University of Thi-Qar Journal Vol.14 No.4 Des 2019
Web Site: https://jutq.utq.edu.iq/index.php/main
Email: utj@utq.edu.iq

Privacy Preserving Scheme for Online Image Sharing

https://doi.org/10.32792/utq/utj/vol14/4/10

Suhad Abbas Yassir
Southern Technical University, Shatra Technical Institute, Iraq
Suhadabbas@yahoo.com
سهاد عباس ياسر
الجامعة التقنية الجنوبية/ المعهد التقني الشطرة

Abstract:

This paper presents a privacy protection solution for online photo share by obscuring faces in images, which keeps persons anonymous. The proposed system contains two modules. The first is the face detection module to identify region of interest (ROI) which is faces. The second is a face encryption module, which encrypts the ROI pixels using keys so that the access to the faces is restricted. The face detection module uses skin color detector in YCbCr color space to detect skin areas in the image. Also, to overcome the illumination problems in color images, two color constancy methods were adopted for color correction and lighting of the input images. The edges of the image are utilized to separate the faces segments from the background or object that have similar skin color. Morphological operations such as erosion are applied to remove small areas and hole filling to remove any holes in the binary segments. In addition, the correct faces are located by using a set of features. The face encryption module uses two chaotic logistic maps. One map is used for shuffling the face area pixels and another map is used for encrypting the pixels. Both shuffling and encryption are done using a keys. The face detection was tested on Caltech face database and showed a high detection rate and can localize face under different illumination conditions. The experiments on face encryption showed satisfactory results in various tests in terms of key space, PSNR, MSE and entropy analysis.

Keywords: face detection; image encryption; photo sharing; privacy; chaotic cryptography

الملخص:

تقدم هذه الورقة حلاً لحماية الخصوصية لمشاركة الصور عبر الإنترنت من خلال إخفاء الوجوه في الصور ، والتي تبقي الأشخاص مجهولين. يحتوي النظام المقترح على وحدتين. الأول هو وهي الوجوه. والثاني هو وحدة تشفير (ROI) وحدة الكشف عن الوجوه لتحديد منطقة الاهتمام باستخدام المفاتيح بحيث يكون الوصول إلى الوجوه ROI الوجه ، والتي تقوم بتشفير بكسلات للكشف عن YCbCr مقيدًا. تستخدم وحدة الكشف عن الوجوه كاشف لون البشرة في مساحة لون مناطق الجلد في الصورة. أيضا ، للتغلب على مشاكل الإضاءة في الصور الملونة ، تم تبني طريقتين لثبات اللون لتصحيح الألوان وإضاءة الصور المدخلة. تُستخدم حواف الصورة لفصل مقاطع الوجوه عن الخلفية أو الكائن ذي لون البشرة المماثل. يتم تطبيق العمليات المورفولوجية مثل التعرية لإزالة المساحات الصغيرة وملء الثقب لإزالة أي ثقوب في الأجزاء الثنائية. بالإضافة إلى ذلك ، توجد الوجوه الصحيحة باستخدام مجموعة من الميزات. تستخدم وحدة تشفير الوجه خريطتين لوجستيتين فوضويتين. يتم استخدام خريطة واحدة لخلط وحدات بكسل مساحة الوجه ويتم استخدام خريطة أخرى لتشفير وحدات البكسل. تتم كل من خلط ورق اللعب والتشفير للوجه وأظهر معدل اكتشاف Caltech باستخدام مفاتيح. تم اختبار كشف الوجه في قاعدة بيانات مرتفعًا ويمكنه توطين الوجه تحت ظروف إضاءة مختلفة. أظهرت التجارب على تشفير الوجه نتائج مرضية في اختبارات مختلفة من حيث المساحة الرئيسية.
،

الكلمات المفتاحية: كشف الوجه؛ تشفير الصور مشاركة الصور؛ خصوصية؛ التشفير الفوضوي

1. Introduction

Due to the increased development of information technology and the widespread of digital contents, images can be frequently transmitted and stored over networks [1]. Users can use online social network (OSN) to share their images which includes Facebook and Twitter or image sharing platforms such as Flicker and Instagram. In Facebook, for instance, there are about 1.2 billion active user daily and near 300 million

