Image Encryption Based on Edge Information

Yicong Zhou*[a], Karen Panetta[a], Sos Agaian[b]
[a] Department of Electrical and Computer Engineering, Tufts University, Medford, MA 02155
[b] Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249

ABSTRACT

This paper presents a new concept of image encryption which is based on edge information. The basic idea is to separate the image into the edges and the image without edges, and encrypt them using any existing or new encryption algorithm. The user has the flexibility to encrypt the edges or the image without edges, or both of them. In this manner, different security requirements can be achieved. The encrypted images are difficult for unauthorized users to decode, providing a high level of security. We also introduce a new lossless encryption algorithm using 3D Cat Map. This algorithm can fully encrypt 2D images in a straightforward one-step process. It simultaneously changes image pixel locations and pixel data. Experimental examples demonstrate the performance of the presented algorithm in image encryption. It can also withstand chosen-plaintext attack. The presented encryption approach can encrypt all 2D and 3D images and easily be implemented in mobile devices.

Keywords: image encryption, edge information, 3D cat map, chosen-plain attack.

1. INTRODUCTION

With the growth and development of network and wireless communication technologies, people all over the world can access the internet by computers and cell phones. Every day, people put vast quantities of images or videos online for different purposes. These images or videos may contain private information, or copyrighted material, or security data. Providing security for images or videos becomes an important issue not only for individuals and companies but also for government and military applications. Image encryption is an effective method to protect images and videos to help preserve the integrity of private or copyrighted materials.

There are many different approaches for image encryption. Traditional methods for image encryption are based on cryptograph concept such as Data Encryption Standard (DES) [1] and Advanced Encryption Standard (AES) [2, 3]. They consider image or videos as a data sequence or stream and encrypt them byte by byte or block by block. However, their encryption/decryption processes have huge computation complexity. Many interesting encryption methods are based on different recursive sequences such as Fibonacci number [2, 3], Gray code [4, 5]. These approaches encrypt images by changing image pixel positions using recursive sequences. Nevertheless, their security levels are extremely low due to lack of security keys or small key spaces.

To efficiently encrypt images while providing higher levels of security, our previous work presented some image encryption algorithms using P-Fibonacci sequence [6], P-recursive sequence [7], and Generalized P-Gray Code [8]. These encryption approaches provide larger number of security keys such that the unauthorized users have difficulty to decode the images by exhaust searching all possible combinations of security keys to deduce the correct security keys. However, the permutation-only based image encryption algorithm is vulnerable when subjecting to plaintext attacks [9].

One solution is to change image pixel values while changing the image pixel positions. Some encryption algorithms have been presented recently which are based on different chaotic maps. The encryption algorithms frequently use two different chaotic maps: One is used to change image pixel positions; the other is for changing image data. For example, the algorithm using the Arnold cat map and Chen's chaotic system is presented in [10, 11], and the algorithm based on the hyperchaotic map and chaotic logistic map is shown in [12]. However, their approaches are not efficient.

* Yicong.Zhou@tufts.edu; phone 1 617 627-5183; fax 1 617-627-3220

Multimedia on Mobile Devices 2009, edited by Reiner Creutzburg, David Akopian, Proc. of SPIE-IS&T Electronic Imaging, SPIE Vol. 7256, 725603 · © 2009 SPIE-IS&T · CCC code: 0277-786X/09/$18 · doi: 10.1117/12.805512

Another possible solution is to separate image into two different images using a specific algorithm, such as the edge detection method, and encrypt them individually. Since edge information is widely used in image enhancement, compression, segmentation and recognition, we investigate a new application of edge information in image encryption.

In this paper, we introduce a new concept of image encryption using edge information. This method first separates the image into edges and the image without edges, and then encrypts them using the existing or new encryption algorithms. The users have flexibility to use any existing or new encryption method to encrypt edges, or the image without edges, or both of them to meet different security requirements. The presented approach can be used to encrypt 2D images and 3D images such as grayscale images, medical images and color images in real-time applications, for example, wireless communication and mobile phone services. Since the edge information is frequently used in image compression, the presented encryption approach can also embedded in image compression process such that edge information can be preserved in the compression process and encryption process can provide security for images.

In addition, we introduce a novel image encryption algorithm based on a new 3D cat map which is an example to demonstrate the performance of the presented concept. The encryption algorithm can change the positions and values of the image pixels simultaneously. The edges and the image without edges of a certain image are different when the edge detection methods or their thresholds are different. These ensure the unauthorized user's difficulty to decode the encrypted images. As a result, the original images can be protected with high level of security. The experimental results show that the algorithm is lossless encryption method. The original images can be completely reconstructed without any distortion. The presented algorithm can withstand the chosen-plaintext attack.

The rest of this paper is organized as followed. Section 2 will introduce the new concept of image encryption using edge information. A new 3D cat map and a new 3D cat map based image encryption algorithm will be introduced in Section 3. Experimental results and security analysis will be discussed in Section 4 to demonstrate the performance of the presented encryption algorithm. A conclusion will be reached in Section 5.

