Image compression-encryption algorithm combining compressive sensing with log operation

RONG-LING CHEN, YING ZOU, MING LUO, AI-DI ZHANG, LI-HUA GONG*

Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

*Corresponding author: ncuglh@163.com

Based on compressive sensing and log operation, a new image compression-encryption algorithm is proposed, which accomplishes encryption and compression simultaneously. The proposed image compression-encryption algorithm takes advantage of not only the physical realizability of partial Hadamard matrix, but also the resistance of the chosen-plaintext attack since all the elements in the partial Hadamard matrix are 1, –1 or log 1 = 0. The proposed algorithm is sensitive to the key and it can resist various common attacks. The simulation results verify the validity and reliability of the proposed image compression-encryption algorithm.

Keywords: image encryption, image compression, compressive sensing, log operation.

1. Introduction

Images provide a lot of information along with the development of network technology. While transmission channels are always insecure and bandwidth-constrained, so it is desired to transmit the data after encryption and compression. Recently, compressive sensing (CS) [1, 2] has been proposed as a new theory or tool. The theory has attracted much attention for its breakthrough in the traditional sampling methods. CS can accomplish sampling and compression at the same time compared with the traditional method. Because of the advantage of CS, it is of great significance that compressive sensing and image encryption algorithm are fused together to complete compression and encryption simultaneously. The secrecy properties of compressive sensing for noisy are covered in [3] and it was indicated that the inherent multidimensional projection perturbation feature made it hard to breach the privacy. HUIMIN ZHAO and YANMEI FANG examined the security and robustness via compressive sensing based on a fingerprint watermarking signal and demonstrated that CS can provide an effective security of compression and encryption [4]. In 2017, an image encryption scheme was formulated, in which the parameters of the logistic map and the order of discrete fractional transform are the key to the image encryption algorithm [5]. LINFEI CHEN et al. took the six phase masks and the six diffraction distances as the key to the decryption process [6]. It
was stated that the encryption matrix in compressive sensing based algorithms is perfectly secure if it can be seen as a one-time pad [7]. The security was investigated when eavesdroppers have no idea of the measurement matrix and a computational notion of secrecy was demonstrated [8]. Fucheng Yin et al. verified the effectiveness of the known plaintext attack with the dual random phase coding [9].

Some image encryption algorithms have been investigated since the potential capability of measurement matrix in CS. Compressive sensing was employed to lower the encryption data volume in an image encryption method based on double random-phase encoding due to the dimensional decrease properties of CS [10]. Kumar and Vaish compressed the image according to the importance of the image coefficients [11]. The original image was divided into blocks as one-dimensional vectors, and then the authors encrypted and compressed these vectors with CS and block Arnold scrambling [12]. Based on compressive sensing, Xinpeng Zhang et al. proposed an image encryption algorithm where they encrypted the original image by orthogonal transformation and then compressed by CS with a pseudo-random measurement matrix [13]. A concise pixel-permutation algorithm was used to reduce the encryption time [14]. Zhengjun Liu et al. adopted some physical parameters of optical system as the key to enhance the security of the color image encryption system [15]. Ponna and Amutha put forward an image encryption scheme, where the keys depend on the input data and the initial parameters of the chaotic map [16]. In order to enhance the security of the image encryption system, Hamdi et al. realized multiple encryption of the image via three phases of confusion and diffusion [17], since CS-based encryption method alone fails to resist against the chosen-plaintext attack. Hence, the output of CS is again encrypted based on the multi-chaotic system [18]. A parallel image encryption method based on CS was proposed, where a block cipher structure consisting of scrambling, mixing, S-box and chaotic lattice XOR was designed to resist against the chosen-plaintext attack effectively [19]. Rawat et al. proposed a scheme where both compressive sensing and Arnold scrambling are employed to encrypt a digital image [20]. Nanrun Zhou et al. proposed a novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing, where the measurement matrices were constructed as partial Hadamard matrices [21]. Subsequently, Nanrun Zhou et al. introduced a new image compression-encryption scheme where the original image was compressed and encrypted simultaneously by measuring matrices in two directions [22]. Endra proposed a novel method of constructing optimized sensing matrix and exploited it to compress and encrypt images simultaneously [23]. Xingbin Liu et al. proposed a novel approach based on compressive sensing, where the source images were measured with the key-controlled pseudo-random measurement matrix constructed using logistic map to reduce the data and realizes the initial encryption [24]. Based on 2D compressive sensing and discrete fractional random transform (DFrRT) [25], an image compression-encryption scheme with simple operation was proposed, where the original image was measured by the measurement matrices in two orthogonal directions during the encryption process and the matrices were constructed with logistic map to control
the row vectors of the Hadamard matrix [26]. In 2017, GUIQIANG HU et al. devised an image coding scheme, where the CS sampling and the CS reconstruction were performed in parallel [27].