uploaded images every day [2]. The shared images can be easily browsed, downloaded or even used in inappropriate goals [3]. Secure image delivery is therefore becoming a great demand [4]. Encryption of images is a vital method for protecting image privacy in online communications. Many studies focused on protecting the privacy of image such as Lin et. al [5]. He proposed a privacy protection system that can be used in mobile phones. It consists of three stages which are face detection, face recognition and face encryption. In the face detection state, the authors adopt the skin color mode which is based on YCbCr color to detect the faces. Then, for face recognition, facial features are extracted using local binary patterns (LBP) method. Extracted facial features are used as key for encryption and decryption. In the encryption stage, a special lookup table embedded with face features is used to hide the face area. Experimental results show that the proposed system can demolish the face details and the encryption time is fast. Cutillo et. al. [6] presented a method of protecting user privacy of images in online social networks (OSN). Firstly, all faces in in the images are automatically obscured and then if the user meets the access policy rule of a co-worker the co-worker's face in the image can be revealed, otherwise the face also is hidden. Experimental tests show that the proposed system scheme can protect the user's faces in OSN environment. Lawrence et. al. [7] came up with privacy protection technique based on skin color, principle component analysis (PCA) and DES algorithm. For face detection stage, the authors convert the input image into NCC color model to identify skin color and refined the resulting segments to localize the faces. The PCA is applied on the detected face to extract the feature vectors that used as encryption key. The detected face regions are encrypted using DES algorithm. Experiments tests show that the proposed system can detect and hide face area of the images. Khashan et. al. [8] proposed an encryption scheme for protection the privacy of images. The scheme has two stages which are face detection and face encryption. In the face detection step, the authors used OpenCV Haar cascade classifier to identify the face region in the input image. Next, Blowfish algorithm with 128-bit key is used to encrypt the detected faces in the image.

Experimental results show that the proposed encryption scheme has a better encryption time in comparison to full encryption and it is suitable for real-time application. Zhang et. al. [9] presented a secure system for photo sharing and searching for mobile phones. The proposed system has several options, one of them is face obscuring choice. In that option, the user can choose the face area automatically or manually for preparing to encryption. Then, the user has three options to encrypt the face area. The first choice (Mask) replaces the face pixels with zeros. The second choice (P3) encrypts the high frequency parts of the DCT coefficients. The third choice (Blur) uses a filter box to blur the face area. Experimental results indicate a fast communication and low computation overhead. He et. al. [10] proposed a secure image sharing technique based on encrypting region of interest (ROI) in the image. The proposed technique consists of two stages: ROI detection and distortion of ROI. In the ROI detection stage, the system can either automatically detect ROI such faces or manually by user. Next, the ROI encryption uses a key to encrypt DCT coefficients to hide detected ROI. The authors used 19,000 images to test the system performance. The tests showed that the system is effective for privacy protection and require small computation time. Li et. al. [11] presented a privacy protection scheme for secure image sharing in instant messaging platforms. The proposed system composed of three main stages. In first stage (face recognition); the system performs face recognition for all the faces in the input image. The second stage (face hiding) encrypts each recognized face with generated random key. The final stage (message dispatching) is used to send the encrypted images along with the encryption keys to the receivers. Performance analysis of the proposed system found that it is suitable for instant messaging system.

In this paper, a privacy protection scheme for images is introduced. It divides the image into two parts: privacy part or referred to region of interest (ROI) and non-privacy part. The ROI is identified using face detection module that is based on skin color detection. Then, the localized faces is scrambled using two chaotic maps.

2. YCbCr Color Space

In YCbCr, Colors are represented in terms of luminance (Y channel) and chrominance (Cb and Cr channels) [12]. The linear transformations between RGB and YCbCr is expressed in Eq. (1).

$$\begin{aligned} Y &= (0.2989 * R) + (0.5866 * G) + (0.1145 * B) \\ C_b &= (0.1688 * \mathrm{R}) - (0.3312 * \mathrm{G}) + (0.5 * \mathrm{B}) \\ C_r &= (0.5 * \mathrm{R}) - (0.4184 * \mathrm{G}) - (0.0816 * \mathrm{B}) \end{aligned} \quad (1)$$

3. Logistic Chaotic Map

Logistic map is one of the simplest chaos functions that have been studied extensively for cryptographic systems [13]. The logistic map function can be expressed in Eq. (2).

$$\mathrm{X_{n+1}} = \mathrm{ax_n} \times (1 - \mathrm{X_n}) \quad (2)$$

Where X(n) is the initial value that can be in interval (0,1) and (a) is the control parameter that lies in (0,4). The logic map behavior is shown in Fig. 1.

