EURASIP Journal on Wireless
Communications and Networking

RESEARCH Open Access

Coverless image steganography using morphed face recognition based on convolutional neural network

Yung-Hui Li[1], Ching-Chun Chang[2*], Guo-Dong Su[3], Kai-Lin Yang[1], Muhammad Saqlain Aslam[1] and Yanjun Liu[3]

*Correspondence:
c.c.chang@warwickgrad.net
[2] Department of Computer Science, University of Warwick, Coventry CV4 7AL, UK
Full list of author information is available at the end of the article

Abstract

In recent years, information security has become a prime issue of worldwide concern. To improve the validity and proficiency of the image data hiding approach, a piece of state-of-the-art secret information hiding transmission scheme based on morphed face recognition is proposed. In our proposed data hiding approach, a group of morphed face images is produced from an arranged small-scale face image dataset. Then, a morphed face image which is encoded with a secret message is sent to the receiver. The receiver uses powerful and robust deep learning models to recover the secret message by recognizing the parents of the morphed face images. Furthermore, we design two novel Convolutional Neural Network (CNN) architectures (e.g. MFR-Net V1 and MFR-Net V2) to perform morphed face recognition and achieved the highest accuracy compared with existing networks. Additionally, the experimental results show that the proposed schema has higher retrieval capacity and accuracy and it provides better robustness.

Keywords: Data hiding, Steganography, Deep learning, Morphed face recognition, Information security

1 Introduction

The significant advances of internet and multimedia technology have promoted large amounts of digital message acquisition, processing, and transmission on public channels in recent years. In particular, most of these messages transferred on public channels are secret and sensitive, and they are very fragile at being damaged and counterfeited by intentional attacks. Thus, an essential issue to be considered is to ensure the security of messages in covert transmissions. A traditional method to protect secret message is cryptography [1, 2] in which the sender encrypts the messages with a specified key and then delivers them to the intended receiver. The receiver can retrieve the original messages after decryption. Nevertheless, it is just very time-consuming to perform the processes of encryption and decryption due to the complicated cryptographic algorithms that are used. To remedy the weakness of cryptography, data hiding has been put forward and emerged as a dominating method for message protection.

Data hiding (steganography) is referred to as a technique that embeds secret messages into a trustable cover carrier, such as text, image, audio, and video, for secure information conveying [3–10] and digital forensics [10, 11]. Given that image is the most extensively utilized cover carrier, researches on image data hiding is flourishing. In contrast with cryptography, the messages concealed in the image can be imperceptibly delivered to the receiver, greatly reducing the suspicion raised by malicious attackers. Unfortunately, some image distortions are inevitably introduced by embedding secret messages [5, 6]. Thus, the most important task must be to diminish these distortions as far as possible for avoiding the awareness of the existence of hidden messages. Therefore, visual quality and embedding capacity are considered as key performance indicators for image data hiding [4]. Visual quality is defined as the distortions to the cover image after embedding, while embedding capacity indicates the total amount of data embedded in the cover image. Ideally, good visual quality and embedding capacity are expected to be achieved simultaneously. However, these two factors can inversely affect each other, that is, increasing the visual quality would incur some decrease in embedding capacity.

Without loss of generality, conventional image data hiding falls into three categories, i.e., the methods for the spatial domain, for the transformed domain, and the compression domain [3, 12]. The spatial domain-based method is probably the most intuitive of data hiding options that straightly embed secret messages into pixel values of the original cover image. Some popular kinds of data hiding algorithms in the spatial domain are the least significant bit (LSB) [4, 13], prediction error [5], histogram-based approaches [7], secret sharing method [14], modulo operation [8, 9], and quantization-based methods [15]. Generally speaking, the spatial domain has a higher embedding capacity. However, it has some drawbacks such as it generates visual distortion and has insufficient robustness. On the other hand, scholars introduced the transform domain method to embed the secret message by changing the transform coefficients so as to improve the robustness. There are several transform domain methods which include Discrete Wavelet Transform (DWT) [16–18], Discrete Fourier Transform (DFT) [19, 20], and Discrete Cosine Transform (DCT) [21, 22]. In the compressed domain-based information hiding method, cover objects are mainly stored in compressed forms, for example, joint photographic experts' group (JPEG), search ordering coding (SOC), and vector quantization (VQ). Furthermore, the compressed domain method joins the compression and information hiding processes, and it adequately restricts the perceptual coding attacks [12, 23].

The objective of this research is to hide the secret message using a morphed face and the technique of face recognition. Face morphing is defined as a process to transfer one face to another as shown in Fig. 1. Given two images of different person faces (as the source and target face image in Fig. 1), it produces intermediate images or faces which is called a morphed face.

The main contributions of this paper are summarized as follows:

1. We proposed a novel and efficient data hiding method to embed a secret message into a morphed face image. An encrypted secret message is sent to the designated receiver. The receiver needs to do morphed face recognition to decrypt the parent ID

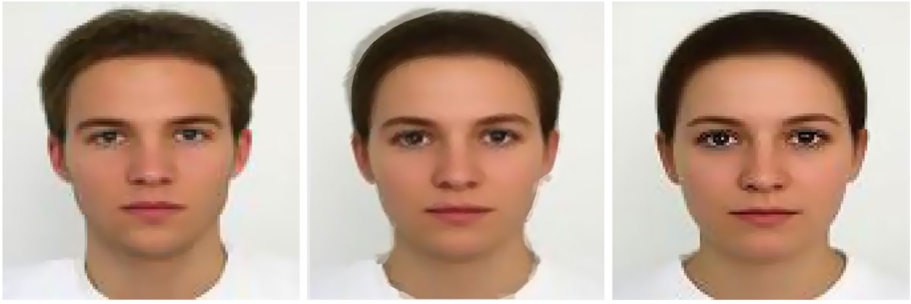

Fig. 1 Face morphing. left: source face image. middle: morphed face. right: target face image

of the morphed face. Based on correspondence between decoded parent ID and the secret message table, s/he can further decode the embedded secret message.

2. A face morphing technique was presented to produce a large amount of morphed face images from a relatively small-scale face image dataset. This greatly contributes to reduce the size of image dataset compared to other coverless information hiding schemes.
3. We proposed two new CNN architectures named MFR-Net V1 and MFR-Net V2 to achieve highly accurate morphed face recognition.
4. Additionally, the experimental results show that the proposed schema has higher retrieval capacity and accuracy and it provides better robustness.

The rest of this paper is organized as follows: Sect. 2 introduces the related works. The proposed data hiding scheme and face morphing recognition are depicted in Sect. 3. Experimental results and analysis are provided in Sect. 4. Finally, the conclusion is drawn in Sect. 5.

2 Related work

As we know that the traditional data hiding scheme leaves a modification trace on the cover image, causing some distortion in the stego-image so that it makes successful steganalysis possible. Therefore, many coverless data hiding approaches have been proposed in recent years to address this issue, where the secret message can be hidden without any modification on the cover image.

In 2012, a novel cover selection-based data hiding scheme was proposed by Fridrich and Kodovsky [24]. In their scheme, an image is directly selected from the image dataset according to the secret message and transmitted to the receiver to implement the secret message transmission. Subsequently, the data hiding schemes based on cover selection were presented by Sun et al. [25], Chen et al. [26], and Zhou et al. [27]. For a given secret message, the image of which the binary bits of hash value equal to the binary bits of the secret message is selected and transmitted. At the recipient side, we can easily extract the secret message from the received image by the same hash operation.

Additionally, other related studies [3, 28–36] aim to hide the secret message by constructing the mapping relationships between the cover image and the secret message. In Zhou et al.'s scheme [28], the visual words are firstly extracted from each image using a BOW model, and then a mapping relationship between the secret messages and the image visual words is established. In Yuan et al.'s scheme [29] and Zhou et al.'s scheme [30], the feature sequences are generated by using the special feature-based hashing algorithm. Then, a mapping relationship between the robust feature hash sequences and the secret messages is constructed. So, we can transmit natural images, whose features are the same as the secret information to receivers. For Zhang et al.'s scheme [3], images are classified into several topics using the latent Dirichlet allocation topic model. For images in each topic, the robust feature sequence is generated based on the relationship of DCT coefficients. Finally, an inverted index that contains the feature sequence, location coordinates, and image path is created. To achieve secret transmission, the image whose feature sequence equals to a secret message is chosen as the cover image according to the index.

