently transformed into a cancellable template. Figure 1 presents the layout of the proposed technique whose details are discussed in the remainder of this section.

3.1 Deep multi-exposure technique

As outlined in Fig. 1, as inputs for an enrolle, the multi-exposure deep fusion unit uses the separate modalities from iris, fingerprint, and finger vein biometrics consisting of images of each finger from a hand, its vein and iris, making seven input biometrics altogether. The fusion process utilises a sequence of convolutional layers to extract relevant features from these input biometric images. Following that, an additional layer is used to generate a feature map from each image, and, finally, a reconsideration network is used to generate the fused image.

Meanwhile, as elucidated in Fig. 2, in the case of multi-exposure fusion, the enumerated process is repeated recursively for each pair of images. Furthermore, execution of the convolutional neural network (CNN)-based deep fusion process for each pair of biometric images is accomplished in three phrases. In the first phase, targeted features are extracted from the input images and used to generate a feature mapping where the input images are fused, i.e., during the second phase. Finally, in the third phase, the fused feature map is reconstructed using a reconstruction network. In terms of configuration, the feature extraction phase consists of two channels, C_1 and C_2, each composed of two convolution layers, (i.e., $C_{1,1}$, $C_{1,2}$, and $C_{2,1}$, $C_{2,2}$) for the second feature extraction channel. On its part, the fusion layer uses an addition operation to fuse feature maps F_1 and F_2. Finally, the reconstruction phase consists of three convolution layers C_3, C_4 and C_5. The enumerated three phases combine to accomplish the multi-exposure deep fusion process that feeds the deep dream cancellable unit of our proposed MBCS scheme. Further details of the intrigues involved in the multi-exposure deep fusion and deep dream cancellable processes are outlined in the sequel.

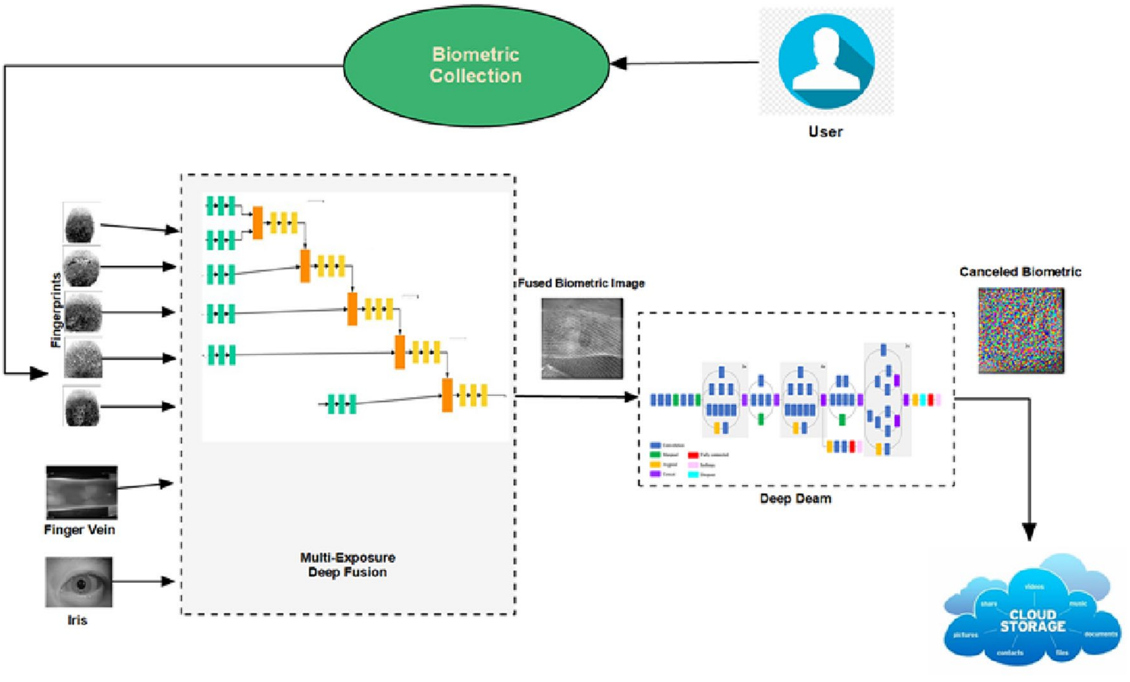


Fig. 1 Outline of proposed multi-biometric cancellable system (MBCS)

