Telecommun Syst
DOI 10.1007/s11235-011-9461-0

Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system

C.K. Huang · C.W. Liao · S.L. Hsu · Y.C. Jeng

Abstract When the grays of images present a strong contrast, merely encrypting the gray-level of image pixels is unable to eliminate the image outlines. The adoption of pixel shuffling can eliminate the image outlines, but cannot disrupt the characteristics of gray-level spectrum. Since a chaotic system is highly sensitive to the initial values and the chaotic trajectory is unpredictable, the application of this method to communication encryption and decryption renders a high level of security. In this paper, the chaotic system is adopted as the fundamental base and combined with row, column shuffling, and gray-level encryption to not only eliminate image outlines, but also disrupt the distributional characteristics of gray level, and the resulting increases of key space. Various statistical methods, such as correlation coefficient, NPCR (Number of Pixels Change Rate), UACI (Unified Average Changing Intensity), and entropy, provide analysis of the efficacy of the encryption method proposed. Our example reveals that the proposed encryption method can obtain highly secure encrypted images.

C.K. Huang (✉) · C.W. Liao · Y.C. Jeng
Department of Industrial Education and Technology, National Changhua University of Education, Changhua City, 500, Taiwan
e-mail: ckhuang@cc.ncue.edu.tw

C.W. Liao
e-mail: tcwliao@cc.ncue.edu.tw

Y.C. Jeng
e-mail: jengyc@seed.net.tw

S.L. Hsu
Department of Leisure Services, Chaoyang University of Technology, Wufong Township, Taichung County, 41349, Taiwan
e-mail: slhsu@cyut.edu.tw

Published online: 04 June 2011

Keywords Pixel shuffling · Gray-level encryption · Chaotic system · Correlation coefficient · Entropy

1 Introduction

Data transmission has become an important focus for future development in the information industry. How to ensure information transmission security is a crucial issue. For decades, a many researchers and scholars have investigated the issue of data encryption and decryption in order to ensure security of communications during transmission. Since the dynamic response of the chaotic system is highly sensitive to the initial values and parameters of the method and the chaotic trajectory is unpredictable, its application to communication encryption and decryption is highly valued. To prevent data interception during transmission, the to-be-transmitted data is first hidden in chaotic status [1–3].

While few researchers have applied the scatter and disorder characteristics of the chaotic system to encryption and security communication, few have used these characteristics to the encryption of digital images. Although the application of a one-dimension chaotic method for image encryption is convenient and quick, it is not able to provide sufficient security [4]. Therefore, the use of a multiple dimension chaotic system is more appropriate in order to ensure communication security. In 1999, Lee and Chen [5] produced chaotic codes with the Lorenz chaotic system, applied these codes to the encryption and decryption of gray-level images, and obtained satisfactory results. Moreover, Yang and Yuan produced encryption codes out of chaotic sequences [6]. The fundamental principle was to take an amount of chaotic element as data sequence, transform them into binary codes, and subsequently shuffle the bits in order. Zhang and He combined chaotic sequences as encrypted

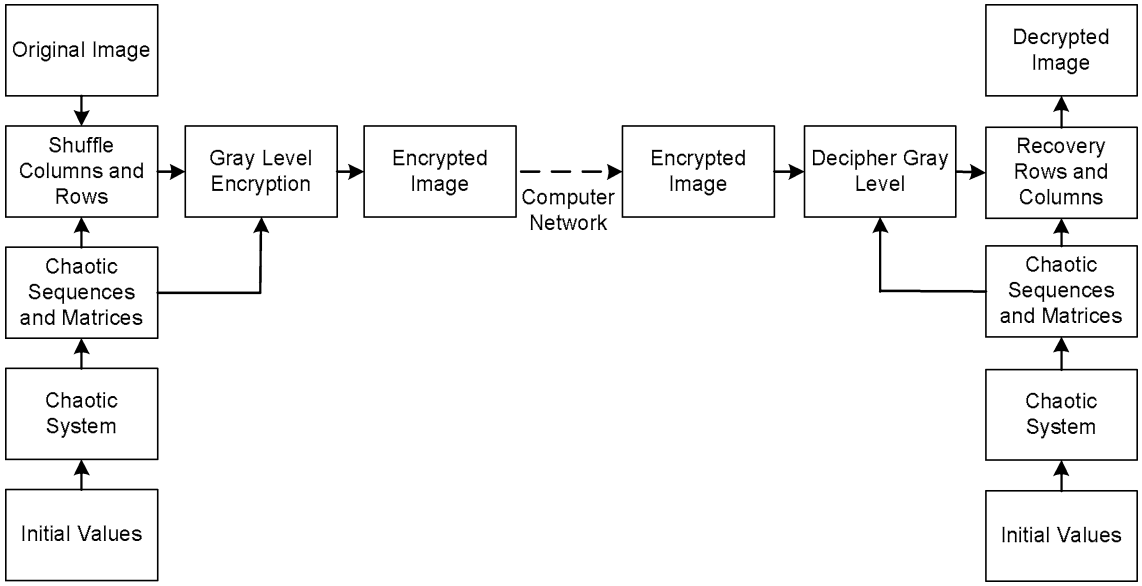


Fig. 1 Flowchart of the encryption and decryption methods

matrices, encrypted the plain text matrix and then hid cipher text matrix with a two dimensional chaotic system for the sake of security enhancement [7].

