SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

May 2018, Vol. 61 058104:1–058104:3
doi: 10.1007/s11432-017-9191-x

Spatial image encryption algorithm based on chaotic map and pixel frequency

Guodong YE[1,2*] & Xiaoling HUANG[1]

[1]*Faculty of Mathematics and Computer Science, Guangdong Ocean University, Zhanjiang* 524088*, China;*
[2]*College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou* 310027*, China*

Received 19 May 2017/Accepted 19 July 2017/Published online 20 November 2017

Citation Ye G D, Huang X L. Spatial image encryption algorithm based on chaotic map and pixel frequency. Sci China Inf Sci, 2018, 61(5): 058104, doi: 10.1007/s11432-017-9191-x

Images, as a multimedia resource, for example, medical, education, sensing, and military images, have been playing an important role in digital information communications. To prevent unauthorized access and protect the security of an image, a direct approach is to encrypt the image [1, 2] to hide its information. Chaotic maps (systems) have some excellent inherent properties [3, 4], such as nonlinearity, sensitivity to initial conditions, and ergodicity. Therefore, they have received increasing attention and have been widely used in image encryption schemes. Tong et al. [5] proposed a hyper-chaotic system-based image encryption scheme together with data compression. A discrete cosine transformation dictionary was used to sparsely represent the plain-image, followed by a diffusion operation, to implement the encryption. In this scheme, however, the plain-image cannot be fully recovered due to the compression of data. To balance security and efficiency in designing a chaos-based image encryption algorithm, the image encryption scheme presented in [6] simulates a one-time pad design. In this scheme, with a key of 256 fixed bits and 128 random bits, a chaotic map was iterated to generate four chaotic sequences. Then, pixels with scrambling and value transformation were used to encrypt the plain-image. However, the keystreams were produced independent of the plain-image.

Aiming to enhance security, many algorithms have also been proposed with the help of chaotic maps or systems, for example, DNA and SHA-3. Unfortunately, many algorithms, such as [3], have been found to be insecure. Main reasons include: (1) only one round of permutation, (2) only one round of diffusion, (3) keystream generated independent of the plain-image, and (4) small key space. Higher-dimensional chaotic maps or systems, and quantum maps for generating random sequences have been proposed to resolve the small key space problem by using more initial conditions as inputs. Using two or more rounds of encryption, and making the keystreams dependent on the plain-images, seem to show higher security. Yet, most of these algorithms suffer from unsatisfactory sensitivity to the plain-image [7] due to the invariance of the pixel summation. Moreover, some need extra information transmissions [8].

In this article, considering the aforementioned technical issues, the use of random confusion for the plain-image is suggested, with the help of pixel frequency, followed by double diffusion operations to change the pixel distribution. The keystreams used in both stages of confusion and diffusion are produced in dependence on the plain-image. The pixel frequency is introduced to produce a random sequence in the confusion stage and select a chaotic sequence in the diffusion stage, with respect to different plain-images. As a result, the known-plaintext and chosen-plaintext attacks are infea-

* Corresponding author (email: guodongye@hotmail.com, guodongye@gmail.com)
The authors declare that they have no conflict of interest.

sible. Also, an extra transmission is not needed in the proposed image encryption algorithm, which has a high sensitivity to the invariance of pixel summation. Furthermore, any tiny change to the pixel frequency in the same plain-image would lead to an abstruse cipher-image.

Our algorithm. A 3D cat map [4] with three positive Lyapunov characteristic exponents, $\lambda_1 = 7.1842$, $\lambda_2 = 0.2430$, and $\lambda_3 = 0.5728$, is chosen as the pseudo-random number generator, which can show more complex chaotic properties (See Appendix A for chaotic behavior). The map is described by

$$\begin{cases} x_{i+1} = 2x_i + y_i + 3z_i \bmod 1, \\ y_{i+1} = 3x_i + 2y_i + 5z_i \bmod 1, \\ z_{i+1} = 2x_i + y_i + 4z_i \bmod 1. \end{cases} \tag{1}$$