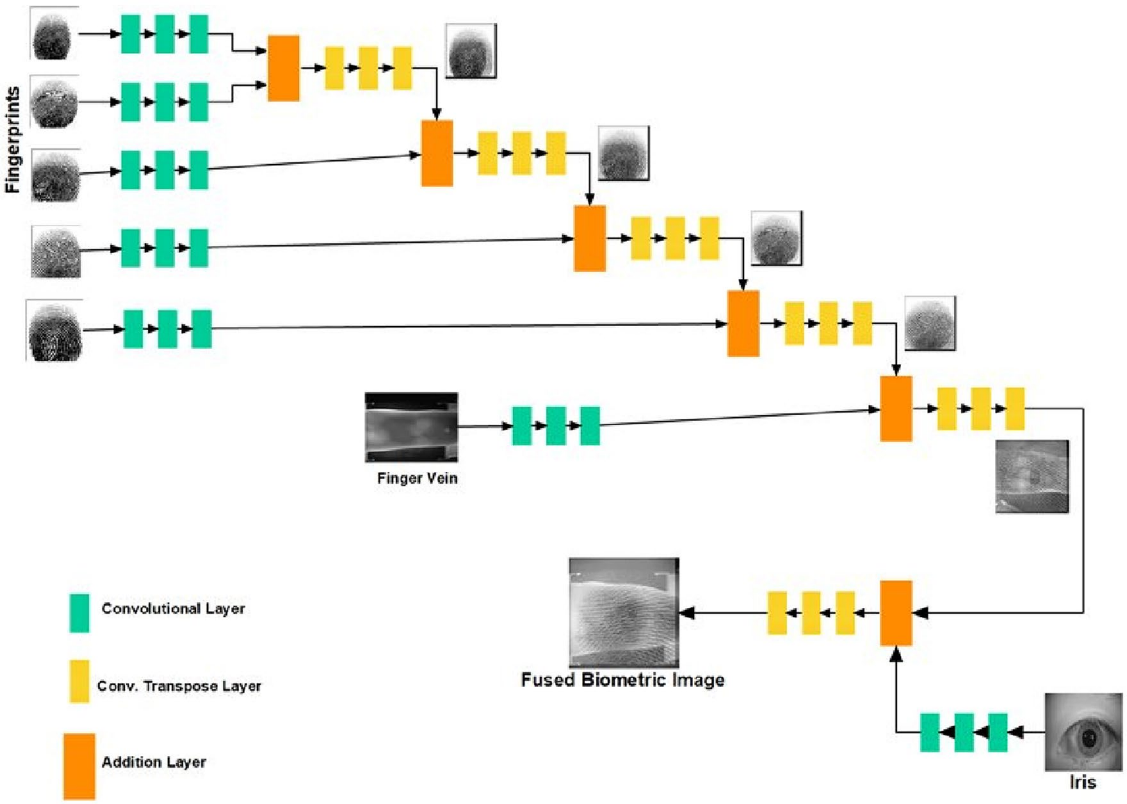


Fig. 2 Description of multi-exposure deep fusion process

3.1.1 Loss function and optimisation

As a deep learning algorithm, the proposed multi-exposure fusion (MEF) process is optimised during the training phase. The loss function minimises the error between real and estimated targets for an instance of data. However, this would depend on whether the application is classification or fusion. For example, in classification applications, there are different loss functions, such as cross entropy and mean square error, so loss functions are deployed to minimise the error between the real and estimated classes. In contrast, since the main goal of fusion applications (Fig. 3) is to generate an image with quality close to the input images then the fused image should manifest qualities as close to the input image as possible. Consequently, the structural similarity index measure (SSIM) would be a good loss function for such applications. SSIM computes the pixel-wise similarity between images and as such a low SSIM would indicate concordance between the fused and input images as deduced from Eqs. (1)-(5).

$$l\left(y_k\,,\,y_f\right)=\frac{2\mu_{y_k}\,\mu_{y_f}\;+C_1}{\mu_{y_k}^2\;+\mu_{y_f}^2\;+C_1},\tag{1}$$

$$c\left(y_k\,,\,y_f\right)=\frac{2\sigma_{y_k}\,\sigma_{y_f}\;+C_2}{\sigma_{y_k}^2\;+\sigma_{y_f}^2\;+C_2},\tag{2}$$

$$s\left(y_k\,,\,y_f\right)=\frac{\sigma_{y_k\,y_f}\;+C_3}{\sigma_{y_k}\,\sigma_{y_f}\;+C_3},and\tag{3}$$

$$SSIM(y_k\,,y_f\,)=[l(y_k\,,y_f\,)]\alpha\cdot[c(y_k\,,y_f\,)]\beta\cdot[s(y_k\,,y_f\,)]\gamma\tag{4}$$

where μ_G and μ_I, σ_G and σ_I, and σ_{GI} are the local means, standard deviations, and cross-covariance for input and output image patches y_k and y_f, respectively, while C_1, C_2, and C_3 are stabilisation constants. If the parameters $\alpha=\beta=\gamma=1$ (i.e., the default values used in exponents), and $C_3=C_2/2$ (i.e., the default selection of C_3) then the simplified SSIM index is defined as:

$$SSIM\left(y_k\,,y_f\,\right)=\frac{(2\mu y_k\;\mu y_f\;+C1)(2\sigma y_k\;y_k\;+C2)}{(\mu 2y_k+\mu 2y_f+C1)(\sigma 2y_k+\sigma 2y_f+C2)}\tag{5}$$

whose score at a certain pixel p is:

$$score(p)=SSIM\left(y_k\,,y_f\,\right),\tag{6}$$

and the total loss is calculated using (7).

$$Loss=\frac{1}{N}\sum_{p\in P}score(p),\tag{7}$$

where N is the total number of pixels in the image and P is the set of all pixels in the input image.

The computed loss is backpropagated during the network training and it can be inferred that the choice of SSIM as performance indicator for MEF is attributed to its objective function which maximises structural consistency between each fused and input image pairing.

3.2 Deep dream algorithm

As presented in earlier Fig. 1 and the discussion that followed it, the second unit of our proposed multi-biometric cancellable system (MBCS) is the so-called deep dream algorithm (Cox 2019), which curtails losses associated with convolutional layers of our deep learning architecture. These losses arise because CNN perfoms digital filtering operations where each filter extracts features from input images. Since a CNN network consists of multiple layers and each layer includes a certain number of filters selected by a dedicated design, then a layer comprising of $\boldsymbol{N_l}$ distinct filters would have $\boldsymbol{N_l}$ feature maps each of size $\boldsymbol{M_l}$, where $\boldsymbol{M_l}$ is a multiplication of the height and width of the feature map. Furthermore, the responses in a layer l can be stored in a matrix $\boldsymbol{F^l}\in\boldsymbol{R}^{N_l\times M_l}$ where $\boldsymbol{F^l_{ij}}$ is the activation of the $\boldsymbol{ith}$ filter at position $\boldsymbol{j}$ in layer $\boldsymbol{l}$.

Consequently, the new value of a certain pixel $\boldsymbol{p_{new}}$ is computed as the summation of the surrounding old pixels $\boldsymbol{p}$ multiplied by the applied filter elements $\boldsymbol{w}$, as formalised in (8).

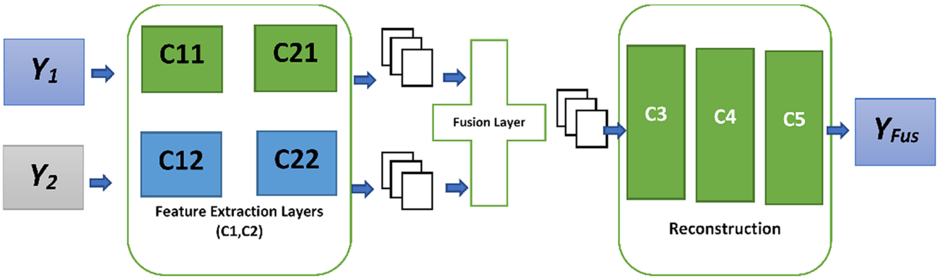


Fig. 3 Illustration of fusion process for image pairs

$$p_{new} = \sum_{i\in s} p_i.w_i \tag{8}$$

If we consider $\tilde{\boldsymbol{p}}$ and $\tilde{\boldsymbol{x}}$ as the original and generated images and $\boldsymbol{P^l}$ and $\boldsymbol{F^l}$ as their respective feature representations at layer $\boldsymbol{l}$, then the squared-error loss between the two feature representations could be defined in the form presented in (9).

