Information Sciences xxx (2015) xxx–xxx

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Image encryption: Generating visually meaningful encrypted images

Q1 Long Bao, Yicong Zhou*

Department of Computer and Information Science, University of Macau, Macau, China

A R T I C L E I N F O

Article history:
Received 24 November 2014
Revised 24 April 2015
Accepted 28 June 2015
Available online xxx

Keywords:
Image encryption
Discrete wavelet transform
Visually meaningful encrypted image

A B S T R A C T

To protect image contents, most existing encryption algorithms are designed to transform an original image into a texture-like or noise-like image which is, however, an obvious visual sign indicating the presence of an encrypted image and thus results in a significantly large number of attacks. To address this problem, this paper proposes a new image encryption concept to transform an original image into a visually meaningful encrypted one. As an example of the implementation of this concept, we introduce an image encryption system. Simulation results and security analysis demonstrate excellent encryption performance of the proposed concept and system.

1. Introduction

In the past ten years, “Cloud” has become a popular keyword in the computer society. To overcome the limitations in the storage and computation capability of a single computer, cloud computing technology provides individuals and organizations a sufficiently large online space to store multimedia data (e.g. documents, videos and images), and offer people a convenient way to access and share data over the network. Due to the fact that these multimedia data may contain private, valued or even classified information, preventing the information from leakage becomes an important and urgent issue for individuals and organizations [33,34]. Image encryption is an efficient tool to provide security to these multimedia data.

Many image encryption algorithms have been proposed to protect images by changing their pixel values and/or locations using different technologies [5,19,35]. They can be classified into the frequency-domain and spatial-domain image encryption algorithms. Using security key coefficients, the frequency-domain image encryption algorithms are designed to change image data in the frequency domain or alter the transform function, such as the discrete fractional Fourier transform [18,21,26], quantum Fourier transform [31] and reciprocal-orthogonal parametric transform [6]. The spatial-domain image encryption algorithms are based on the famous Substitution-Permutation Network (SPN) that utilizes a substitution process to change image pixel values and a permutation process to change image pixel positions. These permutation and substitution processes are based on different technologies including the advanced encryption standard (AES) [24], P-Fibonacci transform [40], wave transmission [20], elliptic curve ElGamal [8], gray code [36], random grids [10], Latin squares [30] and chaotic systems [9,17,38,41]. Both the spatial-domain and frequency-domain image encryption algorithms are able to protect images with a high level of security [27,39]. Their output encrypted images are all visually texture-like or noise-like, such as images in Fig. 1(a) and (b). However, since the formats of these encrypted images are limited to noise-like and texture-like, it is easy to distinguish them from normal visually meaningful images. From the security point of view, this texture-like or noise-like feature is an obvious visual sign indicating the presence of

* Corresponding author. Tel.: +853 88228458; fax: +853 88222426.
E-mail address: yicongzhou@umac.mo (Y. Zhou).

http://dx.doi.org/10.1016/j.ins.2015.06.049
0020-0255/© 2015 Published by Elsevier Inc.

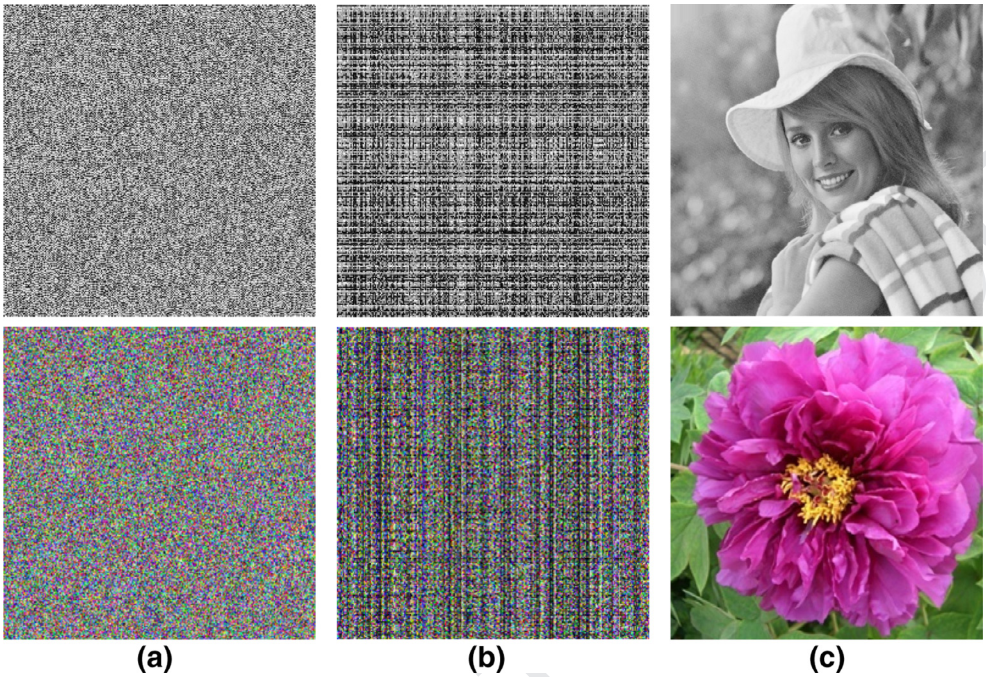

Fig. 1. Different encrypted images: (a) noise-like; (b) texture-like; (c) visually meaningful.

an encrypted image [37] that may contain important information. As a result, an encrypted image with similar features as noise-like or texture-like definitely brings increasing people's attentions and thus leads to a large number of attacks and analysis. These include different types of cryptanalysis, illegal edition, modification or even deletion of image contents. All these increase the possibility of information leakage or loss.

To address these problems, in this paper, we propose a new concept of image encryption to transform original images into visually meaningful encrypted images, such as images in Fig. 1(c). This is because people generally consider these images as normal images rather than encrypted ones. Based on this concept, we introduce an image encryption system. It not only protects images in a normal way that most existing encryption methods do, but also provides an additional visual protection. Simulation results and security analysis are provided.

2. New concept of image encryption

Most existing image encryption algorithms protect original images by transforming them into texture-like or noise-like encrypted images with a nearly uniform distribution of pixel values. As a result, the encrypted images can withstand different types of attacks, protecting original image information with a high level of security. However, this texture-like or noise-like feature is an obvious visual sign of encrypted images. It definitely catches more people's attentions and thus brings a significantly large amount of attacks and cryptanalysis to encrypted images. The risk of information leakage or loss exponentially increases.

On the contrary, a visually meaningful or good-looking image, such as images in Fig. 1(c), has generally a high possibility of being treated as a normal image rather than an encrypted one. But images in Fig. 1(c) are indeed encrypted images. This would significantly reduce the risk of an encrypted image being attacked and modified. This interesting phenomenon motivates us to propose a new concept for image encryption as shown in Fig. 2.

