Image Encryption Using the Image Steganography Concept and PLIP Model

Yicong Zhou, *IEEE Member*
Department of Vision Science
New England College of Optometry,
Boston, MA 02115, USA
ZhouY@neco.edu

Sos Agaian, *Senior Member, IEEE*
Department of Electrical and Computer Engineering,
The University of Texas at San Antonio,
San Antonio, TX 78249, USA
Sos.Agaian@utsa.edu

***Abstract*— This paper introduces a new method of applying the image steganography concept for image encryption. Using the PLIP (Parameterized Logarithmic Image Processing) addition [1] to embed the scrambled original image into a selected cover image, the new algorithm generates an encrypted image. Computer simulation and security analysis are given to show that the algorithm has a very large key space and can withstand several common attacks.**

***Keywords*—image encryption, image steganography, image scrambling, parameterized logarithmic image processing**

I. INTRODUCTION

Ubiquitous Network technologies and advances in cloud computing provide a large amount of opportunities for individuals and organizations to share, transmit, and store images and videos. Providing security for these images and videos is an important and urgent issue. Many applications require robust security methods. Examples includes preserving privacy for images/videos in social networks and medical images for clinical applications, enforcing copyright protection for design graphs, images and videos for commercial purposes, and providing security for personal identification and video monitoring in homeland security applications. Image encryption is an effective method to protect images and videos by transforming them into an unrecognized format such that unauthorized users have difficulty decoding the encrypted objects [2].

Cryptography studies mathematical techniques related to different aspects of information security such as data confidentiality, integrity, and entity authentication [3]. Many encryption schemes based on the principles of cryptography apply different techniques to the original images in either the transform domain [4, 5] or the spatial domain [6, 7] in order to change their pixel/block locations, their pixel values, or both. To withstand some advanced cryptanalysis attacks such as plaintext attacks, these encryption methods try to generate the encrypted images that visually look like noise images with a uniform or Guassian histogram distribution. However, they may have high computation cost. An image with the noise-like feature is an obvious sign indicating that it is an encrypted image.

On the other hand, Steganography is the art and science of hiding information in ways that prevent the detection of hidden messages [8]. Image steganography embeds the original information into a cover image. Bloisi and Iocchi introduced an system performing both cryptography and steganography simultaneously in the frequency domain [9]. In order to hide the secret message into the cover image, the system modifies the DCT (Discrete Cosine Transform) coefficients of the cover image by comparing with a key image, DCT coefficients and secret message bits. However, the system algorithm is complicated and may have high computation cost.

The parameterized logarithmic image processing (PLIP) model is a mathematical framework based on set of precise operations that can be applied to the processing of intensity images valued in a bounded range. The PLIP model has been proved to be physically justified in the setting of transmitted light and to be consistent with several laws and characteristics of the human visual system. The PLIP model has been used in many applications of image processing such as image enhancement, restoration, fusion and segmentation [1].

In this paper, we extend the PLIP application to image encryption and introduce a novel method to apply the concept of image steganography for image encryption. It first scrambles image pixel locations. Using a simple PLIP addition, the scrambled image is then embedded into a cover image to obtain the encrypted image. Instead of obtaining a noise-like encrypted image, its encrypted image is visually in presence of the same as the cover image, even if their histograms are slight different. As a result, the original image is fully encrypted by concealing into the cover image.

The rest of this paper is organized as follows. Section II reviews the PLIP model operations. The 2D cat map and its transforms are also presented to be used for the new image encryption method proposed in Section III. To show the new algorithm's encryption performance, Section IV provides several simulation results and Section V analyzes its security issues. A conclusion is drawn in Section VI.

II. BACKGROUND

This section reviews the operations of the Parameterized Logarithmic Image Processing (PLIP) model. The 2D cat map and its transforms are also presented. They will be used for the proposed new image encryption algorithm.