$$L\ \ (\tilde{p},\tilde{x},l) = \frac{1}{2}\sum_{i,j}\left(F^l_{ij} - P^l_{ij}\right)^2, \tag{9}$$

and the derivative of this loss with respect to the activations in layer l is computed using:

$$\frac{\partial L}{\partial F^l_{ij}} = \begin{cases} F^l_{ij} - P^l_{ij} & if \quad F^l_{ij} > 0 \\ 0 & if \quad F^l_{ij} < 0 \end{cases} \tag{10}$$

3.2.1 Implementation of deep dream algorithm

As outlined in Cox (2019), the execution of the deep dream algorithm (DDA) on a Convnet pretrained ImageNet model requires access to many Convnets, such as VGG16, VGG19, Xception, and ResNet 50. While DDA can be executed with any of them, the choosen convnet will naturally affect the visualisations because different convnet architectures result in different learned features. Moreover, Inception is known to intuitively produce decent looking Deep Dreams (Cox 2019). Motivated by this, we utilise Inception V3 model, whose layout is presented in Fig. 4, for the DDA unit of our proposed MBCS scheme.

Subsequently, loss value is maximised during the gradient-ascent process. For filter visualisation, the target is to maximise the value of a specific filter in a specific layer, which entails maximising the activations of filters in different layers simultaneously. Specifically, the objective is to maximise a weighted sum of the $\boldsymbol{L2}$ norm of the activations in a set of high-level layers. Since the choice of exact set of layers (as well as their contribution to the final loss) has a major influence on the visuals that will be produced, then these parameters must be easily configurable. Moreover, it has been established that lower layers result in geometric patterns, whereas higher layers produce visuals wherein some classes can be recognised from ImageNet (Cox 2019). Consequently, while the implementation starts with a somewhat arbitrary configuration involving four layers, eventually it trancends many other configurations.

Furthermore, the maximisation process is performed on the loss gradients of the convnet layers where three main parameters are used to control the gradient ascent process, maximum loss L_{max}, gradient step S and number of iterations I. In this regard, the gradient ascent X for loss gradients of layer l at an iteration i can be computed using (11).

$$X = \sum_{i,l} S \times L_{i,l} \quad if \quad X < L_{max} \tag{11}$$

Finally, a list of scales (i.e., octaves) generated by dream rein junction at each layer define subsequent points to process the images. Moreover, the rein junction can be utilised to upscale the input image at each layer and increase its cancellability. Therefore, each successive scaling is larger than the previous one by a factor of 1.4, which results in 40% increase in the initial dimensions of the image. Therefore, the rein junction process starts with a small image that is successively up scaled as demonstrated in Fig. 5.

As illustrated in the figure, at each step of the deep dream generation, from the smallest image to the largest, gradient ascent is performed to maximise the previously

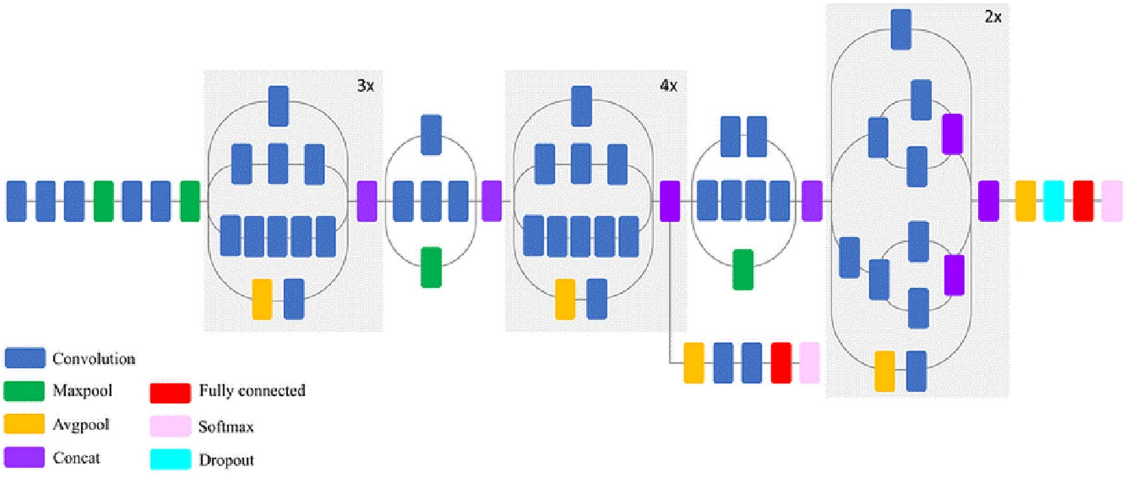


Fig. 4 Layout demonstrating the architecture and layers of Inception V3 deep learning model (Cox 2019)

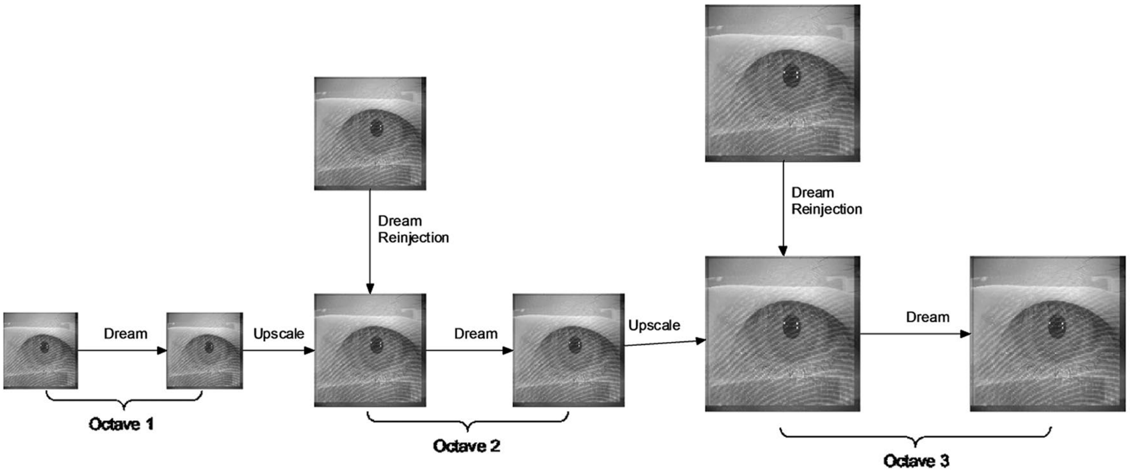


Fig. 5 Illustration of deep dream image generation Cox (2019)

defined loss function. Additionally, since the resulting image is upscaled by 40% then, to avoid losing a lot of image detail, after each successive scale-up (resulting in increasingly blurry or pixelated images), there is need to reinject some of the lost details back into the image. Therefore, given a small image I_s and a larger image I_L, the difference between the original image resized to size I_L and the original image resized to size I_s quantifies the image details lost when going from I_s to I_L.