2. IMAGE-EDGE ENCRYPTION

Edge information is frequently used for image enhancement, denoising, compression, segmentation and recognition. In this section, we introduce a new concept of image encryption using edge information. The encryption algorithm will be also presented in this section. The presented algorithm can be used for encrypting 2D and 3D images, for example, grayscale image, medical images and color images, in real-time applications such as wireless communication, mobile phone services and many others.

2.1. 2D Image-Edge Encryption Algorithm

The 2D images such as grayscale images and 2D medical image are 2D data matrices. The image encryption algorithm based on edge information first gets edge map of the image using any existing edge detection method with a specific threshold, separates the image into edges and the image without edges, and then applies any existing or new encryption algorithm to encrypt the edges, or the image without edges, or both of them, combines the encrypted edges and the encrypted image without edges to get the encrypted 2D image with a format of the complex number, for example, set the encrypted edges into the imaginary part of the complex number, and put the image without edges into the real part of the complex number. The block diagram of the algorithm is shown in Fig.1.

The user has flexibility to choose any existing or new edge detector and its threshold to get the edge maps of the images, and encrypt the edges or the image without edges, or both of them to achieve the different security requirements for real-time applications. He also has flexibility to select any existing encryption algorithm or create a new algorithm for the encryption process. The security keys of the presented encryption algorithm are the combination of the type of the edge detector, the threshold of the edge detector, and the security keys of the encryption algorithm used to encrypt edges and the image without edges.

To reconstruct the original image, the encrypted image is separated into the encrypted edges and the encrypted image without edges. They are decoded individually to reconstruct the edges and the image without edges. The reconstructed image can be obtained by combing the recovered edges and the reconstructed image without edges.

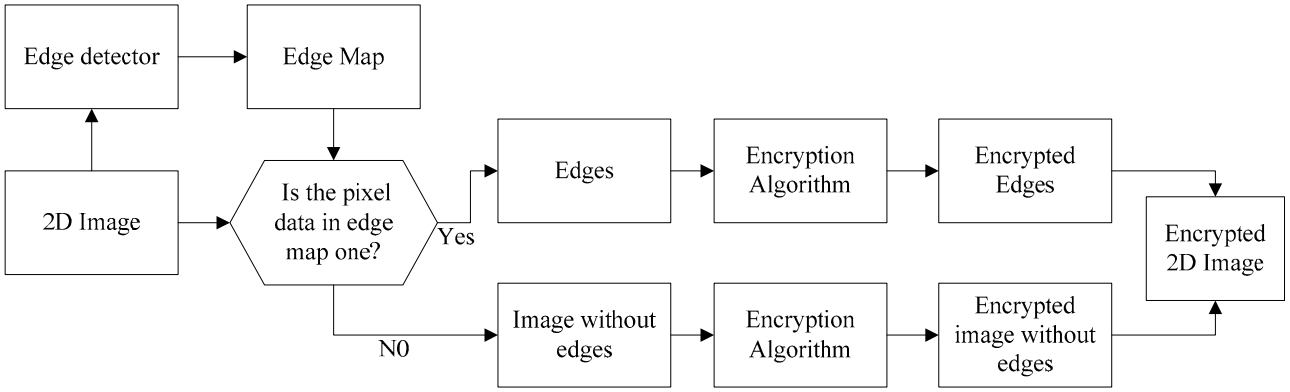

Fig. 1: Image-Edge Encryption Algorithm.

2.2. 3D Image Encryption

The 3D images contain three 3D data matrices. For example, color images consist of three 2D data matrices in which each of them stands for one color plane. Each 2D data matrix, called the 2D component, can be considered as a 2D image. The 3D image encryption can be accomplished by encrypting three 2D components one by one using the presented 2D image encryption algorithm.

3. THE 3D CAT MAP BASED IMAGE ENCRYPTION ALGORITHM

In this section, we will introduce a new 3D Cat Map and its corresponding transforms. A new image encryption algorithm using this 3D Cat Map will be also introduced as an example of the presented encryption concept.

3.1. The 3D Cat Map and its Transforms

Definition 3.1: The 2D Arnold cat map is a chaotic map defined as [11, 13].

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = (A \begin{bmatrix} x_n \\ y_n \end{bmatrix}) \bmod N = (\begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix}) \bmod N \tag{1}$$

where a, b are positive integers, $\det(A) = 1$.

Definition 3.2: The 3D Arnold cat map is defined as.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} == (A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix}) \bmod N = (\begin{bmatrix} 1 & a & b \\ c & ac+1 & bc \\ d & abcd & bd+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix}) \bmod N \tag{2}$$

where a, b, c, d are positive integers, $\det(A) = 1$.

Definition 3.3: Let (x, y) be the location of an image pixel with value I in an $N \times N$ image, the following transformation is called the cat map transform.

$$\begin{bmatrix} x' \\ y' \\ I' \end{bmatrix} = (\begin{bmatrix} 1 & a & b \\ c & ac+1 & bc \\ d & abcd & bd+1 \end{bmatrix} \begin{bmatrix} x \\ y \\ I \end{bmatrix}) \bmod N \tag{3}$$

where a,b,c,d are positive integers, (x',y') is the new location of the pixel with a new value $I'(x,y)$, $x,y,x',y' = 1,2,...N$ and $0 \le I, I' \le 255$.