A. The PLIP model

The PLIP operations based on a parameterized grey tone function $g(i,j)$ are listed on Table I [1]. $f(i,j)$ is the original

978-1-61284-471-8/11/$26.00 ©2011 IEEE

image intensity. $g(i,j)$, g_1, g_2, and g are the gray tone functions. c and β $(c,\beta>0)$ are real constants. Parameters $\mu,\gamma,k,$ and λ are constants or functions of the maximum value of an image. $\widetilde{\oplus},\widetilde{\Theta},\widetilde{\otimes},$ and $\tilde{*}$ are the PLIP addition, subtraction, scalar multiplication, and image multiplication, respectively.

TABLE I. THE PLIP OPERATIONS

PLIP Operations	**Definition**
Gray tone	$g(i,j)=\mu-f(i,j)$
Addition	$g_1\widetilde{\oplus}g_2=g_1+g_2-\frac{g_1g_2}{\gamma}$
Subtraction	$g_1\widetilde{\Theta}g_2=k\frac{g_1-g_2}{k-g_2}$
Scalar Multiplication	$c\widetilde{\otimes}g=\gamma-\gamma\left(1-\frac{g}{\gamma}\right)^c$
Image Multiplication	$g_1\tilde{*}g_2=\tilde{\varphi}^{-1}\left(\tilde{\varphi}(g_1)\bullet\tilde{\varphi}(g_2)\right)$ $\tilde{\varphi}(g)=-\lambda\ln^{\beta}\left(1-\frac{g}{\lambda}\right)$ $\tilde{\varphi}^{-1}(g)=\lambda\left[1-\exp\left(-\frac{g}{\lambda}\right)^{1/\beta}\right]$

This paper will use the PLIP addition and subtraction for image encryption.

When $\gamma=k$, we can easily obtain:

$$g_1\widetilde{\oplus}g_2\widetilde{\Theta}g_2=g_1 \tag{1}$$

Since,

$$g_1\widetilde{\oplus}g_2\widetilde{\Theta}g_2=k\frac{\left(g_1+g_2-\frac{g_1g_2}{\gamma}\right)-g_2}{k-g_2}=\frac{\frac{kg_1}{\gamma}(\gamma-g_2)}{k-g_2}$$

For $\gamma=k$, then $g_1\widetilde{\oplus}g_2\widetilde{\Theta}g_2=g_1$.

This property is very important for the proposed image encryption algorithm. It will be use for reconstructing the original images.

Other properties of the PLIP model have been proven in [1]. For example, when $\mu=\gamma=k=M$, the equations (2) and (3) become the addition and subtraction of the traditional logarithmic image processing (LIP) model [10], respectively. When γ and k approach infinity, the PLIP addition and subtraction will be linear arithmetic addition and subtraction, respectively.

B. The 2D cat map and its transforms

The 2D cat map is a chaotic map defined as [11].

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix}=(A\begin{bmatrix} x_n \\ y_n \end{bmatrix})\bmod N=(\begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}\begin{bmatrix} x_n \\ y_n \end{bmatrix})\bmod N \tag{2}$$

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

The proposed image encryption algorithm will use the 2D cat map to change image pixel locations. For this purpose, we define a cat map transform,

$$\begin{bmatrix} x' \\ y' \end{bmatrix}=(\begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix})\bmod N \tag{3}$$

where (x,y) is the image pixel location of an $N\times N$ image. a,b are positive integers, (x',y') is the new pixel location, $x,y,x',y'=1,2,...N$.

The cat map transform above can efficiently scramble the 2D images. The user can choose the number of iterations for applying the cat map transform to the image in order to achieve a higher level of security. The parameters a,b and iteration times n can act as security keys for the image scrambling process.

To reconstruct the original image, we cannot directly use the cat mp transform due to the mod operation. Therefore, we introduce two coefficient matrices: the row coefficient matrix and the column coefficient matrix [12].

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 change with the combinations of parameters a,b and iteration times n. An example is shown in Table II.

TABLE II. COEFFICIENT MATRICES OF THE CAT MAP TRANSFORM FOR AN 8×8 IMAGE

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

To reconstruct the original image, an inverse cat map transform is needed.

Let S be the scrambled 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:

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

where R is the reconstructed image.