4 Simulation results

Guided by Sedik et al. (2020a), the validation and performance evaluation for our proposed MBCS scheme is undertaken using three biometric inputs, namely: fingerprint, finger vein and iris. The dataset comprises of nine images from each modality, i.e., fingerprint, finger vein and iris as presented in Fig. 6a–c. Finger veins are collected using an infrared (IR) sensor, while the fingerprints are collected using a special device equipped with a light emitting diode (LED) to generate the fingerprint image (Peng et al. 2014). Finally, the iris images are obtained via the CASIA iris dataset in Wang et al. (2013) where further details regarding its collation are presented.

As presented in preceding sections of this study, the objective of our MBCS scheme is to generate a secure cancellable template to replace the hitherto separate biometric input images. Therefore, applying our outlined MBCS scheme on the dataset in Fig. 6a–c, produces the cancellable templates in Fig. 6d for each block of the biometric inputs.

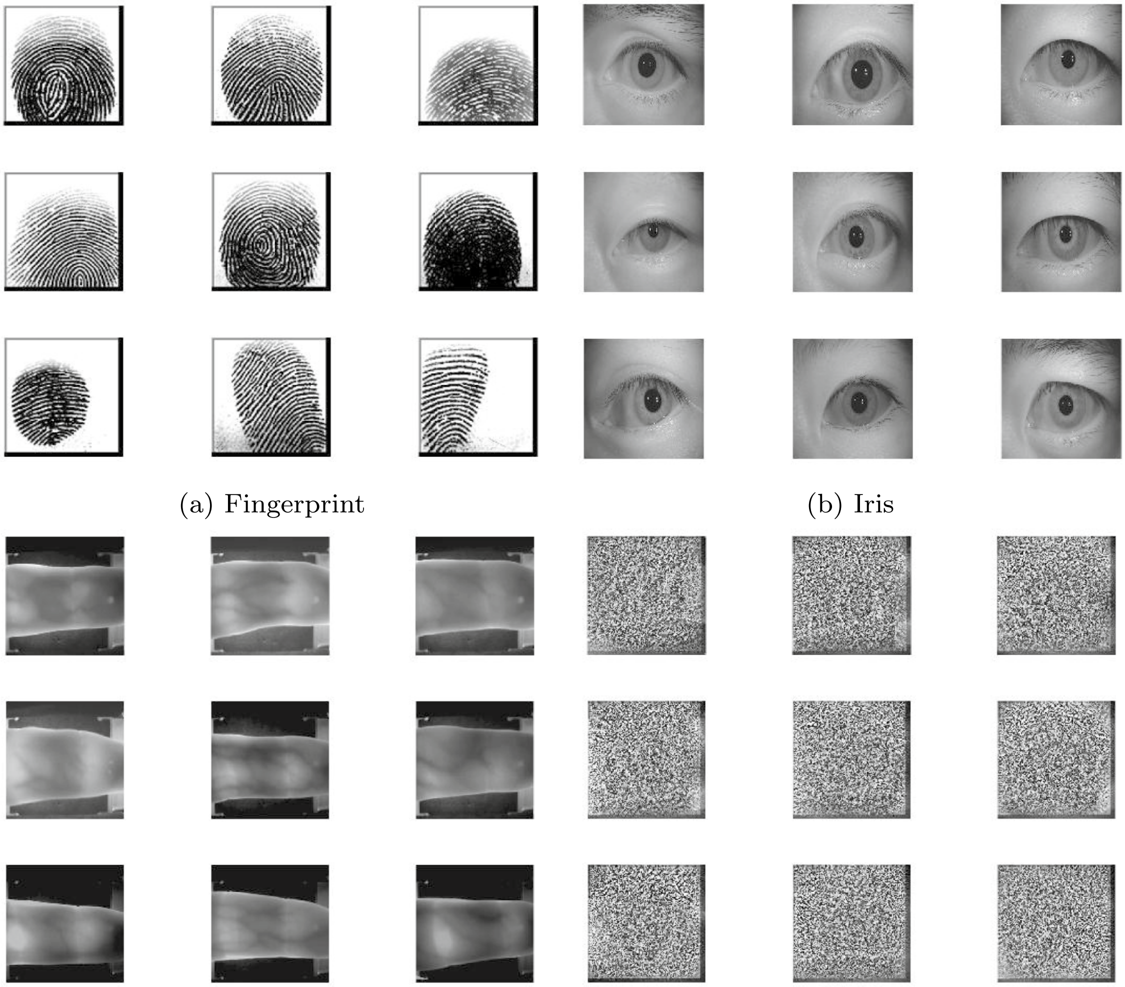
Our proposed MBCS scheme is implemented via a workstation equipped with Python, Intel® Core ^{TM} i7 on a NVIDIA GPU with 4 GB and each analysis is undertaken using standard metrics as reported in subsequent subsections. Similarly, in this section, we report outcomes of our extensive evaluation that covers visual and statistical performance indicators with the former (i.e., visual evaluation) further divided into histogram and correlation analyses whilst the latter (i.e., statistical evaluation) is similarly further divided into quantitative, qualitative, and complexity analyses. These metrics and their outcomes are presented in the sequel.

4.1 Visual evaluation

The visual evaluation includes the histogram, genuine and imposter correlation scores, and receiver operating characteristics (ROC) which are aimed at establishing the visual performance of the proposed scheme.

4.1.1 Histogram analysis

Histograms provide insightful visualisation of the pixel-wise intensity distribution in an image (Abd-El-Atty et al. 2021). A good cancellable scheme should exhibit identical distribution for the generated templates. Figure 7a–c present respective histograms for the fingerprint, finger vein and iris biometrics (i.e., those presented earlier in Fig. 6a–c) whereas Fig. 7d presents the histograms for the generated cancellable templates, i.e., those in Fig. 6d. As observed in Abd-El-Atty et al. (2021), histogram plots indicate the scheme's vacuity or permeation of noise, which is also a confirmation of its capacity to withstand statistical attacks.