Taking advantage of the facts that all the elements in the Hadamard matrix are 1 or –1 and \( \log 1 = 0 \), we explore a new compression-encryption algorithm based on CS and log operation, which can encrypt and compress an image simultaneously and resist the so-called chosen-plaintext attack. The simulation results show that the proposed algorithm has good security and compression performance.

2. Image compression-encryption algorithm based on CS and log operation

The measurement matrix \( \Phi \) is constructed as a partial Hadamard matrix and controlled by a logistic map. The logistic map is defined as:

\[
x_{n+1} = \mu x_n (1 - x_n), \quad x_n \in (0, 1)
\]

If \( \mu \in [3.57, 4] \), it becomes chaotic.

The construction steps are as follows:

1) Generate a sequence of length \( 2N \) by logistic map with initial condition \( r \), abandon the preceding \( N \) elements to obtain the index sequence \( s = [s_1, s_2, \ldots, s_N] \);
2) Sort the nature sequence \( n = [1, 2, \ldots, N] \) with the index sequence \( s \), note the sorted sequence as \( p = [p_1, p_2, \ldots, p_N] \), where \( p_i \in [1, N] \);
3) Generate the Hadamard matrix \( H \) of order \( N \), and choose the row vectors, \( H(p_1, :) \), \( H(p_2, :) \), \ldots, \( H(p_M, :) \), to group into the measurement matrix \( \Phi \), i.e.,

\[
\Phi = \begin{bmatrix} H(p_1, :) \\ H(p_2, :) \\ \vdots \\ H(p_M, :) \end{bmatrix}
\]

where \( H(p_i, :) \) denotes the \( p_i \)-th row vector of \( H \).

The proposed image compression-encryption algorithm is fitted to operate on the image whose length and width both are the multiples of 4 since the measurement matrix is constructed as a partial Hadamard matrix. The proposed image compression-encryption algorithm is illustrated in Fig. 1, and the image compression-encryption steps are as follows:

1) Extend \( x \) in the \( \Psi \) domain to obtain \( \alpha \).
2) Construct the measurement matrix \( \Phi \) and measure \( \alpha \) to obtain \( y \). To enhance the security, not \( x \) but \( \alpha \) is measured by \( \Phi \), i.e.,

\[
y = \Phi \alpha = \Phi \Psi^T x
\]
It is equivalent to presume that $\Phi \Psi^T$ is the measurement matrix, and the sensor matrix $\Theta = \Phi$. Thus the attacker needs both $\Phi$ and $\Psi$, or else he/she cannot reconstruct $x$ even if $\alpha$ is available.

3) If $y(i, j) \neq 0$, perform the following operation on $y$ to obtain the encrypted image $C$

$$C = \frac{\left(\frac{y}{|y|} \log |y| + K\right) \times 255}{2K}$$

(4)

where $|\cdot|$ denotes absolute value, and $K = \text{ceil} \left[\max(y)\right]$; the function $\max(A)$ returns the largest element in $A$ and the function $\text{ceil}(A)$ rounds $A$ to the nearest integer greater than or equal to $A$. The log operation is performed on the measurement to resist the chosen-plaintext attack since the elements in the measurement matrix are 1 or –1 and $\log 1 = 0$. And all the elements in $y$ would be in $[0, 255]$, which is the range of the pixel values of images.

Image $\hat{y}$ can be obtained by performing the inverse operation on the encrypted image

$$\hat{y} = \frac{2KC/255 - K}{[2KC/255 - K]} \times 10^{2KC/255 - K}$$

(5)

Then one can obtain the decryption image with the SL$_0$ algorithm [28].

![Fig. 1. Image compression-encryption algorithm.](image1.png)

![Fig. 2. Lena (a), encryption Lena (b), and decryption Lena (c).](image2.png)
3. Simulation and discussion

The gray image Lena with resolution 256 × 256 is served as the test image, which is shown in Fig. 2a. Without loss of generality, 2D DCT is adopted as Ψ and Φ are $M \times N$ ($M = 192$, $N = 256$) partial Hadamard matrices. The parameters $r$ and $\mu$ in simulation are 0.11 and 3.99, respectively. The encrypted image is shown in Fig. 2b, and the corresponding decryption image is shown in Fig. 2c.

3.1. Performance of compression

To measure the quality of the decryption digital image, the peak-to-peak signal-to-noise ratio (PSNR) is used:

$$\text{PSNR} = 10 \log \frac{255^2}{\frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} [R(i,j) - I(i,j)]^2}$$  \hspace{1cm} (6)

where $R(i,j)$ and $I(i,j)$ are the pixel values in the decryption image and the original one, respectively. The experimental results show that the quality of the decryption digital image is acceptable and the PSNR value is about 35.8940 dB. The results for different compression ratios are compiled in Table 1. The quality of the reconstructed image is acceptable to some degree even if the compression ratio is 4:1. And the compression performance would be better with the development of reconstruction algorithm in CS.