The idea of this concept is straightforward. It directly encrypts an original image into a visually meaningful encrypted image (VMEI). Because a VMEI has a visual feature similar to a normal image, attackers have extreme difficulty distinguishing VMEIs from large amount of normal images. Furthermore, for a given original image, as can be seen in Fig. 2, various encryption algorithms or an encryption algorithm with different security keys may yield a large number of VMEIs with completely different appearances or formats. This further increases attackers' difficulty of obtaining the correct VMEIs before their cryptanalysis. Thus, the proposed concept is able to protect original images with a much higher security level than most existing encryption algorithms.

Fig. 2. The new concept of image encryption.

Please cite this article as: L. Bao, Y. Zhou, Image encryption: Generating visually meaningful encrypted images, Information Sciences (2015), http://dx.doi.org/10.1016/j.ins.2015.06.049

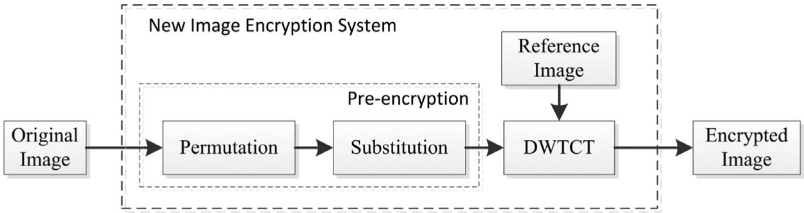

Fig. 3. The block diagram of the new image encryption system.

3. New image encryption system

The key issue of the proposed concept is how to generate VMEIs. Motivated by technologies of image hiding and watermarking, this section introduces a new image encryption system (NIES) as an implementation example of the proposed concept.

3.1. Encryption process

The structure of NIES is shown in Fig. 3. The underlying fundamental idea of NIES is that it uses a normal image as the reference image and yields a VMEI that has an appearance similar to the reference image. NIES consists of two parts: a pre-encryption process and a discrete-wavelet-transform-based content transform (DWTCT). The pre-encryption process uses permutation and substitution to change image pixel locations and values. The pre-encrypted image is usually a noise-like image. It is then transformed by DWTCT into a VMEI that is visually similar to the reference image.

The pre-encryption process is a transformation function to change image pixel values and locations. The pre-encrypted image P can be defined by,

$$P = \mathbb{F}(O,\ K_p) \tag{1}$$

where O is the original image with a size of $M \times N$; $\mathbb{F}$ and K_p are the transformation function and its security key set, respectively.

Any existing image encryption algorithm can be used in the pre-encryption process. The pre-encrypted image P is a noise-like image. Thus, the pre-encryption process protects the original image with a security level as same as those of existing encryption algorithms.

DWTCT further transforms the pre-encrypted image P into a VMEI with appearance similar to the reference image R. Using different reference images, NIES generates completely different VMEIs. This DWTCT is defined in Eq. (2),

$$E = \mathbb{T}(P, R, K_t) \tag{2}$$

where $\mathbb{T}$ denotes DWTCT; K_t is the parameter set of DWTCT which defines the wavelet filter set for the discrete wavelet transform (DWT); R and E are the reference and final encrypted images with the same size of $2M \times 2N$.

DWTCT uses an integer DWT proposed by Calderbank in 1998 [7]. This integer DWT is completely invertible and able to transform an integer to another integer. The final encrypted images after the inverse DWT are integers and the original image can be reconstructed without any data loss.

A pseudo code implementation of DWTCT is described in Algorithm 1 where C_A, C_H, C_V and C_D denote the LL, HL, LH, and HH sub-bands (L = Low-frequency, H = High-frequency), $\lfloor\cdot\rfloor$ and mod are the floor and modulo operators, respectively. The objective

Algorithm 1 DWTCT.

Input: Pre-encrypted image P with a size of $M \times N$, reference image R with a size of $2M \times 2N$, and parameter K_t,

Apply DWT defined by parameter K_t to the reference image R, obtain C_A, C_H, C_V and C_D
for $m = 1$ to M **do**
  for $n = 1$ to N **do**
    $C_V(m, n) = \lfloor \frac{P(m,n)}{10} \rfloor$
    $C_D(m, n) = P(m, n) \bmod 10$
  end for
end for
Apply the inverse DWT to C_A, C_H, C_V and C_D sub-bands

Output: The final encrypted image E with a size of $2M \times 2N$

of DWTCT is to divide each pixel value of the pre-encrypted image into two portions and put them into C_V and C_D. C_V keeps the decimal portion in the 10th and 100th positions. C_D stores the decimal portion in the unit position. For example, if a pixel value is 234, $C_V = \lfloor \frac{234}{10} \rfloor = 23$, namely C_V keeps 23; and $C_D = 234 \bmod 10 = 4$, thus C_D stores 4. In this manner, it ensures that the data range of the final encrypted image is the same as the pre-encrypted image such as [0, 255]. Thus, the authorized users are able to completely reconstruct the original image without any data loss in the image decryption process.

Please cite this article as: L. Bao, Y. Zhou, Image encryption: Generating visually meaningful encrypted images, Information Sciences (2015), http://dx.doi.org/10.1016/j.ins.2015.06.049