III. Image Encryption Algorithm

Inspired from image steganography that conceals data into a host image, this section introduces a new method of image encryption. Its underlying foundation is to scramble the original image in order to change image pixel locations, and to embed the scrambled result into a cover image in order to hide image data. The cover image has the same size as the original image.

In this manner, the unauthorized users can only recognize the cover image with no information about the original image. The original image is fully encrypted and protected.

Based on this idea, we introduce a new image encryption algorithm called the PLIPaddEncrypt algorithm as shown in Figure 1.

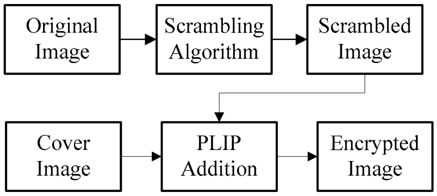

Figure 1. The new PLIPaddEncrypt algorithm.

The PLIPaddEncrypt algorithm contains two simple processes. Using any image scrambling algorithm, the PLIPaddEncrypt algorithm first scrambles the original image to change the image pixel locations. This step increases unauthorized user's difficulty to break the images. Therefore it enhances the algorithm's security.

Making use of the PLIP addition, the PLIPaddEncrypt algorithm embeds the scrambled original image into a cover image to obtain the final encrypted image. When the PLIP's parameters change, the encrypted images will be different. Therefore, the security keys of the PLIPaddEncrypt algorithm consist of the cover image, the PLIP's parameters and the security keys of the image scrambling algorithm.

The cover image is part of the security keys of the PLIPaddEncrypt algorithm. To ensure the unauthorized users' difficulty disclosing the original image, the cover image should be selected from non-public or/and newly generated images.

To demonstrate the PLIPaddEncrypt algorithm, this paper selects the cat map transform as an example of the image scrambling algorithms. In this case, the security keys of the PLIPaddEncrypt algorithm consist of the cover image, the parameters of the PLIP addition (μ and γ), and the parameters of the cat map transform (a, b and iteration times n). Users have flexibility to choose any another scrambling algorithm.

To reconstruct the original image, the authorized users should be provided all security keys. The cover image is first subtracted from the encrypted image by using the PLIP subtraction with $\gamma = k$. By using the inverse cat map transform with correct security keys, the image is then unscrambled to reconstruct the original image.

IV. Simulation Results

The proposed PLIPaddEncrypt algorithm has been successfully applied to more than 30 images. To show its encryption performance, Figures 2 and 3 provide two encryption examples.

