Advance Journal of Food Science and Technology 9(5): 361-366, 2015
DOI: 10.19026/ajfst.9.1916
ISSN: 2042-4868; e-ISSN: 2042-4876

Submitted: March 9, 2015 Accepted: April 1, 2015 Published: August 20, 2015

Research Article

A Design of New Fast Image Permutation Approach for Food Intellectual-property Protection

Feng Huang, Wei Zou and Qingzheng Li
The Cooperative Innovation Center of Wind Power Equipment and Energy Conversion,
Hunan Institute of Engineering, Xiangtan, China

Abstract: The security of food image was important in food intellectual-property protection. Permutation could protect security of image which charged the correlation among adjacent pixels. Some chaotic maps were used in image permutation; act as baker map or some other maps. But the plain image must be square. At the same time the plain image always is stretched to a line firstly. Obviously, it wasted precious time. The study found the pixels location could arrange freely using some new maps without stretching and those also could encrypt rectangle images not only square image. The ideas of maps were: firstly the plain image was divided into two halves. Using two different scanning methods it could stretch the halves to two different lines. Then it inserted the pixels of a line into the adjacent pixels of another line in order. Lastly the new line could be fold to a new image. For different of scanning methods, it got some different map patterns. A permutation approach was developed which used those patterns. It used decimal numbers as the keys and could permute rectangle images easily. The permutation process was quite fast and enough safe. Deciphering process was an invertible process using the same keys. Some studies proved that high correlation among adjacent pixels was rapidly charged. The approach could satisfy the most security requirements in Internet.

Keywords: Chaotic map, food intellectual-property protection, image permutation, information security

INTRODUCTION

Communications technology is developing very fast. Especially, WIFI signal is everywhere and 4G technology is already commercially available. More and more food images are transmitted over the wireless networks or the Internet. Food intellectual-property protection is increasingly becoming a serious problem. Without protection, people are food insecure and enterprises face business failures.

Image security technology is an important means to protect safety of kinds of food image. Act as image permutation can shuffle the positions of image pixels and converts a food image into a new image not recognizable by its attackers. It fleetly enhance food image security and can protect food image and against statistical cryptanalysis. The more important is it is the basis of other image encryption algorithm.

Some classic chaotic maps are suitable for food image permutation including the cat map, the baker map etc (Zheng and Gao, 2011; Chen *et al*., 2015; Enayatifar *et al*., 2014; Wang and Wang, 2014; Wang *et al*., 2011). In Fridrich (1998), she designed a symmetric image encryption approach for square image. It can be seen the image permutations induced by the baker map behave as typical random permutations. In Chen *et al.* (2004) and Mao *et al.* (2004) two symmetric image encryption approaches based on three dimensional cat map or baker map are proposed. The image permutation employed by those chaotic maps is an important part of encryption. In Yoon and Kim (2010), it proposed a new image encryption algorithm using a large pseudorandom permutation by the permutation matrix. But the plain images in the approaches almost must be square image and the speed of encryptions weren't fast enough.

Researchers designed some new chaotic map for fast image permutation. In Huang and Feng (2007), a new chaotic map was proposed. Theoretically the encryption has enough keys space. But unfortunately, there are some week keys, duplicate keys and security risks. At the same time the encryption time may disclosure the key. Those affect the security of the encryption algorithm.

SCAN patterns are another method to permute image. Because SCAN patterns can generate very large number of scanning paths or space filling curves, it can confirm the security of image. In Maniccam and Bourbkis (2004) is first stage compression-based frames differences and encryption of video whose compression error can be bounded pixel wise by a user specified value, very large number of encryption keys.

Corresponding Author: Feng Huang, The Cooperative Innovation Center of Wind Power Equipment and Energy Conversion, Hunan Institute of Engineering, Xiangtan, China

The SCAN patterns are patterns language-based two dimensional spatial accessing methodologies. So they are more flexible than chaotic maps. But one of the questions is that the method requires the plain image must be square image and its size must be even.

As we see, image security is important for food intellectual property rights. In Internet, most food image is rectangle. How to encrypt them is important issue. At the same time, with the network speed increases, large-size food image are becoming more common. So the speed of permutation must be enough fast. Based on the above two issues, it is very necessary to design new fast permutation for large-size rectangle food images. And the encryption must be enough safe and satisfy need of protection.

MATERIALS AND METHODS

In design, it utilized an important characteristic of images: each pixel of column of image can be inserted into adjacent two pixels of row of image.

Suppose that a rectangle image consists of $N \times M$ pixels with L gray levels. Here N is an even number. If N isn't an even number, the size of image can be $N' \times M$ ($N' = N+1$).