In this paper, the chaotic system is the fundamental base. Usage of chaotic variable elements will be by row and by column shuffling coupled with gray-level value encryption on image pixels in order to enhance the security of encrypted images. Finally, statistical analysis tests image security.

2 Encryption and decryption

Several scholars have researched image encryption conduct pixel-shuffling encryption on images by means of encryption algorithm [8]. Although this provides a certain degree of security, this encryption only eliminates the outlines of images. The method proposed in this paper of row, column, and gray-level encrypting, not only dissipates image outline, but also alters the distribution characteristics of gray-level values and accordingly enhances encryption security. Figure 1 shows the encryption and decryption scheme.

2.1 Encryption

Abundant image statistic analysis proves that neighboring pixels in an image are closely related. On average, a high correlation exists between eight to sixteen pixels of the horizontal, vertical, and diagonal directions. To disturb this relationship and prevent interceptors from decoding, this paper uses chaotic variable sequences X, Y, Z, produced by chaos. Following is row and column chaotic shuffling on images with X and Y, and the gray encryption on the gray levels of target images with Z in order to enhance the security of encrypted images. Figure 2 outlines the encryption process and the encryption procedures follow:

Step 1. Input the initial values of the chaotic system, x_0, y_0, z_0.

Step 2. Propose the gray-level matrix of original images $A_{M\times N}$.

Step 3. Create chaotic variable element sequences X, Y, and Z, then elicit variable element matrices of the same dimension as original images A, $X_{1(i,j)}$, $Y_{1(i,j)}$.

Step 4. Conduct column indexing and shuffling on $A_{(i,j)}$ and $X_{1(i,j)}$ one by one, with the function $sortrows(\bullet)$. The $sortrows(\bullet)$ are the function of sorting index, representing the ascending order of $\bullet$ sequence.

Step 5. Judge whether j is equal to N, and if not, repeat step 4. When $j = N$ is reached, the column shuffling of pixels is completed, and an encrypted image A_{e1} is obtained. Figures 3 and 4 illustrate the index shuffling.

Step 6. Conduct row indexing and shuffling on $A_{e1(i,j)}$ and $Y_{1(i,j)}$, one by one, with the function $sortrows(\bullet)$.

Step 7. Judge whether i is equal to M, and if not, repeat step 6. When $i = M$ is reached, the column shuffling of pixels is completed, and an encrypted image A_{e2} is obtained. Figure 5 illustrates the index shuffling.

Step 8. Transfer the encrypted image $A_{e2(M\times N)}$ to $A_{e2(1\times MN)}$.

Step 9. Conduct bits indexing and shuffling on $A_{e2(1\times MN)}$ (binary) and Z, we can get the shuffled level matrix $A_{e2(1\times MN)}$.

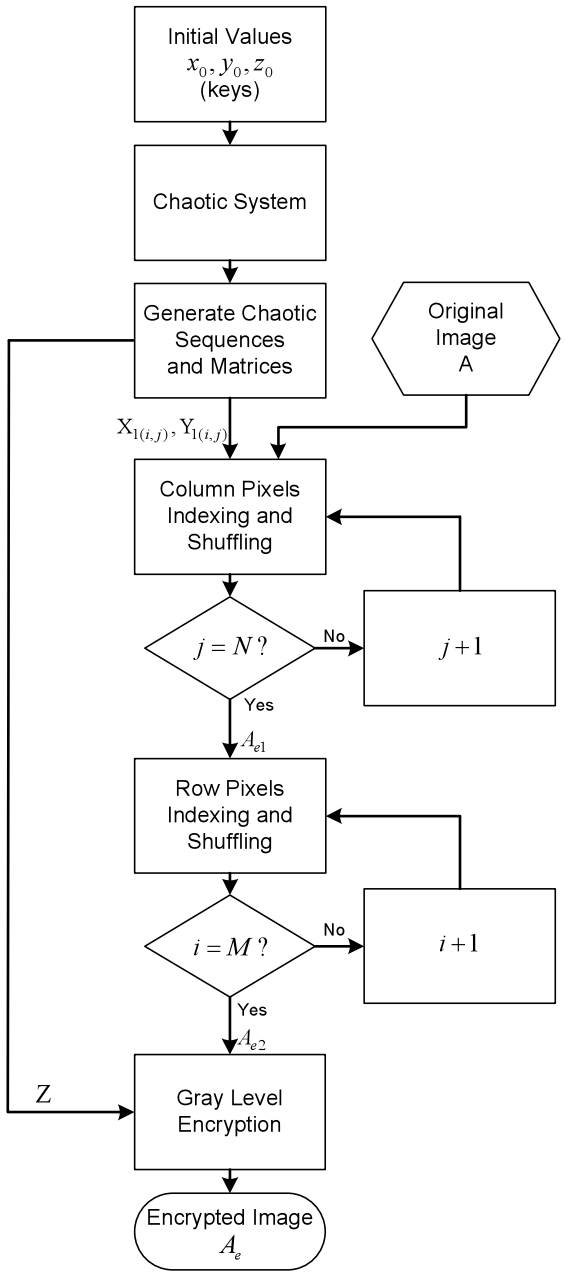


Fig. 2 Procedures of row and column shuffling and gray level encrypting

Step 10. Conduct the dimension transform ($1 \times MN \rightarrow M \times N$), and therefore the encrypted image $A_{e(M\times N)}$ can be obtained.

