Send Orders for Reprints to reprints@benthamscience.ae

The Open Automation and Control Systems Journal, 2015, *7*, 2023-2028

Research on Image Encryption and Mapping Algorithm Based on Fuzzy Entropy Thresholding and R Weighted Mean Algorithm

Lu Yiping, Qin Jing and Ye Yunlong

HeBei North University, Hebei, Zhangjiakou 075000, China

Abstract: In this paper, we prompt a new algothim based on fuzzy entropy thresholding and R weighted mean algorithm for the image encryption and mapping. The image was divided into the upper and lower blocks, making the encryption factor associate with the plain text and the cipher text. The encryption formula was improved which complicated the relationship between the cipher text and the plain text and keys. The experiment is taken to do the comparison for the effect of encryption and mapping before and after using the new algoritm. The experiment results show that improved algorithm has better performance in encryption and mapping for the image and can be widely used in the image encryption engineering.

Keywords: Image encryption, mapping, algorithm, fuzzy entropy thresholding, R weighted mean algorithm.

1. INTRODUCTION

With the rapid development of the Internet, it is becoming very popular to transfer image information via network. Because The transfer mode is not subject to geographical restrictions, and also is very fast and efficient and can save a lot of cost. However, since network owns the defects in the protocol and system etc. aspects, in the enjoyment of convenience that network brings, people have to consider how to improve the security of the image information [1].

Image encryption technology is to prevent the important image information from illegal theft or tampering [2, 3]. At present, the image encryption technology has been widely applied to many areas, such as government, military, medical, commercial and personal security system, and plays an important role.

Image security has become an important topic in the field of information security [4]. At present, various image encryption algorithms have been proposed, including the well-known image encryption algorithm based on fractional Fourier transform which is a hot research topic and attracts the attention of many researchers. In addition, in order to meet the real-time requirement of image data transmission, the encryption algorithm should not add to the transmission load too much. In recent years, the algorithms of multiple images encryption and color image encryption become a focus.

However, the rapid popularization of the computer and Internet, the exchange of information plays an important role in the modern society and images are widely used as a good information carrier in many fields [5]. Thus, image security has become an important topic in the field of information security. At present, various image encryption algorithms have been proposed, including the well-known image encryption algorithm based on fractional Fourier transform which is a hot research topic and attracts the attention of many researchers. In addition, in order to meet the real-time requirement of image data transmission, the encryption algorithm should not add to the transmission load too much. In recent years, the algorithms of multiple images encryption and color image encryption become a focus [6].

Optical information processing, which has been developing over forty years, is a very important part of information science. Recently, the information security techniques based on optical theory and methods have received increasing attention because of the potential for new technological applications in telecommunications. The optical technique has many advantages over the traditional information security technology, such as mufti-dimension, large-capacity and the natural ability of parallel data processing, and so on. As the image, which is simple, lively characteristic, is one of the main carriers of information, how to prevent unauthorized user from modifying, copying, transmitting and printing images has become a very important issue. Thus, the exploration and development of optical image encryption technique has great academic and application values [7]. Optical information security, which is a branch of the information processing, becomes a new research topic of the information science. The main methods are implemented by the optical transforms, such as the fractional Fourier transforms, with the random key generation algorithms. The fractional Fourier transforms are new analysis methods due to its extensive applications in the areas of optics information security, signal processing, pattern recognition and image processing and are applied to the optical image encryption successfully. However it is showed in this dissertation that the image encryption methods based on the fractional Fourier transform have the common drawbacks in security. Therefore searching the more secure and effective image encryption methods are of great theoretical and practical application values.