The cat map transform above can change the image pixel positions and pixel values simultaneously. It can efficiently encrypt the 2D images. The user has flexibility to choose the number of iterations for applying the cat map transform to achieve different levels of security. The parameters a,b,c,d and iteration times n can act as security keys for image encryption.

To reconstruct the original image, we cannot directly use the cat mp transform due to the mod operation in the transform. Therefore, we introduce two coefficient matrices: the row coefficient matrix and the column coefficient matrix.

The row coefficient matrix of the cat map transform $T_r(N,N)$ can be generated as

$$T_r(x,j) = \begin{cases} 1 & (x,x') \\ 0 & otherwise \end{cases} \tag{4}$$

where $x, j = 1,2,...,N$.

The column coefficient matrix of the cat map transform $T_c(N,N)$ can be generated as

$$T_c(i,y) = \begin{cases} 1 & (y',y) \\ 0 & otherwise \end{cases} \tag{5}$$

where $i, y = 1,2,...,N$.

These two coefficient matrices will differ based on the combination of the parameters a,b,c,d and iteration times n. Some examples are given in the Table 1.

Table 1. Coefficient matrices of the cat map transform for an 8×8 image.

(a,b,c,d,n)	T_r	T_c
(3,5,10,20,5)	$\begin{pmatrix} 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \end{pmatrix}$	$\begin{pmatrix} 0&0&0&0&0&1&0&0 \\ 1&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&1&0&0&0&0&0 \end{pmatrix}$

Definition 3.4: Let E be the encrypted image, T_r^{-1}, T_c^{-1} be the inverse matrices of the row and column coefficient matrices defined in equation (4) and (5) respectively. The following transformation is called the Inverse cat map transform:

$$R = T_r^{-1} E T_c^{-1} \tag{6}$$

where R is the reconstructed image.

To recover the pixel values of the original image, we introduce another one dimensional matrix. Let the input of cat map transform be $I = (0,1,2,...,255)$, the output of the cat map transform will be $I' = (I_1', I_2', I_3', ..., I_{256}')$ for a certain combination of the parameters a,b,c,d. The pixel value in the reconstructed image will be,

$$R(x,y) = \alpha - 1 \text{ for } I'_{\alpha} = E(x,y) \tag{7}$$

where $R(x,y)$ is the pixel value of the reconstructed image with location (x,y), $E(x,y)$ is the pixel value of the encrypted image with location (x,y).

Each pixel value among 0 to 255 in original data matrix I has a unique corresponding value in the encrypted data matrix I'. In this manner, we can recover the pixel values of the original image by searching the value in the encrypted data matrix I'.

3.2. The 3D Cat Map Based Image Encryption Algorithm

The 2D image is separated into edges and the image without edges by applying an existing edge detection method such as Sobel, Canny, Prewitt and many others. Both edges and the image without edges are encrypted by applying the cat map transform. The encryption process is straightforward process. The encrypted image can be obtained by combing the encrypted results with a format of the complex numbers.

Algorithm	***The 3D Cat Map Based Image Encryption Algorithm***
Input	3D Image (or 2D image) to be encrypted
Step 1	Select an edge detection method and its threshold value.
Step 2	Separate the 3D image into three 2D components. (2D image: Skip this step.)
Step 3	Get the edge maps of all 2D components using the selected edge detection method.
Step 4	Separate all 2D components into edges and the images without edges based the corresponding edge maps.
Step 5	Select the parameters (a,b,c,d,n) for the cat map transform.
Step 6	Encrypt all edges and the images without edges individually by applying the cat map transform defined in equation (3).
Step 7	Combine the encrypted edges and the encrypted image without edges for each 2D component into a format of the complex number, for example, put the encrypted edges into the imaginary part of the complex number, and put the image without edges into the real part of the complex number. (2D image: Combine the encrypted edges and the encrypted image without edges to get the encrypted 2D image.)
Step 8	Combined the three encrypted components together to get the encrypted 3D image. (2D image: Skip this step.)
Output	The encrypted 3D image (or the encrypted 2D image)

The type of the edge detection method and its threshold value, the parameters and iteration times of the cat map transform can act as the security keys for the presented 3D cat map based encryption algorithm. These security keys have infinite number of possible combinations. It is impossible for unauthorized user to deduce the correct combination of the security keys by searching all possible cases of the security keys. The encrypted images are extremely difficult for the unauthorized users to decode. As a result, the image can be protected with high level of security.

To reconstruct the original image, the authorized user will be provided the security keys: the type of the edge detection method and its threshold, and the parameters and iteration times of the cat map transform. The decryption process is also straightforward. The encrypted image is separated into edges and the image without edges. They are decoded individually by using the inverse cat map transform. The original image can be reconstructed by combing the recovered edges and the decrypted image without edges. For 3D image, the original image can be reconstructed by recovering the three 2D components one by one.