2.2 Decryption

Image decryption involves restoring the gray levels of the encrypted images, conducting row and column restoration based on the sequence matrix and the restored level matrix and finally obtaining a restored image, as shown in Fig. 6. The decryption procedures are:

Step 1. Follow the steps 1∼3 of encryption to produce X, Y, Z, and $X_{1(i,j)}$, $Y_{1(i,j)}$ of the same dimensions as Lena A.

Step 2. Create a sequence matrix D_0 of the same dimension as the matrix $A_{e2(1\times MN)}$ (binary).

Step 3. Conduct indexing and shuffling on D_0 and Z with *sortrows*(•) and obtain the recovery matrix D_{0r}.

Step 4. Conduct bits indexing and restoring on $A_{e2(1\times MN)}$ (binary) and D_{0r}, we can get the restoration level matrix $A_{e2(1\times MN)}$.

Step 5. Transfer the matrix $A_{e2(1\times MN)}$ to $A_{e2(M\times N)}$.

Step 6. Create a sequence matrix D of the same dimension as the original images, as shown in Fig. 7.

Step 7. Conduct indexing and shuffling on D and Y_1 with *sortrows*(•), and obtain the recovery matrix D_r of dimension $M \times N$. Figure 8 shows the illustration.

Step 8. Conduct row indexing and restoring on $A_{e2(i,j)}$ and $D_{r(i,j)}$ one by one, with *sortrows*(•).

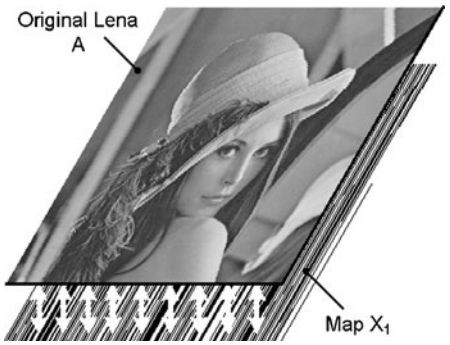
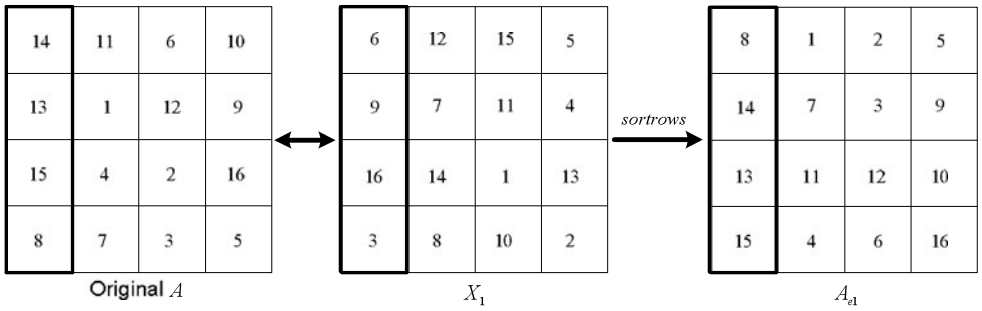


