基于系数融合与锯齿填充曲线的双图像加密算法

闫 娜
(陕西财经职业技术学院 咸阳 712000)

摘 要:为了实现对两幅图像同步加急,有效降低传输负载,提出了系数融合模型与锯齿填充的双图像加密算法。首先,引入离散余弦变换 DCT 与 Zigzag 扫描机制,获取输入明文的系数矩阵,建立明文系数融合模型,将两个明文矩阵转换成融合矩阵,借助逆向离散余弦变换,获取复合图像;随后,设计锯齿填充曲线,对复合图像的像素位置进行扰乱,形成置乱图像;最后,改进引力模型,对置乱图像进行扩散,改变其灰度值。实验结果显示,本算法能够对两幅图像进行同步加密,且具有较高的安全性与密钥敏感性,解密图像的信息损失很小。

关键词:双图像加密;系数融合模型;离散余弦变换;锯齿填空曲线;引力模型;同步加密
中图分类号: TP391.4 TN302 **文献标识码**:A **国家标准学科分类代码**: 520.1060

Double image encryption algorithm based on coefficient fusion and saw tooth filling curve

Yan Na
(Shaanxi Vocational College of Finance and Economics, Xianyang 712000, China)

Abstract: In order to realize the synchronization of two images urgently, effectively reduce the transmission load, the double image encryption algorithm based on coefficient fusion model and saw tooth filling curve was proposed in this paper. Firstly, the coefficients matrix of the input plain was obtained by discrete cosine transform DCT and Zigzag scanning mechanism, and the two plain matrix is transformed into a fusion matrix by constructing the coefficient fusion model, then the composite image was obtained by inverse discrete cosine transform. Subsequently, the design of the zigzag filling curve, the pixel location of the composite image to disturb the formation of scrambling image. Finally, the improved gravity model, the scrambled image diffusion, changes the gray value. The experimental results show that the algorithm can be used to encrypt the two images simultaneously, and it has high security and no loss of information.

Keywords: double image encryption; coefficient fusion model; discrete cosine transform; Zigzag fill curve; gravity model; synchronous encryption

1 引 言

随着全球经济化与政治的密切交流,因特网也成为当前人们实现跨地点跨地区沟通交流的主要手段,尤其是图像,其包含了诸多信息,已成为当前交流最为直观的载体,给人们的生活带来极大便利[1]。但是,由于图像所含有的内容特别多,在开放网络的传输环境中,其信息容易被窃取,导致相关信息外泄,给人们带来了巨大的经济损失[2]。目前,信息安全问题日益突出,引起了全世界人们的重视,如何确保数据信息不被窃取已成为当前的研究热点[3]。而加密技术作为保护图像信息安全传输的强有力手段,得到了广大学者的研究,但是传统的经典加密算法,如数据加密标准 DES、IDEA 算法以及 RSA 算法等,没有考虑到图像具有大数据容量、较高的冗余度等特点,因此将其应用于图像加密会存在较大的不足[4]。对此,为了满足图像信息安全传输的需求,学者们设计了相应的图像加密算法,如浩明等人[5]针为了有效改进图像加密效果及安全性,提出了多个混沌系统及位运算的图像加密算法,利用 Logistic 混沌映射生成的序列对明文完成置乱,再利用二维 Arnod 变换改变图像的像素值,实现了置乱-扩散,实验结果验证了其算法的安全性。宋鑫超等人[6]为了克服独立的置乱与扩散操作的加密结构带来的不足,提出了内联时延混沌映射耦合 Lorenz 系统的图像加密算法,利用 Logistic 映射来生成 Arnold 映射的初值,同时利用明文像素

收稿日期:2016-12

点构造 Arnold 映射迭代次数计算模型，从而建立其映射控制参数的计算函数，获取随机序列，以完成图像置乱，最后利用超混沌 Lorenz 系统对置乱图像完成扩散，实验结果验证了其算法的有效性。Zhang 等人[7]针对未知授权的网络攻击，设计了基于整体扰乱与双向扩散的数字图像加密技术来确保图像的安全传输，通过迭代高维混沌来获得随机序列，从而改变明文像素位置，同时，为了提高加密效率，提出了像素双向扩散机制，实现置乱图像的正反方向扩散，测试数据表明其算法具有较高的加密效率与安全性。

虽然当前的图像加密能够较好地避免图像在网络中受到外来攻击，具有较高的安全性，但是此类算法主要是针对单图像的置乱与扩散，不能实现对 2 幅及以上的图像的同步加密，当需要加密多幅图像时，此类技术会产生较高的时耗与传输负载。