The PSNRs of the decryption images under different sampling ratios are shown in Table 2. It can be seen that the proposed scheme has a higher peak signal-to-noise ratio when the compression ratio is same. Therefore, the proposed image compression and encryption scheme has better compression performance.

3.2. Statistical analysis

Statistically, the correlation of two adjacent pixels in a meaningful digital image is usually close to 1, while that of the encrypted image should be as little as possible or even close to 0. To measure the correlations of adjacent pixels, 16000 pairs of two adjacent pixels are selected randomly in horizontal, vertical and diagonal directions, respectively. The correlation coefficient can be obtained by

$$\text{CC} = \frac{\sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N} (x_i - \bar{x})^2 \sum_{i=1}^{N} (y_i - \bar{y})^2}}$$  \hspace{1cm} (7)

where $x_i$ and $y_i$ represent two adjacent pixels value, the mean values $\bar{x}$ and $\bar{y}$ correspond to $\frac{1}{N} \sum_{i=1}^{N} x_i$ and $\frac{1}{N} \sum_{i=1}^{N} y_i$, respectively. The results are compiled in Table 3. It
can be seen that the proposed algorithm has a smaller correlation coefficient of the encryption image than that of the original image. Thus, the proposed image compression and encryption scheme has a good encryption property in terms of correlation.

**Table 1.** The results of different compression ratios.

<table>
<thead>
<tr>
<th>Compression ratio</th>
<th>Compressed and encrypted image</th>
<th>Decryption image</th>
<th>PSNR [dB]</th>
</tr>
</thead>
<tbody>
<tr>
<td>4:3</td>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td>35.8490</td>
</tr>
<tr>
<td>2:1</td>
<td><img src="image3.png" alt="Image" /></td>
<td><img src="image4.png" alt="Image" /></td>
<td>32.0432</td>
</tr>
<tr>
<td>4:1</td>
<td><img src="image5.png" alt="Image" /></td>
<td><img src="image6.png" alt="Image" /></td>
<td>29.7391</td>
</tr>
<tr>
<td>4:3</td>
<td><img src="image7.png" alt="Image" /></td>
<td><img src="image8.png" alt="Image" /></td>
<td>32.9292</td>
</tr>
<tr>
<td>2:1</td>
<td><img src="image9.png" alt="Image" /></td>
<td><img src="image10.png" alt="Image" /></td>
<td>30.2002</td>
</tr>
<tr>
<td>4:1</td>
<td><img src="image11.png" alt="Image" /></td>
<td><img src="image12.png" alt="Image" /></td>
<td>29.1040</td>
</tr>
</tbody>
</table>

**Table 2.** PSNRs of the decryption images under different compression ratios.

<table>
<thead>
<tr>
<th>Compression ratio</th>
<th>4:3</th>
<th>2:1</th>
<th>4:1</th>
</tr>
</thead>
<tbody>
<tr>
<td>The proposed algorithm</td>
<td>35.8490</td>
<td>32.0432</td>
<td>29.7391</td>
</tr>
<tr>
<td>Ref. [22]</td>
<td>30.4936</td>
<td>24.8739</td>
<td>17.4172</td>
</tr>
<tr>
<td>Ref. [26]</td>
<td>30.6295</td>
<td>25.6473</td>
<td>17.4287</td>
</tr>
</tbody>
</table>
It is the best if the values in the histogram of the encrypted images are fairly uniformly distributed, or the histograms of the encrypted images corresponding to the different original images are similar to each other. Figures 3a–3d show the histograms of images Lena, encrypted Lena, Cameraman and encrypted Cameraman, respectively. The histograms of different original images are obviously different, while their encrypted images have similar histograms. After a large number of parallel experiments, it is found that the histograms of the encrypted images of different original images are also similar.

![Histograms](image)

**Table 3. Correlation coefficient.**

<table>
<thead>
<tr>
<th></th>
<th>Correlation coefficient</th>
<th>Horizontal</th>
<th>Vertical</th>
<th>Diagonal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td></td>
<td>0.9590</td>
<td>0.9217</td>
<td>0.9017</td>
</tr>
<tr>
<td>The proposed algorithm</td>
<td></td>
<td>0.0678</td>
<td>0.0557</td>
<td>0.0233</td>
</tr>
<tr>
<td>Ref. [26]</td>
<td></td>
<td>0.0909</td>
<td>0.2389</td>
<td>0.0126</td>
</tr>
<tr>
<td>Cameraman</td>
<td></td>
<td>0.9585</td>
<td>0.9346</td>
<td>0.9063</td>
</tr>
<tr>
<td>The proposed algorithm</td>
<td></td>
<td>0.0466</td>
<td>0.0226</td>
<td>0.0229</td>
</tr>
<tr>
<td>Ref. [26]</td>
<td></td>
<td>0.1284</td>
<td>0.2637</td>
<td>−0.0158</td>
</tr>
</tbody>
</table>

Fig. 3. Histograms: Lena (a), encrypted Lena (b), Cameraman (c), and encrypted Cameraman (d).
to Figs. 3b and 3d. That is to say, the proposed image compression and encryption algorithm can frustrate the statistical analysis attack.