Firstly the rectangle image $A(i, j)$ is divided into two equal size halves $A_1(i, j)$ and $A_2(i, j)$, as seen in Fig. 1. Secondly it uses some scanning modes which stretched the image to two different lines $L_1(n)$ and $L_2(n)$, here $n = floor(N+M+1)/2$. Then it inserts the pixels of $L_2(n)$ into the adjacent pixels of $L_1(n)$ in order. Lastly the new line is fold to a new image $B(i, j)$ different from plain image. The principle of new maps is shown in Fig. 1.

In Fig. 1, it must use two or more scan modes. In the study, there are four scan modes, as seen in Fig. 2. They can get ten different maps. In Fig. 3 map (a), it use the first scan mode twice for different halves. So the plain image was stretched the image to two different lines. Then it inserts the pixels of a line into the adjacent pixels of another line in order. The principles of other maps in Fig. 3 are similar.

An example is given here. An image with 6×4 pixels, that is $N = 6$, $M = 4$. The process of one map is shown in Fig. 4. Firstly the image is divided into two halves: the left part and the right part. Secondly, it uses the first scan mode twice for two parts. So the plain image is stretched to two different lines. At the time, it can take each pixel of one line insert into pixels of another line. So it joins a new line. Lastly the new line is fold over to a new image of same size of plain image. Repeating the process, the positions of image pixels are shuffled obviously.

The algorithm of the maps: Supposing the dimension of a square image is $N \times M$, where N and M are integers. $A(i, j)$ is the matrix of a rectangle image, in which each element corresponds to a gray-level value of the pixel (i, j), $i = 0, \ldots, M-1$, $j = 0, \ldots, N-1$; $L(i)$, $i = 0,1, \ldots, MN$ is a one dimensional vector mapped from A. The formulas of ten different maps in Fig. 3 are as follows:
The map (a) in Fig. 3:

$$L(i \times N + 2j) = A(i, j) \tag{1}$$

While $j<N/2$:

$$L(i \times N + 2j - N + 1) = A(i, j) \tag{2}$$

While $j \geq N/2$.
The map (b) in Fig. 3:

$$L(i \times N + 2j) = A(i, j) \tag{3}$$

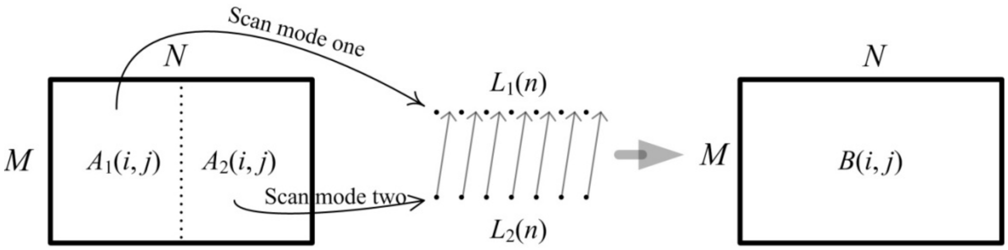


Fig. 1: The principle of new maps

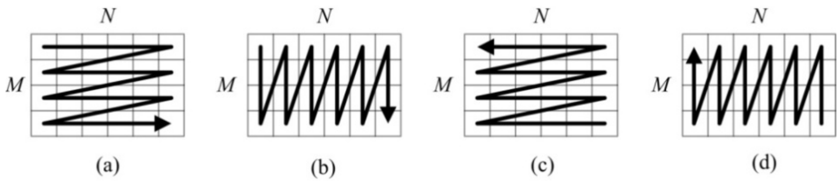
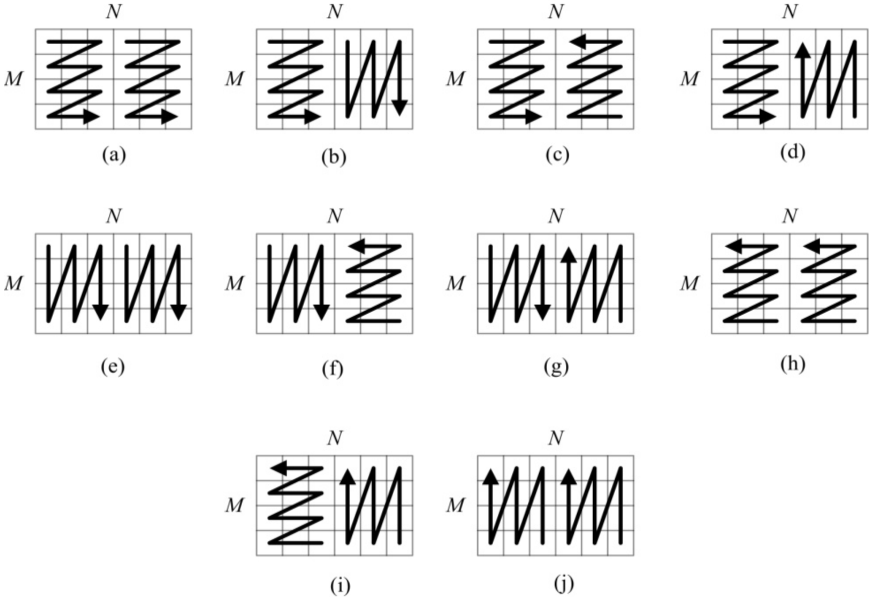