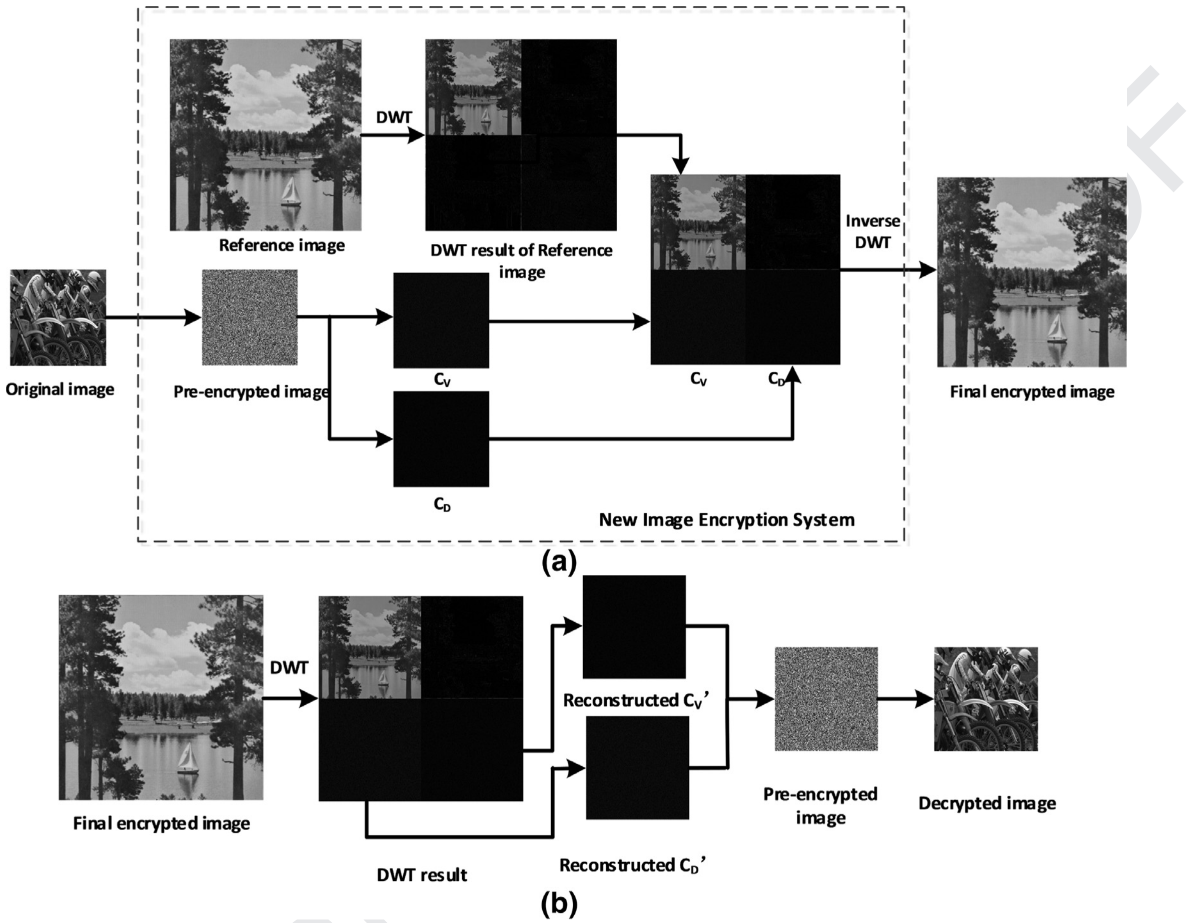

Fig. 4. An illustrative example of NIES in the (a) encryption process, and (b) decryption process.

3.2. Decryption process

The security keys of NIES consist of the pre-encryption algorithm and its security key set K_p, and parameter K_t of DWTCT. Using these security keys, the authorized users can reconstruct the original image directly from the encrypted image E without knowing the reference image R. An illustrative example is shown in Fig. 4. The change of images in each step can be observed clearly.

In image decryption, the encrypted image is firstly decomposed into four sub-bands by the wavelet filters defined by K_t. The reconstruction of the pre-encrypted image can be defined by,

$$P'(m,n) = 10C'_V(m,n) + C'_D(m,n) \tag{3}$$

where C'_V and C'_D are sub-bands corresponding to C_V and C_D of the encrypted image. $P'(m,n)$ is the reconstructed pre-encrypted image.

Following the corresponding decryption process of the pre-encryption algorithm with the security key set K_p, the user is able to reconstruct the original image.

3.3. Discussion

The proposed NIES ensures security of the original images in two aspects: (1) image data security and (2) image appearance security.

Image data security is performed by the pre-encryption process. It changes image pixel locations and/or values using an existing encryption method, such as existing image encryption algorithms. The pre-encrypted images are generally noise-like or texture-like.

The goal of image appearance security is to generate VMEIs. Compared with noise-like or texture-like encrypted images which are generated by most existing encryption algorithms, NIES further transforms the pre-encrypted images into VMEIs that provide an additionally visual protection to the images. Thus, it ensures the attackers' difficulty of distinguishing the final

Please cite this article as: L. Bao, Y. Zhou, Image encryption: Generating visually meaningful encrypted images, Information Sciences (2015), http://dx.doi.org/10.1016/j.ins.2015.06.049

encrypted images from normal images. NIES protects the original images with a much higher security level than most existing image encryption algorithms.

Even though NIES is motivated by technologies of image hiding and reversible watermarking [2,12,16,22,25], DWTCT differs from these in the following aspects:

(1) *Different objectives.* The objective of image hiding and reversible watermarking is to embed secret messages or watermarks into a cover image while minimizing distortions to the cover image [1,13,15]. The resulting stego image (image with embedded messages/watermarks) is extremely similar to the cover image. Thus, the unauthorized users have difficulty of detecting the existence of messages or watermarks using various computer tools. On the other hand, the objective of DWTCT is to solve the security weakness of noise-like encrypted images generated by existing image encryption algorithms. It transforms the noise-like or texture-like appearance of the pre-encrypted image into a visually meaningful one and provides an additionally visual protection to the images on the top of security provided by existing image encryption algorithms. Moreover, reversible watermarking intends to reconstruct both watermarks and the cover image without any distortion, while DWTCT recovers only the pre-encrypted image but not the reference image.

(2) *Different requirements.* In NIES, as long as the final encrypted image is visually meaningful for the person, its similarity to the reference image is not important to DWTCT. That is, NIES considers only naturalness of visual quality of the final encrypted image, while image hiding and reversible watermarking prefer the high similarity between the stego image and cover image [3,11,14]. This naturalness property ensures that the final encrypted image has a high possibility to be regarded as a normal image. For real-time applications, DWTCT is required to be time efficient and a low computation cost. On the contrary, image hiding or reversible watermarking embeds messages or watermarks while minimizing distortions to the cover image, without considering the computational cost.

In DWTCT, the original image has the same size as a DWT sub-band, which is four times smaller than the reference image. The final encrypted image of the proposed NIES has the same size as the reference image. Thus, the final encrypted image of NIES is four times larger than the original image. In real applications, the users have the flexibility to choose different types of integer DWTs and/or an even larger size of the reference image. These can act as a part of the security key, benefitting the security of the proposed NIES. However, selecting a larger size of the reference image may result in higher costs of transmission and storage.

For the proposed NIES, the security and computation complexity are the primary concerns. DWTCT is designed to balance the tradeoff among the security, computational cost, and the visual quality of the encrypted image.

4. Simulation results and performance analysis

This section provides several simulation examples and performance analysis to show the NIES's encryption performance. In this paper, all reference images are four times larger than the original images to be encrypted.

4.1. Simulation results

NIES is able to protect different types of images. Four types of images are selected as original images including binary, grayscale, biometrics, and medical images. The pre-encryption process selects Bao's algorithm [4], AES [24], Chen's algorithm [9] and Liao's algorithm [20], individually. The encryption results are shown in Fig. 5. NIES can transfer different types of original images into the similar VMEIs, using a specific reference image but different pre-encryption algorithms, such as images in the second and fourth rows in Fig. 5. For a specific original image, such as the medical image in Fig. 5(d), NIES can yield the final encrypted images with different visual appearances using the same pre-encryption algorithm but different reference images. In additional to these four types of images, NIES can also be utilized to encrypt color images. NIES encrypts each color plane of the original color image one by one using the corresponding color plane of a color reference image. The final encrypted color planes are combined together to generate the final encrypted color image, such as images in Fig. 7(f)–(h).

Next, we investigate how the pre-encryption algorithm and reference image affect the final encryption results of NIES. As mentioned in Section 3, any existing image encryption algorithm can be used in the pre-encryption process of NIES. Fig. 6 shows the encryption results using different pre-encryption algorithms with a specific original and reference image. As can be seen, NIES with different pre-encryption algorithms are able to transform the original image into different encrypted images with similar visual appearances. Their histograms shown in Fig. 6 are slightly different. Hence, using different pre-encryption algorithms leads to a slight change in the histogram of encrypted images. This, on the other hand, offers another security benefit that the users have the flexibility to select an encryption algorithm for the pre-encryption process, and thus significantly increases the security key space of our proposed encryption system.