Algorithm ***The 3D Cat Map Based Image Decryption Algorithm***

Input	The encrypted 3D Image (or 2D image) to be decrypted
Step 1	Separate the encrypted 3D image into three 2D components. (2D image: Skip this step.)
Step 2	Separate all 2D components into edges and the images without edges.
Step 3	Generate the row and column coefficient matrices T_r, T_c and image value matrix I' using the cat map transform and parameters (a, b, c, d, n)
Step 4	Apply the inverse cat map transform to all edges and images without edges separately to recover the pixel locations.
Step 5	Recover the pixel values of all edges and images without edges separately based on the equation (7).
Step 6	Combine the recovered edges and the reconstructed image without edges to get corresponding reconstructed 2D components. (2D image: Combine the recovered edges and the reconstructed image without edges to get reconstructed 2D image.)
Step 7	Combined the three 2D components together to get the reconstructed 3D image. (2D image: Skip this step.)
Output	The reconstructed 3D image (or 2D image)

4. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

We successfully implement the 3D cat map based image encryption algorithm in several 2D and 3D images. Some experimental results will be provided to show the performance of the presented encryption method in this section. Canny edge detector is used to get edge maps in our experiments. We encrypt both edges and the image without edges in all experimental examples in this section.

4.1. 2D Image Encryption

The 2D image consists of only one 2D data matrix. Fig.1 gives an example of grayscale image encryption. The edges in Fig.2 (b) contain all pixels in the original image with the same locations of the edge map generated by using Canny edge detector with threshold 0.1. The image without edges in Fig.2 (c) is the results of difference between the original image (Fig.2 (a)) and its edges (Fig.2 (b)).

Both of them are encrypted by the presented 3D cat map based image encryption algorithm with security key: $a = 15, b = 17, c = 18, d = 100, n = 20$. The encrypted image shown in Fig.2 (d) contains a data format of complex number in which the imaginary part is the encrypted edges and the real part is the encrypted image without edges. Its histogram in Fig. 1(i) shows that the distribution of pixel values of the encrypted image is almost uniform. The encrypted image is significantly different from the original image. This makes the encrypted image completely unrecognizable.

The original image can be completely reconstructed without any distortion. The reconstructed image in Fig.2 (e) is visually the same as the original image. This can be also demonstrated by the histogram of difference between the original image and the reconstructed image shown in Fig.2 (j).

Another example of grayscale image encryption is shown in Fig.3. In this example, we choose Sobel method for edge detection with threshold 0.1 and select different parameters of 3D cat map, $a = 3, b = 5, c = 10, d = 20, n = 5$, for encryption process. The edges and the image without edges are different after applying different edge detection methods and thresholds. The original image can also be completely recovered without any distortion.

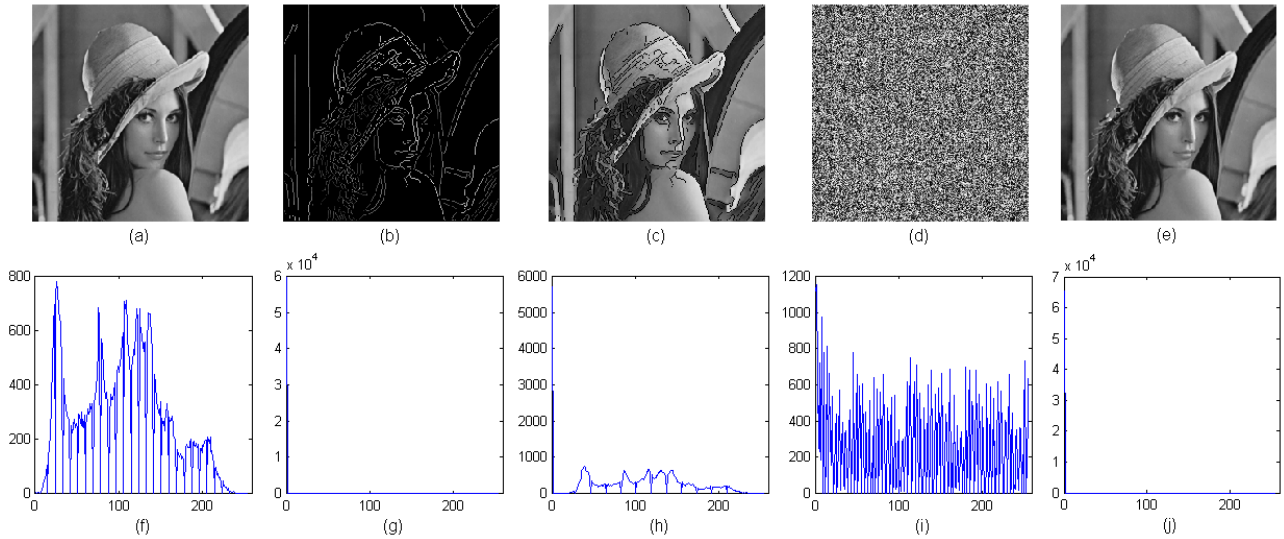

Fig. 2: Grayscale image encryption (a) The original grayscale image; (b) Edges using Canny edge detector with threshold 0.1; (c) Image without edges; (d) Encrypted grayscale image with security keys, $a=15, b=17, c=18, d=100, n=20$; (e) Reconstructed image; (f) Histogram of (a); (g) Histogram of (b); (h) Histogram of (c); (i) Histogram of (d); (j) Histogram of the difference between (a) and (e).