Fig. 2: Four scan modes



(a) (b) (c) (d) (e) (f) (g) (h) (i) (j)

Fig. 3: Ten different maps

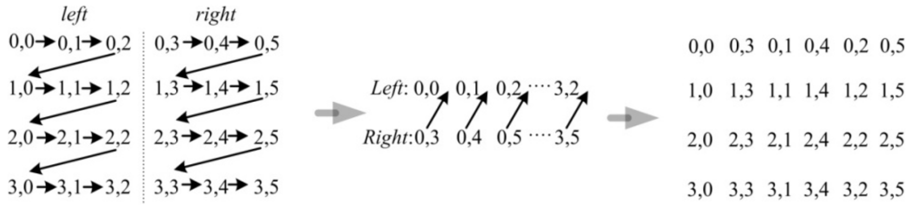


Fig. 4: An example

While $j<N/2$:

$$L[(2j-N)\times M+2i+1]=A(i,j) \qquad (4)$$

While $j\geq N/2$.
The map (c) in Fig. 3:

$$L(i\times N+2j)=A(i,j) \qquad (5)$$

While $j<N/2$.

$$L[2(N-1-j+i\times\frac{N}{2})+1]=A(i,j) \qquad (6)$$

While $j\geq N/2$时,
The map (d) in Fig. 3:

$$L(i\times N+2j)=A(i,j) \qquad (7)$$

While $j<N/2$:

$$L[2(N-1-j)\times M+2(M-1-i)+1]=A(i,j) \qquad (8)$$

While $j\geq N/2$.

The map (e) in Fig. 3:

$$L(2j\times M+2i)=A(i,j) \qquad (9)$$

While $j<N/2$:

$$L[2(j-\frac{N}{2})\times M+2i+1]=A(i,j) \qquad (10)$$

While $j\geq N/2$.
The map (f) in Fig. 3:

$$L(2j\times M+2i)=A(i,j) \qquad (11)$$

While $j<N/2$:

$$L[2(N-1-j)+i\times N+1]=A(i,j) \qquad (12)$$

While $j\geq N/2$.
The map (g) in Fig. 3:

$$L(2j\times M+2i)=A(i,j) \qquad (13)$$

While $j<N/2$:

Table 1: The map patterns

	Map Patterns	Form of map Patterns
0	map (a)	Formula (1)+formula (2)+formula (21)
1	map (b)	Formula (3)+formula (4)+formula (21)
2	map (c)	Formula (5)+formula (6)+formula (21)
3	map (d)	Formula (7)+formula (8)+formula (21)
4	map (e)	Formula (9)+formula (10)+formula (21)
5	map (f)	Formula (11)+formula (12)+formula (21)
6	map (g)	Formula (13)+formula (14)+formula (21)
7	map (h)	Formula (15)+formula (16)+formula (21)
8	map (i)	Formula (17)+formula (18)+formula (21)
9	map (j)	Formula (19)+formula (20)+formula (21)

$$L[2(N-1-j)\times M+2(M-1-i)+1]=A(i,j) \qquad (14)$$

While $j \geq N/2$.
The map (h) in Fig. 3:

$$L(N-2-2j+i\times N)=A(i,j) \qquad (15)$$

While $j<N/2$:

$$L[2(N-1-j)+i\times N+1]=A(i,j) \qquad (16)$$

While $j \geq N/2$.
The map (i) in Fig. 3:

$$L(N-2-2j+i\times N)=A(i,j) \qquad (17)$$

While $j<N/2$:

$$L[2(N-1-j)\times M+2(M-1-i)+1]=A(i,j) \qquad (18)$$

While $j \geq N/2$.
The map (j) in Fig. 3:

$$L[(N-2-2j)\times M+2(M-1-i)]=A(i,j) \qquad (19)$$

While $j<N/2$:

$$L[2(N-1-j)\times M+2(M-1-i)+1]=A(i,j) \qquad (20)$$

While $j \geq N/2$.

