Stego Optical Encryption Based on Chaotic Baker's Map Transformation

Iqtadar Hussain[a] and Muhammad Asif Gondal[b]

[a] National University of Computer and Emerging Sciences, Islamabad, Pakistan
[b] Department of Mathematics and Sciences, Dhofar University, Salalah, Oman

Reprint requests to I. H.; E-mail: iqtadarqau@gmail.com

Z. Naturforsch. **69a**, 249 – 253 (2014) / DOI: 10.5560/ZNA.2014-0016
Received October 11, 2013 / revised March 15, 2014 / published online May 21, 2014

In this article, an optical image encryption algorithm based on chaotic baker's map is presented. The stego-image is encrypted with the help of double random phase encoding algorithm and then produced disorder with the help of chaotic transformation. Security test shows that the reading of proposed algorithm is very close to the optimal values.

Key words: Image Encryption; Optical Security; Double Random Phase; Chaotic Baker's Map.

1. Introduction

1.1. Steganographic Optical Image Cryptosystem: an Over View

In [1] an adaptive data steganographic optical cryptosystem has been proposed for colour images. This technique is based on the encryption technique presented in [2]. A stego image S is constructed by embedding a confidential image C into the phase term of a host image H. S is transformed into Fourier plane after multiplying it with a random mask V in input spatial plane where it is multiplied by another random phase mask W. Finally, ciphered image E is obtained in the output spatial plane by taking its inverse Fourier transform. Mathematical the encryption produce can be expressed as

$$S(x,y) = H(x,y)\cdot \mathrm{e}^{\mathrm{i}\frac{\pi}{2}C(x,y)}$$
$$E(x,y) = F^{-1}\left[F\left(S(x,y)\cdot \mathrm{e}^{\mathrm{i}2\pi v}\right)\cdot \mathrm{e}^{\mathrm{i}2\pi w}\right],$$

where (x,y) denotes the spatial indices of the image C, and $C(x,y)$ is an integer in the interval $[0,2^k-1]$ which denotes the intensity of a pixel at the position (x,y). $V = \mathrm{e}^{\mathrm{i}2\pi v}$, $W = \mathrm{e}^{\mathrm{i}2\pi w}$, v and w are random numbers equal to the size of the image belonging to $[0,1]$. F and F^{-1} denotes the Fourier and inverse Fourier transforms, respectively.

In the decoding process the ciphered image E is multiplied with the conjugate of the mask V after taking its Fourier transform. Then it is inverse Fourier transformed and multiplied with the conjugate of the mask W to obtain the deciphered image D in the output spatial plane. The confidential and host images can be retrieved by computing the complex argument and modulus of D respectively. The mathematical expressions of decoding process are

$$D(x,y) = F^{-1}\left[F(E(x,y))\cdot \mathrm{e}^{-\mathrm{i}2\pi w}\right]\cdot \mathrm{e}^{-\mathrm{i}2\pi v},$$
$$C(x,y) = \frac{\arg(D(x,y))}{\pi/2},$$
$$H(x,y) = |D(x,y)|.$$

This optical cryptosystem is shown in Figures 1 and 2. A zero least significant bit sorting technique is used to embed the seeds to generate the random phase data into the ciphered images.

1.2. Process of Data Hiding and Data Extraction

In this section, we discuss the process of data hiding and data extraction given in [1]. The data hiding steps are given below.

Step 1: Assume that there are N bits in the secret data $B = \{b_1, b_2, \ldots, b_N\}$. The values of real parts in the encrypted stego-image I_{e} are sorted in ascending order with their absolute values. The sorted set of the first $N+2$ numbers except the maximum and the minimum is chosen and defined as $\Delta = \{\alpha_1, \alpha_2, K, \alpha_N\}$, where $|\alpha_i| \le |\alpha_{i+1}|$, α_i and $|\alpha_{i+1}| \in \Delta$. Note that the maximum and minimum in the first $N+2$ numbers are