Suppose that the gray scale plain-image is A of size $m \times n$. To resist statistical attack, a weight factor is designed:

$$s = \frac{\sum_{i=1}^{256} r_i^2 v_i + 1}{255 \sum_{i=1}^{256} r_i^2 + 2}, \tag{2}$$

where $v_i = i - 1$ $(i = 1, 2, \ldots, 256)$ denotes the values from 0 to 255, and r_i is the pixel frequency of v_i in A. Obviously, $0 < s < 1$, because $\sum_{i=1}^{256} r_i^2 v_i + 1 \leqslant 255 \sum_{i=1}^{256} r_i^2 + 1 < 255 \sum_{i=1}^{256} r_i^2 + 2$. This s is used to update the initial keys x_0, y_0, and z_0 in the following equation:

$$\begin{cases} x_0' = x_0 + s/3 \bmod 1, \\ y_0' = y_0 + s/5 \bmod 1, \\ z_0' = z_0 + s/7 \bmod 1. \end{cases} \tag{3}$$

One thus gets new x_0', y_0', and z_0', respectively. By iterating the 3D cat map for some steps using the updated keys, the sequences x', y', z' can be obtained. To avoid the transient effect, the first 100 iterated values are dropped. Then, two random vectors, p and q, generated from these iterated values, can be computed by

$$\begin{cases} p_i = \lceil (x_i' + y_i') \times 10^{14} \rceil \bmod n, i = 1, 2, \ldots, m, \\ q_j = \lceil (y_j' + z_j') \times 10^{14} \rceil \bmod m, j = 1, 2, \ldots, n, \end{cases} \tag{4}$$

where $\lceil x \rceil$ is the *floor* operation. To that end, vectors p and q are employed to perform a circular confusion (permutation) for rows and columns, respectively. As a result, a confused image, P, is obtained.

The diffusion operation is usually adopted after confusion. Here, differing from traditional diffusion methods, pixel frequency is employed to control the random sequence generation. With old keys x_0, y_0, and z_0, the 3D cat map is iterated again for certain steps to yield $T = \{x_{101}, y_{101}, z_{101}, x_{102}, y_{102}, z_{102}, \ldots\}$ (counted after the 100th iterated values). Row diffusion is implemented in the first place, as summarized in Algorithm 1 (a pseudo code). Similarly, the diffusion operation is performed in the column directions, as summarized in Algorithm 2 (another pseudo code). However, $E(0, :)$ and $C(:, 0)$ are constant vectors. Finally, the cipher-image C is obtained. It is noted that, in both algorithms, the s, computed using the pixel frequency, is employed to select the keystream from the T generated by the 3D chaotic map.

Algorithm 1 (For encryption)

Input: image P, keys x_0, y_0, z_0.
Output: image E.
Let $D = P$, $E = zeros(m, n)$;
for $i = 1 : m$ **do**
  D(1, :)=[ ];
  Compute s using Eq. (2) for D;
  $s = floor(s \times 10^{14}) + i \bmod m$;
  $H = T((i-1)n + 1 + s : in + s)$;
  $E(i, :) = P(i, :) + H + E(i-1, :) \bmod 256$;
end for

Algorithm 2 (For encryption)

Input: image E, keys x_0, y_0, z_0.
Output: cipher-image C.
Let $D = E$, $C = zeros(m, n)$;
for $j = 1 : n$ **do**
  D(:, 1)=[ ];
  Compute s using Eq. (2) for D;
  $s = floor(s \times 10^{14}) + j \bmod n$;
  $L = T((j-1)m + 1 + s : jm + s)$;
  $C(:, j) = E(:, j) + L + C(:, j-1) \bmod 256$;
end for

As for the decryption process, using keys x_0, y_0, and z_0, the matrix, T, can be obtained from the 3D cat map after some iterations. Then, D is set to be a zero matrix in the diffusion operation, and the last column $E(:, n) = C(:, n) - C(:, n-1) \bmod 256$ is recovered. For other jth columns, from $n-1$ to 1, $E(:, j)$ can also be restored with L and s, as summarized in Algorithm B1 (See Appendix B). Similarly, the inverse process is performed for row diffusion as summarized in Algorithm B2 (See Appendix B). Afterwards, the confused image P can be obtained. Then, s is computed again for P, and the initial keys x_0, y_0, and z_0 are updated. To that end, the p and q for confusion can be easily obtained. Finally, the plain-image A can be recov-

ered by applying an inverse circular confusion to matrix P.