3.3. Key sensitivity
The algorithm succeeds the sensitivity of logistic map to the initial value, thus it is very sensitive to the key. In order to evaluate the difference between the decryption image and the original image, the mean square error (MSE) between the decryption image and the original one is introduced as

$$\text{MSE} = \frac{1}{L \times H} \sum_{x, y} [I(x, y) - D(x, y)]^2$$

(8)

where \(L \times H\) represents the total number of pixels of the image, \(I(x, y)\) and \(D(x, y)\) denote the pixel values at point \((x, y)\) of the input image and the output image, respectively. The larger MSE means the greater differences between the decryption image and the original image. Figure 4 shows the MSE curves for \(r\). One can see that the MSE value is very large with a little deviation \(\Delta = 1 \times 10^{-16}\) to \(r\), and the MSE value is very small if and only if \(r\) is correct, thus the decryption image can only be recognized when the key is correct, i.e., the proposed image encryption algorithm is sensitive enough to the key.

3.4. Noise attack
It is inevitable that the noises at the stage of image processing and image transmission would directly impact the quality of the decryption image. Suppose the encrypted image is contaminated by the noises as:

$$C' = C + kG$$

(9)

where \(C'\) and \(C\) are the noisy encrypted image and the intact original encrypted image, respectively, \(k\) is a coefficient related to the noise intensity, and \(G\) is the white Gaussian noise. The larger MSE means the greater differences between the decryption image and the original image. Figure 4 shows the MSE curves for \(r\). One can see that the MSE value is very large with a little deviation \(\Delta = 1 \times 10^{-16}\) to \(r\), and the MSE value is very small if and only if \(r\) is correct, thus the decryption image can only be recognized when the key is correct, i.e., the proposed image encryption algorithm is sensitive enough to the key.

Fig. 4. MSE curve for the key (a), and decryption Lena with wrong \(r = 0.11 + 10^{-16}\) (b).
noise with zero-mean and identity standard deviation. The results of noise attacks with different noise intensities are shown in Fig. 5. The quality of the decryption images does not degrade too much and the decryption image from the contaminated encrypted image with $k = 4$ is still acceptable.

### 3.5. Chosen-plaintext attack

If an attacker knows the used algorithm and possesses a certain amount of plaintext information, the attacker can crack the correct key of a linear encryption system. Compressive sensing is a linear operation process, thus the attacker can obtain key information in the above case. Under the known compressive sensing theory, the attacker will choose a unit matrix as the original image, and then measure the unit matrix to generate a measurement matrix. Finally, the attacker $Eve$ uses the measurement matrix to reconstruct the image which she wants to steal.

However, as for the proposed image compression and encryption algorithm, if the attacker $Eve$ tries to attack the proposed algorithm with the chosen-plaintext attack, i.e., $\alpha$ is set as $I_{N \times N}$, which is an $N \times N$ unit matrix, then she would only obtain

\[
y_I = \left( \frac{\Phi}{|\Phi|} \log(\Phi) + K \right) \times \frac{255}{K}
\]  

(10)
Since all the elements in $\Phi$ are 1 or −1, thus $y_1$ is 0, the attacker cannot obtain the correct measurement matrix to decrypt the image.

4. Conclusion

We propose an image compression-encryption algorithm by combining compressive sensing with log operation to implement compression and encryption operations simultaneously. The proposed algorithm is practical since the measurement is constructed as a partial Hadamard matrix, which is controlled by logistic map. The proposed algorithm can resist the chosen-plaintext attack by taking advantage of the fact that all the elements in measurement matrix are 1 or −1 and $\log 1 = 0$. We demonstrate the proposed image compression-encryption algorithm with high security and good compression performance with simulation results.

Acknowledgments – The work is supported by the National Natural Science Foundation of China (Grant No. 61462016), the Major Academic Discipline and Technical Leader of Jiangxi Province (Grant No. 20162BCB22011), the Cultivation Plan of Applied Research of Jiangxi Province (Grant No. 20181BBE58022) and the Natural Science Foundation of Jiangxi Province (Grant No. 20171BAB202002).

References


[22] NANRUN ZHOU, SHUMIN PAN, SHAN CHENG, ZHIHONG ZHOU, Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing, Optics and Laser Technology 82, 2016, pp. 121–133.


Received November 20, 2017
in revised form January 28, 2018