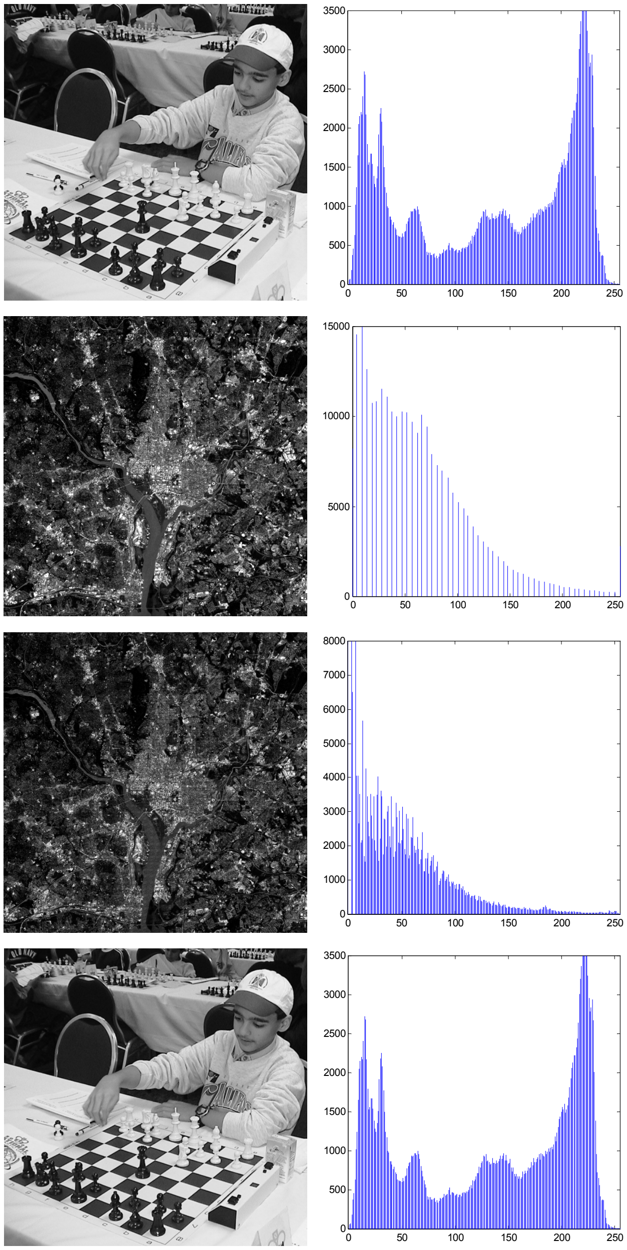

Figure 2. Image encryption, $a = 3, b = 5, n = 15, \mu = 801, k = \gamma = 800$. First row: The original image and its histogram; Second row: The cover image and its histogram; Third row: Encrypted image and its histogram; Fourth row: The reconstructed image and its histogram.

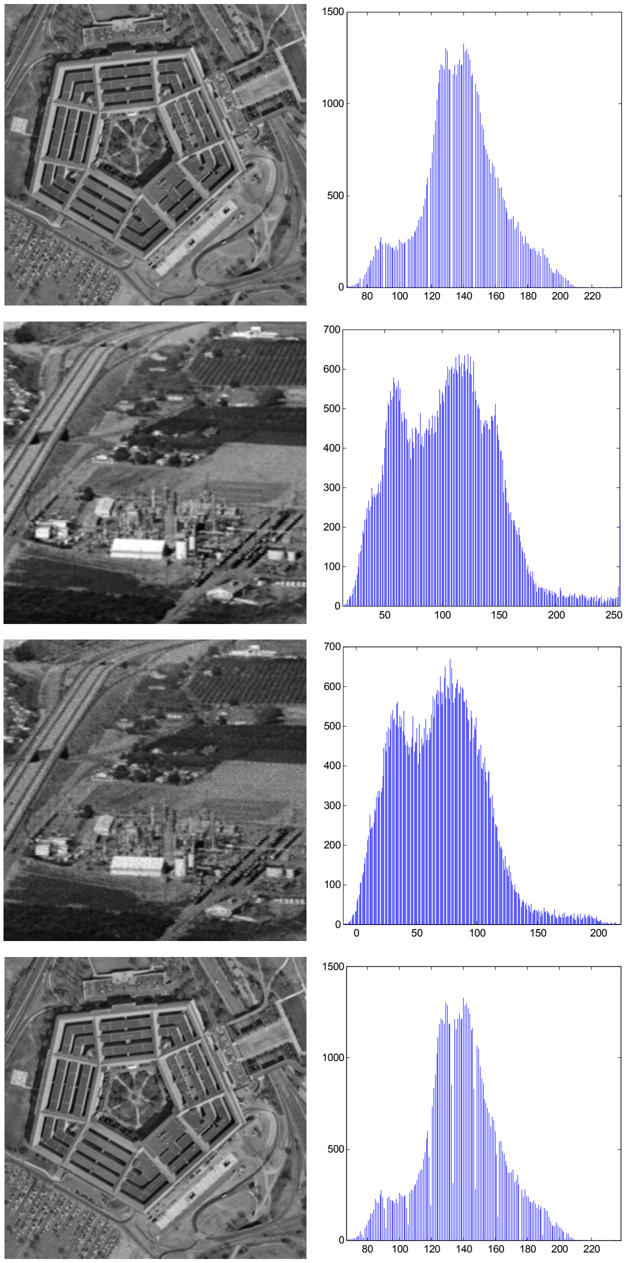

Figure 3. Image encryption, $a = 3, b = 5, n = 15, \mu = 700, k = \gamma = 800$ .First row: The original image and its histogram; Second row: The cover image and its histogram; Third row: Encrypted image and its histogram; Fourth row: The reconstructed image and its histogram.