The reference image plays a significant role to the appearance of encrypted images in NIES. Fig. 7 shows the encryption results using NIES with different reference images and applying the PSCS-IE algorithm [38] in the pre-encryption process. As can be seen, using different reference images, NIES can generate completely different VMEIs. There is no standard or criteria of selecting reference images because NIES is adaptive to a wide range of images. The users have the flexibility to select any specific image as the reference image according to their personal preference. This also results in an unlimited number of formats of encrypted images. Each visually meaningful image has a possibility to be the encrypted image. This ensures the attackers' difficulty of distinguishing encrypted images from different types of normal images.

Please cite this article as: L. Bao, Y. Zhou, Image encryption: Generating visually meaningful encrypted images, Information Sciences (2015), http://dx.doi.org/10.1016/j.ins.2015.06.049

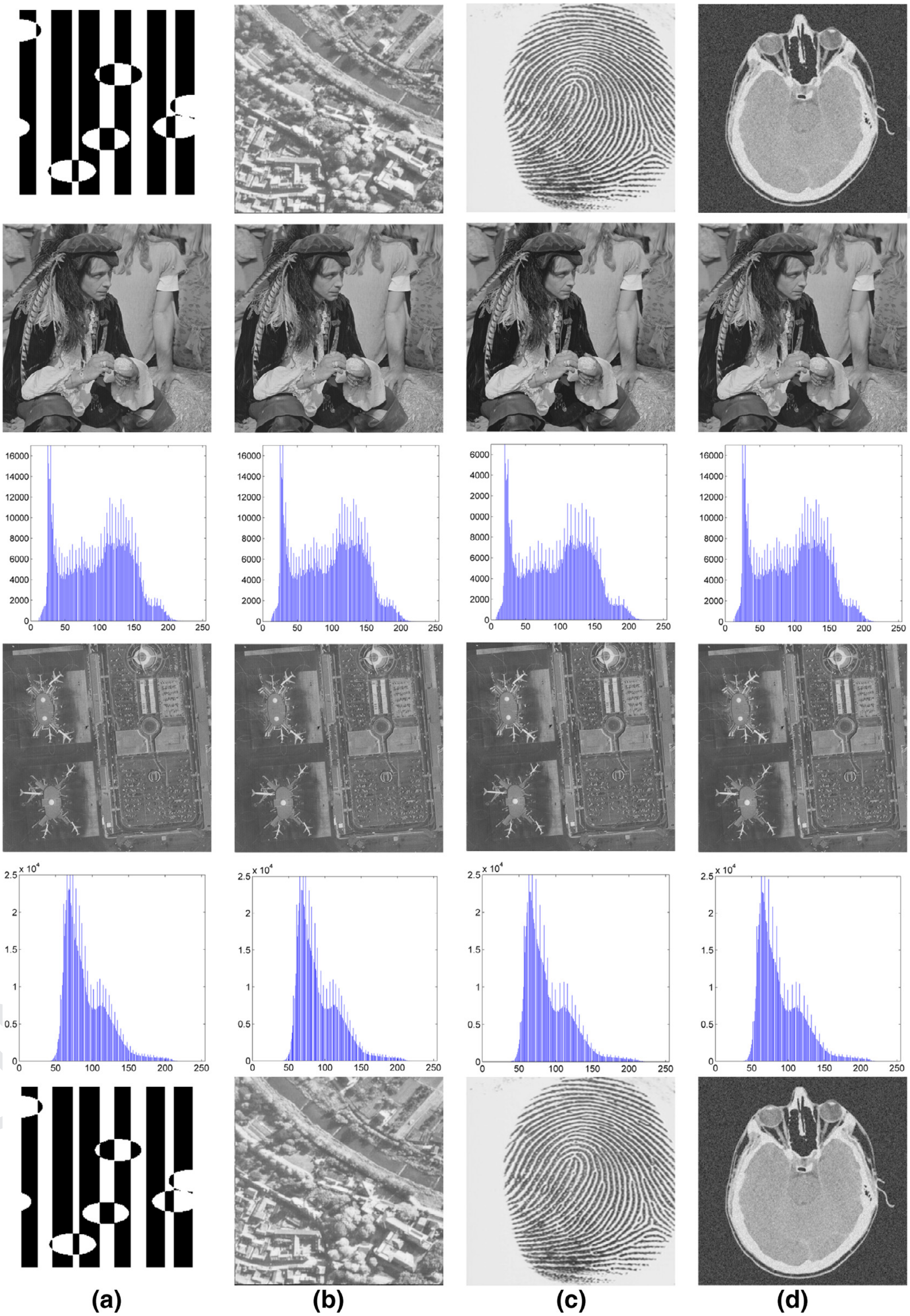

Fig. 5. Simulation results. The first row shows the original images; the second and third rows show the final encrypted images and their histograms using a man image as the reference image; the fourth and fifth rows show the final encrypted images and their histograms using a satellite image as the reference image. (a) binary image encryption using Bao's algorithm [4] in the pre-encryption process; (b) grayscale image encryption using the AES [24] in the pre-encryption process; (c) biometric encryption using Chen's algorithm [9] in the pre-encryption process; (d) medical image encryption using Liao's algorithm [20] in the pre-encryption process.

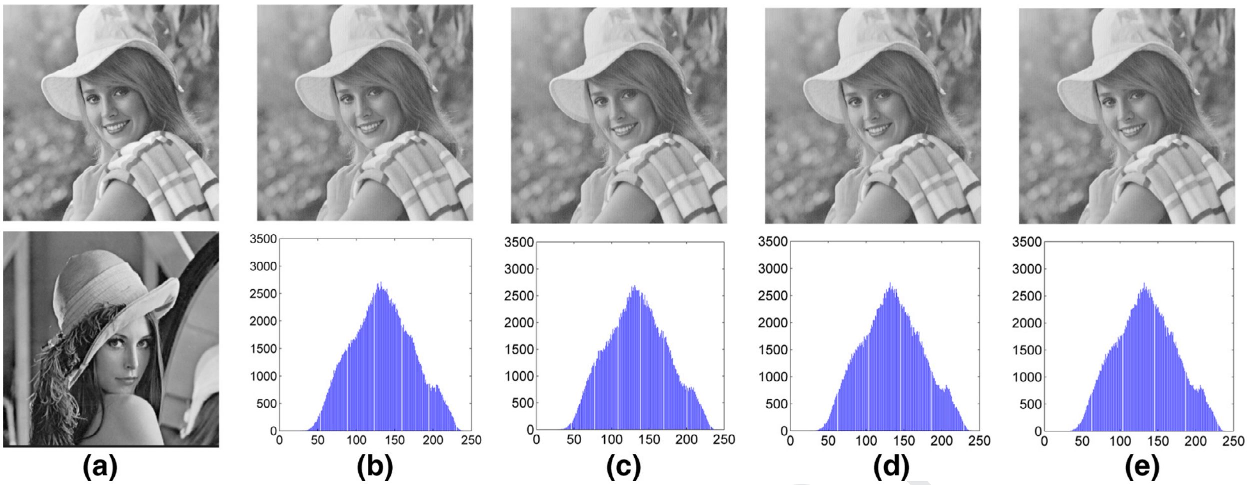

Fig. 6. Image encryption using NIES with different pre-encryption algorithms: (a) the reference image (upper) and original image (bottom); (b)–(e) show the encrypted images when the pre-encryption process uses the: (b) Chen's algorithm [9], (c) Liao's algorithm [20], (d) PSCS-IE algorithm [38], and (e) Wu's [29].