In 2018, Zhou et al. [31] proposed a novel coverless data hiding scheme based on partial-duplicate image retrieval for transmitting a secret color image, without any modification on the cover image. In 2019, a visual vocabulary tree-based partial-duplicate image retrieval for coverless image steganography was presented by Mu and Zhou [33]. In their scheme, a set of duplicates of a given secret image is used as stego-images, and each of those stego-images shares one similar image patch with the secret image. The same year, Zou et al. [32] proposed a novel coverless data hiding scheme based on the average pixel values of sub-images to address the problem of the lower hiding capacity. Inspired by [3], in 2020, Liu et al. [34] proposed a coverless data hiding scheme based on image retrieval DenseNet features and DWT sequence mapping. The main difference is that the robust feature sequence is generated by the joint use of the DenseNet model and DWT of sub-images. Also, Luo et al. [35] proposed another coverless data hiding scheme based on the image block-matching and DenseNet model. In 2020, to improve the hiding capacity, a novel coverless data hiding scheme based on the Most Significant Bit (MSB) technique was proposed by Yang et al. [36]. In [36], the cover image is divided into several image fragments and the average intensity of each fragment is calculated. Then, a one-to-one mapping between the MSB of the image fragments and the secret message is established and served to secret transmission. In 2021, Lu et al. [37] proposed a coverless information hiding method based on constructing a complete grouped basis with unsupervised learning, and the base image of the complete grouped basis is used to map the secret message for obtaining coverless information hiding. Also, Abdulsattar's scheme explored the effectiveness of coverless information hiding using only one cover image to transmit secret information based on eigen decomposition, and performed coverless information hiding by establishing mapping relationships between the hash codes of the image blocks and the characters of the secret message. As a result, their scheme achieves a considerable hiding capacity. However, its weakness is that it is difficult to maintain the quality of stego-image.

Most existing coverless data hiding scheme can resist the steganalysis or achieve a considerable hiding capacity. However, generally speaking, the number of natural images that is required to represent the secret message is 2^n if we want to conceal n-bit secret messages into an image. The number of images increases exponentially with the length of the secret message, which makes those approaches impractical. This paper proposes a secret message transmission scheme based on morphed face recognition. Firstly, a large number of the morphed face image are automatically generated from a small-scale face image dataset. Followingly, a mapping relationship between the morphed face images and the secret messages is constructed to serve for data hiding. At the recipient side, our approach can accurately recover the secret image from the morphed face image using the proposed morphed face recognizer based on our proposed CNN model.

3 Proposed data hiding method

In this section, we present the process of our proposed data hiding and extraction scheme. The flowchart of our approach is shown in Fig. 2.

In our proposed data hiding scheme, we collect a lot of images from the internet to construct a face dataset. Let us assume that this dataset has N images and those images are sorted with any pre-defined rule, such as sorting by the alpha-numeric order of the last names. By randomly picking two faces to form a pair, the total number of pair that can be formed is $N(N+1)/2$ (assuming the two faces in a pair can be the same identity). By applying the proposed face morphing technique (which will be described in detail in Sect. 3.1) to any pair, a morphed face can be synthesized. Therefore, a set of morphed faces (the number of which is $N(N+1)/2$) can be generated, and the specific order for each morphed face is recorded as well. Followingly, a mapping relationship between the morphed face images and the secret messages is constructed to serve for data hiding. Specifically, the se_i-th morphed face image is used to carry secret digit se_i. During the process of data hiding, the morphed face image is firstly selected according to the secret digit and then transmitted through the internet such that the secret digit se_i has been imperceptibly carried. Among them, the secret digit se_i is the encryption version of the secret message s_i. It is also worth noting that, the dataset and its sorting rule should be shared in advance for both the sender and recipient.

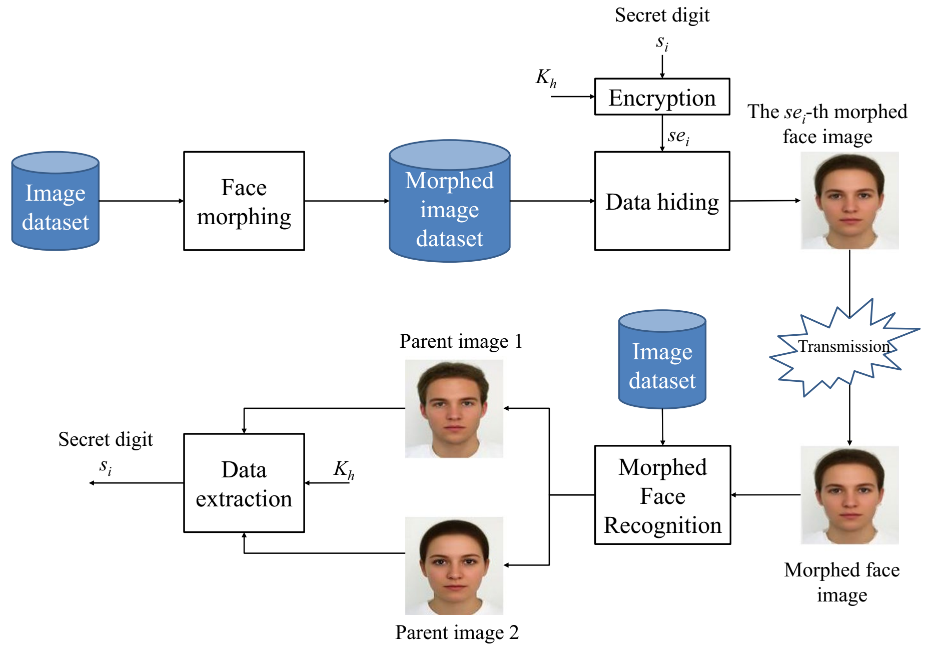

Fig. 2 Flowchart of our approach for secret message transmission

When the recipient receives the morphed face image, it can extract the secret digit with error-free. Firstly, the recipient feeds the morphed face image into the morphed face recognizer, which decodes (recognizes) the two corresponding parent identity. Then, the mapping relationship can be reconstructed using the pre-shared image dataset and sort rule. After that, according to those parent identities, the order number of the morphed face image can be decoded according to the pre-shared sorting rule. As a result, the secret digit se_i is determined and further decrypted as s_i using encryption key K_h.

3.1 Face morphing technique

In this paper, face morphing is defined as a process to generate a sequence of transitional images from a source face image and a target face image, making that the morphed face image implicitly has the similar appearance from both parent images. The overall flow of the proposed face morphing algorithm is given in Fig. 3. Firstly, several landmarks are selected both in the source face image and the target image. Using the selected landmarks, the relationship between the source face image and the target face image is constructed. According to this relationship, the source face image and the target face image are warped and then further combined to generate the required morphed face images. Details are shown as below.