(a) Fingerprint

(b) Iris

(c) Finger vein

(d) Generated cancellable template

Fig. 6 Input biometric images and generated cancellable template

4.1.2 Correlation analysis

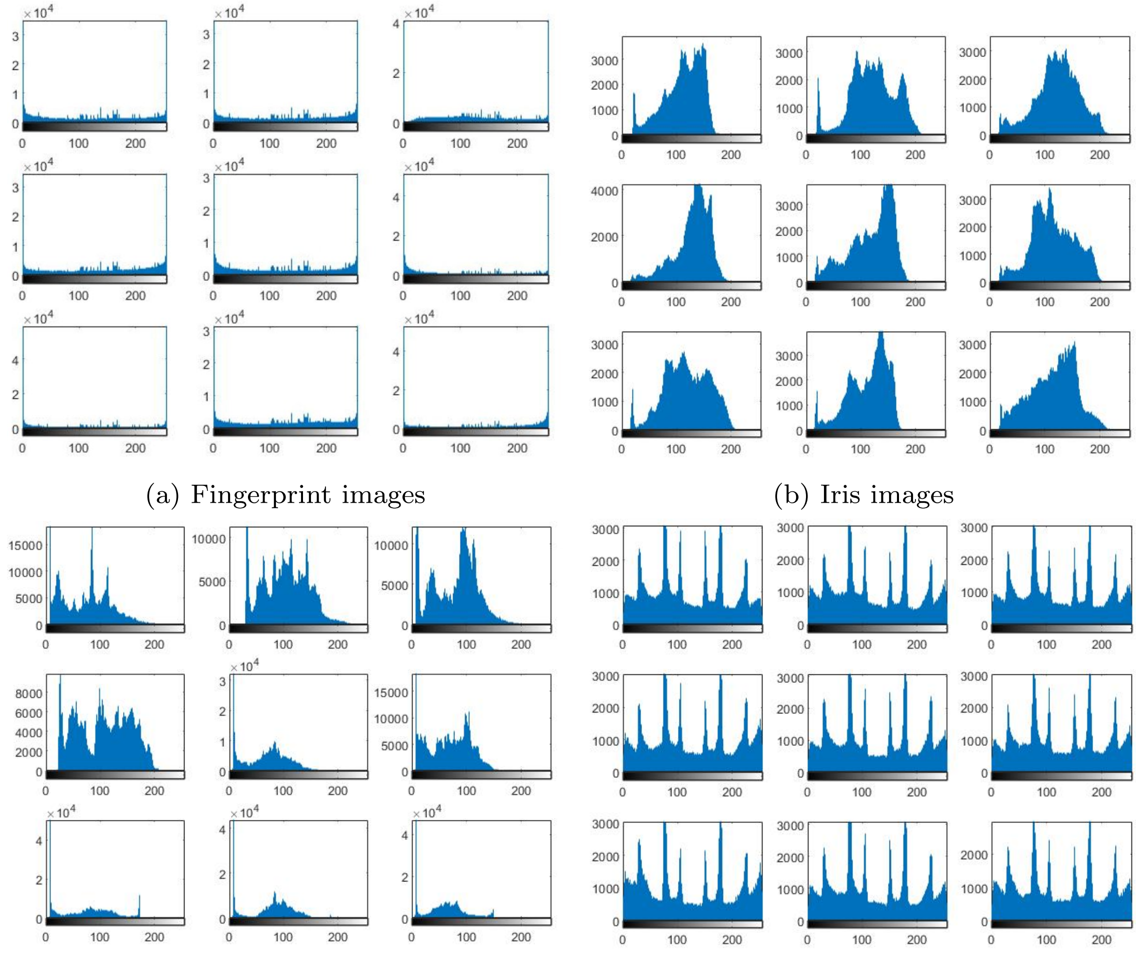
Correlation coefficient is another metric that is useful in visualising the discombobulation expected in cancellable schemes. The correlation coefficient of neighbouring pixels $C_{A,B}$ is used in correlation analysis to assess the relationship between an input biometric image and its generated cancellable template (Kaur and Khanna 2020; Akdogan et al. 2018; Wang et al. 2017). In this regard, the neighbouring pixels of the pristine input biometric should be highly correlated with values close to unity whilst those in the cancellable template should have values closer to zero (Yan et al. 2013).

We compute $C_{A,B}$ using (12) and report plots of $C_{A,B}$ for auto and cross correlation in Fig. 8a, b, respectively.

$$R_{xy}=\frac{\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})}{\sigma_x\sigma_y}, \tag{12}$$

where N is the total number of pixels, x and y are the encrypted stored template in the database and the new subject encrypted template.

Figure 8c presents the correlation score for the original and generated images, while the ROC curve is plotted in Fig. 8d. This curve shows that based on the area under the curve (AUC) metric, an accuracy of 99% was achieved, which suggests potential applications for the proposed MBCS in safeguarding confidentiality of cybersecurity systems.



(a) Fingerprint images

(b) Iris images

(c) Finger vein images

(d) Cancellable templates

Fig. 7 Histograms for the three input biometrics and their generated templates

4.2 Statistical evaluation

Outcomes of our statistical evaluation comprising of qualitative and quantitative analyses that utilise different metrics to assess the quality of the generated cancellable template and correlation of its signal to noise ratio are presented and discussed in this section.

4.2.1 Quantitative analysis

The performance of our proposed MBCS scheme is evaluated in terms of three quantitative metrics, namely: percentage pixel change rate (NPCR), unified average changing intensity (UACI) and peak signal to noise ratio (PSNR).