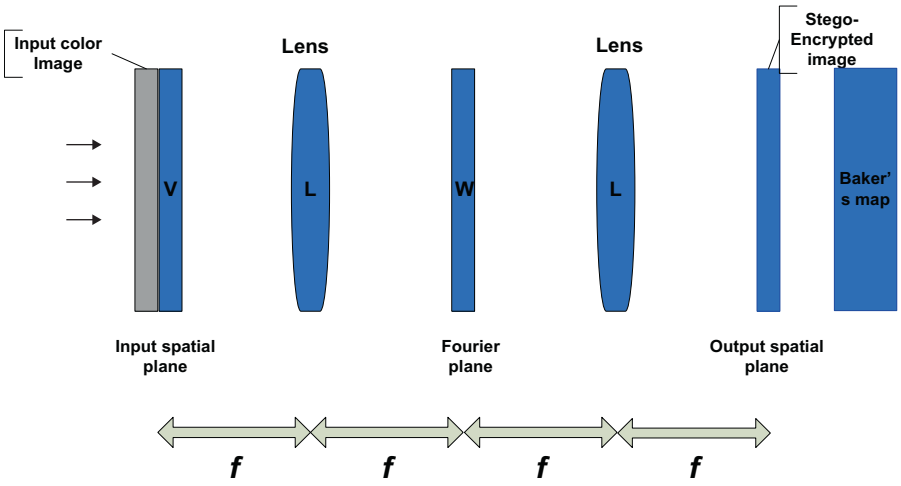

Fig. 1 (colour online). Process of encryption based on Fourier transformation and substitution box transformation.

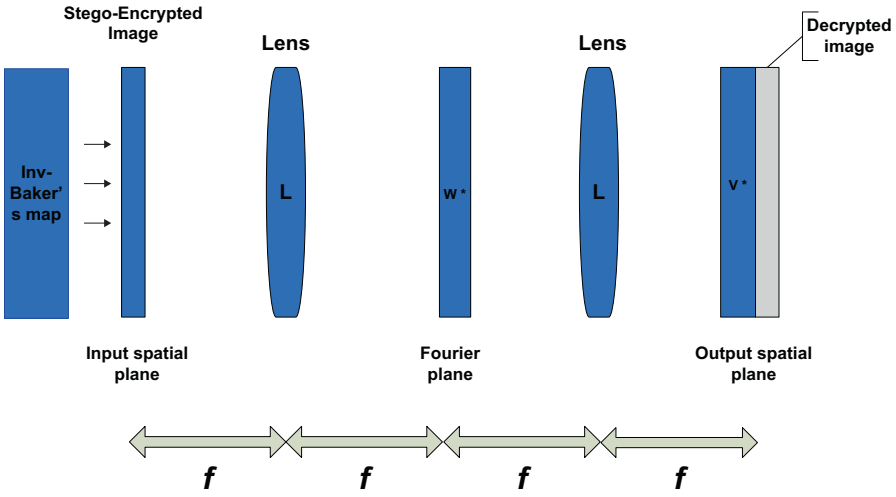

Fig. 2 (colour online). Process of decryption based on inverse Fourier transformation and inverse substitution box transformation.

not used to be quantized and hidden data because the quantization step size is computed from them.

Step 2: The sorted set Δ is quantized to become $\Delta_Q = Q_L(\Delta) = \{\alpha_{q1}, \alpha_{q2}, \ldots, \alpha_{qN}\}$, where $Q_L(.)$ denotes a quantize with L levels.

Step 3: The zero-LSB (least significance bit) set $\Delta_{QZ} = \{\alpha_{qz1}, \alpha_{qz2}, \ldots, \alpha_{qzN}\}$ is obtained by setting all LSBs of Δ_Q to be zero. The elements in Δ_{QZ} are sorted in ascending order with their absolute values to get $\Delta_{QZS} = \{\alpha_{qZS_1}, \alpha_{qZS_2}, \ldots, \alpha_{qZS_N}\}$, where $|\alpha_{qZS_i}| \leq |\alpha_{qZS_{i+1}}|$, α_i and $|\alpha_{qZS_{i+1}}| \in \Delta_{QZS}$.