1874-4443/15

2. THE BACKGROUND AND FRAME WORK OF FUZZY ENTROPY THRESHOLDING

With the development of information technology, such as information storage, information transmission and Internet, the security of information transmission has been heightened. As a main method of protecting image information, image encryption has made great strides in recent years. Chaos, the theory of relativity and quantum mechanics, are listed as the 20th century's greatest discoveries. It possesses the sensitive dependence on initial conditions and control parameters, pseudo random orbits and topological transitivity. These inherent properties can be well applied in the image encryption. So a large number of image encryption algorithms based on chaotic theory have emerged since the end of last century, and many exciting results are obtained. However, with the deep research and progress of information technology, the algorithms of image encryption which was once considered a strong safety and high efficiency, but now are proved to be unsafe, low efficiency and even unusable algorithms. How to base on the latest research results and to design a chaotic encryption algorithm for digital image with high efficiency and security by thorough analysis is becoming to the problem that will be solved urgently.

This section firstly introduces the basic knowledge of digital image encryption based on chaotic theory, combines with the results of digital image encryption based on chaotic theory, and analyzes the current image encryption algorithms. The disadvantages of the algorithms are pointed out and improved. The original fuzzy entropy thresholding algorithm for digital image is proposed in this section, where the step for fuzzy entropy thresholding algorithm should be stated as follows [8]:

STEP 1: (1) In order to select the appropriate structure of chaotic image encryption for the different needs, the existing structures of chaotic image encryption are compared. Firstly, this dissertation analyzes the key steps used in encryption. The normal indicators are introduced in detail. Then, compared with the existing structures of chaotic image encryption, we find the best structure for chaotic image encryption by experimental results. Finally, the ant jamming capability of encryption structures is analyzed.

STEP 2: An algorithm of chaotic image encryption based on enhancing key is proposed. Compared with traditional algorithm, this algorithm possesses running effect and time without redundant operations. Compared with new algorithms, the proposed algorithm possesses better encrypting effect for different sizes and various test images. Finally, the ant jamming capability of proposed algorithm is analyzed.

STEP 3: (3) An image encryption algorithm based on chaotic theory is cryptanalyzed and improved. According to the theory of cryptanalysis, the image encryption which is based on Logistic chaotic mapping and proposed by Ye is analyzed. This dissertation proves that the algorithm has a defect by solving differential equations, and designs an experiment to break it successfully. According to the defect, two improved algorithms are proposed.

STEP 4: In order to prevent maliciously tampering for the encrypted image, an image encryption and authentication algorithm based on reversible integer transform is proposed. Firstly, the plain-image is divided into low-frequency part and high-frequency part. Then, the former is used to encrypt image by chaotic theory, and the latter is used to embed watermarking by histogram modification. The encrypted image with watermarking is obtained by inverse integer transform. The embedding rate and peak signal-to-noise ratio are better than previous works. Aiming at this problem that above algorithm cannot effectively encrypt the outline information of plain-image, an improved algorithm is proposed to solve this problem. Finally, the ant jamming and anti-attack capability of proposed watermarking algorithm are analyzed.

STEP 5: A novel constraint condition for DNA coding is proposed, and used to design a chaotic image encryption based DNA coding. Compared with the existing constraint based on Hamming distance, the best combinational constraint for DNA coding is obtained by experimental results.

The detected impulses will be removed by R algorithm. Let $f'_{i,j}$ be the value of the sample at statistics location (*i*,*j*). For the corrupted statistics (*i*, *j*), the sample size $(2L_f+1)\times(2L_f+1)$ is used. Starting with L_f =1, this sample size iteratively extends outward by one statistics in its four sides until the number of free statistics (denoted by $P_{i,j}$) within this sample size is not less than 1. Let $W'_{i,j}$ denote the values of free statistics in the concerned area, i.e.,

$$W'_{i,j}=\{f'_{i+s,j+t}\mid b_{i+s,j+t}=0,b_{i,j}=1,\ (s,t)\neq(0,0),-L_f\le s,t\le L_f\} \tag{1}$$