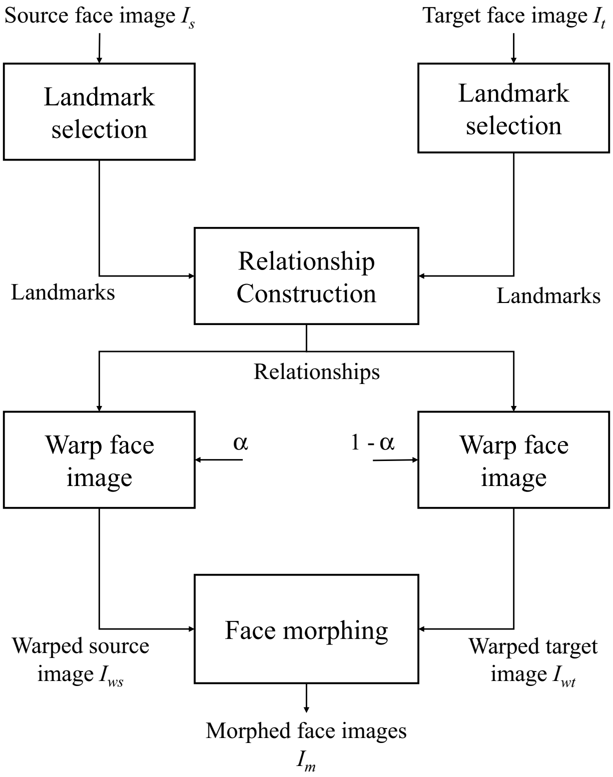

Fig. 3 The overall flowchart of the proposed face morphing algorithm

3.1.1 Landmark selection

The coordinates of the landmarks decide where to warp the source face image and the target face image. Also, it is crucial for achieving a good visual quality of the morphed images. Thus, the selection of the landmarks should be good enough to represent the features of the source face image and the target face image. For example, the landmarks should be located on the edge of the eyes, nose, mouth, and facial contour, etc. Among them, Supervised Descent Method (SDM) algorithm [38, 39], which has achieved impressive performance for the face alignment tasks, is employed to detect facial features for the purpose of precise features localization. Figure 4 shows the flowchart of landmark selection. The process of this algorithm is described as follows:

Step 1: **Facial landmarks selection**

Firstly, using SDM algorithm, several landmarks located on face contour, eye, eyebrow, pupil, nose, and mouth, are automatically selected. Moreover, it is worth mentioning that, some auxiliary interpolation landmarks are calculated and added as the facial features compared to the landmark selection in basic SDM, in order to make the face image wrapping more accurate and smoother. As we can see from Fig. 4a, the result of facial features selection for the image I_s is illustrated as I_{s1}, where there are 92 landmarks in total on the face region.

Step 2: **Edge landmarks selection**

Inspired by the idea of Mao et al.'s scheme [40], we first detect the edge outline of the image I_s using the Canny operator, as shown in Fig. 4b. Take the point on the tip of the nose which has been located during **Step 1** as the origin of the axis and two axes can be determined. Then, the landmarks located on the edge outline is selected by the following procedure:

Step 2–1: Find the topmost point and the bottom-most point, for which the x-coordinates are E_{top} and E_{bottom}, respectively.

Step 2–2: For each row from E_{top} to E_{bottom}, search the edge point from right to the center axis and determine the first edge point in each row as the candidate point on the right part of the face outline. Similarly, search the edge point from left to the center axis and determine the first edge point in each row as the candidate point on the left part of the face outline.

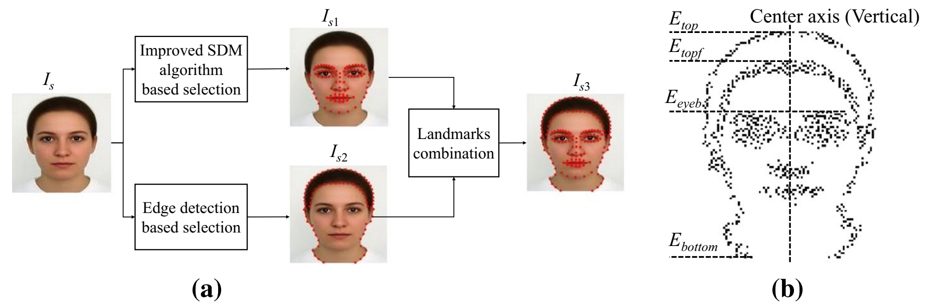

Fig. 4 The algorithm of landmark selection. **a** Lankmarks combinations; **b** edge outline of the image

Step 2–3: Find the topmost point of the forehead region near the vertical axis, for which the x-coordinates are E_{topf}. According to the landmarks on the eyebrow marked in I_{s1}, we find the top point of the eyebrow, for which the x-coordinates are E_{eyeb}.

Step 2–4: For each row from E_{topf} to E_{eyeb}, find the edge point from the center axis to its right and consider the first edge point in each row as the candidate point on the right part of the forehead region. Find the edge point from the center axis to its left and consider the first edge point in each row as the candidate point on the left part of the forehead region.

Step 2–5: Among the aforementioned candidate points, select 72 points in total as the final landmarks on the edge outline. Therein, there are 53 landmarks distributed on the face outline and others are for the forehead region. The result of edge landmarks selection for the image I_{s} is illustrated as I_{s2}.

Step 3: Combine the landmarks on I_{s1} and I_{s2}, to derive the final version of landmarks, i.e., I_{s3}. Note that, the 8 landmarks located on the cheek region provided by I_{s1} are employed in our experiments, rather than those of I_{s2}.

3.1.2 Relationship construction

After the landmarks of the images I_{s} and I_{t} have been prepared, the projection relationship between the coordinates of the landmarks of the I_{s} (or I_{t}) and those of the warped image I_{ws} (or I_{wt}) is constructed. Here, let us assume the coordinates of the landmarks of the image I_{s} and I_{t} are C_{s} and C_{t}, respectively. The matrices C_{s} and C_{t} are sized $K \times 2$, where Ks the quantity of the selected landmarks. Hence, the coordinates of the landmarks in the wrapped face image can be determined as

$$C_{\mathrm{w}} = \alpha C_{\mathrm{s}} + (1 - \alpha) C_{\mathrm{t}}, \tag{1}$$

where α is the morphing ratio, which represents the contribution percentage of the source face image for synthesizing the warped face image. Correspondingly, the contribution percentage of the target face image is $(1 - \alpha$.

Based on the determined landmarks (e.g., C_{w}, C_{s}, C_{t}), some triangle areas are constructed without overlapping. An example of constructing triangle areas is given in Fig. 5. As we can see, each triangle area includes three pairs of coordinates of the landmarks. Taking the I_{s} and I_{ws} as an example, the relationship of coordinates of landmarks is constructed as follows:

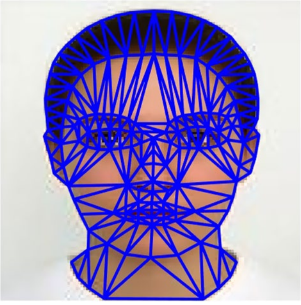

Fig. 5 An example of constructing triangle areas using landmark set

Step 1: Construct the triangle areas on I_s and denoted as TR_s, construct the triangle areas on $I_{ws,}$ and denoted as TR_{ws}.

Step 2: Take a triangle area from TR_s and TR_{ws}. Calculate the differences by

$$dif = \mathrm{TR}_\mathrm{s}(1,:) - \mathrm{TR}_{ws}(1,:). \tag{2}$$

Step 3: According to the differences, coordinate alignment of TR_s is performed by

$$\mathrm{TR}_\mathrm{s}^{'} = \mathrm{TR}_\mathrm{s} - dif. \tag{3}$$

Step 4: Construct the relationship of coordinates of pixels with the triangle area. For each coordinate ($\mathrm{TR}_{ws}(x)$, $\mathrm{TR}_{ws}(y)$), its projected coordinate ($\mathrm{TR'}_{ws}(x)$, $\mathrm{TR'}_{ws}(y)$) can be projected as

$$\left(\mathrm{TR}_{ws}^{'}(x),\mathrm{TR}_{ws}^{'}(y)\right)=\left(\mathrm{TR}_{s}^{'}\left(x^{'}\right),\mathrm{TR}_{s}^{'}\left(y^{'}\right)\right)\Bigg|argmin\left(\left(\mathrm{TR}_{ws}(x)-\mathrm{TR}_{s}^{'}\left(x^{'}\right)\right)^{2}+\left(\mathrm{TR}_{ws}(y)-\mathrm{TR}_{s}^{'}\left(y^{'}\right)\right)^{2}\right)+dif. \tag{4}$$

where ($\mathrm{TR}_\mathrm{s}{}'(x')$, $\mathrm{TR}_\mathrm{s}{}'(y')$) represents the coordinate of the pixel which locates inside the triangle area TRs.