Step 4: The sequence $S = \{s_1, s_2, \ldots, s_N\}$, where $s_i \in \{1, 2, \ldots, N\}$ and $i = 1, 2, \ldots, N$ generated by the set Δ_{QZS}, is used to be the data hiding index. That is, the secret data is successively embedded into the LSBs of the set Δ_Q according to the sequence S, i.e. $\Delta_{QS} = \{\alpha_{qs_1}, \alpha_{qs_2}, \ldots, \alpha_{qs_N}\}$, where $\alpha_{qS_i} \in \Delta_Q$.

Step 5: The hiding rule is defined as

$$\Delta_{QS}^{E} = \Delta_{QS} + \mathrm{sgn}(B - \mathrm{mod}(\Delta_{QS}, 2)),$$

where $\mathrm{sgn}(.) \in \{-1, 0, 1\}$ is the signum function and $B = \{b_1, b_2, \ldots, b_N\}$ is the secret data. The set with hidden data is $\Delta_{QS}^{E} = \{\alpha_{qs_1}^{e}, \alpha_{qs_2}^{e}, \ldots, \alpha_{qs_N}^{e}\}$.

Step 6: Finally, the set Δ_{QS}^{E} is de-quantized to obtain $\Delta_{S}^{E} = Q_L^{-1}(\Delta_{QS}^{E}) = \{\alpha_{s_1}^{e}, \alpha_{s_2}^{e}, \ldots, \alpha_{s_N}^{e}\}$, where $Q_L^{-1}(.)$ is the de-quantizer with L levels.

The data extraction procedure is given below.

Step 1: This step is the same as the first step in the data hiding procedure to find the sorted set. The set is defined as $\Delta^E = \{\alpha_1^e, \alpha_2^e, \ldots, \alpha_N^e\}$, where $|\alpha_i^e| \leq |\alpha_{i+1}^e|$, $\alpha_i^e \in \Delta^E$. The sequence in the sorted set Δ^E is different from that in the sorted set Δ.

Step 2: The sorted set Δ^E is quantized with L levels to be $\Delta_Q^E = Q_L(\Delta^E) = \{\alpha_{q_1}^e, \alpha_{q_2}^e, \ldots, \alpha_{q_N}^e\}$.

Step 3: All LSBs of Δ_Q^E are set to zero to obtain the zero-LSB set $\Delta_{QZ}^E = \{\alpha_{qz_1}^e, \alpha_{qz_2}^e, \ldots, \alpha_{qz_N}^e\}$. The elements in Δ_{QZ}^E are sorted in ascending order with their absolute values to get $\Delta_{QZS}^E = \{\alpha_{qzs_1}^e, \alpha_{qzs_2}^e, \ldots, \alpha_{qzs_N}^e\}$, where $|\alpha_{qzs_i}^e| \leq |\alpha_{qzs_{i+1}}^e|$, $\alpha_{qzs_i}^e, \alpha_{qzs_{i+1}}^e \in \Delta_{QZS}^E$.

Step 4: Now, the set Δ_{QZS}^E is equal to the set Δ_{QZS} with the same sequence $S = \{s_1, s_2, \ldots, s_N\}$. The hidden data is extracted from the LSBs of the set $\Delta_{QS}^E = \{\alpha_{qs_1}^e, \alpha_{qs_2}^e, \ldots, \alpha_{qs_N}^e\}$, i.e.

$$\begin{cases} b_i = 0 & \text{if} \quad \text{mod}\left(\alpha_{qs_i}^e, 2\right) = 0, \\ b_i = 1 & \text{if} \quad \text{mod}\left(\alpha_{qs_i}^e, 2\right) = 1, \end{cases}$$

where $i = 1, 2, \ldots, N$.

Because in this paper we want to transform the encrypted image of [1] with chaotic linear fractional S-box, so we will discuss the construction of linear fractional transformation substitution box in the next section.