The weighted mean value $g_{i,j}$ of the statistics values in $W'_{i,j}$ is defined as:

$$g_{i,j}=\frac{\sum_{f_{i+s,j+t}\in W'_{i,j}} w_{i+s,j+t}f'_{i+s,j+t}}{\sum_{f_{i+s,j+t}\in W'_{i,j}} w_{i+s,j+t}} \tag{2}$$

where $w_{i+s,j+t}$ means the weight of $f'_{i+s,j+t}$. Let $m'_{i,j}$ be the median value of $W'_{i,j}$. Because the median value has the least probability to be the value of the corrupted statistics [1], $m'_{i,j}$ is utilized to determine $w_{i+s,j+t}$. It is easy to understand that the smaller the absolute difference between $f'_{i+s,j+t}$ and $m'_{i,j}$, the larger the weight $w_{i+s,j+t}$ should be to strengthen the influence of $f'_{i+s,j+t}$ on $g_{i,j}$. Based on extensive simulations which indicate that $w_{i+s,j+t}$ is dependent on both above absolute difference and noise ratio, $w_{i+s,j+t}$ is chosen as:

$$w_{i+s,j+t}=R+(1-R)\sqrt{\frac{\dfrac{|f'_{i+s,j+t}-m'_{i,j}|}{f'_{\max}-f'_{\min}}}{1-\dfrac{|f'_{i+s,j+t}-m'_{i,j}|}{f'_{\max}-f'_{\min}}}} \tag{3}$$

Where $f'_{\max}$ and $f'_{\min}$ denote the maximum statistics value and the minimum one in the concerned area, respectively.

The output is obtained by:

$$h_{i,j} = b_{i,j} \cdot g_{i,j} + (1 - b_{i,j}) f'_{i,j} + \Delta\omega_{i,j} \tag{4}$$

Then we have:

$$q_i = \left[x, y, z, \psi, \theta, \phi\right]_i^T \quad , \quad q = \left[q_1^T, q_2^T, ..., q_n^T\right]^T \tag{5}$$

The equation is established. The R weighted mean algorithm takes the Cartesian coordinates and Euler angle that respectively shows the position and direction of sample orient as the generalized coordinate, and establishes statistics equation by R weighted mean algorithm:

$$\frac{d}{dt}\left(\frac{\partial T}{\partial \dot{q}}\right)^T - \left(\frac{\partial T}{\partial q}\right)^T + \phi_q^T \rho + \theta_{\dot{q}}^T \mu = Q \tag{6}$$

Integrity Constraint Equation:

$$\phi(q, t) = 0 \tag{7}$$

Non-Integrity Constraint Equation:

$$\theta\left(\dot{q}, q, t\right) = 0 \tag{8}$$

3. THE FUZZY ENTROPY THRESHOLDING ALGORITHM

Let $x_{i,j}$ be the gray-level value of the image X of size $M \times N$ at pixel position (i,j). According to the fuzzy subset theory, the image X can be represented using the following fuzzy matrix:

$$X = [\mu(x_{i,j})]_{M \times N} \quad 1 \le i \le M; 1 \le j \le N \tag{9}$$

where $\mu(x_{i,j})$ $(0 \le \mu(x_{i,j}) \le 1)$ is the membership degree of $f_{i,j}$. The membership degree $m(x_{i,j})$ and its Shannon function $S(m(x_{i,j}))$ are defined as [5-8]:

$$\mu(x_{i,j}) = \begin{cases} 0 & x_{i,j} < T_0 \\ \dfrac{(x_{i,j} - T_0)^2}{(T - T_0)(T_1 - T_0)} & T_0 \le x_{i,j} \le T_1 \\ 1 - \dfrac{(x_{i,j} - T_1)^2}{(T_1 - T_0)(T_1 - T_0)} & T \le x_{i,j} \le T_1 \\ 1 & x_{i,j} > T_1 \end{cases} \tag{10}$$

$$\begin{aligned} S(\mu(x_{i,j})) &= -\mu(x_{i,j}) \ln(\mu(x_{i,j})) \\ &-(1 - \mu(x_{i,j})) \ln(1 - \mu(x_{i,j})) \end{aligned} \tag{11}$$

The interval between T_0 and T_1 constitutes the fuzzy region. Let $\mathrm{D}T = T_1 - T_0$ and $T = (T_0 + T_1)/2$. The fuzzy entropy $E(T, \mathrm{D}T)$ of image X is defined as:

$$E(T, \Delta T) = \frac{1}{MN \ln 2} \sum_{i=1}^{M} \sum_{j=1}^{N} Sn(\mu_{ij}(x_{ij})) \tag{12}$$