Step 5: Perform Steps 2 to 4 until all triangle areas have been processed.

Finally, we can obtain the $\mathrm{TR}_\mathrm{ws}{}'$. It means that, in the morphing phase, the pixel values in I_s ($\mathrm{TR}_\mathrm{ws}{}'(x)$, $\mathrm{TR}_{ws}{}'(y)$) will be filled into the pixel values in I_{ws} ($\mathrm{TR}_{ws}(x)$, $\mathrm{TR}_\mathrm{ws}(y)$). In the same way, we can also construct the projection relationship between the coordinates of the landmarks of the I_t and those of the warped image I_{wt}. The result is represented as $\mathrm{TR}_{wt}{}'$, which indicates that the pixel values in I_t ($\mathrm{TR}_{wt}{}'(x)$, $\mathrm{TR}_\mathrm{wt}{}'(y)$) will be filled into the pixel values in I_{wt} ($\mathrm{TR}_{wt}(x)$, $\mathrm{TR}_\mathrm{wt}(y)$).

3.1.3 Face morphing

After the relationship construction, the set of $\mathrm{TR}_\mathrm{ws}{}'$ and $\mathrm{TR}_\mathrm{wt}{}'$ are obtained. Thus, the warped face images I_{ws} and I_{wt} are performed by

$$I_{ws}\left(\mathrm{TR}_{ws}(x),\mathrm{TR}_{ws}(y)\right)=I_{s}\left(\mathrm{TR}_{ws}^{'}(x),\mathrm{TR}_{ws}^{'}(y)\right), \tag{5}$$

$$I_{wt}\left(TR_{wt}(x),\mathrm{TR}_{wt}(y)\right)=I_{t}\left(TR_{wt}^{'}(x),\mathrm{TR}_{wt}^{'}(y)\right). \tag{6}$$

Finally, the morphed image is derived using Eq. (7).

$$I_m(x,y)=\alpha I_{ws}(x,y)+(1-\alpha)I_{wt}(x,y), \tag{7}$$

where $I_m(x,y)$ represents the pixel value of the coordinate (x, y) in the morphed image. An illustration of the morphed image set is given in Fig. 6, where α varies from 0.1 to 0.9.

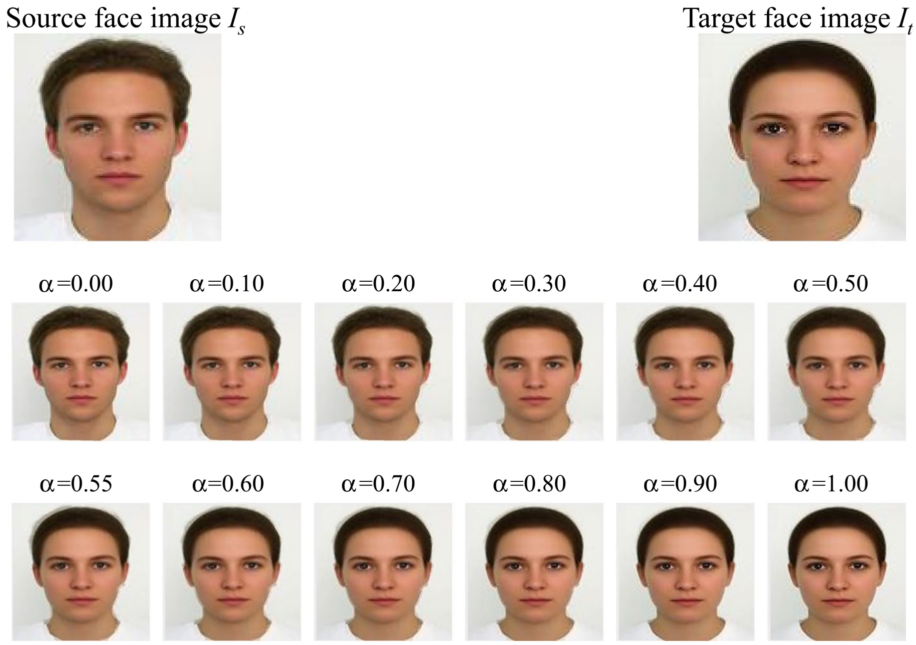

Fig. 6 A set of example images of morphed images under various α

Table 1 MFR-Net V1 network architecture

Type	Output size
Input	224 × 224
Con2D 7 × 7, 64, stride 2 Batch normalization leaky ReLU	112 × 112
Max pool, 3 × 3, stride 2	56 × 56
(Residual block, 64) × 3	
(Residual block, 128) × 4	28 × 28
(Residual block, 256) × 6	14 × 14
(Residual block, 512) × 3	7 × 7
Global average pool	512
FC L2 norm, 300-d	300
Softmax	

3.2 Face morphing recognition

In this section, we presented our proposed MFR-Net network to perform the morphed face recognition. Furthermore, we also conduct a comparison between the proposed network and other well-known deep learning networks.

3.2.1 MFR-Net V1

The details of the proposed MFR-Net V1 network are presented in Table 1 and the architecture diagram is shown in Fig. 7. In this paper, we constructed two smaller networks: one for identifying parent image 1, and the other for identifying parent image 2. At the end, we combine these two networks into one big model that is called MFR-Net V1.

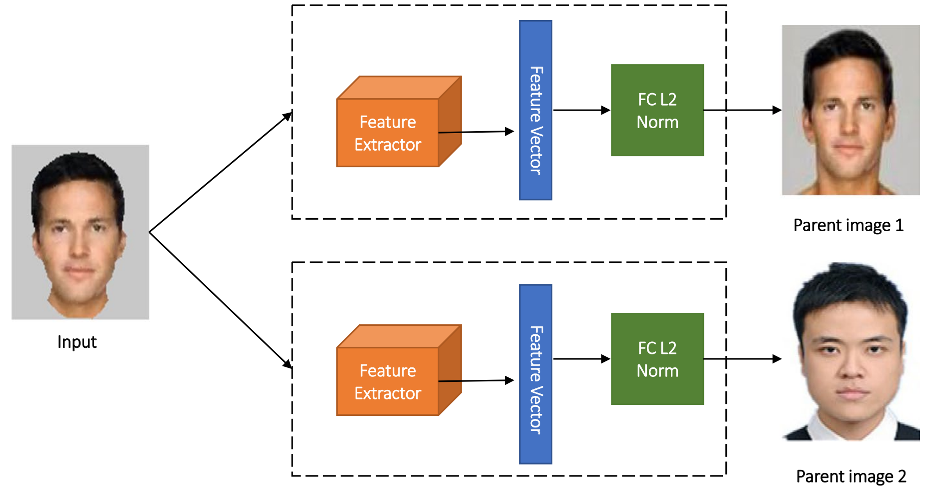

Fig. 7 MFR-Net V1 architecture diagram

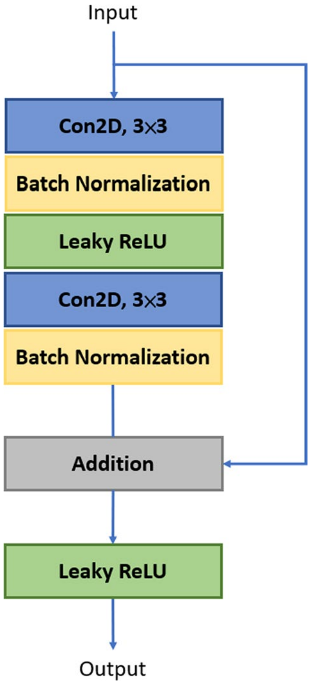

Fig. 8 Residual block

MFR-Net V1 adopted the idea of shortcut connection in ResNet [41] and uses the Residual Block (shown in Fig. 8) as the backbone of the network model.

$$\mathrm{FC}_{L2Nrom} = W_j^T x_i = \|W_j^T\|_2 \|x_i\|_2 \cos\theta_j \quad (8)$$

As shown in Eq. 8, in the fully connected layer, we performed the inner product between the weights and the feature of the image, which is equivalent to taking the product of the L2-Norm of the weights, the feature vectors and the cosθ where θ is the angle