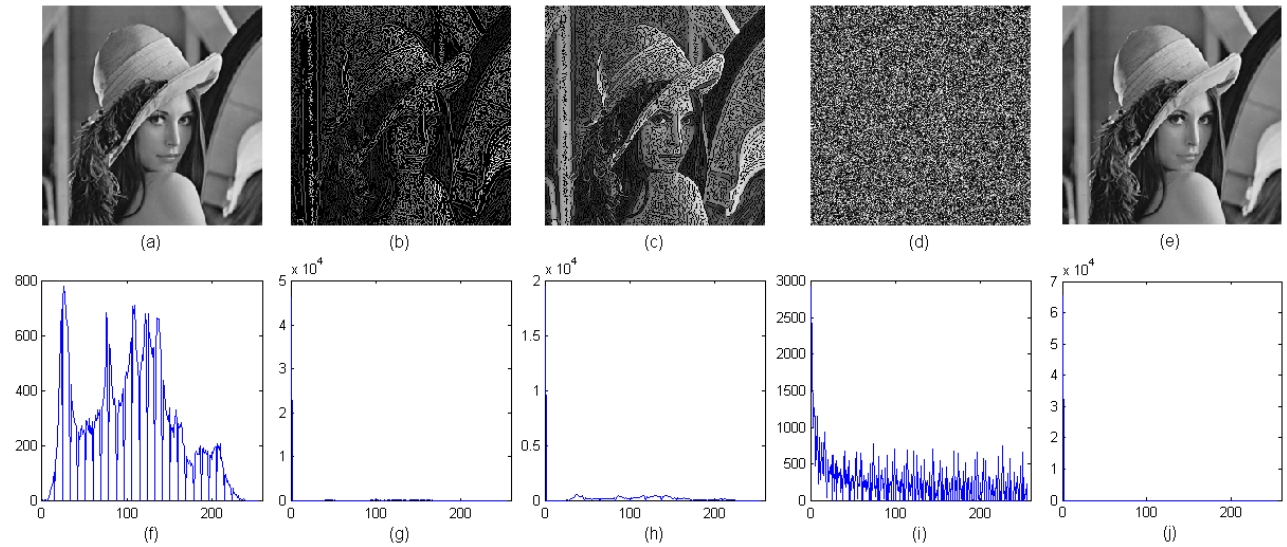

Fig. 3: Grayscale image encryption (a) The original grayscale image; (b) Edges using Sobel edge detector with threshold 0.1; (c) Image without edges; (d) Encrypted grayscale image with security keys, $a=3, b=5, c=10, d=20, n=5$; (e) Reconstructed image; (f) Histogram of (a); (g) Histogram of (b); (h) Histogram of (c); (i) Histogram of (d); (j) Histogram of the difference between (a) and (e).

Fig.4 gives a result of medical image encryption which is another example of the 2D image encryption. The edge detection and encryption processes are the same as that in Fig.2 but the threshold for edge detection process and security keys in the encryption process are different. The original image can be fully encrypted (shown in Fig.4 (d)) and completely reconstructed (shown in Fig.4 (e)). This perfect reconstruction can be demonstrated by the reconstructed

image in Fig.4 (e) and the histogram of the difference between the original image and the reconstructed image in Fig.4 (f). All these verify that the presented algorithm is a lossless encryption approach.