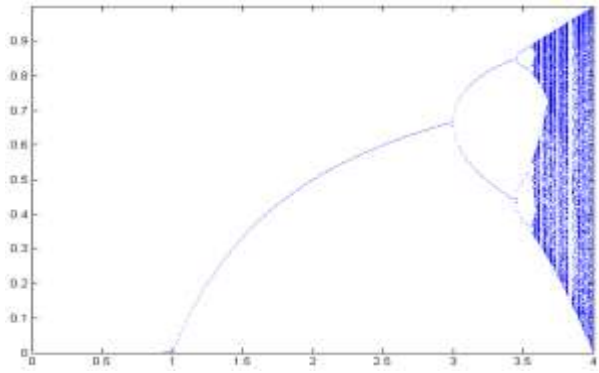


Fig. 1. Logistic map bifurcation [14].

4. Proposed System Layout

The proposed scheme consists of two main stages which are face detection and face encryption. The overall structure is illustrated in Fig 2.

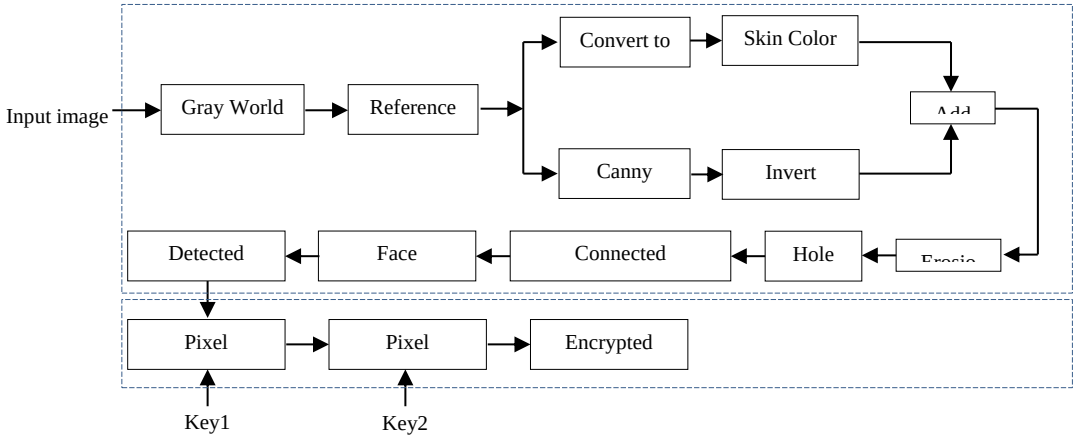


Fig. 2 Layout of the proposed privacy protection scheme

5. Face Detection

This section will discuss the different procedures in detail for the proposed face detection schemes.

5.1. Gray World Assumption

The skin color is usually affected by light condition in image which can lead to color deviation of the real skin color. Color constancy algorithm called Gray World Assumption (GWA) is used to perform color correction in images [15]. The GWA method can be defined in Eqs. (3-6).

$$R' = R \times \frac{K}{R_{average}} \quad (3)$$

$$G' = G \times \frac{K}{G_{average}} \quad (4)$$

$$B' = B \times \frac{K}{B_{average}} \quad (5)$$

$$K = \frac{R_{average} + G_{average} + B_{average}}{3} \quad (6)$$

Where $R_{average}$, $G_{average}$ and $B_{average}$ represents the mean of each color channel of the image. Fig. 3 shows the result of applying GWA on an image.

(a) (b)

Fig. 3 Gray World (a) Original image (b) Gray World image

5.2. Reference White

To detect faces under different lighting conditions, reference white scheme is utilized for illumination compensation. In this scheme, the top 5% of luminance values in the image is considered as the reference white in case of the number of pixels, is satisfactorily large (> 100). The RGB channels of the original image are adjusted so that the average gray value of the reference white pixels is scaled to 255 [16]. Reference white can be calculated according to Eqs. (7-8).

$$M_{top} = \sum_{i=l_u}^{255} i \times f_i / \sum_{i=l_u}^{255} f_i \quad (7)$$

$$X_{new} = X_{old} / M_{top} \times 255, where\ X \in \{R, G, B\} \quad (8)$$

Where i ∈ [*lu*,255] be the top 5% gray levels, *fi* is the pixel number with gray level *i* in an image. Reference white results is shown is Fig. 4.

Fig. 4. Reference white (a) Original image (b) Reference white image

5.3. Skin Color Detection

Skin color model can be constructed using a variety of color spaces, the YCbCr color model is the most common one [17]. To build this model, a set of skin patches is used for training the system. It consists of 110 images that have about (91,674) skin pixels. A sample of skin patches is shown in Fig. 5.