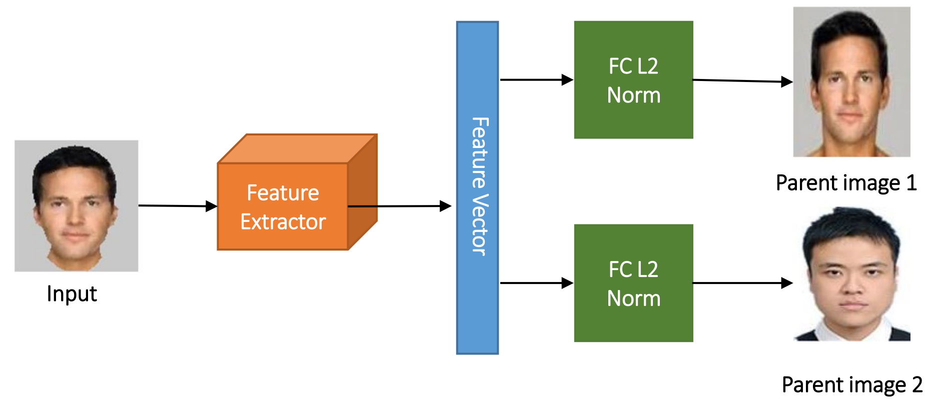

Fig. 9 MFR-Net V2 architecture diagram

Table 2 MFR-Net V2 Network architecture

Type		Output size
Input		224 × 224
Con2D 7 × 7, 64, stride 2 Batch Normalization Leaky ReLU		112 × 112
Max pool, 3 × 3, stride 2		56 × 56
(Residual block, 64) × 3		
(Residual block, 128) × 4		28 × 28
(Residual block, 256) × 6		14 × 14
(Residual block, 512) × 3		7 × 7
Global average pool		512
FC L2 norm, 300-d	FC L2 norm, 300-d	300
Softmax		

between feature vector and weights. Then rescale according to the first S, and then use Softmax as the final output.

$$ArcFaceLoss = -\frac{1}{N}\sum_{i=1}^{N}\log\frac{e^{s\cos(\theta_{y_i}+m)}}{e^{s\cos(\theta_{y_i}+m)}+\sum_{j=1,j\neq i}^{n}e^{s\cos\theta_j}}. \tag{9}$$

In this paper, during network training, we adopted the idea of ArcFace Loss [42] as the objective function of network training. As shown in Eq. 9. ArcFace Loss can simultaneously enhance the intra-class compactness and inter-class discrepancy.

3.2.2 MFR-Net V2

In the subsequent experimental stage, we first use MFR-Net V1 to identify the two sources of Morphed Face, and after getting good experimental results, based on MFR-Net V1, we

Table 3 MFR-Net V1 test results for α values

α	Parent image 1	Parent image 2	Total
Test accuracy (%)			
0.2	100	99.9977	99.9977
0.4	100	100	100
0.6	100	100	100
0.8	100	100	100

Table 4 Test results of MFR-Net V1 with α between 0.45–0.55 (excluding 0.5)

α	Parent image 1	Parent image 2	Total
Test accuracy (%)			
0.45	100	100	100
0.46	100	100	100
0.47	100	100	100
0.48	100	100	100
0.49	100	100	100
0.51	100	100	100
0.52	100	100	100
0.53	100	100	100
0.54	100	100	100
0.55	100	100	100

propose a new network architecture MFR-Net V2, which is a simplified and reduced version. As shown in Fig. 9 and Table 2, this network uses single feature extractor to extract face features and sent them into two fully connected layers, one for recognizing parent one and another for parent two. In this way, the complexity of the network is greatly reduced, and the recognition speed is twice as fast as the previous version of MFR-Net V1 without decreasing accuracy.

4 Results and discussion

4.1 Morphed face dataset

In this paper, we used 300 face images as our source dataset. A morphed face is generated by randomly selecting two face images from the source dataset. Since we allow two parent images to be the same, finally, a total number of 45,150 (300,299/2 + 300) morphed faces were generated. Also, we use a parameter α to adjust the appearance of the generated morphed face to parent image 1 or parent image 2, which allows the sender to arbitrarily select the value of α in the application to generate a morphed face with a different appearance. The receiver uses the proposed deep learning network model for identification and then decode the secret message. In terms of number of images in the dataset, 225,750 images with $\alpha \in \{0.1, 0.3, 0.5, 0.7, 0.9\}$ are used as training data, and 180,600 images with $\alpha \in \{0.2, 0.4, 0.6, 0.8\}$ are used as test data.

Table 5 MFR-Net V2 test results

Loss function	Test accuracy (%)
ArcFace [42]	**100**
SphereFace [44]	99.9996
CosFace [45]	99.9999
Combined margin	**100**
Softmax Loss	0.0001

Bold indicates best result

Table 6 Various feature extractor test results

Feature extractor	Test accuracy (%)	FPS
MFR-Net V2	**100**	327
VGG16 [46]	0.00001	306
MobileNet V2 [47]	0.0013	**415**
DenseNet121 [48]	93.02	290
InceptionResNetV2 [49]	96.85	258

Bold indicates best result

4.1.1 Training parameter fine-tuning

The image size is of 224 × 224, and the network is trained with 8 Titan X Pascal GPU cards with a learning rate of 0.1 and batch size 128. We applied Adam [43] as the optimizer, with $m = 0.5$ and $s = 64$ (similar as the parameters in [42]). In this study, we used two identical CNN models to identify parent image 1 and parent image 2 of the morphed face and trained 100 epochs and 200 epochs, respectively. The experimental results are shown in Table 3.

As shown in Table 4, we additionally generated and identified the morphed face with α between 0.45 and 0.55. We obtained the perfect results and the identification speed reach 190 FPS with GPU acceleration of a single Titan X Pascal. This shows that it is feasible to use the proposed steganography scheme for information encryption, and the decryption process is highly efficient and perfectly accurate, which demonstrates its robustness and practicability.

We also performed experiments to compare accuracy when using different loss functions. Several state-of-the-art loss functions which were proposed in the field of face recognition, such as SphereFace (margin is set to 1.35), CosFace (margin is set to 0.35), ArcFace (margin is set to 0.5), and combined margin with the three (in the order of the former margin is set to 1, 0.2 and 0.3 in sequence), are tested. The results are shown in Table 5. According to the results, all loss functions can help us to achieve the perfect results except for Softmax Loss. The training data used in this experiment is the same as the former MFR-Net V1, which uses 225,750 images (when $\alpha \in \{0.1, 0.3, 0.5, 0.7, 0.9\}$) as training data, and the remaining 632,100 morphed images (when $\alpha \in \{0.2, 0.4, 0.45, 0.46, 0.47, 0.48, 0.49, 0.51, 0.52, 0.53, 0.54, 0.55, 0.6, 0.8\}$) as test data.

We also performed experiments to compare the proposed MFR-Net V2 with a variety of state-of-the-art object recognition networks as the backbone of feature extraction. In this experiment, the combined margin is adopted as the loss function. And the accuracy and speed of various networks are recorded. The results are shown in Table 6. According to the experimental results, the MobileNet V2 network has the fastest speed (but with incredibly low accuracy), and our proposed MFR-Net V2 network achieved the highest accuracy with satisfactory speed.

4.2 Hiding capacity analysis

In most existing schemes, the secret messages are directly mapped to the feature sequence of the image, thus, the length of the feature sequence is proportional to the hiding capacity. The larger the hiding capacity is, the more carrier images are needed.