Let T and $\mathrm{D}T$ be encoded as 8 bit variables in the binary mode. The single chromosome is composed of the two variables. To get the threshold using the maximum fuzzy entropy principle, the fuzzy entropy (objective function) will be mapped into the fitness function as follows:

$$f(T, \mathrm{D}T) = E(T, \mathrm{D}T) \tag{13}$$

The standard GA generates initial population randomly. This method tends to produce a narrow search space, which is disadvantageous to the acquisition of the global optimal solution. To improve the convergence characteristics of GA, the initial population is generated using uniform partition based generation method. This method evenly divides the range of optimized parameters into regions with their number equal to population scale Gs. In every small region, an individual will be generated randomly. This method can quicken the convergence speed and increase the possibility of converging to global optimal solution.

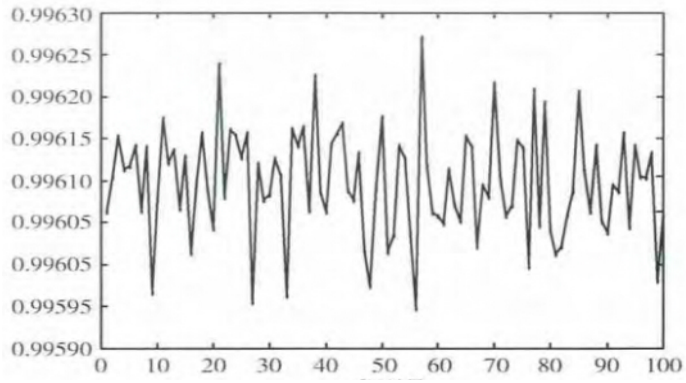
Image encryption technology is to prevent the important image information from illegal theft or tampering. Crossover probability P_c and mutation probability P_m are fixed in the standard GA. But they should vary with the distribution of individuals in the population. In the early evolutionary period, the individuals are distributed dispersedly and so P_c should take higher value to realize the combination of effective modes while P_m should take a small value to prevent the damage of effective gene. In the later evolutionary period, the individuals tend to have close fitness and so P_c should be reduced while P_m should be increased to avoid the inbreeding between two individuals and preserve the diversity of the population. Based on the above analysis, the crossover probability P_c^t at t-th generation will be defined as:

$$P_c^t = \begin{cases} P_{\max} - \dfrac{(P_{\max} - P_{\text{temp}})(f_b^t - f_{\text{avg}}^t)}{f_{\max}^t - f_{\text{avg}}^t} & f_b^t \ge f_{\text{avg}}^t \\ P_{\max} & f_b^t < f_{\text{avg}}^t \end{cases} \tag{14}$$

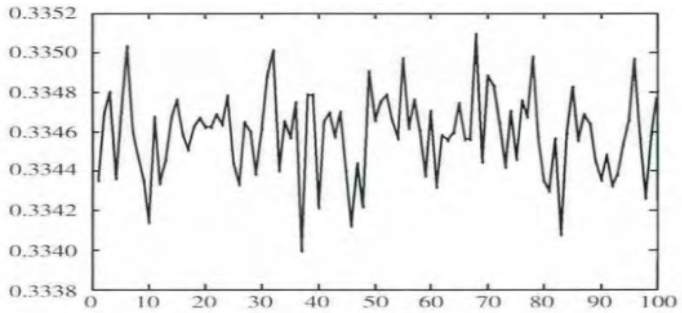
Where:

$$P_{\text{temp}} = \begin{cases} P_{\min} & P_{\max} e^{-\frac{t}{T_l}} \le P_{\min} \\ P_{\max} e^{-\frac{t}{T_l}} & P_{\max} e^{-\frac{t}{T_l}} > P_{\min} \end{cases} \tag{15}$$

where $P_{\max}$ and $P_{\min}$ are the maximum crossover probability and the minimum one, T_l be the maximum iteration times, f_b^t be the bigger fitness of two individuals chosen for crossover operation at t-th generation, $f_{\max}^t$ and f_{avg}^t denote the