Fig. 3 Index shuffling of original Lena by map X_1

Fig. 4 Illustration of column indexing and shuffling



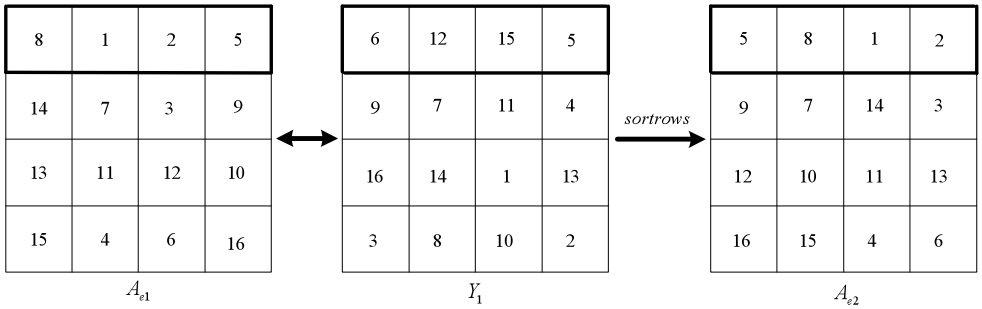


Fig. 5 Illustration of row indexing and shuffling

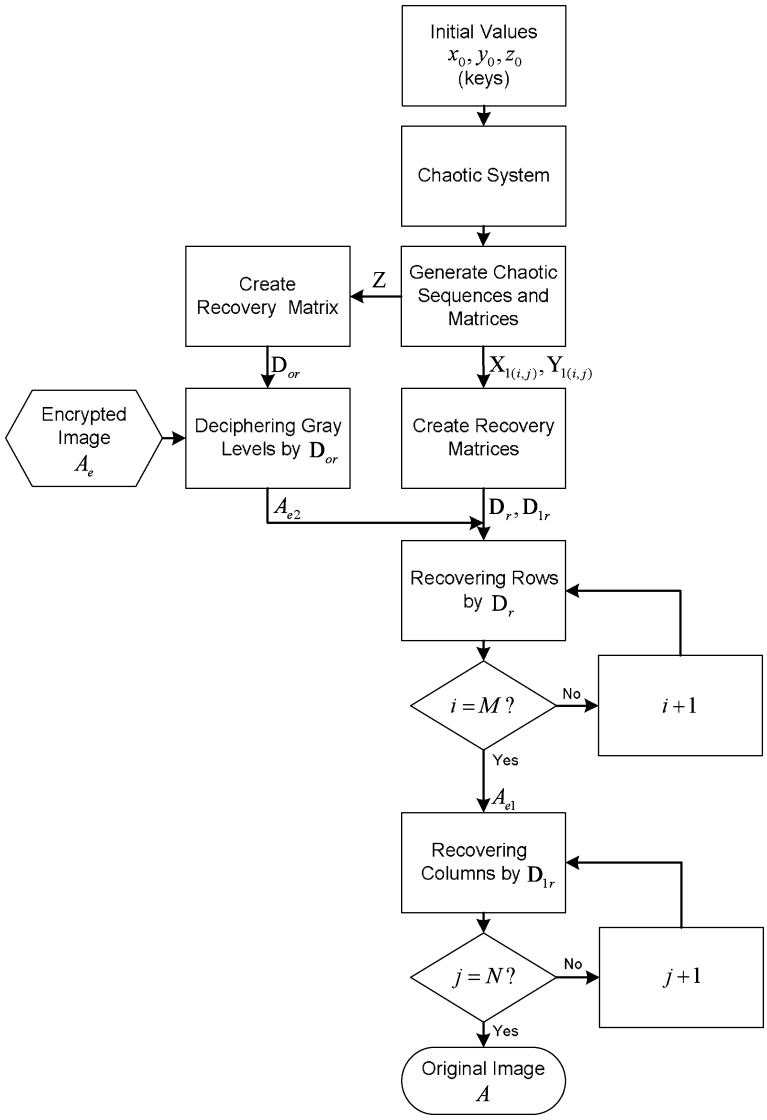


Fig. 6 Flowchart of row and column restoring, and gray decryption

Step 9. Judge whether i is equal to M, and if $i \neq M$, repeat step 8. When $i = M$ is reached, the row restoration is completed, and A_{e1} is obtained. Figure 9 illustrates this indexing and restoration.

Step 10. Create a sequence matrix D_1 of the same dimension as the original image A, as shown in Fig. 10.

Step 11. Conduct indexing and shuffling on D_1 and X_1 with $sortrows(\bullet)$, and obtain the recovery matrix D_{1r}. Figure 11 illustrates this indexing and shuffling.

Step 12. Conduct column indexing and restoring on $A_{e1(i,j)}$ and $D_{1r(i,j)}$ one by one, with $sortrows(\bullet)$.

Step 13. Judge whether j is equal to N, and if $j \neq N$, repeat step 12. When $j = N$ is reached, the original image

A is obtained. Figure 12 illustrates this indexing and restoring.

3 Example

The following example is presented in order to verify the plausibility of the proposed method, which encrypts and decrypts gray image Lena (256 × 256) as described in Sects. 3.1 and 3.2 and illustrate its efficacy.

The following equation presents the Chua chaotic systems applied in this paper [9]:

$$\dot{x} = \alpha(y - x - h(x)), \tag{1a}$$

$$\dot{y} = x - y + z, \tag{1b}$$

$$\dot{z} = -\beta y - \gamma z, \tag{1c}$$

$$h(x) = m_1 x + 0.5(m_0 - m_1)(|x + 1| - |x - 1|) \tag{1d}$$

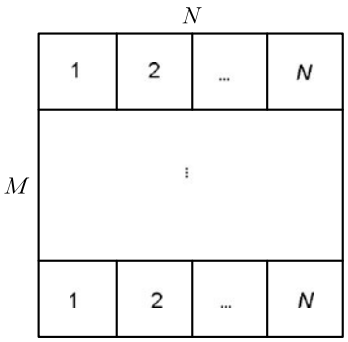


Fig. 7 Sequence matrix D

where $\alpha = 10, \beta = 14.78, \gamma = 0.0385, m_0 = -1.27, m_1 = -0.68$.

3.1 Image encryption

The first step is a dynamic simulation using the initial values of the chaotic system $x_0 = 0.1, y_0 = 0.6, z_0 = 0.1$. Meanwhile, the function *reshape*(•) is used to produce the variable element sequence and matrices X_1, Y_1, Z. The function *sortrows*(•) is used to conduct column indexing and shuffling on the Lena images A and X_1 and as a result, an encrypted image A_{e1} is obtained, as shown in Fig. 13(c). Again, row indexing and shuffling on A_{e1} and Y_1 is conducted and an encrypted image A_{e2} is obtained, as shown in Fig. 13(e). Finally, we performed gray levels encryption to obtain encrypted image A_e by Z. Figures 13(a)–(g) illustrates the image encryption method.