Fig. 5 Variety of skin patches

Each sample is converted to YCbCr color space. The mean and covariance between Cb and Cr is computed for all skin samples as shown in Eq. (9) and (10).

$$\sigma = \frac{1}{n} \sum_{k=1}^{n} x_k \quad (9)$$

$$\Sigma = \frac{1}{n}\sum_{k=1}^{n}(x_k - \sigma)(x_k - \sigma)^T \quad (10)$$

Where n is the number of skin samples, x_k is the vector representing the kth sample and σ and Σ are the mean vector and covariance matrix of the gaussian probability distribution function. The resulting probability density skin model can be represented by Eq. (11) and skin color distribution is illustrated in Fig. 6. Algorithm 1 explains the skin color training model.

$$p(x) = \frac{1}{(2\pi)^{\frac{d}{2}}|\Sigma|^{1/2}} \times exp\left\{-\frac{1}{2}(x-\sigma)\Sigma^{-1}(x-\sigma)^T\right\} \quad (11)$$

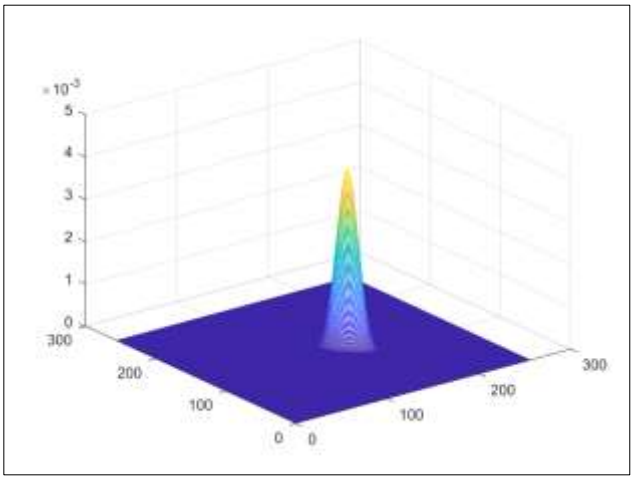


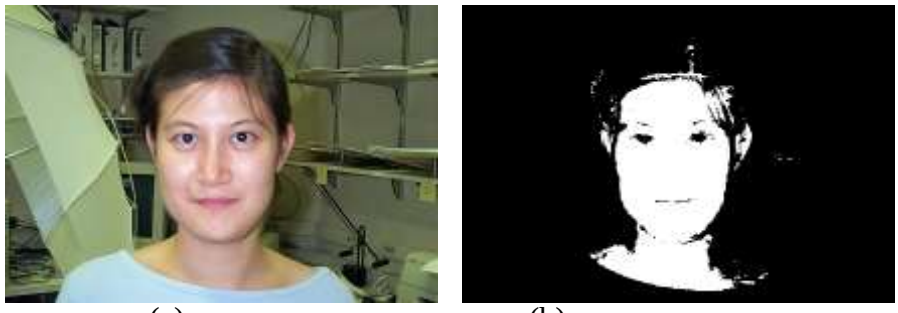
Fig. 6. Gaussian distribution in YCbCr color

Algorithm (1) skin color training

Input: RGB skin image sample
Output: Cbmean, Crmean and CbCrCov

1: Begin
2: Set Cb_sum 0
3: Set Cr_sum 0
4: Set N ← number of image samples
5: Loop k from one to the N
6: Set Img ← traing_img(k)
7: Set Cb(k) ← 0.1688 ×R- 0.3312×G+0.5 × B
8: Set Cr(k) ← 0. 5 ×R – 0.4184×G - 0.0816 × B
9: Set Cbmean ← Cbmean + Cb(k)
10: Set Crmean ← Crmean + Cr(k)
11: End k loop
12: For i from one to N
13: Set ← Sum_all = sum_all + (Cb(i) – Cbmean) × (Cr(i) – Crmean(i))
14: End For i
15: Set CbCrCov ← Sum_all / N
16: End

Applying equation (11) will result in grayscale image which is called skin likelihood image. Using thresholding process, it will be transformed into binary image with only 0 and 1. Fig. 7 shows the resulting binary image of input image. Algorithm 2 shows the skin color detection function.