为此，本文提出了系数融合模型与锯齿填充的双图像加密算法。根据离散余弦变换 DCT 与 Zigzag 扫描机制，设计明文系数融合模型，将两个明文矩阵转换成融合矩阵，从而得到复合图像；并利用锯齿填充曲线对复合图像进行高度混淆，产生置乱图像，再利用改进的引力模型改变其灰度值。最后，验证了所提双图像同步加密技术的安全性。

2 双图像同步加密算法设计

本文提出的系数融合模型与锯齿填充的双图像加密流程如图 1 所示，其主要包含了：1）设计系数融合模型，联合逆向 DCT 变换，输出复合图像；2）设计锯齿填充曲线，对复合图像完成高效置乱；3）改进引力模型，对置乱图像完成库扩散。

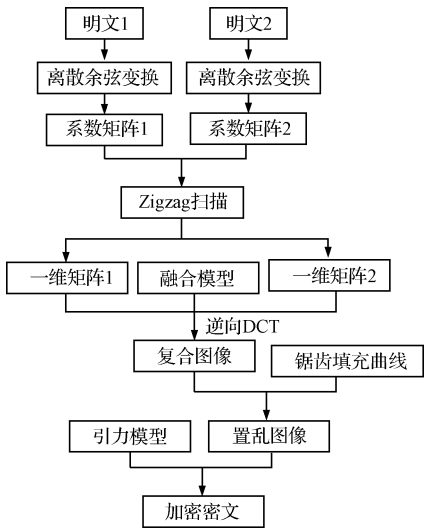


图 1 本文双图像加密过程

2.1 基于系数融合矩阵的双明文复合

要实现对 2 幅图像进行同步置乱与扩散，必须将其复合成单图像。因此，本文利用 DCT（discrete cosine transform）变换[8]与 ZigZag 机制，通过设计系数融合模型，将两个输入明文变成复合图像。复合图像的步骤如下：

1）由于图像是由很多信号组成，且其利用 DCT 变换[8]后，其信号能量主要聚集在直流分量与交流分量。因此，首先将两个输入图像进行分割，得到 $j\times j$ 分块，再利用 DCT 变换将其变为系数矩阵 $\boldsymbol{A}_1$，$\boldsymbol{A}_2$：

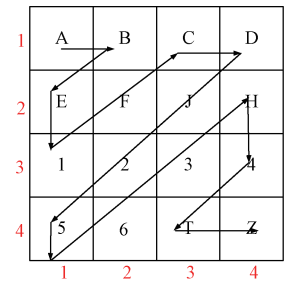
$$\boldsymbol{F}(u,v)=K(u)K(v)\sqrt{\frac{2}{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cdot\cos\left[\frac{\pi}{M}u\left(x+\frac{1}{2}\right)\right]\cos\left[\frac{\pi}{N}v\left(y+\frac{1}{2}\right)\right] \tag{1}$$

式中：$\boldsymbol{F}(u,v)$ 是系数矩阵；x,y 为输入明文 $f(x,y)$ 的像素点的坐标；$M\times N$ 是初始图像的尺寸；u,v 是 $F(u,v)$ 的数据坐标值；$\cos(A)$ 是余弦变换；$K(u)$，$K(v)$ 均为常数：

$$K(u)=\begin{cases}\sqrt{\frac{1}{2}}, & u=0\\ 1, & 1\leqslant u\leqslant M-1\end{cases}$$

$$K(v)=\begin{cases}\sqrt{\frac{1}{2}}, & v=0\\ 1, & 1\leqslant v\leqslant N-1\end{cases} \tag{2}$$

2）再利用 ZigZag 技术[9]，对 $\boldsymbol{A}_1$，$\boldsymbol{A}_2$ 完成扫描，根据图 2的扫描轨迹，将 $\boldsymbol{A}_1$，$\boldsymbol{A}_2$ 变成一维数组 $\boldsymbol{B}_1$，$\boldsymbol{B}_2$。



(a) 扫描示意

A	B	E	1	F	C	D	J	2	5	6	2	H	4	T	Z

(b) 含16个元素的一维矩阵

图 2 ZigZag 扫描示意

3）基于复数理论[10]，设计系数融合模型：

$$\boldsymbol{C}=\boldsymbol{B}_1+\boldsymbol{B}_2\mathrm{j} \tag{3}$$

式中：$\boldsymbol{C}$ 是系数融合矩阵；$\boldsymbol{f}_1$，$\boldsymbol{f}_2$ 分别是输入明文 1、明文 2 对应的 DCT 系数矩阵；$\mathrm{j}=\sqrt{-1}$ 为复数参数。