3.2 Image decryption

The first step is the initial value inputting of the chaotic system $x_0 = 0.1, y_0 = 0.6, z_0 = 0.1$ together with a dynamic simulation. Meanwhile, the function *reshape*(•) is used to produce variable element sequence and matrices (X_1, Y_1 and Z). Following is decryption of the gray level of A_e by D_{or} (created by Z) occurs to obtain a restored image A_{e2}, as shown in Fig. 14(c). The function *sortrows*(•) is again used to produce a sequence matrix D of the same dimension as the original image and conduct indexing and shuffling on D and Y_1 to obtain a recovery matrix D_r. Once again, the function *sortrows*(•) is used to conduct row indexing and restoration on D_r and A_{e2}, to obtain row restoration im-

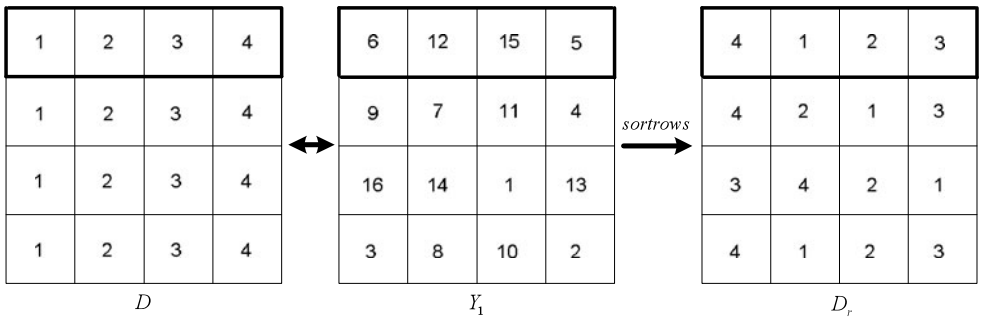


Fig. 8 Procedures of indexing and shuffling on D and Y_1

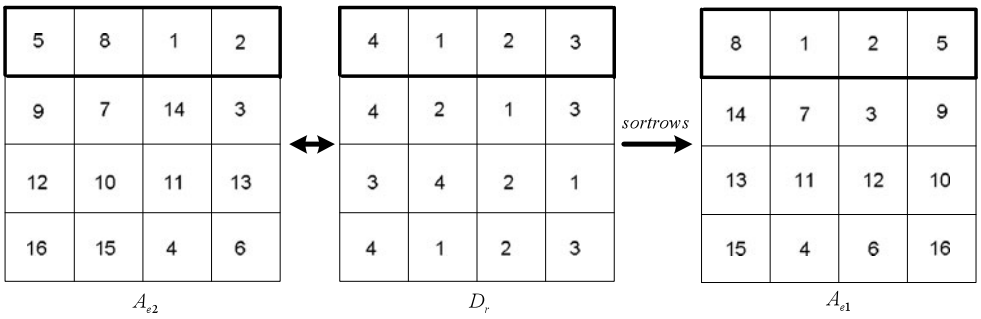


Fig. 9 Illustration of indexing and restoring on A_{e2} and D_r

age A_{e1}, as shown in Fig. 14(e). In addition, the function *sortrows*(•) is used to produce a sequence matrix D_1 of the same dimension as the original image and conduct indexing and shuffling on D_1 and X_1 to obtain a recovery matrix D_{1r}. Column indexing and restoration is performed on D_{1r} and A_{e1}, to obtain the restored Lena A_d, as shown in Fig. 14(g). Figures 14(a)–(g) shows the complete image decryption.

4 Security analysis

This section describes analysis of the security of encrypted images with five statistical methods in order to measure encryption efficacy.

4.1 Key space

The chaotic system adopted in this paper is highly sensitive to the trace variations of initial values and the sensitivity variation is $x_0 = 10^{-16}$, $y_0 = 10^{-16}$ and $z_0 = 10^{-16}$. Therefore, the key space of this encryption system can reach as high as 10^{48}.

4.2 Correlation coefficient

Correlation coefficient measures the dependence of two adjacent variables at a certain direction. The more closely related these two variables are, the closer the correlation coefficient approaches 1. Conversely, if they are less closely related, the value of correlation coefficient approaches 0. The two variables are not related and unpredictable when the coefficient is close to 0. The calculation equation is [10]:

$$r = \frac{n(\sum_{i=1}^{n} X_i Y_i) - (\sum_{i=1}^{n} X_i)(\sum_{i=1}^{n} Y_i)}{\sqrt{[n(\sum_{i=1}^{n} X_i^2) - (\sum_{i=1}^{n} X_i)^2][n(\sum_{i=1}^{n} Y_i^2) - (\sum_{i=1}^{n} Y_i)^2]}} \quad (2)$$

Table 1 Correlation coefficient tests

Image	Axis		
	Diagonal	Vertical	Horizontal
Original Lena	0.9198	0.9573	0.9201
Encrypted Lena	−0.0025	−0.0006	−0.0050