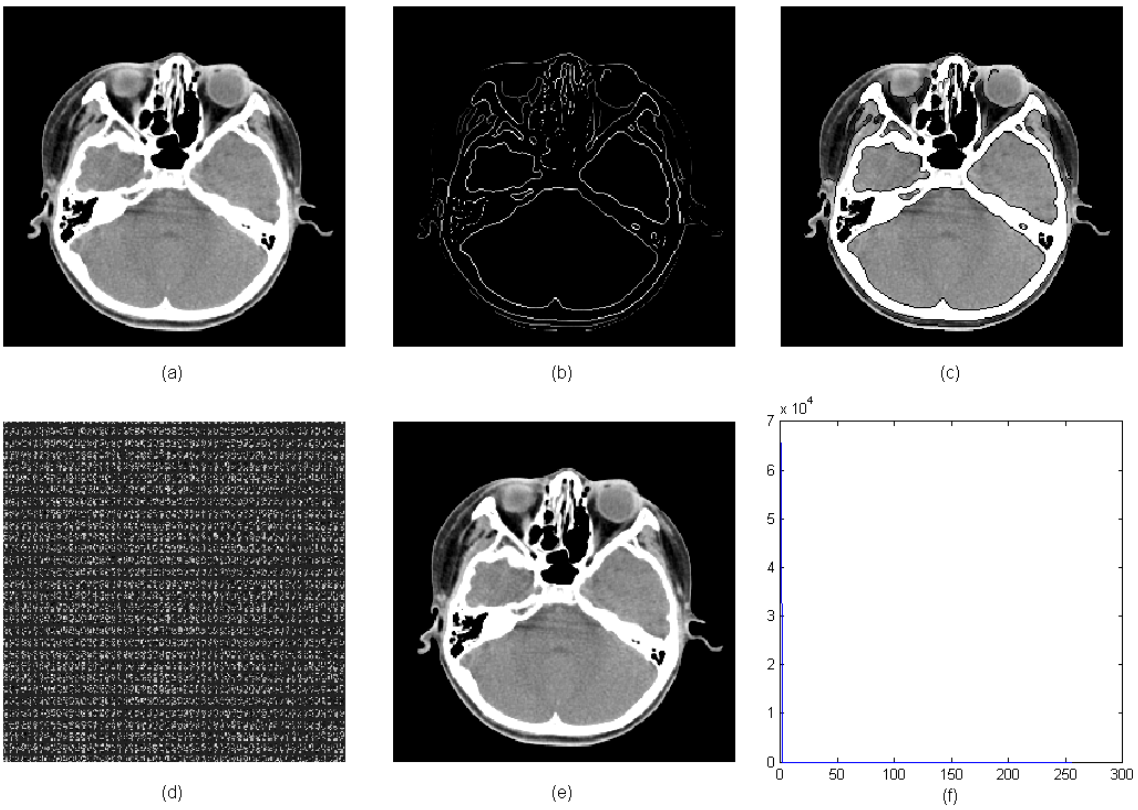

Fig. 4: Medical image encryption (a) The original medical image; (b) Edges using Canny edge detector with threshold 0.3; (c) Image without edges; (d) Encrypted medical image with security keys, $a=5, b=7, c=8, d=10, n=7$; (e) Reconstructed image; (f) Histogram of the difference between (a) and (e).

4.2. 3D Image Encryption

The 3D images such as color images contain three 2D components. The 3D image encryption can be done by encrypting the three 3D components one by one. An example of color image encryption is shown in Fig.5. The Canny edge detection method and threshold 0.1 are used to obtain edges and the image without edges. Security keys for encryption process are $a=3, b=5, c=10, d=20, n=5$. The original image can be completely recovered which is shown in Fig.5 (e). The histogram in Fig.5 (f) demonstrates this lossless reconstruction.

Fig.6 presents another example of color image encryption. The Sobel edge detector with threshold 0.3 is used to get edges and the image without edges in this example. The results of the edges (shown in Fig.6 (b)) and the image without edges (shown in Fig.6 (c)) are different from these in Fig.5. The different combination of the parameters of 3D cat map, $a=5, b=7, c=8, d=10, n=7$, is also applied to encryption process. The original image can also be completely reconstructed. These further demonstrate that the presented algorithm is a lossless encryption method.

The edge detector, threshold value and the parameters of the 3D cat map are the same for all 2D components of the 3D images in the results in Fig.5 and Fig.6. The users have flexibility to choose different edge detector, threshold, and the parameters for each 2D component providing higher levels of security to meet different security requirements in the real-time applications such as the wireless communication and mobile phone services.