The original image in Figure 2 is a chessplayer. A satellite urban image is selected as the cover image. The parameters for the 2D cat map are $a = 3, b = 5$ and iteration times $n = 15$. Parameters for the PLIP model are $\mu = 801, k = \gamma = 800$. The encrypted image visually looks the same as the cover image even if their histograms are obviously different. The original image is successfully concealed into the cover image. The scrambling algorithm is used to change image pixel locations increasing the hacker's difficulty to break the protected image.

Using the correct cover image and security keys, the original images is completely reconstructed as shown in the last row of Figures 2. Similar results are also shown in Figure 3.

The scrambled images visually look like noise or textile images. To obtain a better encryption result, the cover images should have the detailed or/and darksome background so that they are not sensitive to the noise effect.

V. Security Analysis

In this section, we discuss several security issues of the PLIPaddEncrypt algorithm such as security key space, key sensitivity and several attacks.

A. *Security Key Space and Brute Force Attack*

The security keys of the PLIPaddEncrypt algorithm are the cover image, parameters of the PLIP model, and security keys of the scrambling algorithm. The users have flexibility to select any scrambling algorithm to change image pixel locations. Therefore, there are a very large number of possible choices for the type of the scrambling algorithm and its security keys.

The users can utilize any image as a cover image, which has the same size as the original image. This further enlarges the security key space of the PLIPaddEncrypt algorithm. Including the possible choices of the PLIP's parameters, the algorithm's security key space is sufficiently large.

The brute force attack is an attack model which tries to guess the security keys of the encryption algorithm by exhaustively searching all the possible combinations of security keys. The PLIPaddEncrypt algorithm can overcome the brute force attack due to its adequately large key space.

B. *Key Sensitivity*

The correct combination of the security keys is very important for the PLIPaddEncrypt algorithm.

Figure 4 provides an example of image reconstruction. In this case, we assume the unauthorized user obtains the cover image and tries to break the original image without knowledge of other security keys. Figure 4 (d) shows that the original image can be completely reconstructed only when the correct security keys are being utilized. Otherwise, the reconstructed images are unrecognizable even if we only change one of the security keys. This is shown in Figure 4(e) and (f), demonstrating that the PLIPaddEncrypt algorithm is highly sensitive with the key change. This property is another advantage of the PLIPaddEncrypt algorithm.

C. *Plaintext Attacks*

Since the cover image is the part of the security keys for the PLIPaddEncrypt algorithm and is selected from a new or non-public image. This increases the attacker's difficulty obtaining the correct cover image to break the original image.

The PLIP addition is a parametric fusion process. It conceals the original image data into the cover image. This further increases the attacker's difficulty to disclose the original image using plaintext attacks, achieving a higher level of security. Therefore, the PLIPaddEncrypt algorithm is able to withstand the plaintext attacks.