Table 2 NPCR and UACI tests

Image	Test method	
	NPCR	UACI
Encrypted Lena	99.54%	28.27%

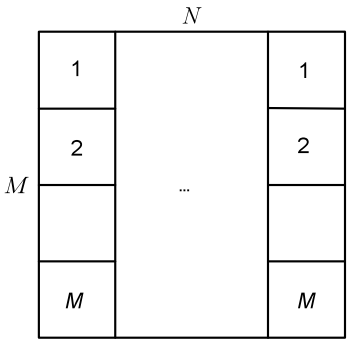


Fig. 10 Sequence matrix D_1

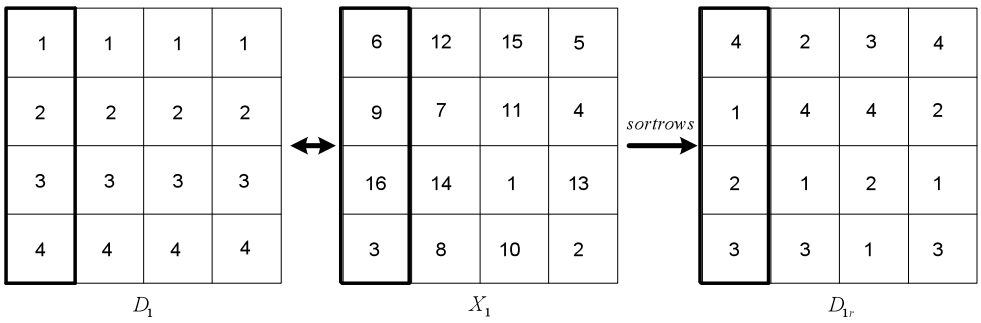


Fig. 11 Indexing and shuffling on D_1 and X_1

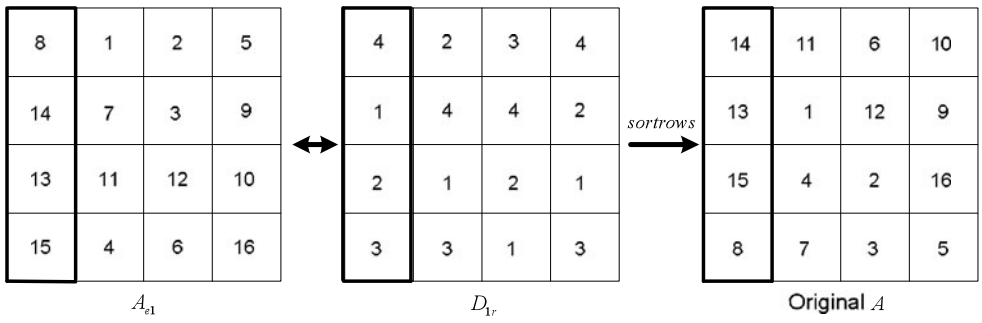


Fig. 12 Indexing and restoring of A_{e1} and D_{1r}

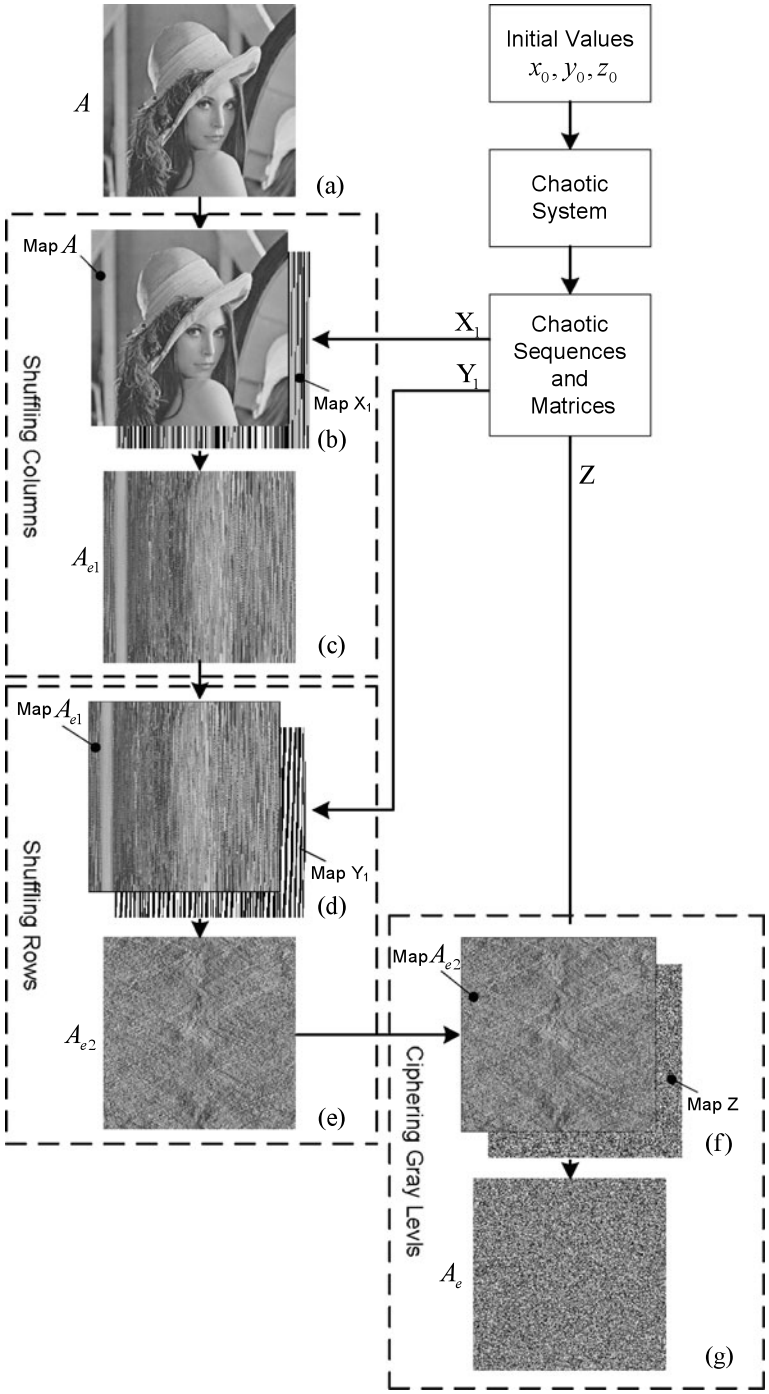


Fig. 13 A diagrammatic explanation of the image encryption: (**a**) original Lena, (**b**) index original Lena with X_1, (**c**) column-shuffled Lena A_{e1}, (**d**) index A_{e1} with Y_1, (**e**) row- and column-shuffled Lena A_{e2}, (**f**) mapping A_{e2} with Z, (**g**) encrypted Lena A_e

where $n(\sum_{i=1}^{n} X_i Y_i) - (\sum_{i=1}^{n} X_i)(\sum_{i=1}^{n} Y_i)$ represents the sample variation, and $[n(\sum_{i=1}^{n} X_i^2) - (\sum_{i=1}^{n} X_i)^2]$ and $[n(\sum_{i=1}^{n} Y_i^2) - (\sum_{i=1}^{n} Y_i)^2]$ are the sample standard variation of X and Y, respectively. Table 1 shows the outcome of the correlation coefficient calculation.