再引入 IDCT（inverse discrete cosine transform）函数[8]，将 $\boldsymbol{C}$ 矩阵转成复合图像：

$$f(x,y)=S(u)S(v)\sqrt{\frac{2}{LH}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}C(u,v)\cdot\cos\left[\frac{\pi}{L}u\left(x+\frac{1}{2}\right)\right]\cos\left[\frac{\pi}{H}v\left(y+\frac{1}{2}\right)\right] \tag{4}$$

以图 3(a)、(b)为样本，根据系数融合模型，得到复合图像如图 4 所示。

2.2 基于锯齿填充曲线的图像置乱

为了提高加密算法的安全性，本文设计了置乱-扩散

(a) 明文1　(b) 明文2

图 3　明文图像

图 4　复合图像

的加密结构，首先基于锯齿曲线模型[10]，设计空间填充置乱机制，提高其通用性。锯齿曲线模型[10]如图 5 所示，其表达式为：

$$y = a\left(1 - \frac{x}{T}\right) \quad 0 < x < T \tag{5}$$

式中：a 是曲线高度；T 为曲线周期。

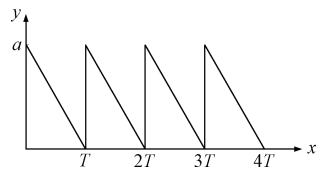


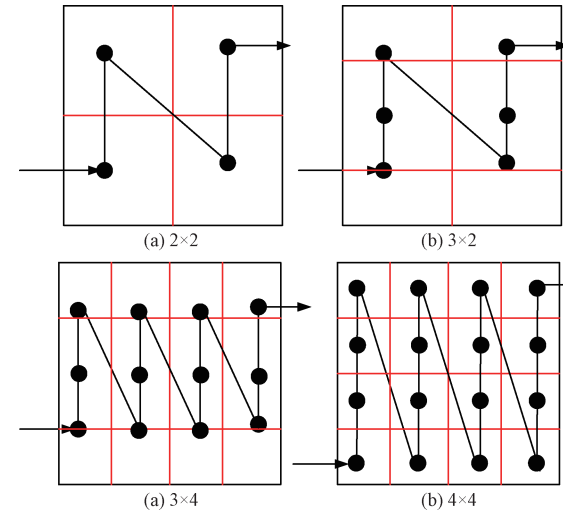
图 5　锯齿曲线示意

由式(5)设计锯齿填充置乱机制，见图 6。由图 6 可知，所提锯齿填充置乱机制包含了许多的直角三角形，通过接触其 3 个点进行一次遍历，彻底混淆明文像素位置。为了保证该置乱技术能够加密非矩形的明文，本文赋予 a 约束条件：a 值一定可被其分辨率整除。因此，根据该约束条件，对初始的锯齿空间填充曲线进行拓展，如图 6 所示($a = 4$)。

在本文的加密技术中，取 $a = 4$ 的锯齿模型 4×4 对图 5进行置乱，结果如图 7 所示。根据该置乱质量可知，两幅输入明文的信息被高度混淆，肉眼无法看到其任何内容。

2.3　基于锯齿填充曲线的图像置乱

若仅仅改变其像素位置，没有改变其像素值，则密文



(a) 2×2　(b) 3×2　(a) 3×4　(b) 4×4

图 6　不同分辨率的锯齿模式

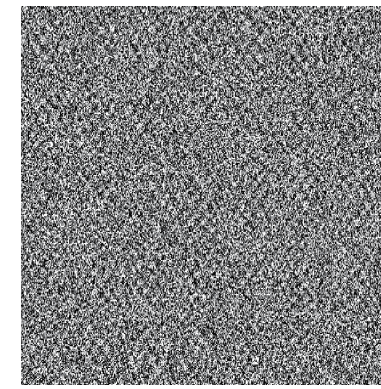


图 7　锯齿填充置乱结果

的安全性还是比较低，因此，本文通过改进引力模型[11]，进一步改变像素值。

假设锯齿填充置乱图像是 $I' = \{0 \leqslant f(i,j) \leqslant 256; i = 1,2,\cdots,M, j = 1,\cdots,N\}$，并将置乱图像内所有的像素均作为粒子。根据引力概念[11]，P 与 I' 中任意像素之间存在着引力，因此，本文利用引力作用来混淆其像素值。文献[12]在早期就利用引力模型对单幅图像进行加密：

$$B'_{ij} = \left[\frac{G \times m(x,y,z) \times m_{ij}(i,j)}{(x-i)^2 + (y-j)^2 + z^2}\right] \bmod 256 \oplus B_{ij} \tag{6}$$