(**a**) Pixel rate change. (X – Order number. Y - Pixel rate change)



(**b**) The average intensity rate of the pixel. (X – Order number. Y - The average intensity rate of the pixel)

Fig. (1). Differential Performance Analysis.

maximum fitness and average fitness of the population at t-th generation. Similarly, the mutation probability P_m^t at t-th generation will be defined as:

$$P_m^t = \begin{cases} P'_{\max} - \dfrac{(P'_{\max} - P'_{\text{temp}})(f_k^t - f_{\text{avg}}^t)}{f_{\max}^t - f_{\text{avg}}^t} & f_k^t \geq f_{\text{avg}}^t \\ P'_{\max} & f_k^t < f_{\text{avg}}^t \end{cases} \quad (16)$$

Where:

$$P'_{\text{temp}} = \begin{cases} P'_{\min} & P'_{\max}(1 - e^{-\frac{t}{T_l}}) \leq P'_{\min} \\ P'_{\max}(1 - e^{-\frac{t}{T_l}}) & P'_{\max}(1 - e^{-\frac{t}{T_l}}) > P'_{\min} \end{cases} \quad (17)$$

where $P'_{\max}$ and $P'_{\min}$ are the maximum mutation probability and the minimum one, f_k^t be fitness of the individual chosen for mutation operation at t-th generation.

There are such regenerating methods as E method, G method, B method and N method. E method preserves only one parental individual. G method regenerates partial individuals in a certain proportion. B method regenerates the new individuals by choosing the excellent ones simultaneously among parents and children. N method completely replaces the previous generation. Because these methods can not achieve both excellent global searching capability and excellent convergence speed, the updating strategy based on preference between two generations is proposed. In the new updating strategy, the fitness of all the individuals in the parent generation and child generation is first separately sorted in the descending order. Then the fitness of the individual in the sorted parent generation is compared with that of the corresponding individual in the child generation. The individual with greater fitness will be preserved in the new generation. The new updating strategy preserves the excellent individuals between the two generations, which is conducive to the improvement of both global searching capability and convergence speed.

Without increasing computation cost and the complexity of the optical hardware, the image encryption based on the weighted unitary transforms not only have all the advantages as the weighted fractional Fourier transform have, but also overcome all the drawbacks resulting from the image encryption methods based on the fractional Fourier transforms. The image encryption method is based on the weighted unitary transforms enhance security and validity of the optical image encryption methods. The optical image encryption methods based on weighted unitary transform-I is proposed,

which overcomes the second and third kinds of drawbacks. The optical image encryption methods based on the weighted unitary transform-II is proposed, which overcomes the upper three kinds drawbacks. The optical image encryption methods based on the weighted unitary transform-III is proposed, which overcomes all four kinds of drawbacks. The double blind image encryption method based on the weighted unitary transform-III is proposed on the basis of the upper optical image encryption methods.

4. THE EXPERIMENT AND DATA ANALYSIS

Images are often corrupted by impulse noise in the process of transmission over noisy communication channels or recording by noisy sensors. The median filter, a kind of effective nonlinear filter, has been widely used for removing impulse noise because of its superior performance in noise suppression and edge preservation in comparison with the linear filters. However, the AGA-FET is implemented uniformly across the entire image without taking account of whether a pixel is corrupted or not. Inevitably, the AGA-FET will modify both noise pixels and undisturbed good pixels, thus causing the blurring or furthermore loss of fine details in the image.

A good encryption algorithm should be very sensitive to changes in key. 2 with a slight difference of the encryption key, should produce a completely different cipher text image. Similarly, 2 with a slight difference decryption key, to decrypt the cipher text is also the same result should be completely different.