4.3 NPCR & UACI

NPCR is the comparison of gray levels of relational positions between original and encrypted images in order to ensure that the pixels of every level matrix can be altered. UACI is, on the other hand, the percentage of the average level matrix change between the relational positions of two images. The following equations define NPCR and UACI [11]:

$$\text{NPCR} = \frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} D(i,j)}{m \times n} \times 100\% \tag{3}$$

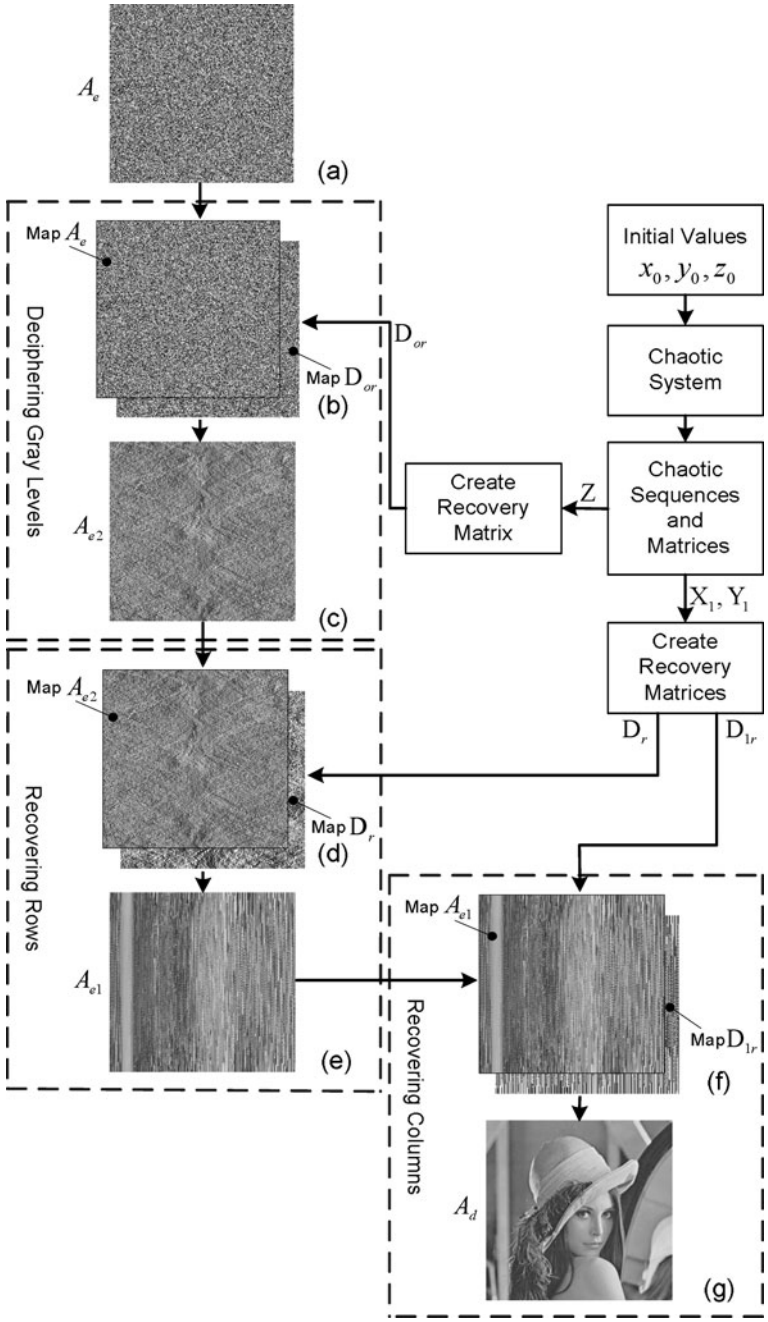


Fig. 14 A diagrammatic explanation of the image decryption: (**a**) encrypted Lena, (**b**) mapping A_e with D_{or}, (**c**) gray level decrypted Lena, (**d**) index A_{e2} with D_r, (**e**) row-restored Lena A_{e1}, (**f**) index A_{e1} with D_{1r}, (**g**) decrypted Lena

$$\mathrm{UACI} = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \frac{|A(i,j) - A_{CS}(i,j)|}{255} \times 100\% \quad (4)$$

where

$$D(i,j) = \begin{cases} 0, & A(i,j) = A_{CS}(i,j) \\ 1, & A(i,j) \neq A_{CS}(i,j) \end{cases},$$