1.3. Chaotic Baker's Map

The baker's map is a two-dimensional chaotic map in real space and discrete time domain. In a chaotic system the output is predictable if certain information is known, while in the absence of ample initial knowledge about the system, it is challenging to predict the output behaviour. With the progression of time, the system shows random behaviour and depicts interesting properties desirable for encryption applications [3 – 10]. These systems are highly dynamic in nature; therefore, this property is useful in obscuring information for encryption applications. In tandem with chaotic maps, the system shows dynamic properties that reflect resistance to cryptanalysis. This work focuses on the application of baker's map to attain suitable encryption components that demonstrate highly random behaviour. The iteration process is used in the baker's map to repeatedly process the output, which is also used as an input.

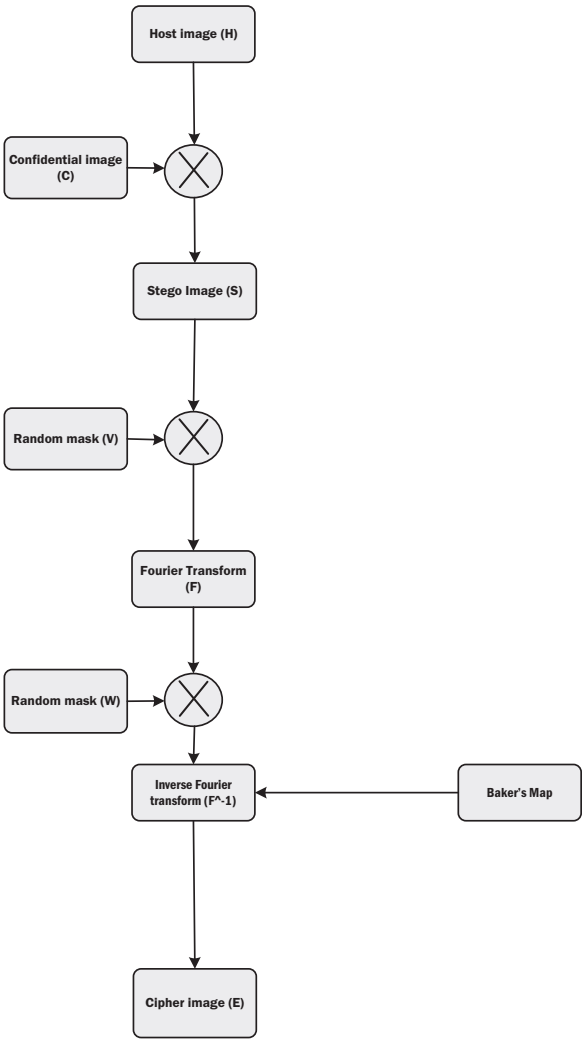

Fig. 3. Flowchart of proposed image encryption.

1.4. Proposed Algorithm

In this algorithm, an optical image encryption algorithm with an information hiding technique is presented. The process is explained in Figure 3. In Step 1, a secret image is implanted into the cover image, moreover the data hiding and extraction technique of the proposed algorithm are same as in [1]. After that the stego-image is encrypted with the help of the double random phase encoding algorithm of [1]. In Step 3 we transform the cover image with the help of chaotic baker's map transformation to improve its security.

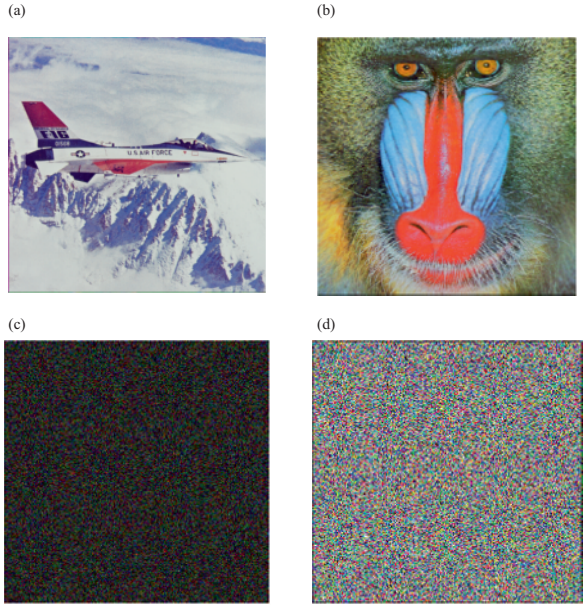

Fig. 4 (colour online). (a) Original host images. (b) Secret image. (c) Optical encrypted image. (d) Image after chaotic substitution box transformation.