The folding algorithm: The line of *MN* pixels *L*(*i*) is further mapped to a same size *N*×*M* rectangle image, *B*. Here there is a simple method to do this.

The map from line *L* to image *B* is described with the following formula, here $i = 0, \ldots, M\text{-}1$, $j = 0, \ldots, N\text{-}1$.

$$B(i,j)=L(i\cdot N+j) \qquad (21)$$

The map patterns: Using the above maps and six folding methods, it can get ten chaotic maps. Act as the map a may means using the left map stretched the square image to a line and using formula (21) fold the line to another image. One of design is shown in Table 1.

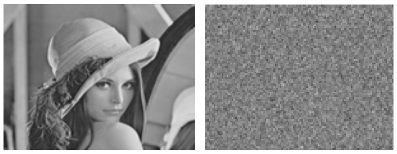

(a) (b)

Fig. 5: Plain image and cipher image; (a) Plain image, (b) Cipher image

Table 2: Key space size VS keys length

Key length (digit)	6	7	8	9
Key space size	10^6	10^7	10^8	10^9

Table 3: Correlation coefficients of two adjacent pixels

	Plain image	Cipher image (keys)
Horizontal	0.9404	0.0061
Vertical	0.9683	0.0106
Diagonal	0.9024	0.0074

RESULTS AND DISCUSSION

An image permutation approach is carried out based on the map patterns. The plain image and cipher image are shown in Fig. 5. It has 256×240 pixels with 256 grey levels. The plain image is encrypted using the maps by the *keys* "0123456789". It can be seen that the plain image has been encrypted. It shows the image encryption using the chaotic map has no message loss. The time of encryption by *keys* is 0.0149s; the time of decryption by *keys* is 0.01487s. (the CPU of PC is Intel's core i5 2.5 Ghz, the ram is 4G and the operating system is Windows 7).

Key space: Since the length of the keys in permutation has no limit, its key space can be calculated according to the length of the key. Suppose the key are represented in decimal. The relationship between the key space size and the key length is shown in Table 2. In theory, security key can be any long integer to satisfy the different security requirements.

Correlation: Correlation of two adjacent pixels in a cipher image, $cov(x,y) = E(x - E(x))(y - E(y))$, $r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$, Where *x* and *y* are gray-scale values of two adjacent pixels in the image.

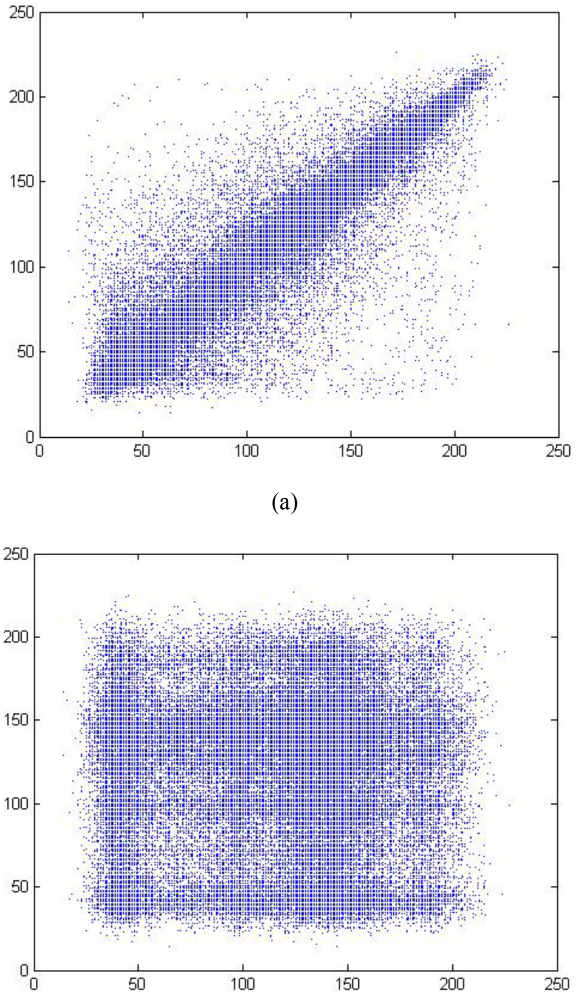
Figure 6 shows the correlations of two horizontally adjacent pixels in plain image and cipher image (*keys*): the correlation coefficients are 0.9442, 0.0001. Similar results for diagonal and vertical directions were obtained and are shown in Table 3.