Decryption experiments, respectively, the key k2, k5, k6 fine-tuning (plus 10^{-15}). Decryption results shown in Fig. (**1**), the visible key minor changes will lead to erroneous decryption result. Table **1** lists the N_{PCR} and U_{ACI} trimming k2, k5, k6 after decryption result between. The results show that the error between the decryption results is completely different, the algorithm has a strong sensitivity of the decryption key, and other keys to fine-tune a similar result can be obtained.

In encryption experiments, tune key k3, k7 (plus 10-15). Table **1** and **2** lists the initial key cipher text, fine-tuning and fine-tuning after k3 and k7 N_{PCR} and U_{ACI} between cipher texts. The results show that small changes in the cipher text will image different encryption key. Algorithm of the encryption key is also very sensitive to small changes in the other keys are also obtained similar results.

Table 1. Sensitivity of Decryption Key.

Cipher Text Image	Fine Tuning Decryption Key		
	k2 and k5	k2 and k6	k3 and k6
N_{PCR}	0.996049	0.996058	0.996009
U_{ACI}	0.334764	0.334787	0.334650

Table 2. Sensitivity of Encryption Key.

Cipher Text Image	Fine Tuning Decryption Key		
	Initial Key & Fine Tuning k3	Initial Key & Fine Tuning k7	Initial Key & Fine Tuning k3 and k7
N_{PCR}	0.996049	0.996058	0.996009
U_{ACI}	0.334764	0.334787	0.334650

CONCLUSION

The encryption algorithms for multiple images and color image are proposed based on the fuzzy entropy rhresholding and R weighted mean algorithm. The technology of rate-distortion control is utilized during the spectrum cutting to balance the qualities of the multiple decrypted images. The zigzag scanning is used in the process of spectrum cutting and this scanning way makes the low frequency cutting precisely in every coefficient. The numerical simulations demonstrate the validity and efficiency of these algorithms. The robustness of the schemes against occlusion attack and noise attack is also examined. It possesses the sensitive dependence on initial conditions and control parameters, pseudo random orbits and topological transitivity. These inherent properties can be well applied in the image encryption. At last, the experiment results show that improved algorithm has better performance in encryption and mapping for the image and can be widely used in the image encryption engineering.

FUND SUPPORT

1. Smart car air conditioning energy conservation and emissions reduction optimization research (QN2014203).

2. Based on the public platform to expand research and application of the digital library intelligent service (1411072B).

CONFLICT OF INTEREST:

The authors confirm that this article content has no conflicts of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] X.N. Fu, S.M. Yin and S.Q. Liu, "A improved adaptive fuzzy entropy entropy thresholding method on image segmentation", *Acta Photonica Sinica,* vol. 32, pp. 605-607, 2003.

[2] S. Gattoufi, M. Oral, and A. Reisman, "Data envelopment analysis literature: a bibliography update (1951-2001)," *Socio-Economic Planning Sciences*, no. 38, pp. 159-229, 2004.

[3] M. Keen, and J. Mintz, "The Optimal Threshold for a Value-added Tax," *Journal of Public Economics,* vol. 88, pp. 559-576, 2004.

[4] X. Wang, and J. Sun, "analysis of issues related to development of beach volleyball in colleges and universities in China," *Journal of Tianshui*, vol. 29, pp. 100-102, 2009.

[5] Q. Yan, and P. Gong, "Investigation on the Nutrition Knowledge Attitudes and Dietary Behaviors of University Students," *Modern Preventive Medicine*, vol. 3, pp. 520-524, 2008.

[6] J. Aim, "What is an Optimal System," *National Tax Journal,* vol. 49, pp. 156-161, 1996.

[7] A. Akhavan, A. Samsudin, and A. Akhshani, "A symmetric image encryption scheme based on combination of nonlinear chaotic maps", *Journal of the Franklin Institute-engineering and Applied Mathmatics,* vol. 8, pp. 1797-1813, 2011.

[8] B. Nooshin, F. Yolset, and A. Karim, "A novel image encryption/decryption scheme based on chaotic neural networks". *Engineering Applications of Artificial Intelligence,* vol. 4, pp. 753-765, 2012.

Received: June 16, 2015 Revised: August 10, 2015 Accepted: September 19, 2015