A is the original image of $m \times n$ dimensions, and A_{CS} is the encrypted image. Table 2 lists the results of the NPCR and UACI calculations.

4.4 Entropy

Rudolf Clausius (1864) was the first to propose the concept of entropy. This theory was first employed in information theory by Claude Elwood Shannon (1948). If the entropy of encrypted images is less than, but approaching eight, it will reduce the probability of successful restoration of images by interceptors. On the contrary, if the entropy is more than eight, then interceptors easily decode the encrypted images. The calculation of entropy is [12]:

$$entropy = -\sum_{i=0}^{2^N-1} P_i \log_2 P_i, \quad (5)$$

where P_i is the probability of the pixel's grey-level value i. After the calculation, the entropy of encrypted image A_e is 7.9967.

5 Conclusions

This paper uses graphic method to demonstrate the main results for the image encryption, the application of variable elements of a chaotic system to pixel row and column shuffling and gray level encryption has resulted in highly secure images. Moreover, statistical analyses show that key space is 10^{48}, correlation coefficient of classical Lena encrypted images is less than 0.005 for all three directions, and entropy is 7.9967. In addition, NPCR and UACI prove it is possible to obtain excellent pixel alteration effects. Accordingly, the encryption technique proposed in this paper will render outstanding image encryption effects and high transmission security.

References

1. Cuomo, K. M., Oppenheim, A. V., & Strogatz, S. H. (1993). Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on Circuits and Systems II, Express Briefs*, *40*, 626–633.
2. Yang, T., & Chua, L. O. (1996). Secure communication via parameter modulation. *IEEE Transactions on Circuits and Systems I, Fundamental Theory and Applications*, *43*, 817–819.
3. Yang, T., Wu, C. W., & Chua, L. O. (1997). Cryptography based on chaotic systems. *IEEE Transactions on Circuits and Systems I, Fundamental Theory and Applications*, *44*, 469–472.
4. Kocarev, L. (2001). Chaos-based cryptography: a brief overview. *IEEE Transactions on Circuits and Systems I, Fundamental Theory and Applications*, *1*, 6–21.
5. Lee, B. H., & Chen, Y. Y. (1999). *Implementation of chaotic stream ciphers using chaotic pseudorandom number generator*. Thesis of National Taiwan University, Taiwan.
6. Yang, W. A., & Yuan, D. M. (2006). A new method of key generation based on chaotic sequence. *China Academic Journal Electronic Publishing House Mathematics in Practice and Theory*, *36*, 160–164.
7. Zhang, W., & He, R. C. (2006). An encryption and hiding algorithm based on logistic chaotic sequences. *China Academic Journal Electronic Publishing House, Journal of Lanzhou Jiaotong University (Natural Sciences)*, *25*, 80–82.
8. Sun, Z. J., Chen, Y., Wang, Y. X., & Liao, X. F. (2007). New image encryption algorithm based on Chua's circuit. *China Academic Journal Electronic Publishing House, Computer Engineering and Design*, *28*, 3328–3330.
9. Chua, L. O., & Lin, G. N. (1990). Canonical realization of Chua's circuit family. *IEEE Transactions on Circuits and Systems*, *37*, 885–902.
10. Bluman, A. G. (1998). *Elementary statistics* (3rd edn.). McGraw-Hill, New York.
11. Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons and Fractals*, *21*, 749–761.
12. Behnia, S., Akhshani, A., Ahadpour, S., Mahmodi, H., & Akhavan, A. (2007). A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps. *Physics Letters A*, *366*, 391–396.

C.K. Huang received a Ph.D. degree in Engineering Science and Technology from National Yunlin University of Science and Technology, Taiwan, in 2004. He is now an associate professor with National Changhua University of Education. His current research involves chaotic system and image encryption.

C.W. Liao received both M.S. and Ph.D. in Industrial Education from National Taiwan Normal University, Taiwan, in 1994 and 2002, respectively. Since August 2007, he has been an associate professor with National Changhua University of Education in Taiwan. His research interests include technology and vocational education, energy education of technology, and image encryption.

S.L. Hsu received the Ph.D. degree in Department of Industrial Education & Technology, National Changhua University of Education, Taiwan. She also is an assistant professor in the Department of Leisure Services of Chaoyang University of Technology, Taiwan. Her research interests include human resources management, leisure services management, and image encryption.

Y.C. Jeng received his Ph.D. and Master degrees at Iowa State University. From 1988 to 2010, he is the professor at the Department of Industrial Education and Technology, National Changhua University of Education, Taiwan. His interesting research area is vocational & technical education, and his major teaching areas are engineering mechanics and vocational & technical education.