(a) (b)

Fig. 7. Skin color detection (a) input image (b) skin region in binary

Algorithm (2) skin color detection

Input: RGB image, Cbmean, Crmean and CbCrCov
Output: Binary Image

Begin
1: Set Col ← Number of Image Columns
2: Set Row ← Number of Image Rows
3: Set T ← Threshold
4: For i from one to Col
5: For j from one to Row
6: Set Cb ← 0.1688 ×R- 0.3312×G+0.5 × B
7: Set Cr ← 0. 5 ×R – 0.4184×G - 0.0816 × B
8: Set x ← [(cb-bmean); (cr-rmean)]
9: Set skinlikelihood (i,j) ← exp(-0.5 × x^T × inv(brcov) × x)
10: End i Loop
11: End j Loop
12: For i from one to Col
13: For j from one to Row
14: If Set skinlikelihood (i,j) > T
15: Bin_img(I,j) = 1
16: End if
17: End i Loop
18: End j Loop
End

5.4. Edge image with skin image combination

The most common face detection algorithms that are based on skin color can function well in case of images containing non-skin color background or the persons are wearing non-skin color cloths. An image containing similar skin color backgrounds or cloths can lead to identifying the entire region as skin segment [18] as shown in Fig. 8a. In such case, the candidate face region may merged with the background or any object with same skin color. Therefore, it is necessary to use a mechanism that it is able to separate the candidate face region from background region for easy face localization. To solve this issue, the edges of the image is combined with resulting binary image of the skin detector as in Fig. 8b.

(a) (b)

Fig. 8. (a) face segment connected with background (b) face segment disconnected from background

5.5. Morphological operations

Morphological operation such as erosion and hole filling are utilized for the skin area that are loosely connected. The morphological erosion is used to ensure that any is not connected to any other object or background in case of being not fully detached [19]. Then, morphological hole filling is applied to fill any holes found in the detected skin segments [20]. Next, connected component labeling is used for the resulting binary image to label all clustered pixels group [16] for further analyzing to determine whether it is face region or not as shown in Fig. 9.

Fig. 9 binary labeled image

5.6. Face Verification

This step is used to verify the labeled face segments in the binary image. It is an essential one as it filers the resulting face segments and detects the correct face segments. Fig. 9 shows a binary image after applying the verification step. Usually, the verification process consists of several features which eliminate non-face segments including:

- **Area:**

The area refers to the number of pixels in a specific segment. Small segments are eliminated that which have area less than 5% of the total image as illustrated in Fig. 10.

Fig. 10. Face verification

- **Aspect ratio:**

The aspect ratio represents the maximum width of the face segment divided by the maximum height [21]. Any segment within the values of 0.5 to 0.9 is considered as a face segment according to the experiments.

- **Extent:**

The extent is calculated by Eq. (12). It was found that the extent between the range 0.5 to 0.9 is identified as face segments.

$$\text{Extent} = \frac{Area}{l1\ l2} \quad (12)$$

Where l1 and l2 are the maximum width and height respectively.

Ellipse Area:

The elliptical area is computed according to Eq. (13). Experiments showed that ellipse area of segment between is 1.04 to 0.5 considered a face segment.

$$\text{Ellipse area} = \frac{4A}{\pi l1 l2} \quad (13)$$

After the face is detected, a boundary box coordinates is sent for the next stage which is face encryption.

6. Face Encryption

The localized faces in the image are passed into encryption stage. This stage performs the encryption by two methods which are pixel permutation followed by pixels encryption. Both steps use chaotic logistics maps to perform these tasks. The encryption steps are described as the follows:

Step 1: Input the detected face area coordinates in the image, key1,key2,

Step 2: Apply pixel permutation using chaotic logistic map as follows:

- Convert the face area image box into a 1D array of M×N.
- Generate chaotic sequences of length M×N using chaotic logistic map; key1 is used as the initial value and key2 used as the control parameter.
- Chaotic numbers are sorted in ascending order.
- Obtain the permutated face image box by mapping the value position of the face box to its corresponding index position in the sorted chaotic logistic map sequence.

- Convert the resulting face image sequence into a 2D array of (M×N).

The face permutation is explained in Algorithm 3.