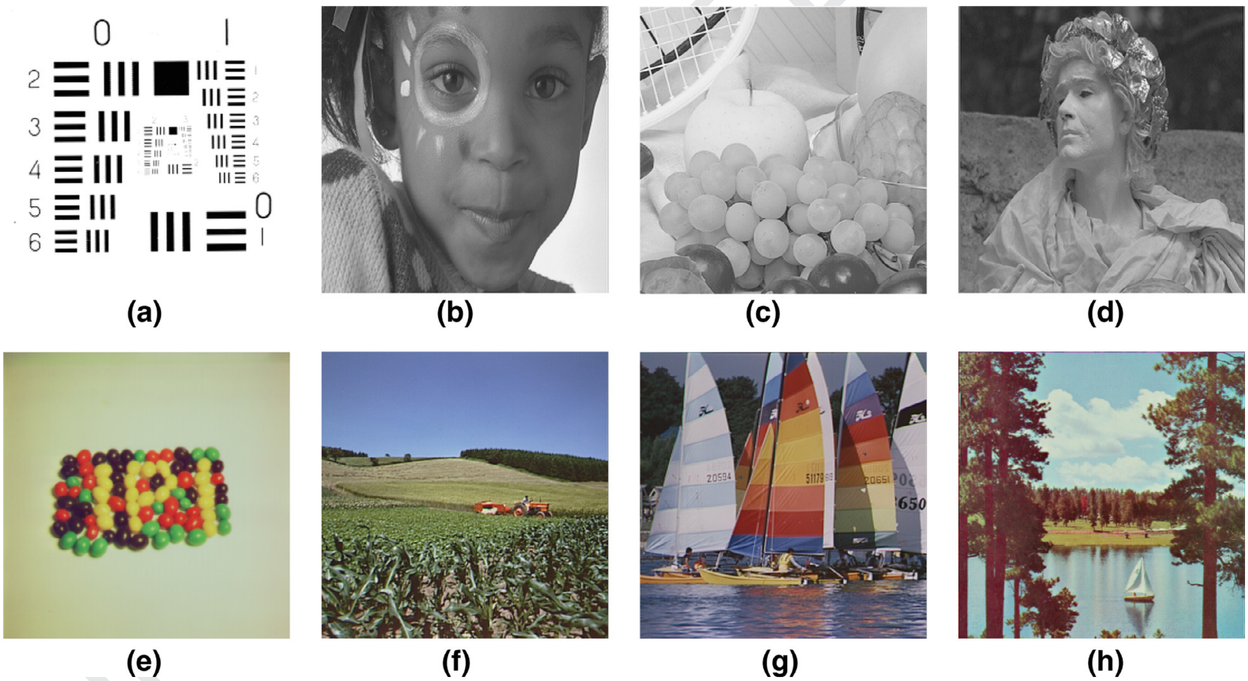

Fig. 7. Image encryption using NIES with different reference images: (a) the original grayscale image; (b)–(d) show the encrypted images using NIES with different grayscale reference images; (e) the original color image; (f)–(h) show the encrypted images using NIES with different color reference images.

4.2. Objective evaluation

Several experimental results have been presented to show visual quality of the encrypted images in Section 4.1. The goal of the proposed NIES is to generate a visually meaningful encrypted image that is similar to a natural image. Here, an objective quality assessment algorithm called TMQI is applied to evaluate the visual quality of the encrypted images of NIES in terms of their naturalness [32]. TMQI combines a multi-scale signal fidelity measure on the basis of a modified structural similarity index and a naturalness measure on the basis of intensity statistics of natural images. The final score (Q) of TMQI is based on the structural fidelity score (S) and statistical naturalness score (N). These three scores are in the range of 0–1. A value closer to 1 means higher quality. Since TMQI is designed only for color images, the encrypted images in the second row of Fig. 7 will be evaluated. The TMQI results are presented in Table 1. Both the naturalness score (S) and final TMQI score (Q) demonstrate that the final encrypted images of NIES are close to natural images. These output encrypted images have demonstrated to solve the problem resulting from the noise-like or texture-like format. If the users want to obtain the resulting images with high

Please cite this article as: L. Bao, Y. Zhou, Image encryption: Generating visually meaningful encrypted images, Information Sciences (2015), http://dx.doi.org/10.1016/j.ins.2015.06.049

Table 1
TMQI test results.

Encrypted images	TMQI values		
	S	*N*	*Q*
Fig. 7(f)	0.9559	0.8533	0.9679
Fig. 7(g)	0.9689	0.9290	0.9822
Fig. 7(h)	0.9649	0.8430	0.9686

Table 2
Execution time comparison of different pre-encryption algorithms (time unit: s).

Algorithms		Pre-encryption (T_1)	NIES (T_2)	DWTCT ($T_2 - T_1$)
AES [24]	**Encryption**	25.6735	25.8734	**0.1999**
	Decryption	36.9069	36.9686	**0.0617**
Wu's [29]	**Encryption**	7.8770	8.0547	**0.1777**
	Decryption	7.7506	7.8113	**0.0607**
Bao's algorithm [4]	**Encryption**	3.9512	4.1354	**0.1842**
	Decryption	3.8867	3.9486	**0.0619**
Wang's algorithm [28]	**Encryption**	11.3704	11.5600	**0.1896**
	Decryption	11.5435	11.6046	**0.0611**

naturalness which may require in specific applications, enlarging the size of the reference image is one potential way to enhance their naturalness.

4.3. Execution time analysis

Computation cost is an important measure of the effectiveness of an encryption algorithm. Because any existing image encryption algorithm can be used in the pre-encryption process, this section mainly discusses the execution time of DWTCT.

In our experiments, we use different encryption algorithms in the pre-encryption process. They are the AES [24], Wu's algorithm [29], Bao's algorithm [4] and Wang's algorithm [28]. The simulation results are shown in Table 2. As can be seen, the third column shows the execution time of DWTCT in the encryption and decryption processes using different pre-encryption algorithms. In average, DWTCT takes only 0.1878s for image encryption and 0.0613s for image decryption. Compared with the execution time of the pre-encryption process, the time consumption of DWTCT is neglectable. This demonstrates that the proposed NIES solves the problem of most existing image encryption algorithms presented in Section 1 without significantly increasing the computation cost.

5. Security analysis

Generally speaking, the security of an encryption algorithm mainly depends on its security key design [23]. The proposed NIES has a sufficiently large key space and high key sensitivity.