Given two images I_1 and I_2, the NPCR, UACI and PSNR are computed using (13), (15) and (16), respectively, where M and N represent the width and height of the images.

$$NPCR(\%) = \frac{1}{M \times N \times 3} \sum_{i=1}^{M} \sum_{j=1}^{N} \sum_{k=1}^{3} S(i,j,k) \times 100, \tag{13}$$

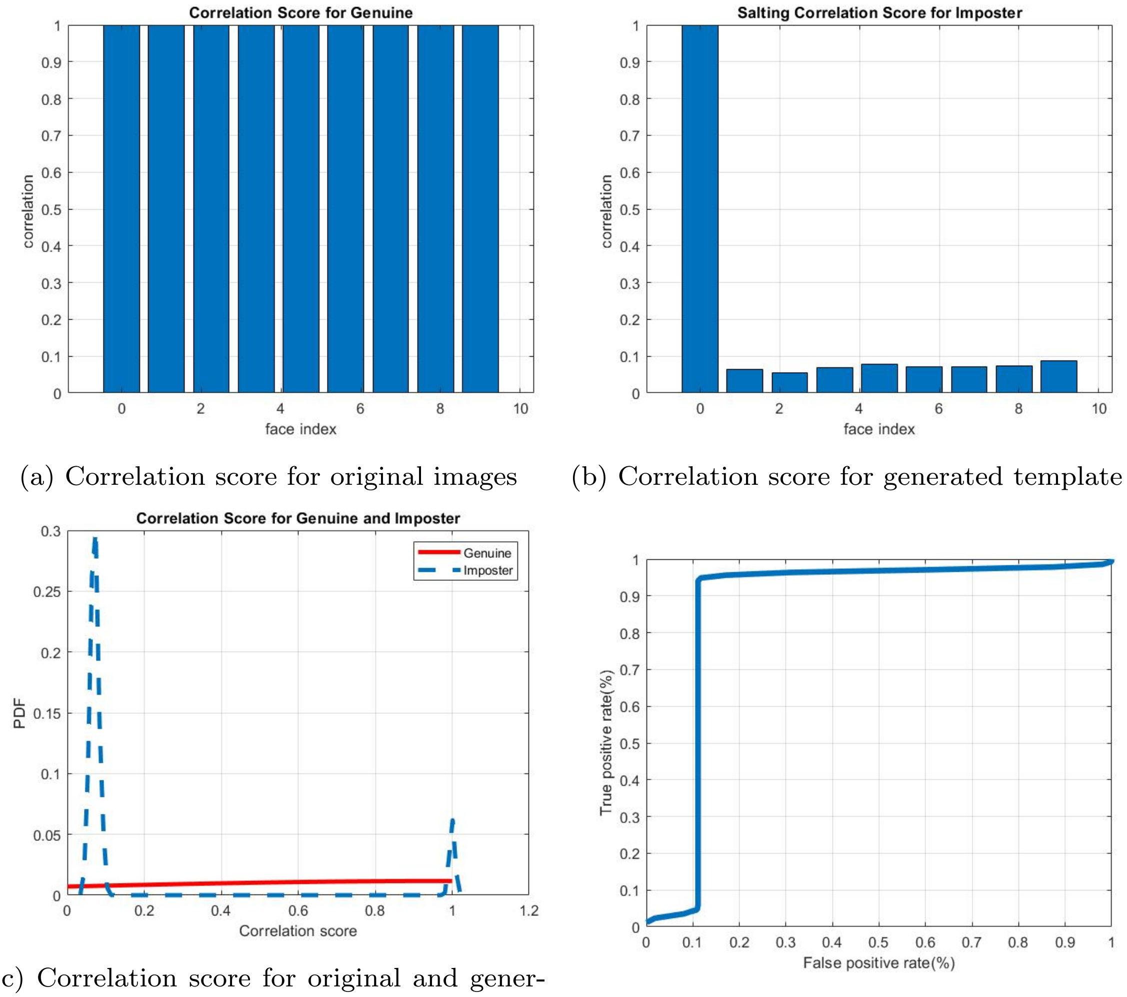
where

$$S(i,j,k) = \begin{cases} 1, & I_1(i,j,k) = I_2(i,j,k) \\ 0, & elsewhere \end{cases}. \tag{14}$$

$$UACI(\%) = \frac{1}{M \times N \times 3} \sum_{i=1}^{M} \sum_{j=1}^{N} \sum_{k=1}^{3} \frac{|I_1(i,j,k) - I_2(i,j,k)|}{255} \times 100. \tag{15}$$

$$PSNR = 20\log_{10}\left[\frac{I_{MAX}}{\sqrt{MSE}}\right], \tag{16}$$

where I_{MAX} is the maximum possible pixel value and MSE is mean square error defined as:



(a) Correlation score for original images

(b) Correlation score for generated template

(c) Correlation score for original and generated templates

(d) ROC Curve

Fig. 8 Plots for visual evaluation of proposed MBCS scheme

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left[I_2(i,\ j) - I_1(i,\ j) \right]. \tag{17}$$

4.2.2 Qualitative analysis

Qualitative evaluation involves the use of quality metrics to analyse the performance of the scheme. Employing spectral distribution (SD) and universal image quality index (UIQ) quality metrics, we report the performance of our proposed MBCS scheme in the remainder of this subsection.

(a) Spectral distortion

Spectral distribution (SD) provides a qualitative assessment of similarity between the spectral information in two images (Benrhouma et al. 2015). It is accepted that SD values indicate congruence between the assessed images (Abd-El-Atty et al. 2021). Mathematically, SD is defined as:

$$SD = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} |x(i,j) - y(i,j)|}{M \times N}, \tag{18}$$

where $M \times N$ is the total number of pixels in the image, $x(i, j)$ and $y(i, j)]$ are the original image and the encrypted image, respectively.

(b) Universal image quality index Universal image quality index (UQI) is another metric that assesses structural concordance between two images (El-Latif et al. 2020). Mathematically, UQI, whose values vary in the range -1 to 1, is computed using (19) with values closer to 1 indicating greater congruity between images (El-Latif et al. 2020).

$$UQI(i,j) = \frac{Cov_{ij}}{\sigma_i \sigma_j} \cdot \frac{2\mu_i \mu_j}{\mu_i^2 + \mu_j^2} \cdot \frac{2\sigma_i \sigma_j}{\sigma_i^2 + \sigma_j^2}, \tag{19}$$

where μ_i and μ_j, s_i and s_j, and Cov_{ij} are the means, variances, and covariance of i and j, respectively.