Algorithm (3) Face area shuffling

Input: RGB image, Face coordinates, key1, key2
Output: Shuffled face

Begin

```
Set r ← key1
Set X(0) ← key2
Set Counter ← 0
Loop n from 0 to Number of image pixels
Set X(n+1) ← r × X(n) × (1-X(n))
Set Map(Counter) ← X(n+1)
Counter ← Counter + 1
End n Loop
Sort Ascending Index () ← Map()
// Store face area into 1D arrays
Set initial counter ← 0
Loop i from 0 to image width
Loop j from 0 to image height
Set 1DRed(counter) ← Red(i,j)
Set 1DGreen(counter) ← Green(i,j)
Set 1DBlue(counter) ← Blue(i,j)
Set Counter ← Counter + 1
End j Loop
End i Loop
// Shuffle pixels
Loop k from 0 to Number of pixels
Loop j from 0 to Number of pixels
If Map(k) = Index(j) then
Set sRed(k) ← aRed(j)
Set sGreen(k) ← aGreen(j)
Set sBlue(k) ← aBlue(j)
End if
End j Loop
End k Loop
```

End

Step 3: Perform pixel encryption using chaotic logistic map as bellow:

- Generate chaotic sequences of length M×N using chaotic logistic map; key3 is used as the initial value and key4 is used as the control parameter.
- Perform XOR operation between random numbers and the localized face pixels.

The face encryption process is described in Algorithm 4.

Algorithm (4) Face area ciphering

Input: Shuffled face area, Face coordinates, key1, key2
Output: encrypted face

Begin
46: Set r ← key1
47: Set X(0) ← key2
48: Set Counter ← 0
49: Loop n from 0 to Number of image pixels
50: Set X(n+1) ← r × X(n) × (1-X(n))
51: Set Map (Counter) ← X(n+1)
52: Set Counter ← Counter + 1
53: End n Loop
54: Loop i from 0 to image width : Loop j from 0 to image height
55: Set cRed(i,j) ← sRed(i,j) XOR MapSin (Counter)
56: Set cGreen(i,j) ← sGreen(i,j) XOR MapSin (Counter)
57: Set cBlue(i,j) ← sBlue(i,j) XOR MapSin (Counter)
58: Set Counter ← Counter + 1
59: End j Loop: End i Loop

End

7. Experimental Results

This section will discuss the experimental results for the face detection and face encryption.

7.1. Face detection results

To test the performance of the proposed face detection scheme, the Caltech face database [22] is used. It contains 450 images that have different illumination levels and variety of facial expressions from various

locations. The image size is 896x592 and each image have one face. MATLAB 2017a software is used for programming with Core i7-6500U CPU.

Table (1)

Face detection results

Total Faces	Detected Faces	Detection Rate
450	391	86.88%

Face detection results are shown in Table 1. Form the table, it is noted that the face detection shows satisfactory results. Fig. 11 shows a sample of face detector results of the proposed method. It can be seen that the proposed method can respond to different skin colors and less sensitive to skin like background. The proposed method detection results are compared with two other schemes and it has higher detention rate as shown in Table (2).

Table (2)
Face detection comparison

Method	Detection rate
Ban et. al [23]	65.4%
Khac et. al [24]	79.08%
Proposed	86.88%

7.2. Encryption analysis

In this section, some security analysis of the proposed algorithm will be discussed in terms of key space analysis, mean square error, peak signal-to-noise ratio and information entropy analysis. Four images were used to test the proposed scheme, as shown in Fig. 12.

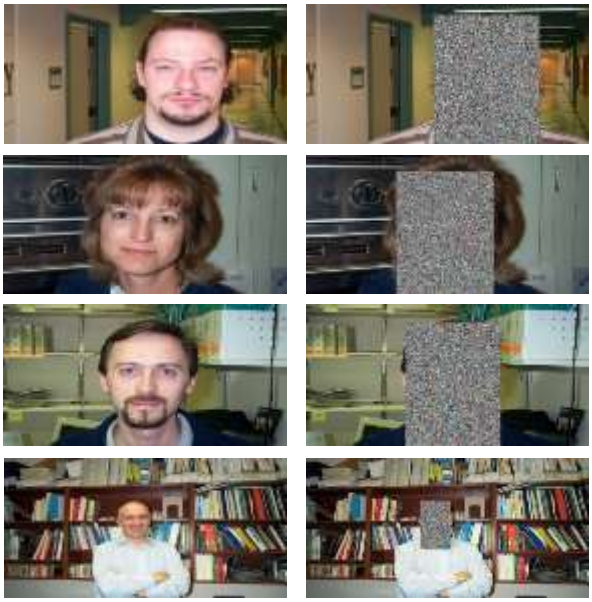


Fig. 12 Test images. Original images Image_134, Image_157, Image_181 and Image_332 left column and encrypted face images for the same images in the right column.