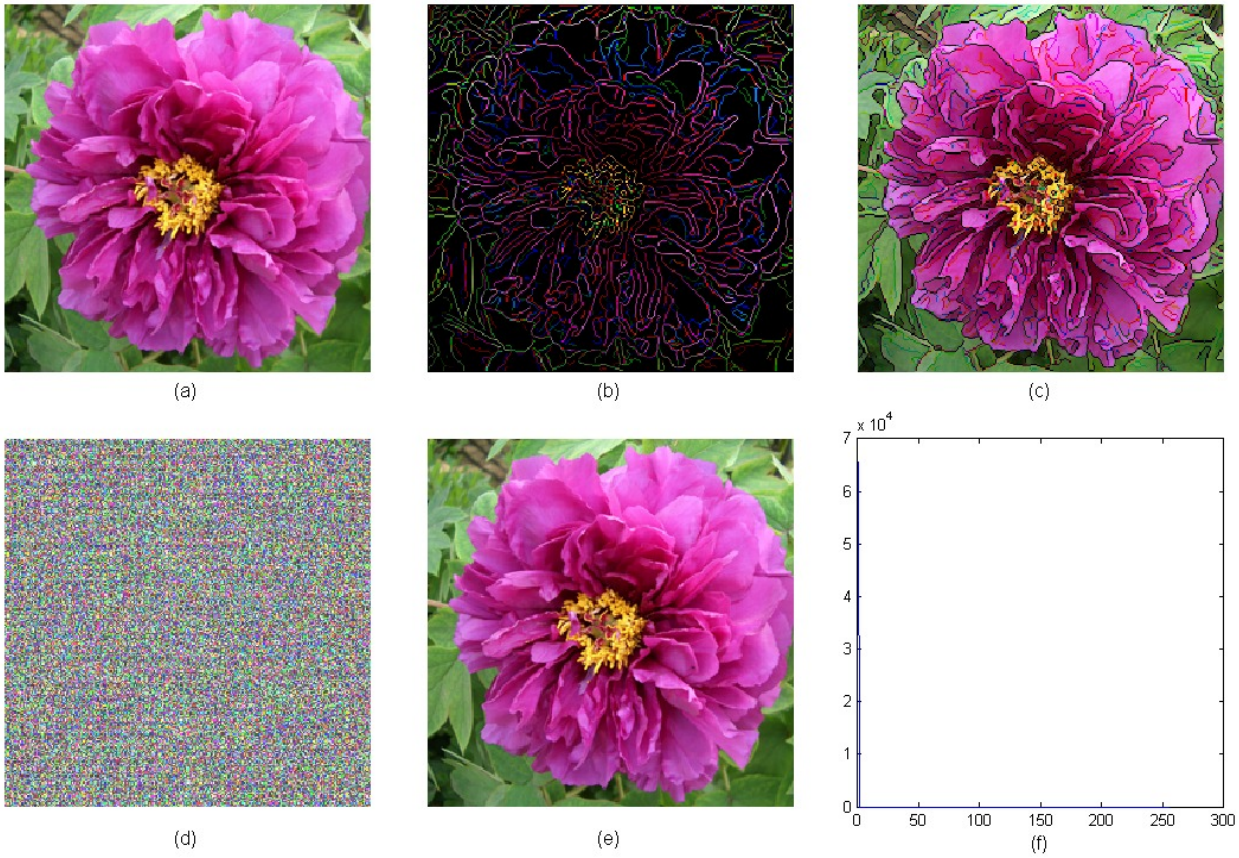

Fig. 5: Color image encryption (a) The original color image; (b) Edges using Canny edge detector with threshold 0.1; (c) Image without edges; (d) Encrypted color image with security keys, $a = 3, b = 5, c = 10, d = 20, n = 5$; (e) Reconstructed color image; (f) Histogram of the difference between (a) and (e).

4.3. Security Analysis

The security key space of the presented 3D cat map based image encryption algorithm consists of the type of the edge detectors, threshold values, the parameters and iteration times of the 3D cat map. Each of them has infinite number of possible choices. Their combination is also infinite. Therefore, the key space of the presented encryption algorithm is unlimited. It is impossible for the unauthorized users to decode the encrypted image by deducing the correct combination of the security keys via exhausted searching all possible choices in the security key space. As a result, the image can be protected with high level of security.

In cryptanalysis, the chosen-plaintext attack is an attack model in which the attacker can choose a number of plaintexts and then get their corresponding ciphertexts. In this manner, the attacker can choose any useful information as plaintext in order to deduce the security keys of encryption algorithms, or reconstruct the original plaintexts from the unknown ciphertexts. This attack can break the encrypted image without knowing the encryption algorithm and its security keys if the image pixel values are not changed by the encryption process.

The 3D cat map based image encryption algorithm changes image pixel values while changing the locations of all image pixels. This ensures that the encrypted image data is not useful for chosen-plaintext attack. As a result, the presented algorithm can withstand the chosen-plain text attack.