Table 1 Quantitative and qualitative evaluation of proposed MBCS scheme

Template number	Quantitative metrics					Qualitative metrics			
	Correlation			NPCR (%)	PSNR (dB)	SSIM	UIQ	SD	UACI
	D	H	V						
1	0.9430	0.9637	0.9198	99.1787	25.9953	0.0669	0.9198	57.1090	22.3957
2	0.9597	0.9749	0.9207	99.0417	24.3861	0.0852	0.9130	59.5490	23.3525
3	0.9524	0.9663	0.9423	99.1631	24.5573	0.0760	0.9051	59.8314	23.4633
4	0.9756	0.9811	0.9066	99.1871	23.7458	0.0783	0.9039	61.9189	24.2819
5	0.9528	0.9688	0.9526	99.1989	24.2830	0.0664	0.9037	61.2844	24.0331
6	0.9593	0.9736	0.9405	98.9891	24.0882	0.0872	0.9008	60.0688	23.5564
7	0.9792	0.9780	0.9397	99.1875	24.3045	0.0839	0.9085	62.2120	24.3969
8	0.9341	0.9433	0.9526	99.1581	24.6180	0.0697	0.9089	60.4679	23.7129
9	0.9565	0.9794	0.9370	99.3188	24.7281	0.0915	0.9209	59.7939	23.4486
Average				99.1581	24.5229	0.0783	0.9093	59.5817	23.6268

Table 2 Execution time (in seconds)

Method	Total
IFL followed by Gaussian RP Peng et al. (2021)	13.14
Homomorphic transform followed by Gaussian RP Peng et al. (2021)	12.18
Proposed method	15.30

To conclude the quantitative and qualitative evaluation, we present (in Table 1) outcomes of the defined metrics for our proposed MBCS scheme. From the table, we can deduce average performance in terms of 99.158% (NPCR), 24.52dB (PSNR), 0.0783 (SSIM), 0.9093 (UIQ), 59.5817 (SD), and 23.6268 (UACI) which indicate proposed scheme's utility as an efficient platform for biometric authentication with potential applications in cloud services and IoT frameworks.

5 Discussion of results and complexity evaluation

The intrigues and resources required to implement an algorithm are assessed in terms its complexity. In this section, we report evaluations of the performance of our proposed MBCS scheme in terms of its execution time and its inherent limiting factor, i.e., the big O analysis.

The time required, in seconds, to implement our MBCS scheme is computed in terms of steps required for its execution for every user (Gudeme et al. 2020; Peng et al. 2021; Kaur and Khanna 2020) where each biometric is an M by N image as enumerated below.

Steps performed for each user:

Table 3 Comparison of computational complexity

Method	Complexity in big-O notation
Proposed	$O(max(n, (n\times (M\times N)))$
Peng et al. (2021)	$O(max(n, (n\times (M\times N)))$
Tarif et al. (2017)	$O(n)$

Table 4 A comparison between the proposed method and works in the literature

Cancellable biometric method	EER	FAR	FRR	AROC
Proposed	0.0032	0.0006	0.0010	0.990
Soliman et al. (2018b)	0.0924	0.0562	0.0257	0.868
Soliman et al. (2018a)	0.0178	0.0071	0.0876	0.896
Algarni et al. (2020)	0.0098	0.0104	0.0180	0.952
Tarif et al. (2017)	0.1081	0.0927	0.0967	0.907
Sree and Radha (2016)	0.0416	0.1955	0.0489	0.873
Dang et al. (2016)	0.0859	0.0435	0.0627	0.718
Kumar et al. (2011)	0.0357	0.0985	0.0612	0.863
Refregier and Javidi (1995)	0.0046	0.0235	0.0929	0.883

1. ($O(1)$) operations to register current biometrics of the user
2. ($O(n\times(M\times N))$) operations to perform feature extraction on an $M\times N$ image, where n is an integer.
3. ($O(2\times n\times (M\times N))$) operations to fuse the features.
4. ($O(M\times N)$) operations to reconstruct the fused image.
5. ($O(5\times n\times M\times N)$) operations to perform the deep dream (which has 5 steps).
6. ($O(n\times(M\times N))$) operations to perform the authentication process leading to acceptance or rejection the user.

Furthermore, the actual time required to execute the proposed scheme is tabulated in Table 2 from which we can infer a moderate execution time especially since generation of the cancellable template is an off-line process (Peng et al. 2021). Furthermore, by noting that the complexity analysis is performed in terms of central processing unit (CPU) operations required to execute the proposed MBCS scheme, running time for each step is estimated.

As reported in Table 3, the authentication process of our MBCS scheme requires $O(max(n, (n\times (M\times N)))$ steps (or operations) which, relative to a recent study in Peng et al. (2021), is considered moderate.

Additionally, Table 4 presents a comparison between the proposed method and others reported in the literature in terms of Equal Error Rate (EER), False Acceptance Rate (FAR), False Rejection Rate (FRR), and area under ROC curve (AROC). As deduced therefrom, with values of 0.0032 (EER), 0.0006 (FAR), 0.001 (ERR) and 0.99 (AROC), our proposed scheme outperforms similar ones reported in Soliman et al. (2018b), Soliman et al. (2018a), Algarni et al. (2020), Tarif et al. (2017), Sree and Radha (2016), Dang et al. (2016), Kumar et al. (2011) and Refregier and Javidi (1995).

6 Concluding remarks

A multi-biometric cancellable scheme (MBCS) has been proposed to generate secure and efficient cancellable templates for fingerprint, finger vein and iris biometric modalities. In doing so, we exploited the potency of deep learning models to build a multi-exposure deep fusion module used to generate a fused biometric template that is subsequently aggregated as the final cancellable template in the deep dream module. Extensive performance evaluation comprising of visual and statistical analyses produced average values of 99.158%, 24.523 dB, 0.079, 0.909, 59.582 and 23.627 for NPCR, PSNR, SSIM, UIQ, SD and UACI, respectively that validate the effectiveness of our proposed scheme. In ongoing efforts, we are expanding the study via integration of new recognition and encryption protocols to be validated on larger and more robust datasets. Furthermore, we are exploring deployment of this refined version of the scheme for real-time biometric applications in airports, banks, surveillance, etc.

Acknowledgements This study is sponsored in full by the Prince Sattam Bin Abdulaziz University, Saudi Arabia via the Deanship for Scientific Research funding for the Advanced Computational Intelligence and Intelligent Systems Engineering (ACIISE) Research Group Project number 2020/01/12173. Support from the Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin El-Koom, Egypt is appreciated.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Availability of data and material The data used in the study can be accessed upon your request to the corresponding author.