7.2.1. Key space analysis

A good encryption algorithm must be sensitive to the secret keys and the key space must also be large enough to make the brute-force attacks difficult for intruders. In the proposed scheme, the initial conditions and control parameters for the chaotic logistic maps can be used as keys. If the single key size is 10^{14}, then the key space can be up to 10^{56} which it is larger than 2^{128}.

7.2.2. Mean Square Error and Peak Signal-to-Noise Ratio

The mean square error (MSE) is a mathematical measure that refers to the average squared difference between the original face image and the encrypted face image. It is computed by adding up the squared differences of all pixels of the image. Then, it is divided by the total number of pixels. The peak signal-to-noise ratio (PSNR) is utilized to obtain the differences between the original face image and the encrypted one. The main benefit of using PSNR is to point out the encrypted face

area noise level. MSE and PSNR are expressed by Eqs. (14) and (15) respectively:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [f(i,j) - \hat{f}(i,j)]^2 \quad (14)$$

$$PSNR = 10 \log_{10} \left[\frac{max_f^2}{MSE} \right] \quad (15)$$

where f(i,j) is the original face image; $\hat{f}$(i, j) is the encrypted face image; M, N are the two dimensions of the face box image; and max_f is the maximum value of an image f. Table 3 demonstrates the MSE and PSNR results for the encrypted face images.

Table (3)

MSE and PSNR values for the encrypted image samples

Image Name	MSE	PSNR
Image_134	5934.5421	10.4309
Image_157	6331.1624	10.1160
Image_181	7762.0603	9.2310
Image_332	6109.6332	10.2707

7.2.3. Entropy Analysis

Information entropy is used to measure the randomness of a source. The information entropy referred to as H(X) is shown in Eq. (16):

$$H(X) = \sum_i p(x_i) \log_2 \frac{1}{p(x_i)} \quad (16)$$

where $p(x_i)$ denotes to the probability of the pixel value (x_i). If the probability of occurrence of each pixel value is the same, then value of the entropy must be 8. This will be the maximum entropy for an encrypted face image that has true uniform pixel distribution. Therefore, the higher entropy value of an encrypted image means that the proposed encryption algorithm is resistant against the entropy attack. Table 4 demonstrates the entropy values for the red, green and blue of the encrypted face images.

Table (4)

Entropy values for encrypted face images

Image Name	Red	Green	Blue
Image_134	7.7512	7.7651	7.7109
Image_157	7.7857	7.7772	7.7612
Image_181	7.7926	7.7532	7.7097
Image_332	7.7741	7.7833	7.7849

8. Conclusions

In this paper, a privacy protection scheme is presented. The proposed scheme has two stages, which are face detection and face encryption. In the face detection stage, skin color model in the YCbCr is used to detect the skin regions. In addition, the edges of the image are combined with the binary image to separate the face segment from the background or any other skin-like object. Then, a set of features is used to discard non-skin segments. In the face encryption stage, two chaotic logistics map is used. One map is used for pixel permutation and another

is used for pixel encryption. Face detection test showed that the detection rate is high and it is able to detect face under different illumination conditions. The face encryption analysis showed that the key space is large, MSE is high, PSNR is low and entropy is close to optimal. Based on these results, it can be concluded that the proposed scheme can provide a privacy protection for the transmitted images in social networks and photo sharing platforms.

References:

[1] S. K. Rajput and A. Konidena, "PERFORMANCE ENHANCEMENT IN IMAGE ENCRYPTION USING AES," *Int. J. Innov. Adv. Comput. Sci.*, vol. 4, no. 1, pp. 16–19, 2015.

[2] M. A. H. Al-Hamami, "A Proposed Framework for Photos Copyright Protection in Facebook," *Int. J. Comput. Appl.*, vol. 162, no. 1, 2017.

[3] K. Liang, J. K. Liu, R. Lu, and D. S. Wong, "Privacy concerns for photo sharing in online social networks," *IEEE Internet Comput.*, vol. 19, no. 2, pp. 58–63, 2014.

[4] J. Chen, Z. Zhu, C. Fu, H. Yu, and L. Zhang, "An efficient image encryption scheme using gray code based permutation approach," *Opt. Lasers Eng.*, vol. 67, pp. 191–204, 2015.

[5] C.-Y. Lin, C.-C. Chang, Y.-H. Chen, and P. Prangjarote, "Multimedia Privacy Protection System for Mobil Environments," in *2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2011, pp. 133–136.