Table 1. Comparisons between the proposed method and the traditional scheme [11] of the average PSNR values (measured in db) of host images and secret image.

	Prosposed method		Traditional scheme [11]	
L	Host	Secret	Host	Secret
8	20.77	32.14	5.57	15.89
16	24.77	36.19	11.56	22.70
32	32.79	44.22	17.57	28.85
64	36.81	50.24	23.57	34.89
128	44.82	55.66	31.59	40.91
256	50.15	60.27	35.64	46.97

2. Experimental Results

In the experiment, one hundred 24-bit 512×512-pixel various colour images (collected from [7]) are examined as host images and the peak signal-to-noise ratio (PSNR) is applied to evaluate the visual quality of the decrypted images. The equation is defined as follows:

$$\mathrm{MSE} = \frac{\mathrm{MSE_R} + \mathrm{MSE_G} + \mathrm{MSE_B}}{3},$$

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{255^2}{\mathrm{MSE}},$$

where $\mathrm{MSE_R}$, $\mathrm{MSE_G}$, and $\mathrm{MSE_B}$ are mean square errors in three channels, respectively. In Tables 1 and 2 we present the strength of proposed algorithm by comparing it with [11].

Table 2. Comparisons between the proposed method and the traditional scheme [11] of the average PSNR values (measured in db) of the 100 decrypted host images and the retrieved secret images when the encrypted stego-images are attacked. ($L = 8$, hidden data 480 000 bits).

Three common attacks	Proposed method		Traditional scheme [11]	
	Host	Secret	Host	Secret
Noising	7.07	16.74	3.42	13.02
Smoothng	5.14	14.20	4.34	11.31
JPEG compression	7.15	17.01	4.69	12.71

3. Conclusion

In this manuscript, the optical colour image cryptosystem with data steganography and chaotic baker's map transformation is proposed. The double random phase encoding algorithm and the adaptive data hiding technique are applied in the proposed colour image cryptosystem with the additional confusion capabilities of baker's transformation. The confidential image is hidden in the phase term of the host image. Then the stage-image is encrypted with the double random phase encoding algorithm. We compare [11] scheme with proposed algorithm and come to know that the results of chaotic substitution box transformation are comparatively extraordinary as shown in Figure 4.

[1] C.-H. Chuang and G.-S. Lin, Int. J. Image Process. **3**, 318 (2008).
[2] P. Refregier and B. Javidi, Opt. Lett. **20**, 767 (1995).
[3] T.-S. Chen, C.-C. Chang, and M.-S. Hwang, IEEE T. Image Process. **7**, 1485 (1998).
[4] Y.-C. Hu, Pattern Recogn. **39**, 1715 (2006).
[5] C.-C. Chang, C.-Y. Lin, and Y.-Z. Wang, Inform. Sciences **176**, 3393 (2006).
[6] W.-Y. Chen, Appl. Math. Comput. **185**, 432 (2007).
[7] B. Javidi and A. Sergent, Opt. Eng. **36**, 935 (1997).
[8] G. Unnikrishnan, J. Joseph, and K. Singh, Opt. Lett. **25**, 887 (2000).

[9] Z. Liu and S. Liu, Opt. Lett. **32**, 2088 (2007).
[10] Z. Liu, Q. Li, J. Dai, X. Sun, and M. A. Ahmad, Opt. Commun. **282**, 1536 (2009).
[11] G.-S. Lin, H. T. Chang, W.-N. Lie, and C.-H. Chuang, Opt. Eng. **42**, 2331 (2003).