References

Abd-El-Atty B, Iliyasu AM, Alanezi A, El-latif AAA (2021) Optical image encryption based on quantum walks. Opt Lasers Eng 138:106403

Akdogan D, Altop DK, Eskandarian L, Levi A (2018) Secure key agreement protocols: pure biometrics and cancelable biometrics. Comput Netw 142:33–48

Al-Azrak FM, Sedik A, Dessowky MI, Banby GME, Khalaf AAM, Elkorany AS, El-Samie FEA (2020) An efficient method for image forgery detection based on trigonometric transforms and deep learning. Multimed Tools Appl 79(25–26):18221–18243

Algarni AD, Banby GME, Soliman NF, El-Samie FEA, Iliyasu AM (2020) Efficient implementation of homomorphic and fuzzy transforms in random-projection encryption frameworks for cancellable face recognition. Electronics 9(6):1046

Alghamdi A, Hammad M, Ugail H, Abdel-Raheem A, Muhammad K, Khalifa HS, El-Latif AAA (2020) Detection of myocardial infarction based on novel deep transfer learning methods for urban healthcare in smart cities. Multimed Tools Appl. https://doi.org/10.1007/s11042-020-08769-x

Benrhouma O, Hermassi H, El-Latif AAA, Belghith S (2015) Chaotic watermark for blind forgery detection in images. Multimed Tools Appl 75(14):8695–8718

Cox CM (2019) Algorithm of the night: google's deepdream and (dis)harmonies of an eternal nocturnal. In: Stahl G, Botta G (eds) Nocturnes: popular music and the night. Springer International Publishing, pp 241–255

Dang TK, Truong QC, Le TTB, Truong H (2016) Cancellable fuzzy vault with periodic transformation for biometric template protection. IET Biometr 5(3):229–235

Dwivedi R, Dey S (2019) Score-level fusion for cancelable multi-biometric verification. Pattern Recognit Lett 126:58–67

El-Ashkar AM, Sedik A, Shendy H, Taha TES, El-Fishawy AS, El-Nabi MA, Khalaf AAM, El-Banby GM, El-Samie FEA (2019) Classification of reconstructed SAR images based on convolutional neural network. Menoufia J Electron Eng Res 28(1):122–125

El-Latif AAA, Abd-El-Atty B, Amin M, Iliyasu AM (2020) Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. Sci Rep 10(1):1930

El-Moneim SA, Hassan SEAA, Sedik A, Nassar MA, Dessouky MI, Ismail NA, El-Fishawy AS, El-Banby GM, Khalaf AAM, El-Samie FIA (2019) Effect of reverberation phenomena on text—independent speaker recognition based deep learning. Menoufia J Electron Eng Res 28(1):19–23

El-Rahiem BA, Sedik A, Banby GME, Ibrahem HM, Amin M, Song O-Y, Khalaf AAM, El-Samie FEA (2020) An efficient deep learning model for classification of thermal face images. J Enterp Inf Manag **(ahead-of-print)**

Elaskily MA, Elnemr HA, Sedik A, Dessouky MM, Banby GME, Elshakankiry OA, Khalaf AAM, Aslan HK, Faragallah OS, El-Samie FEA (2020) A novel deep learning framework for copy-moveforgery detection in images. Multimed Tools Appl 79(27–28):19167–19192

Gudeme JR, Pasupuleti SK, Kandukuri R (2020) Attribute-based public integrity auditing for shared data with efficient user revocation in cloud storage. J Ambient Intell Humaniz Comput 12(2):2019–2032

Kaur H, Khanna P (2015) Gaussian random projection based non-invertible cancelable biometric templates. Procedia Comput Sci 54:661–670

Kaur H, Khanna P (2019) Random slope method for generation of cancelable biometric features. Pattern Recognit Lett 126:31–40

Kaur H, Khanna P (2020) Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing. Future Gener Comput Syst 102:30–41

Kumar P, Joseph J, Singh K (2011) Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator. Appl Opt 50(13):1805

Murakami T, Ohki T, Kaga Y, Fujio M, Takahashi K (2019) Cancelable indexing based on low-rank approximation of correlation-invariant random filtering for fast and secure biometric identification. Pattern Recognit Lett 126:11–20

Peng J, El-Latif AAA, Li Q, Niu X (2014) Multimodal biometric authentication based on score level fusion of finger biometrics. Optik 125(23):6891–6897

Peng J, Yang B, Gupta BB, El-Latif AAA (2021) A biometric cryptosystem scheme based on random projection and neural network. Soft Comput 25(11):7657–7670

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

Refregier P, Javidi B (1995) Optical image encryption based on input plane and Fourier plane random encoding. Opt Lett 20(7):767

Sallam YF, Sedik A, Ghazy R, Abdelwahab N, din H. Ahmed H, Saleeb A, Banby GME, Khalaf AAM, El-Samie FEA (2019) Intrusion detection based on deep learning. Menoufia J Electron Eng Res 28(1):369–373

Sedik A, El-Rahiem BA, El-Samie FEA, El-Latif AAA (2020a) Mbd: multi-biometric dataset. Mendeley Data, V1. https://doi.org/10.17632/94ksjbwnz.1

Sedik A, Iliyasu AM, El-Rahiem BA, Samea MEA, Abdel-Raheem A, Hammad M, Peng J, El-Samie FEA, El-Latif AAA (2020b) Deploying machine and deep learning models for efficient data-augmented detection of COVID-19 infections. Viruses 12(7):769

Soliman RF, Amin M, El-Samie FEA (2018a) A modified cancelable biometrics scheme using random projection. Ann Data Sci 6(2):223–236

Soliman RF, Banby GME, Algarni AD, Elsheikh M, Soliman NF, Amin M, El-Samie FEA (2018b) Double random phase encoding for cancelable face and iris recognition. Appl Opt 57(35):10305

Sree SS, Radha N (2016) Cancellable multimodal biometric user authentication system with fuzzy vault. In: 2016 international conference on computer communication and informatics (ICCCI). IEEE

Tarif EB, Wibowo S, Wasimi S, Tareef A (2017) A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system. Multimed Tools Appl 77(2):2485–2503

Trivedi AK, Thounaojam DM, Pal S (2020) Non-invertible cancellable fingerprint template for fingerprint biometric. Comput Secur 90:101690

Wang N, Li Q, El-Latif AAA, Yan X, Niu X (2013) A novel hybrid multibiometrics based on the fusion of dual iris, visible and thermal face images. In: 2013 international symposium on biometrics and security technologies. IEEE

Wang S, Deng G, Hu J (2017) A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. Pattern Recognit 61:447–458

Yan X, Wang S, El-Latif AAA, Niu X (2013) New approaches for efficient information hiding-based secret image sharing schemes. Signal Image Video Process 9(3):499–510

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

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.