Table 7 shows a comparison among schemes [3, 27, 29, 32, 34, 35] and proposed scheme. In schemes [27, 29], the hiding capacity is directly determined by the length of the feature sequence, resulting in a hiding capacity of 8 bits in their experiments. Schemes [3, 34] achieve the hiding capacity up to 15 bits when they do not consider to divide the image into blocks for capacity. For schemes [3, 34], the priori knowledge with regard to the mapping relationship between the features and secret messages have to be shared between the sender and decoder. Also, the size of the image dataset in schemes [3, 34] is larger than that in schemes [27, 29]. It is worth mentioning that, the higher hiding capacity can be achieved when image division is employed, such as schemes [32, 35, 37]. As we can see in Table 7, scheme [37] obtains the hiding capacity with a value of 16 bits. Among which, the image dataset has to be shared in advance, which is the same as the proposed scheme. As to scheme [32], it provides a high capacity up to 80 bits, and a Chinese dictionary with a size of N × 80 should be shared in advance, where N is the number of images. Its hiding success rate is seriously influenced by the value of N. Although their experiments attempt to prove that the hiding success rate is close to 1 when N is around 1,000,000, theoretically

Table 7 Comparisons with the state-of-the-art on hiding capacity under different priori knowledge and dataset size

Schemes	Size of dataset	Hiding capacity (bits)	Priori knowledge
Zhou et al.'s scheme [27]	$2^8 = 256$	8	None
Yuan et al.'s scheme [29]	$2^8 = 256$	8	None
Zhang et al.'s scheme [3]	2^{15}	15 (without image division)	Mapping relationship
Zou et al.'s scheme [32]	100,000 (hide success rate $\approx$ 1)	80	Chinese dictionary
Liu et al.'s scheme [34]	2^{15}	15 (without image division)	Mapping relationship
Lu et al.'s scheme [37]	2^{16}	16	Image dataset
Luo et al.'s scheme [35]	1	2601	A mapping sequence and a mapping flag; the size of image and image fragments
Abdulsattar's scheme [50]	1	6272	A loop-up table including the location information
Proposed scheme	2^8	15	Image dataset
	300	15	
	2^{15}	29	
	100,000	32	

speaking, to achieve the hiding success rate of 100%, the number of images N should not be less than 2^{80}. For scheme [35], it provides the hiding capacity of 2601 bits when the image size is set to 256×256 and the image fragment is sized 5×5. For scheme [50], it achieves the highest hiding capacity up to 6272 bits when the image size is 512×512 and image block size is set to 18×18. Among these, the mapping sequence and mapping flags have to be sent to the receiver along with the secret image. Unfortunately, the mapping sequence and mapping flag have a strong correlation with the secret message, which makes this approach impractical.

Our proposed scheme sent the morphed face image, which contained a secret digit, to the recipient. Due to a larger number of the morphed face images can be generated from a small-scale image dataset, thus, a relatively high capacity is provided by our approach compared to schemes in [3, 27, 29, 34]. For instance, if the number of images in a dataset is $N = 2^8$, thus, we can generate $N(N+1)\ /2 = 2^8(2^8+1)/2$ distinct morphed images in total using our proposed face morphing technique. For this, in our approach, each morphed image can carry around $\log_2(2^8(2^8+1)/2) \approx 15$ bits secret message, which is greater than the results provided by schemes in [27, 29]. Of course, when N is 2^{15}, our approach can carry around $\log_2(2^{15}(2^{15}+1)/2) \approx 29$ bits secret message, which are 14 bits higher than that of the scheme [3]. Certainly, to implement aforementioned hiding capacity, the small-scale image dataset should be shared between the sender and decoder so that the recipient can successfully decode the secret messages by recognizing the parents of the morphed face images. Also, we can observe that the hiding capacity of the proposed scheme is lower than that of schemes in [32, 35]. That is because those two schemes divide the cover image into several sub-images to generate a series of feature sequences so that more secret messages can

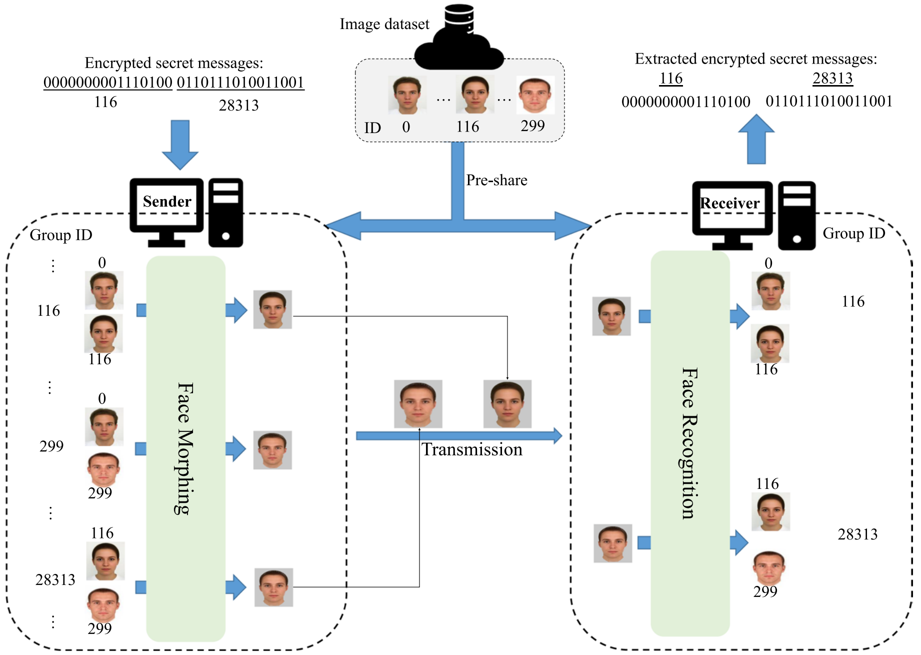

Fig. 10 An example of proposed data hiding scheme. Illustration of the overall process of secret messages embedding, sending, receiving and extraction using the proposed method

be represented. However, more auxiliary information and a larger-scale image dataset are required in their schemes, which limits their applications. In summary, our approach achieves a high hiding capacity while keeping a small-scale image dataset.

4.3 Feasibility and practicability analysis

In this subsection, we first analyze the feasibility of our findings, including face morphing, morphed face recognition and steganography. In the end, we give a study case to further validate the practicability of our findings, as shown in Fig. 10. Details are described as follows:

> *Feasibility in face morphing* In our findings, all possible paired face images are morphed into morphed face images and an expanded experimental dataset is synthesized, which contains as many as $N^{*}(N+1)/2$ morphed face images. To achieve usable morphed face images, several face landmarks should be localized and every face region should be aligned. Obviously, it is well known that the researches from both areas (the face landmark localization [51, 52] and face alignment [38, 53] technologies) have been developed well and deployed in many practical applications, such as Google and Baidu. Not only that, our experimental results also showed the feasibility of our proposed face morphing to make service.
>
> *Precision in morphed face recognition* Firstly, face recognition [44, 54] is a relatively mature research field in the computer vision community. However, the goal of the face recognition in this study is to recognize the identities of both parents from the input morphed face, which is completely different than the traditional face recognition task. To this end, two novel CNN architectures, including MFR-Net V1 and MFR-Net V2, are designed to perform morphed face recognition and achieved the highest accuracy compared with existing networks (See Tables 3, 4, 5, 6).
>
> *Invisibility in steganography* In the aspect of steganography, in this paper, the secret message is encoded with both parent IDs of the morphed face image, instead of modification on any part of the image content itself in spatial or frequency domain. Therefore, steganalysis (e.g., statistical analysis on holistic or partial image) is not applicable to the proposed method. In other words, the proposed method can easily pass any qualitative criteria based on steganalysis. Moreover, the morphed face image can effectively conceal the key feature of its parents while maintaining its usage performance, especially in terms of the harmony and recognizability of the morphed face.
>
> *Case study* To validate the practicability of our findings, we visualized a practical case study to demonstrate the process of secret messages embedding and extraction by the proposed method, as shown in Fig. 10. In Fig. 10, we observed that an image dataset which includes 300 face images with pre-defined IDs should be pre-shared between the sender and receiver. At the sender's side, every two face images from the dataset are paired to form a morphed face image in turn, and then each morphed face image along with its parents is associated with a distinct group ID. For example, the two images whose IDs are 116 and 299 are morphed, and its corresponding group ID is 28313. When the sender wants to transmit the encrypted secret messages '000000000111010001101110100110 01' (11628313 in decimal), the morphed

face images whose corresponding group IDs equal 116 and 28313 are selected and transmitted to the receiver. At the receiver's side, when s/he receives the first morphed face image, its parents can be identified by the proposed CNN model, retrieving the parents' IDs of 0 and 116. Consequently, the receiver can derive the group ID 116, and then the encrypted secret message '0000000001110100' is decrypted correctly. As to the second morphed face image, after the parents' IDs (i.e., 116 and 299) are identified, the encrypted secret message can be decrypted as '0110111010011001'. Following the similar procedure, all secret messages can be encrypted, sent, received and decrypted without any error.