5.1. Key space analysis

The security key of NIES is composed of the pre-encryption algorithm and its security key set K_p, and parameter K_t of DWTCT. Any existing image encryption algorithm can be used as the pre-encryption algorithm. Because the integer DWT has at least 37 types of existing wavelet filters, NIES has a security key space at least 37 times larger than that of the pre-encryption algorithm. For example, if we use Bao's algorithm [4] in the pre-encryption process, the possible choices of K_p are 2^{240}. Thus, the key space of NIES is 37×2^{240}.

Although the reference image is not required for reconstructing the original images in image decryption, it acts as a visual protection to the original images. Different reference images yield completely different encrypted images. Therefore, NIES has a security key space large enough to withstand the brute-force attacks.

5.2. Key sensitivity analysis

High key sensitivity of an encryption system means that a tiny change of the security key yields a different output in the encryption or decryption process. Here, the key sensitivity analysis is performed by applying a tiny change to the security key set ($Key = [K_p, K_t]$) of NIES.

Fig. 8 shows the simulation results in image encryption. The pre-encryption process uses Liao's algorithm [20]. We first use $Key = [K_p, K_t]$ where $K_p = [60\ 50\ 40\ 30\ 20\ 55\ 86\ 55\ 44\ 85\ 26\ 15\ 98\ 125\ 45\ 37]$ and $K_t = r9.7$ to encrypt the original image (Fig. 8(a)) and obtain the final encrypted image (Fig. 8(b)). A different key set $Key_1 = [K_p, K_{t1}]$ with K_p unchanged but $K_{t1} = sym8$ is then used to generate another encrypted image as shown in Fig. 8(c). As can be seen from their histograms in Fig. 8(b) and (c), two

Please cite this article as: L. Bao, Y. Zhou, Image encryption: Generating visually meaningful encrypted images, Information Sciences (2015), http://dx.doi.org/10.1016/j.ins.2015.06.049

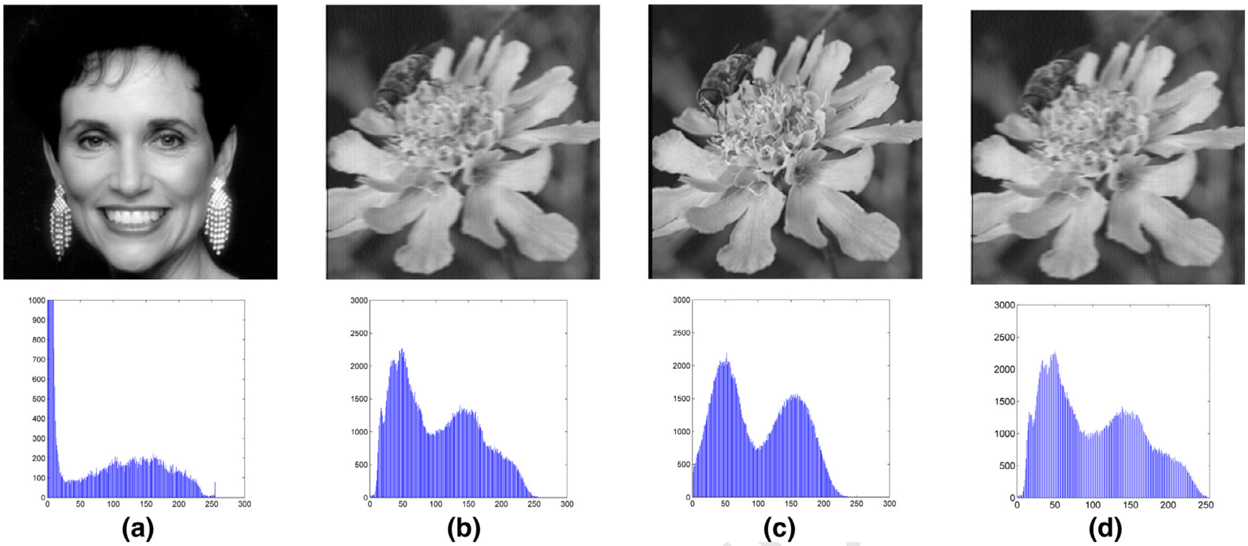

Fig. 8. Key sensitivity test of NIES in image encryption: (a) the original image and its histogram; (b) the encrypted image with *Key* and its histogram; (c) the encrypted image with Key_1 and its histogram; (d) the encrypted image with Key_2 and its histogram.

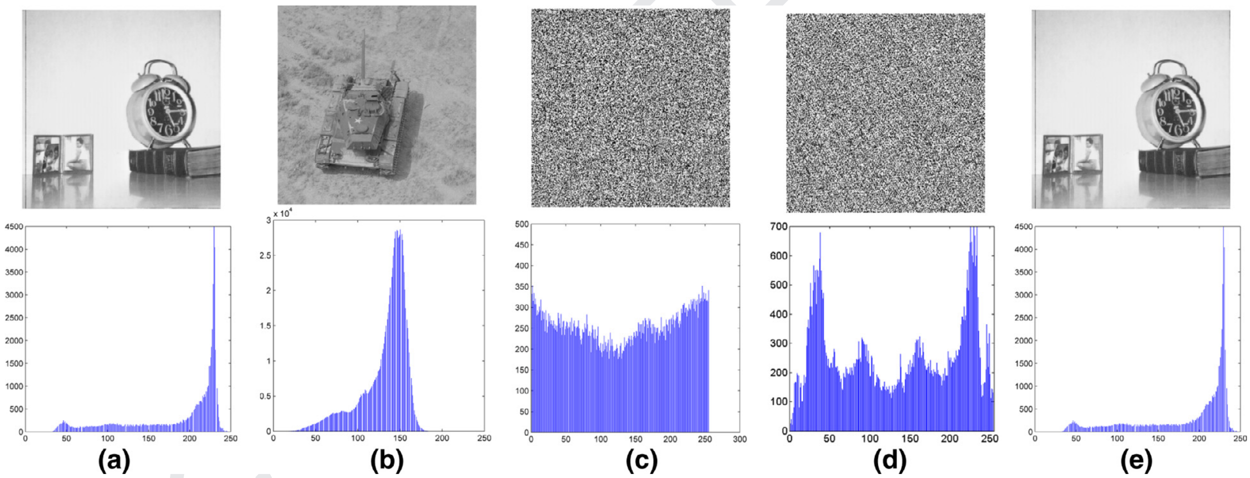

Fig. 9. Key sensitivity test of NIES in image decryption: (a) the original image and its histogram; (b) the encrypted image using Key_3 and its histogram; (c) the decrypted image using Key_4 and its histogram; (d) the decrypted image using Key_5 and its histogram ; (e) the decrypted image using Key_3 and its histogram.

encrypted images are different. This indicates that the change of K_t will result in a different encrypted image. We use $Key_2 = [K_{p1}, K_t]$ with the same $K_t = r9.7$ and a different $K_{p1} = [60\ 50\ 40\ 30\ 20\ 55\ 86\ 55\ 44\ 85\ 26\ 15\ 98\ 125\ 45\ 36]$ to generate an encrypted image as shown in Fig. 8(d). Compared with the encrypted image in Fig. 8(b), they are much similar in terms of visual appearances and histograms. This is because the reference image plays an important role in the format or visual appearance of encrypted images. Changing the security keys only affects the visual quality of encrypted images.