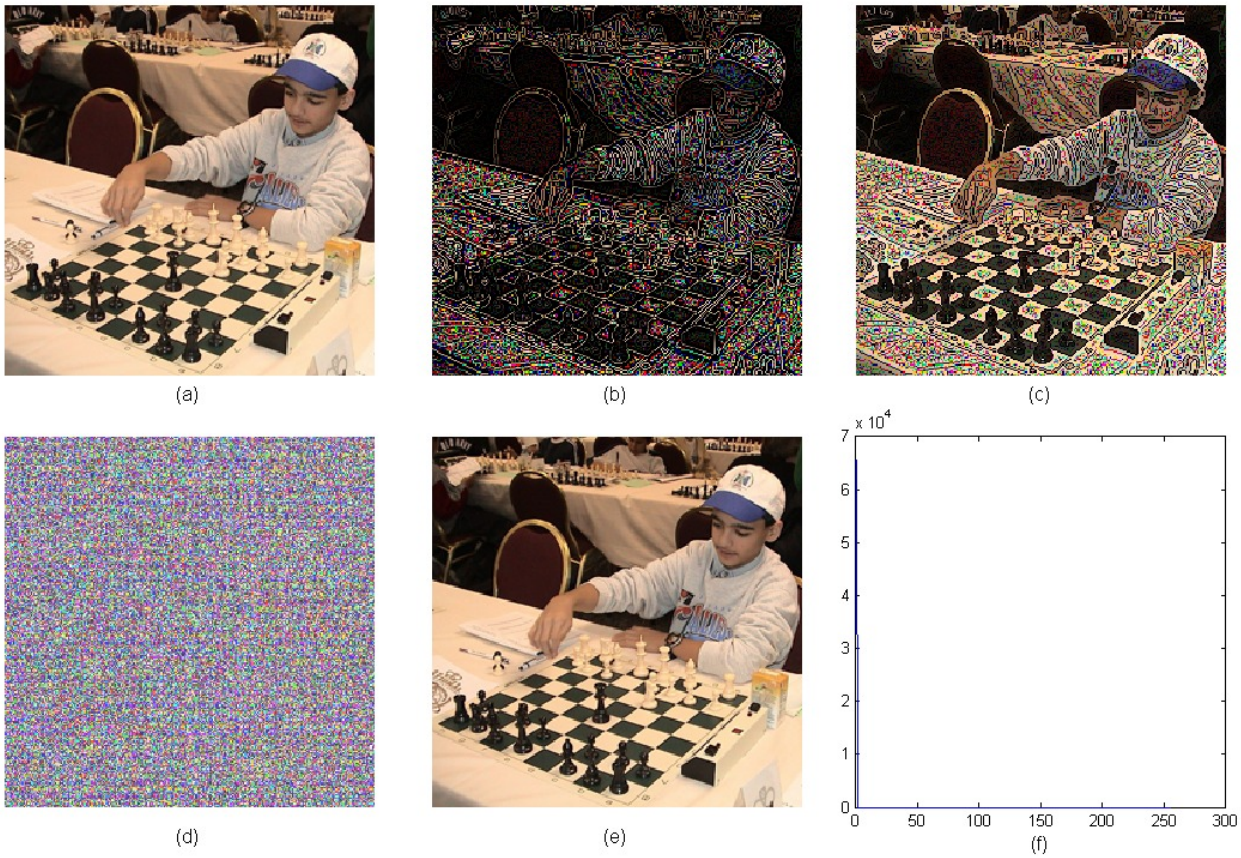

Fig. 6: Color image encryption (a) The original color image; (b) Edges using Sobel edge detector with threshold 0.3; (c) Image without edges; (d) Encrypted color image with security keys, $a = 5, b = 7, c = 8, d = 10, n = 7$; (e) Reconstructed color image; (f) Histogram of the difference between (a) and (e).

5. CONCLUSION

In this paper, we introduced a new concept of image encryption using edge information. The idea of this concept is to separate the image into edges and the image without edges using any existing edge detectors, and then encrypt either edges or the image without edges, or both of them by using any existing or new encryption algorithm, combine the encrypted results to get the encrypted image. To meet different security requirements in real-time applications, the user has flexibility to choose any existing method and its threshold for edge detection, select any encryption method and its security keys for encryption process, and encrypt either edges or image without edges, or bother of them.

To show the performance of the presented new concept, we introduced a new image encryption algorithm using a new 3D cat map as an example of the presented concept. The presented encryption algorithm can efficiently encrypt the 2D and 3D images. The encryption process is straightforward. It changes image pixel positions and pixel data at the same time. The experimental results showed that the presented 3D cat map based algorithm is lossless encryption method because the original images can be completely reconstructed without any distortion.

The security keys of the presented 3D cat map based image encryption algorithm have infinite number of possible combinations. This ensures that the encrypted images are extremely difficult for the unauthorized users to decode. As a result, the images are protected with high level of security. The presented encryption algorithm can also resist the chosen-plaintext attack because the encryption process changes the image pixel values. The presented concept and 3D cat map based encryption algorithm can be used for wireless communication and mobile phones services in real-time applications.

REFERENCES

[1] National Institute of Standards and Technology, "Data Encryption Standard (DES)," http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, 1999.

[2] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001.

[3] Qibin Hou and Yangsheng Wang, "Security traffic image transmission based on EZW and AES," in *Intelligent Transportation Systems, 2003. Proceedings. 2003 IEEE*, 2003, pp. 86-89 vol.1.

[4] Jiancheng Zou, Rabab K. Ward, and Dongxu Qi, "A new digital image scrambling method based on Fibonacci numbers," in *Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International Symposium on*, 2004, pp. III-965-8 Vol.3.

[5] Jiancheng Zou, Rabab K. Ward, and Dongxu Qi, "The generalized Fibonacci transformations and application to image scrambling," in *Acoustics, Speech, and Signal Processing, 2004. Proceedings. (ICASSP '04). IEEE International Conference on*, 2004, pp. iii-385-8 vol.3.

[6] Wei Ding, Weiqi Yan, and Dongxu Qi, "Digital Image Scrambling Technology Based on Gray Code," in *Proc. of International Conference on CAD/CG*, 1999.

[7] Yicong Zhou, Sos Agaian, Valencia M. Joyner, and Karen Panetta, "Two Fibonacci P-code based image scrambling algorithms," in *Image Processing: Algorithms and Systems VI*, San Jose, CA, USA, 2008, pp. 681215-12.

[8] Yicong Zhou, Karen Panetta, and Sos Agaian, "P-recursive sequence and key-dependent multimedia scrambling," in *Mobile Multimedia/Image Processing, Security, and Applications 2008*, Orlando, FL, USA, 2008, pp. 69820H-12.

[9] Shujun Li, Chengqing Li, Guanrong Chen, Nikolaos G. Bourbakis, and Kwok-Tung Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing: Image Communication,* vol. 23, no. 3, pp. 212-223, 2008.

[10] Z. H. Guan, F. J. Huang, and W. J. Guan, "Chaos-based image encryption algorithm," *Physics Letters A,* vol. 346, no. 1-3, pp. 153-157, Oct 2005.

[11] Guanrong Chen, Yaobin Mao, and Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals,* vol. 21, no. 3, pp. 749-761, 2004.

[12] Chuanmu Li and Lianxi Hong, "A New Image Encryption Scheme based on Hyperchaotic Sequences," in *Anti-counterfeiting, Security, Identification, 2007 IEEE International Workshop on*, 2007, pp. 237-240.

[13] Shiguo Lian, Yaobin Mao, and Zhiquan Wang, "3D Extensions of Some 2D Chaotic Maps and Their Usage in Data Encryption," in *Control and Automation, 2003. ICCA '03. Proceedings. 4th International Conference on*, 2003, pp. 819-823.