4.4 Features comparisons

To better explain the difference between our findings and the previously published works, we also compared various features among our approach and other existing steganography schemes [3, 5, 6, 9, 27, 29, 33, 34]. Details are analyzed as follows.

Comparison to the traditional steganography schemes: generally, most of the traditional steganography schemes discussed in literature either exploit the spatial domain or frequency domain to hide the secret messages. Those schemes can achieve high hiding capacity. However, due to the modification to the raw pixel values, a few distortions may be introduced in the stego-images, making them difficult to resist statistical steganalysis. On the contrast, our approach encodes the secret message with both parent IDs of the morphed face image, instead of modification to any part of the image content. Therefore, our approach is robust to resist statistical steganalysis.

Table 8 Comparisons of features among different schemes

Schemes	Coverless	Methodology	Capacity	Scalability in dataset	Resist steganalysis
Chang et al.'s scheme [6]	No	Pixels value modification	Very high	None	Difficult
Wang et al.'s scheme [5]		Pixels value modification	Very high	None	Difficult
Chang et al.'s scheme [9]		Pixels value modification	Very high	None	Difficult
Zhou et al.'s Scheme [27]	Yes	Feature based mapping (Hash)	Low ($\log_2 N$)	No	Easy
Yuan et al.'s Scheme [29]		Feature based mapping (Hash)	Low ($\log_2 N$)	No	Easy
Zhang et al.'s Scheme [3]		Feature based mapping (DCT)	Low ($\log_2 N$)	No	Easy
Mu and Zhou's scheme [33]		Feature based mapping	Low	No	Easy
Liu et al.'s scheme [34]		Feature based mapping (DenseNet)	Low ($\log_2 N$)	No	Easy
Proposed scheme		Mapping by morphing and recognition (MFR-Net)	High ($\log_2((N^2+N)/2)$)	Yes	Easy

Comparison to the coverless steganography scheme: as can be seen from Table 8, either our approach or other coverless steganography schemes embed the secret messages by constructing the mapping relation between the secret messages and the images. The difference is that the proposed scheme is able to significantly expand the size of image dataset, whereas other coverless steganography schemes cannot. Therefore, the hiding capacity provided by our approach is a little greater than that of existing schemes [3, 27, 29, 33, 34], when the size of source image dataset is the same.

5 Conclusions

In this paper, we propose a secret message transmission scheme based on morphed face recognition. Thousands of morphed face images are produced from an organized small-scale image dataset and then transmitted to the recipient, thereby performing secret message transmission. At the recipient's side, the secret message is retrieved by decoding the morphed face using the morphed face recognizer. In the morphed face recognition, we design our own CNN architecture MFR-Net based on deep learning as a backbone to extract the features as well as for identification and information decryption. The experimental results and analysis demonstrate that the proposed schema has relatively high embedding secret messages capacity. Compared with the existing approaches, our proposed MFR-Net V2 network obtained the highest accuracy rate.

In the future, our research will focus on a more effective scalable strategy for dataset to enhance the hiding capacity in deep learning based coverless steganography schemes, and consider the better representation of secret messages using different types of morphed face images of the same parents. In addition, there is also a room for further improvement in the aspect of parameters-based face morphing and face alignment.

6 Method

In our work, we aim to improve the validity and proficiency of the image data hiding approach. To achieve this goal, we used a face morphing technique to generate a large-scale morphed face images from a relative small-scale face image dataset, which contributes to increasing the capacity in carrying secrets provided by our approach. After that, a morphed face image which is encoded with a secret message is sent to the receiver. Those experimental results are generated using MATLAB software and the small-scale face image dataset consists a group of face images downloaded from Internet.

To recover the secret message and recognizing the parents of the morphed face images, we also design two novel Convolutional Neural Network, i.e., MFR-Net V1 and MFR-Net V2, to perform morphed face recognition. Those experimental results are implemented with Pytorch, and an NVIDIA RTX 3090 GPU is used for acceleration.

Abbreviations

CNN: Convolutional neural network; MFR-Net: Multi-level feature review residual network; MSB: Most significant bit; LSB: Least significant bit; DWT: Discrete wavelet transform; DFT: Discrete Fourier transform; DCT: Discrete cosine transform; JPEG: Joint Photographic Experts' Group; SOC: Search ordering coding; VQ: Vector quantization; SDM: Supervised descent method; ReLU: Rectified linear unit; VGG: Visual geometry group.

Acknowledgements
Not applicable.

Authors' contributions

CCC proposed and developed the new idea of the paper. YHL, GDS and YKL are responsible for carrying out the key design and implementation of the proposed model, preprocessing of the data set. YHL, GDS and YL are responsible for the initialization of the drafted manuscript. MSA and GDS have substantially revised it. All authors approved the submitted version. All authors read and approved the fnal manuscript.

Fundings

This study was conducted with the support of the Ministry of Science and Technology of Taiwan under contract nos. MOST 108-2221-E-008-071.

Availability of data and materials

Not applicable.

Declarations

Competing interests

The authors declare that they have no competing interests.

Author details

[1] AI Research Center, Hon Hai Research Institute, Taipei 114699, Taiwan. [2] Department of Computer Science, University of Warwick, Coventry CV4 7AL, UK. [3] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan.

Received: 18 October 2021 Accepted: 10 March 2022
Published online: 29 March 2022

References

1. W. Diffie, M. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory **22**, 644–654 (1976)
2. O. Dorgham, B. Al-Rahamneh, A. Almomani, M. Al-Hadidi, K.F. Khatatneh, Enhancing the security of exchanging and storing DICOM medical images on the cloud. Int. J. Cloud Appl. Comput. **8**, 154–172 (2018)
3. X. Zhang, F. Peng, M. Long, Robust coverless image steganography based on DCT and LDA topic classification. IEEE Trans. Multimedia **20**, 3223–3238 (2018)
4. W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited. IEEE Trans. Inf. Forensics Secur. **5**, 201–214 (2010)
5. J. Wang, X. Chen, J. Ni, N. Mao, Y. Shi, Multiple histograms based reversible data hiding: framework and realization. IEEE Trans. Circuits Syst. Video Technol. **30**, 2313–3232 (2019)
6. C.C. Chang, Y. Liu, T.S. Nguyen, A novel turtle shell based scheme for data hiding, in *2014 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 89–93 (2014)
7. Z. Li, X. Chen, X. Pan, X. Zeng, Lossless data hiding scheme based on adjacent pixel difference, in *2009 International Conference on Computer Engineering and Technology*, IEEE, pp. 588–592 (2009)
8. C.C. Chang, C.T. Li, Y.Q. Shi, Privacy-aware reversible watermarking in cloud computing environments. IEEE Access **6**, 70720–70733 (2018)
9. C.C. Chang, C.T. Li, K. Chen, Privacy-preserving reversible information hiding based on arithmetic of quadratic residues. IEEE Access **7**, 54117–54132 (2019)
10. C.C. Chang, C.T. Li, Algebraic secret sharing using privacy homomorphisms for IoT-based healthcare systems. Math. Biosci. Eng. **16**, 3367–3381 (2019)
11. G.D. Su, C.C. Chang, C.C. Lin, High-precision authentication scheme based on matrix encoding for AMBTC-compressed images. Symmetry **11**, 996 (2019)
12. C.Y. Weng, C.T. Huang, H.W. KAO, DCT-based compressed image with reversibility using modified quantization, in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Springer, pp. 214–221 (2017)
13. H.C. Wu, N.I. Wu, C.S. Tsai, M.S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proc. Vis. Image Signal Process. **152**, 611–615 (2005)
14. G.D. Su, Y. Liu, C.C. Chang, A square lattice oriented reversible information hiding scheme with reversibility and adaptivity for dual images. J. Vis. Commun. Image Represent. **64**, 102618 (2019)
15. G.D. Su, C.C. Chang, C.C. Lin, Effective self-recovery and tampering localization fragile watermarking for medical images. IEEE Access **8**, 160840–160857 (2020)
16. K. Zhiwei, L. Jing, H. Yigang, Steganography based on wavelet transform and modulus function. J. Syst. Eng. Electron. **18**, 628–632 (2007)
17. M.S. Hsieh, D.C. Tseng, Y.H. Huang, Hiding digital watermarks using multiresolution wavelet transform. IEEE Trans. Industr. Electron. **48**, 875–882 (2001)
18. W.H. Lin, S.J. Horng, T.W. Kao, P. Fan, C.L. Lee, Y. Pan, An efficient watermarking method based on significant difference of wavelet coefficient quantization. IEEE Trans. Multimedia **10**, 746–757 (2008)
19. R.T. Mckeon, Strange fourier steganography in movies, in *2007 IEEE International Conference on Electro/Information Technology*, IEEE, pp. 178–182 (2007)
20. W.H. Chen, Color image steganography scheme using set partitioning in hierarchical trees coding, digital fourier transform and adaptive phase modulation. Appl. Math. Comput. **185**, 432–448 (2007)