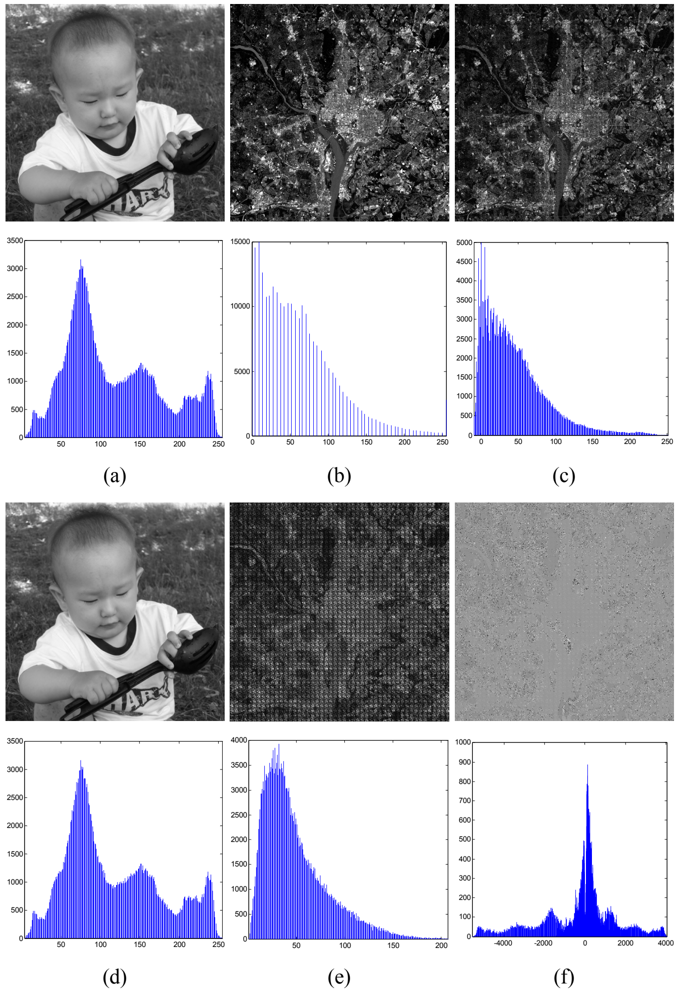

Figure 4. Image reconstruction using different k values. (a) Original image and its histogram; (b) Cover image and its histogram; (c) Encrypted image and its histogram, $a=3, b=5, n=15, \mu=530, \gamma=550$; (d) Reconstructed image and its histogram, $k=550$; (e) Reconstructed image and its histogram, $k=700$; (f) Reconstructed image and its histogram, $k=500$.

VI. CONSLUSION

In this paper, we have introduced a new method of utilizing the concept of image steganography for image encryption, namely encrypting the original image by concealing it into a cover image using a specific encryption process. As an example of this new idea, we have introduced an image encryption algorithm called the PLIPaddEncrypt algorithm. To embed the original image into the cover image, it fuses the scrambled original image with the cover image using the PLIP addition via specific parameters. This also shows a new application of the PLIP model for image encryption.

Simulation results have demonstrated the encryption performance of the PLIPaddEncrypt algorithm. The security analysis has shown that the algorithm have sufficiently large key space and can withstand several common attacks. The algorithm has the potential for applications in privacy and copyright protection.

REFERENCES

[1] K. Panetta, et al., "Parameterized Logarithmic Framework for Image Enhancement," IEEE Trans. Syst. Man Cybern. Part B Cybern., vol. 41, pp. 460-473, 2011.

[2] A. M. Eskicioglu and E. J. Delp, "An overview of multimedia content protection in consumer electronics devices," Signal Process. Image Commun., vol. 16, pp. 681-699, 2001.

[3] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. NY: CRC Press, 1997.

[4] S. Sudharsanan, "Shared key encryption of JPEG color images," IEEE Trans. Consum. Electron., vol. 51, pp. 1204-1211, 2005.

[5] H. Cheng and X. Li, "Partial encryption of compressed images and videos," IEEE Trans. Signal Process., vol. 48, pp. 2439-2451, 2000.

[6] H. Yang, et al., "A fast image encryption and authentication scheme based on chaotic maps," Commun. Nonlinear Sci. Numer. Simul., vol. 15, pp. 3507-3517, 2010.

[7] C. K. Huang and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," Opt. Commun., vol. 282, pp. 2123-2127, 2009.

[8] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, vol. 31, pp. 26-34, 1998.

[9] D. Bloisi and L. Iocchi, "Image based Steganography and Cryptography," in 2nd Int. Conf. on Computer Vision Theory and Applications (VISAPP), 2007, pp. 127-134.

[10] J.-C. Pinoli, "The Logarithmic Image Processing Model: Connections with Human Brightness Perception and Contrast Estimators," J. Math. Imaging Vis., vol. 7, pp. 341-358, 1997.

[11] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos Soliton. Fract., vol. 21, pp. 749-761, 2004.

[12] Y. Zhou, K. Panetta, and S. Agaian, "Image Encryption Based on Edge Information," in IS&T / SPIE Electronic Imaging 2009: Multimedia Mobile Devices 2009, San Jose, CA, 2009, pp. 725603-11.