However, the security keys play a significant role in image decryption. We use Chen's algorithm [9] in the pre-encryption process and select $Key_3 = [K_{p3}, K_{t3}]$, where $K_{p3} = [77\ 55\ 43\ 32\ 80\ 55\ 86\ 55\ 44\ 85\ 26\ 15\ 98\ 125\ 45\ 37]$ and $K_{t3} = db1$, to encrypt the original image. Then we use Key_4, Key_5 and Key_3 in image decryption to obtain the decrypted images shown in Fig. 9(c)–(e). Here, $Key_4 = [K_{p3}, K_{t4}]$ and $Key_5 = [K_{p5}, K_{t3}]$ where $K_{t4} = db3$ and $K_{p5} = [78\ 55\ 43\ 32\ 80\ 55\ 86\ 55\ 44\ 85\ 26\ 15\ 98\ 125\ 45\ 37]$. From the decrypted results in Fig. 9(c)–(e), the original image can be reconstructed only when the correct key (Key_3) is being utilized. Any change in the security key will result in an unrecognized reconstructed image. In summary, NIES is highly sensitive to its security key changes in both image encryption and decryption.

5.3. Data loss attack

Data loss is inevitable in transmission channels. A good encryption system should resist the data loss attack.

Fig. 10 shows the simulation results of the data loss attack. Using the PSCS-IE algorithm [38] in the pre-encryption process and a statue image as the reference image, NIES encrypts the original image (Fig. 10(a)) to obtain the final encrypted image

Please cite this article as: L. Bao, Y. Zhou, Image encryption: Generating visually meaningful encrypted images, Information Sciences (2015), http://dx.doi.org/10.1016/j.ins.2015.06.049

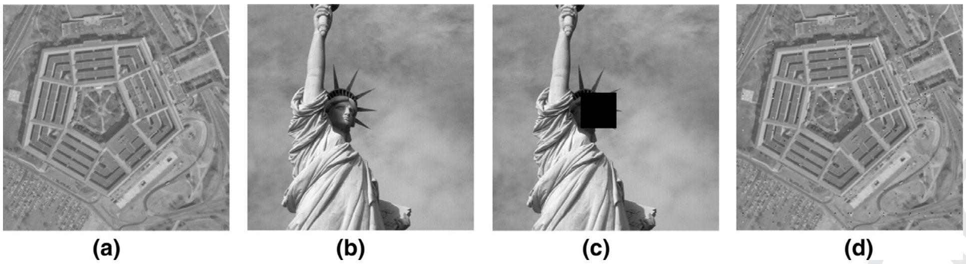

Fig. 10. Data loss attack. (a) The original image; (b) the encrypted image; (c) the encrypted image with 80 × 80 data cutting; (d) the decrypted image from (c).

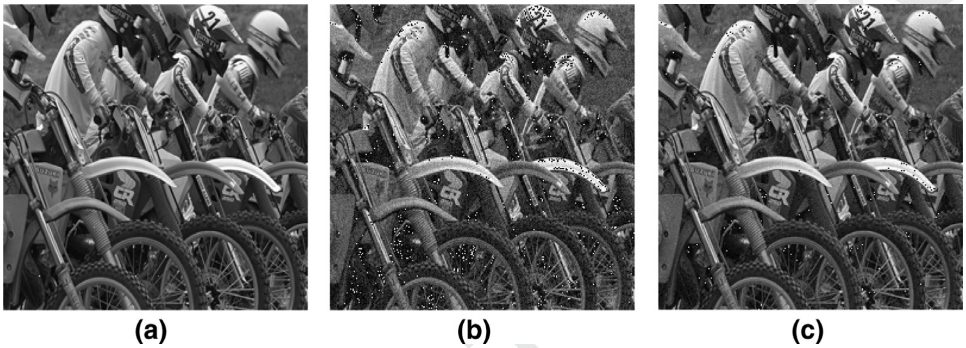

Fig. 11. Reconstructed images after different noise attacks with a noise density of 0.001%. (a) Salt & Pepper noise; (b) Gaussian noise; (c) Speckle noise.

(Fig. 10(b)). A data cutting with a size of 80 × 80 is applied to the encrypted image. The result is shown in Fig. 10(c). The image in Fig. 10(d) is reconstructed from the image in Fig. 10(c). As can be seen, the reconstructed image in Fig. 10(d) contains most visual information of the original image in Fig. 10(a). Only 0.55% pixels are changed after 80 × 80 data loss. This shows that the proposed NIES is able to withstand the data loss attack.

5.4. Noise attack

Images are inevitably contaminated by different types of noise during transmission, amplification and detection. Obviously, an image encryption algorithm with the capability of withstanding noise attack will be suitable for real applications.

To test the proposed NIES against noise attack, we apply three types of noise to the final encrypted images including the Gaussian noise, Salt & Pepper noise and Speckle noise. These images are then reconstructed as the images shown in Fig. 11. From these reconstructed images, the original image contents are shown clearly. These demonstrate that the proposed NIES is able to withstand the noise attacks.

6. Conclusions

To address the security weakness of most existing encryption algorithms whose texture-like or noise-like encrypted images may bring a large number of attacks and analysis, this paper has introduced a new concept of image encryption to generate visually meaningful encrypted images that usually are considered as normal images rather than encrypted ones. With a large amount of formats of encrypted images, the proposed concept ensures the attackers' difficulty of correctly distinguishing and locating the encrypted images from all normal images. Thus, the proposed concept is able to protect the original image with a much higher security level compared with most existing encryption algorithms.

As an implementation example of this concept, we have introduced an image encryption system. It utilizes a pre-encryption process with excellent diffusion and confusion properties to protect the original image contents, and an effective DWT-based content transform to generate visually meaningful encrypted images with many different visual appearances. Simulation results and security analysis have demonstrated that the proposed encryption concept and system show excellent performance and enhance the security of existing image encryption algorithms with a low computation cost. The proposed methods have potential applications for privacy and copyright protection in networks and cloud computing.

Acknowledgment

This work was supported in part by the Macau Science and Technology Development Fund under grant FDCT/017/2012/A1 and by the Research Committee at University of Macau under grants MYRG2014-00003-FST, MRG017/ZYC/2014/FST, MYRG113(Y1-L3)-FST12-ZYC and MRG001/ZYC/2013/FST.