Fixed point ratio: Where *keys* is "0123456789" BD = 0.62%. Those mean the positions of the 99.38% plain image pixels are charged.

Change of the gray: Where *keys* is "0123456789" GAVE = 52.9721. Those mean the average values of the pixels are charged by 20%.

Table 4: Self-correlation of images

m	1	2	3	4	5	6	7	8	9	10
lena	0.3804	0.3847	0.4338	0.4779	0.5158	0.5481	0.5760	0.6001	0.6213	0.6401
keys	0.1304	0.1330	0.1386	0.1444	0.1501	0.1558	0.1614	0.1669	0.1725	0.1779
m	11	12	13	14	15	16	17	18	19	20
lena	0.6569	0.6720	0.6857	0.6982	0.7096	0.7202	0.7300	0.7390	0.7475	0.7554
keys	0.1833	0.1887	0.1941	0.1995	0.2048	0.2100	0.2152	0.2204	0.2256	0.2307



(a)

(b)

Fig. 6: Correlations of adjacent pixels; (a) Plain image, (b) Cipher image

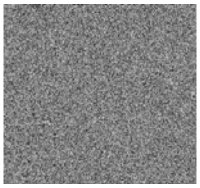


Fig. 7: The sensitivity of keys

Sensitivity of keys: Assume that an image is encrypted using the map with the *key* “0123456789”, just as seen in Fig. 5. Now, the key of decryption is changed. The *keys* “0123456789” is changed to *keys*$_1$ “0123456780”, which is used to decrypt the cipher image by the original *keys*. The decrypted image by different keys is shown in Fig. 7. It can be seen that the image can’t be decrypted by the error keys, which are different from the correct key. Therefore, the security of the image permutation is effective.

***r-m* self-relevance:** Where *r* = 1, the *r-m* self-relevance can seen in Table 3, here *keys* is “0123456789”,. It can be proved the self-relevance of cipher image significantly reduced compared with the plain image. In Table 4, the value of self-relevance is even smaller than the value when *m* = 1. Those mean the effect of permutation is very good.

CONCLUSION

Image security is important for food intellectual property rights. The study proposed a new fast permutation for large-size rectangle food images. The keys of encryption are decimal numbers. It satisfied the most security requirements in food intellectual property rights.

The advantages of the approach can be described as follows:

- The approach is very simple, enough safe and fairly fast
- The plain food image can not only be square image but also rectangle image
- The permutation have no message loss
- The key space can be enough big to satisfy food image security requirements.

ACKNOWLEDGMENT

Authors gratefully acknowledge the Projects Supported by Hunan Provincial Natural Science Foundation of China (12JJ9018) and aid program for Science and Technology Innovative Research Team in Higher Educational Institutions of Hunan Province of China.

REFERENCES

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

Chen, J.X., Z.L. Zhu, C. Fu, H. Yu and L.B. Zhang, 2015. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Commun. Nonlinear Sci., 20(3): 846-860.

Enayatifar, R., A.H. Abdullah and I.F. Isnin, 2014. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt. Laser. Eng., 56: 83-93.

Fridrich, J., 1998. Symmetric ciphers based on two-dimensional chaotic maps. Int. J. Bifurcat. Chaos, 8: 1259-1284.

Huang, F. and Y. Feng, 2007. A symmetric image encryption scheme based on a simple novel two-dimensional map. Int. J. Innov. Comput. I., 3: 591-1600.

Maniccam, S.S. and N.G. Bourbkis, 2004. Image and video encryption using SCAN patterns. Pattern Recogn., 37: 725-737.

Mao, Y., G. Chen and S. Lian, 2004. A novel fast image encryption scheme based on 3D chaotic baker maps. Int. J. Bifurcat. Chaos, 14: 3613-3624.

Wang, X.Y. and Q. Wang, 2014. A novel image encryption algorithm based on dynamic S-boxes constructed by chaos. Nonlinear Dynam., 75(3): 567-576.

Wang, Y., K. Wong, X. Liao and G. Chen, 2011. A new chaos-based fast image encryption algorithm. Appl. Soft Comput., 11: 514-522.

Yoon, J.W. and H. Kim, 2010. An image encryption scheme with a pseudorandom permutation based on chaotic maps. Commun. Nonlinear Sci., 15: 3998-4006.

Zheng, J.M. and W.Z. Gao, 2011. Color image encryption algorithm based on chaotic map. Comp. Eng. Des., 32: 2934-2937.