Simulation and analysis. Some common plain-images are randomly chosen for testing (See Appendix C for more results). Keys $x_0 = 0.5801$, $y_0 = 0.2378$, and $z_0 = 0.8414$ are randomly set. Figure 1 shows the cipher-image for Lena [2] of size 256×256. To maintain high security and avoid linearity, at least two rounds of confusion-diffusion should be implemented in the encryption. Security analysis, including: (1) keyspace analysis, (2) statistical analysis, (3) sensitivity analysis, (4) image structure similarity degree, (5) known-plaintext and chosen-plaintext attacks, (6) extra transmission analysis, (7) randomness test using nist, (8) Chi-square analysis, together with (9) comparisons, show that the proposed algorithm is secure enough to frustrate cryptanalysis in any brute-force attack and resist known-plaintext and chosen-plaintext attacks. One can refer to Appendix C for the simulation results and performance analysis.

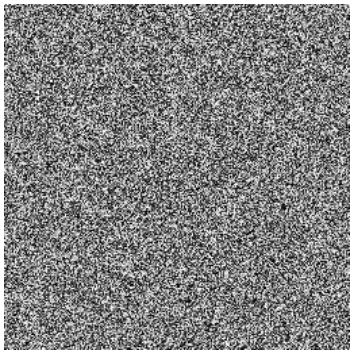

Figure 1 Cipher-image of Lena.

In summary, the main contributions of this work are listed as follows. (1) Pixel frequency is applied in the algorithm. (2) No extra transmission is needed for different plain-images. (3) Keystreams, used in both stages of confusion and diffusion, are dependent on the plain-image. (4) Low sensitivity can be avoided with respect to the invariance of pixel summation. All of these are desirable properties for secure image encryption, as has been commonly acknowledged.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61602124, 61702116), Natural Science Foundations of Guangdong Province of China (Grant Nos. 2016A030310333, 2015A030313614, 2015A030313620), Science and Technology Planning Project of Guangdong Province of China (Grant No. 2017A010101025), China Postdoctoral Science Foundation (Grant No. 2017M611991), Program for Scientific Research Start-up Funds of Guangdong Ocean University of China (Grant No. R17037), and Special Funding Program for Excellent Young Scholars of Guangdong Ocean University of China (Grant No. HDYQ2017006). The authors would like to thank Professor Guanrong Chen at City University of Hong Kong for correcting the expressions in this whole manuscript.

Supporting information Appendix A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Dzwonkowski M, Papaj M, Rykaczewski R. A new quaternion-based encryption method for DICOM images. IEEE Trans Image Process, 2015, 24: 4614–4622
2 Ye G D, Huang X L. An image encryption algorithm based on autoblocking and electrocardiography. IEEE Multimedia, 2016, 23: 64–71
3 Jolfaei A, Wu X W, Muthukkumarasamy V. On the security of permutation-only image encryption schemes. IEEE Trans Inform Foren Secur, 2016, 11: 235–246
4 Chen G R, Mao Y B, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Soliton Fract, 2004, 21: 749–761
5 Tong X J, Zhang M, Wang Z, et al. A joint color image encryption and compression scheme based on hyper-chaotic system. Nonlinear Dyn, 2016, 84: 2333–2356
6 Ge X, Lu B, Liu F L, et al. An image encryption algorithm based on information hiding. Int J Bifurcat Chaos, 2016, 26: 1650192
7 Wang X Y, Liu C M, Xu D H, et al. Image encryption scheme using chaos and simulated annealing algorithm. Nonlinear Dyn, 2016, 84: 1417–1429
8 Belazi A, El-Latif A A A, Belghith S. A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process, 2016, 128: 155–170