Please cite this article as: L. Bao, Y. Zhou, Image encryption: Generating visually meaningful encrypted images, Information Sciences (2015), http://dx.doi.org/10.1016/j.ins.2015.06.049

References

[1] L. An, X. Gao, X. Li, D. Tao, C. Deng, J. Li, Robust reversible watermarking via clustering and enhanced pixel-wise masking, IEEE Trans. Image Process. 21 (8) (2012) 3598–3611.
[2] L. An, X. Gao, Y. Yuan, D. Tao, Robust lossless data hiding using clustering and statistical quantity histogram, Neurocomputing 77 (1) (2012) 1–11.
[3] L. An, X. Gao, Y. Yuan, D. Tao, C. Deng, F. Ji, Content-adaptive reliable robust lossless data embedding, Neurocomputing 79 (0) (2012) 1–11.
[4] L. Bao, Y. Zhou, C.L.P. Chen, H. Liu, A new chaotic system for image encryption, in: Proceedings of the 2012 International Conference on System Science and Engineering (ICSSE), 2012, pp. 69–73.
[5] G. Bhatnagar, Q.M. Jonathan Wu, B. Raman, Discrete fractional wavelet transform and its application to multiple encryption, Inf. Sci. 223 (0) (2013) 297–316.
[6] S. Bouguezel, A reciprocal-orthogonal parametric transform and its fast algorithm, IEEE Signal Process. Lett. 19 (11) (2012) 769–772.
[7] A.R. Calderbank, I. Daubechies, W. Sweldens, B.-L. Yeo, Wavelet transforms that map integers to integers, Appl. Comput. Harmonic Anal. 5 (3) (1998) 332–369.
[8] C.-K. Chen, C.-L. Lin, C.-T. Chiang, S.-L. Lin, Personalized information encryption using ECG signals with chaotic functions, Inf. Sci. 193 (0) (2012) 125–140.
[9] G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons & Fractals 21 (3) (2004) 749–761.
[10] T.-H. Chen, K.-C. Li, Multi-image encryption by circular random grids, Inf. Sci. 189 (0) (2012) 255–265.
[11] C. Deng, X. Gao, X. Li, D. Tao, A local Tchebichef moments-based robust image watermarking, Signal Process. 89 (8) (2009) 1531–1539.
[12] I.-C. Dragoi, D. Coltuc, On local prediction based reversible watermarking, IEEE Trans. Image Process. 24 (4) (2015) 1244–1246.
[13] J. Franco-Contreras, G. Coatrieux, F. Cuppens, N. Cuppens-Boulahia, C. Roux, Robust lossless watermarking of relational databases based on circular histogram modulation, IEEE Trans. Inf. Forensics Secur. 9 (3) (2014) 397–410.
[14] X. Gao, L. An, X. Li, D. Tao, Reversibility improved lossless data hiding, Signal Process. 89 (10) (2009) 2053–2065.
[15] X. Gao, L. An, Y. Yuan, D. Tao, X. Li, Lossless data embedding using generalized statistical quantity histogram, IEEE Trans. Circuits Syst. Video Technol. 21 (8) (2011) 1061–1070.
[16] X. Gao, C. Deng, X. Li, D. Tao, Geometric distortion insensitive image watermarking in affine covariant regions, IEEE Trans. Syst. Man Cybern. Part C: Appl. Rev. 40 (3) (2010) 278–286.
[17] M. Ghebleh, A. Kanso, H. Noura, An image encryption scheme based on irregularly decimated chaotic maps, Signal Process.: Image Commun. 29 (5) (2014) 618–627.
[18] C. Guo, S. Liu, J.T. Sheridan, Optical double image encryption employing a pseudo image technique in the Fourier domain, Opt. Commun. 321 (0) (2014) 61–72.
[19] Z. Hua, Y. Zhou, C.-M. Pun, C.L. Philip Chen, 2d sine logistic modulation map for image encryption, Inf. Sci. 297 (0) (2015) 80–94.
[20] X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, Signal Process. 90 (2010) 2714–2722.
[21] J.B. Lima, L.F.G. Novaes, Image encryption based on the fractional Fourier transform over finite fields, Signal Process. 94 (0) (2014) 521–530.
[22] K. Ma, W. Zhang, X. Zhao, N. Yu, F. Li, Reversible data hiding in encrypted images by reserving room before encryption, IEEE Trans. Inf. Forensics Secur. 8 (3) (2013) 553–562.
[23] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Inc., New York, 1997.
[24] National Institute of Standards and Technology, Advanced encryption standard (AES), 2001.
[25] C. Qin, C.-C. Chang, Y.-P. Chiu, A novel joint data-hiding and compression scheme based on SMVQ and image inpainting, IEEE Trans. Image Process. 23 (3) (2014) 969–978.
[26] M.G. Shan, J. Chang, Z. Zhong, B.G. Hao, Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps, Opt. Commun. 285 (21–22) (2012) 4227–4234.
[27] S. Tedmori, N. Al-Najdawi, Image cryptographic algorithm based on the haar wavelet transform, Information Sciences 269 (0) (2014) 21–34.
[28] X. Wang, X. Wang, J. Zhao, Z. Zhang, Chaotic encryption algorithm based on alternant of stream cipher and block cipher, Nonlinear Dynamics 63 (4) (2011) 587–597.
[29] Y. Wu, G. Yang, H. Jin, J.P. Noonan, Image encryption using the two-dimensional logistic chaotic map, Journal of Electronic Imaging 21 (1) (2012). 013014–1.
[30] Y. Wu, Y. Zhou, J.P. Noonan, S. Agaian, Design of image cipher using latin squares, Information Sciences 264 (0) (2014) 317–339. Serious Games.
[31] Y.-G. Yang, X. Jia, S.-J. Sun, Q.-X. Pan, Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding, Information Sciences 277 (0) (2014) 445–457.
[32] H. Yeganeh, Z. Wang, Objective quality assessment of tone-mapped images, IEEE Transactions on Image Processing 22 (2) (2013) 657–667.
[33] M. Zanin, A.N. Pisarchik, Gray code permutation algorithm for high-dimensional data encryption, Information Sciences 270 (0) (2014) 288–297.
[34] Y.-Q. Zhang, X.-Y. Wang, A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice, Information Sciences 273 (0) (2014) 329–351.
[35] J. Zhou, X. Liu, O.C. Au, Y.Y. Tang, Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation, IEEE Transactions on Information Forensics and Security 9 (1) (2014) 39–50.
[36] Y. Zhou, K. Panetta, S. Agaian, C.L.P. Chen, (n, k, p)-gray code for image systems, IEEE Transactions on Cybernetics 43 (2) (2013) 515–529.
[37] Y. Zhou, S. Agaian, Image encryption using the image steganography concept and PLIP model, in: 2011 IEEE International Conference on System Science and Engineering (ICSSE), 2011, pp. 699–703.
[38] Y. Zhou, L. Bao, C.L. Philip Chen, Image encryption using a new parametric switching chaotic system, Signal Processing 93 (11) (2013) 3039–3052.
[39] Y. Zhou, L. Bao, C.L. Philip Chen, A new 1D chaotic system for image encryption, Signal Processing 97 (2014) 172–182.
[40] Y. Zhou, K. Panetta, S. Agaian, C.L. Philip Chen, Image encryption using P-Fibonacci transform and decomposition, Optics Communications 285 (5) (2012) 594–608.
[41] Z. Zhu, W. Zhang, K.-W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, Information Sciences 181 (6) (2011) 1171–1186.

Please cite this article as: L. Bao, Y. Zhou, Image encryption: Generating visually meaningful encrypted images, Information Sciences (2015), http://dx.doi.org/10.1016/j.ins.2015.06.049