[6] L. A. Cutillo, R. Molva, and M. Önen, "Privacy preserving picture sharing: Enforcing usage control in distributed on-line social networks," in *Proceedings of the Fifth Workshop on Social Network Systems*, 2012, p. 6.

[7] L. Y. Deng, D. L. Lee, and Y. Liu, "Face Recognition Lock," in *2013 International Conference on IT Convergence and Security*

(ICITCS), 2013, pp. 1–2.

[8] O. A. Khashan, A. M. Zin, and E. A. Sundararajan, "Performance study of selective encryption in comparison to full encryption for still visual images," *J. Zhejiang Univ. Sci. C*, vol. 15, no. 6, pp. 435–444, 2014.

[9] L. Zhang, T. Jung, C. Liu, X. Ding, X.-Y. Li, and Y. Liu, "Pop: Privacy-preserving outsourced photo sharing and searching for mobile devices," in *2015 IEEE 35th International Conference on Distributed Computing Systems*, 2015, pp. 308–317.

[10] J. He *et al.*, "Puppies: Transformation-supported personalized privacy preserving partial image sharing," in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2016, pp. 359–370.

[11] F. Li, J. Yu, L. Zhang, Z. Sun, and M. Lv, "A privacy-preserving method for photo sharing in instant message systems," in *Proceedings of the 2017 International Conference on Cryptography, Security and Privacy*, 2017, pp. 38–43.

[12] S. L. Phung, A. Bouzerdoum, and D. Chai, "Skin segmentation using color pixel classification: analysis and comparison," *IEEE Trans. Pattern Anal. Mach. Intell.*, no. 1, pp. 148–154, 2005.

[13] N. Bigdeli, Y. Farid, and K. Afshar, "A robust hybrid method for image encryption based on Hopfield neural network," *Comput. Electr. Eng.*, vol. 38, no. 2, pp. 356–369, 2012.

[14] J. D. D. Nkapkop, J. Y. Effa, J. Fouda, M. Alidou, L. Bitjoka, and M. Borda, "A fast image encryption algorithm based on chaotic maps and the linear diophantine equation," *Comput. Sci. Appl.*, vol. 1, no. 4, pp. 232–243, 2014.

[15] K. H. Bin Ghazali, J. Ma, and R. Xiao, "An innovative face detection based on skin color segmentation," *Int. J. Comput. Appl.*, vol. 34, no. 2, pp. 6–10, 2011.

[16] W.-C. Hu, C.-Y. Yang, D.-Y. Huang, and C.-H. Huang, "Feature-based face detection against skin-color like backgrounds with

varying illumination," *J. Inf. Hiding Multimed. Signal Process.*, vol. 2, no. 2, pp. 123–132, 2011.

[17] M. V Daithankar, K. J. Karande, and A. D. Harale, "Analysis of skin color models for face detection," in *2014 International Conference on Communication and Signal Processing*, 2014, pp. 533–537.

[18] Q. Huynh-Thu, M. Meguro, and M. Kaneko, "Skin-color extraction in images with complex background and varying illumination," in *Sixth IEEE Workshop on Applications of Computer Vision, 2002.(WACV 2002). Proceedings.*, 2002, pp. 280–285.

[19] Q. Liu and G. Peng, "A robust skin color based face detection algorithm," in *2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR 2010)*, 2010, vol. 2, pp. 525–528.

[20] F. Y. Shih, S. Cheng, C.-F. Chuang, and P. S. P. Wang, "Extracting faces and facial features from color images," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 22, no. 03, pp. 515–534, 2008.

[21] H.-J. Lin, S.-H. Yen, J.-P. Yeh, and M.-J. Lin, "Face detection based on skin color segmentation and SVM classification," in *2008 Second International Conference on Secure System Integration and Reliability Improvement*, 2008, pp. 230–231.

[22] W. Zhang, B. Yu, G. J. Zelinsky, and D. Samaras, "Object class recognition using multiple layer boosting with heterogeneous features," in *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, 2005, vol. 2, pp. 323–330.

[23] Y. Ban, S.-K. Kim, S. Kim, K.-A. Toh, and S. Lee, "Face detection based on skin color likelihood," *Pattern Recognit.*, vol. 47, no. 4, pp. 1573–1585, 2014.

[24] C. N. Khac, J. H. Park, and H.-Y. Jung, "Face detection using variance based Haar-like feature and SVM," *World Acad. Sci. Eng. Technol.*, vol. 60, pp. 165–168, 2009.