21. F. Huang, J. Huang, Y.Q. Shi, New channel selection rule for JPEG steganography. IEEE Trans. Inf. Forensics Secur. **7**, 1181–1191 (2012)
22. G.S. Lin, Y.T. Chang, W.N. Lie, A framework of enhancing image steganography with picture quality optimization and anti-steganalysis based on simulated annealing algorithm. IEEE Trans. Multimedia **12**, 345–357 (2010)
23. Z.M. Lu, S.Z. Guo, Lossless information hiding in images. Syngress **2017**, 143–204 (2017)
24. J. Fridrich, J. Kodovsky, Rich models for steganalysis of digital images. IEEE Trans. Inf. Forensics Secur. **7**, 868–882 (2012)
25. H. Sun, R. Grishman, Y. Wang, Active learning based named entity recognition and its application in natural language coverless information hiding. J. Internet Technol. **18**, 443–451 (2017)
26. X. Chen, S. Chen, Y. Wu, Coverless information hiding method based on the chinese character encoding. J. Int. Technol. **18**, 313–320 (2017)
27. Z. Zhou, H. Sun, R. Harit, X. Chen, X. Sun, Coverless image steganography without embedding, in *International Conference on Cloud Computing and Security*, Springer, pp. 123–132 (2015)
28. Z. Zhou, Y. Cao, X. Sun, Coverless information hiding based on bag-of-words model of image. J. Appl. Sci. **34**, 527–536 (2016)
29. C. Yuan, Z. Xia, X. Sun, Coverless image steganography based on SIFT and BOF. J. Internet Technol. **18**, 435–442 (2017)
30. Z. Zhou, Q.J. Wu, C.N. Yang, X. Sun, Z. Pan, Coverless image steganography using histograms of oriented gradients-based hashing algorithm. J. Internet Technol. **18**, 1177–1184 (2017)
31. Z. Zhou, Y. Mu, Q.J. Wu, Coverless image steganography using partial-duplicate image retrieval. Soft. Comput. **23**, 4927–4938 (2019)
32. L. Zou, J. Sun, M. Gao, W. Wan, B.B. Gupta, A novel coverless information hiding method based on the average pixel value of the sub-images. Multimedia Tools Appl. **78**, 7965–7980 (2019)
33. Y. Mu, Z. Zhou, Visual vocabulary tree-based partial-duplicate image retrieval for coverless image steganography. Int. J. High Perform. Comput. Netw. **14**, 333–341 (2019)
34. Q. Liu, X. Xiang, J. Qin, Y. Tan, J. Tan, Y. Luo, Coverless steganography based on image retrieval of densenet features and DWT sequence mapping. Knowl. Based Syst. **192**, 105375 (2020)
35. Y. Luo, J. Qin, X. Xiang, Y. Tan, Q. Liu, L. Xiang, Coverless real-time image information hiding based on image block matching and dense convolutional network. J. Real-Time Image Proc. **17**, 125–135 (2020)
36. L. Yang, H. Deng, X. Dang, A novel coverless information hiding method based on the most significant bit of the cover image. IEEE Access **8**, 108579–108591 (2020)
37. J.F. Lu et al., A coverless information hiding method based on constructing a complete grouped basis with unsupervised learning. J. Netw. Intell. **6**, 29–39 (2021)
38. X. Xiong, F. Dela Torre, Supervised descent method and its applications to face alignment, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 532–539 (2013).
39. M. Zhou, X. Wang, H. Wang, J. Heo, D. Nam, Precise eye localization with improved SDM, in *2015 IEEE International Conference on Image Processing (ICIP)*, IEEE, pp. 4466–4470 (2015).
40. Q. Mao, K. Bharanitharan, C.C. Chang, Edge directed automatic control point selection algorithm for image morphing. IETE Tech. Rev. **30**, 343–243 (2013)
41. K. He, X. Zhang, S. Ren, J. Sun, Deep residual learning for image recognition, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 770–778 (2016)
42. J. Deng, J. Guo, N. Xue, S. Zafeiriou, Arcface: additive angular margin loss for deep face recognition, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 4690–4699 (2019)
43. D.P. Kingma, J. BA, Adam: a method for stochastic optimization (2014). arXiv preprint arXiv:1412.6980
44. W. Liu, Y. Wen, Z. Yu, M. Li, B. Raj, L. Song, Sphereface: deep hypersphere embedding for face recognition, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 212–220 (2017)
45. H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong, J. Zhou, Z. Li, W. Liu, Cosface: large margin cosine loss for deep face recognition, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 5265–5274 (2018)
46. K. Simonyan, A. Zisserman, Very deep convolutional networks for large-scale image recognition (2014). arXiv preprint arXiv:1409.1556
47. M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, L.C. Chen, Mobilenetv2: Inverted residuals and linear bottlenecks, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 4510–4520 (2018)
48. G. Huang, Z. Liu, L. Van der maaten, K.Q. Weinberger, Densely connected convolutional networks, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 4700–4708 (2017)
49. C. Szegedy, S. Ioffe, V. Vanhoucke, A.A. Alemi, Inception-v4, inception-resnet and the impact of residual connections on learning, in *Thirty-first AAAI Conference on Artificial Intelligence* (2017)
50. F.S. Abdulsattar, Towards a high capacity coverless information hiding approach. Multimedia Tools Appl. **80**, 18821–18837 (2021)
51. J.P. Robinson, Y. Li, N. Zhang, Y. Fu, S. Tulyakov, Laplace landmark localization, in *Proceedings of the IEEE International Conference on Computer Vision*, pp. 10103–10112 (2019)
52. J. Zhang, H. Hu, S. Feng, Robust facial landmark detection via heatmap-offset regression. IEEE Trans. Image Process. **29**, 5050–5064 (2020)
53. J. Wan, Z. Lai, J. Liu, J. Zhou, C. Gao, Robust face alignment by multi-order high-precision hourglass network. IEEE Trans. Image Process. (2020). https://doi.org/10.1109/TIP.2020.3032029
54. X. Liu, Z. Guo, J. You, B.V. Kumar, Dependency-aware attention control for image set-based face recognition. IEEE Trans. Inf. Forensics Secur. **15**, 1501–1512 (2019)
55. B. Chen, G.W. Wornell, Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. IEEE Trans. Inf. Theory **47**, 1423–1443 (2001)

Publisher's Note