$$m(x,y,z) = 1$$
$$m(i,j) = 21i^2 + j^3 + 5 \tag{7}$$

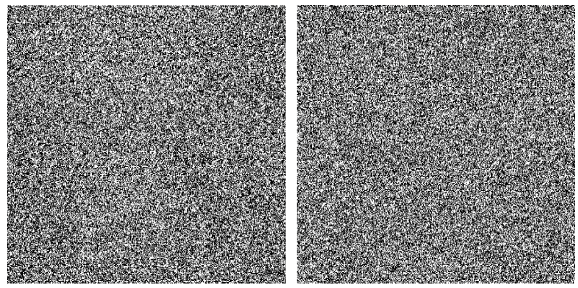
式中：G 为重力系数；$m(x,y,z)$ 是粒子质量；(x,y,z) 是粒子空间位置；$m(i,j)$ 为像素质量；B_{ij} 为置乱图像像素值；B'_{ij} 是扩散像素值。为确保式(14)的分母不为 0，设置 $z \neq 0$ 。

由式(6)可知，文献[12]采用的像素质量 $m(x,y,z)$ 是恒定，致使其动态性不强。为了增强算法的动态性与敏感性，本文利用置乱图像自身的像素空间位置，来设计粒子质量动态变化模型：

$$B'_{ij}=\left[\frac{G\times m_0(x,y,z)\times m_{ij}(i,j)}{(x-i)^2+(y-j)^2+z^2}\right]\bmod 256\oplus B_{ij} \tag{8}$$

$$m(x,y,z)=3\ 000\times \bmod[(12\times x^2+\sqrt{(x+y)^3}),256] \tag{9}$$

由式(9)可知,扩散模型与置乱图像紧密相连,显著提高了其抗明文攻击特性。为了测试改进前后的引力模型的扩散质量,将文献[12]视为对照组,以图7视为目标,相关参数 $x=150$, $y=300$, $z=150$, $G=3\times10^8$,利用式(9)与文献[13]对其完成扩散,结果如图8(a)、(b)所示。通过观察扩散效果可知,本文改进的引力模型具备更好的扩散质量,如图8(b)所示。



(a) 文献[13]算法 (b) 本文算法

图8 改进前后的引力模型扩散质量

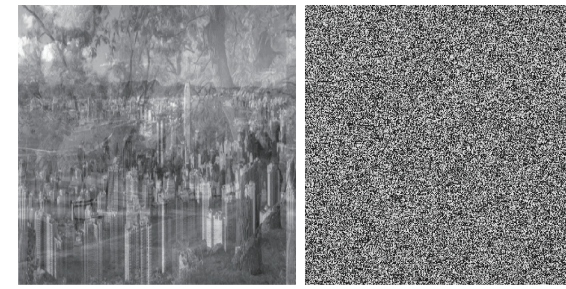
3 实验结果与分析

为了验证本文双图像加密技术的优异性,利用MATLAB平台进行仿真测试,关键参数设置为 $K(u)=1$, $K(v)=1/2$, $x=150$, $y=300$, $z=150$, $G=3\times10^8$, $a=4$。

3.1 双图像加密效果

以方形明文图9(a)、(b)为测试对象,结果如图9所示。根据加密质量可知,本文算法同步将两个输入明文进行加密扩散,两个明文信息融合在一起,如图9(c)所示,其内容信息被高度置乱与扩散,如图9(d)所示,这显示具有较高的安全性。

(a) 输入明文1 (b) 输入明文2



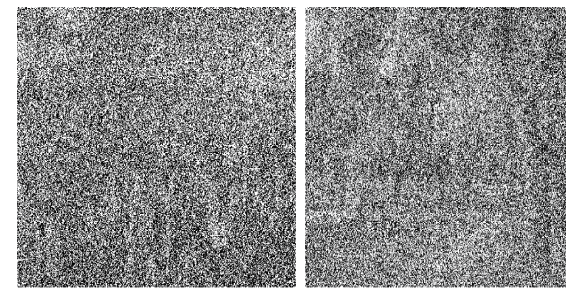
(c) 复合图像 (d) 输出密文

图9 双图像加密测试

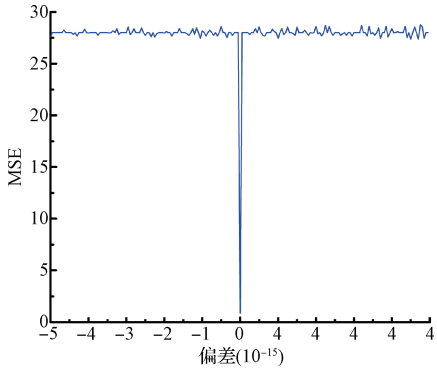
3.2 密钥敏感性测试

数字图像加密算法通常要有强烈的密钥敏感性,满足雪崩效应[13-15],也就是任意一个算法密钥出现了很小的变化时,仍然不能正确的初始图像。故本文测试了锯齿填充曲线的高度参数 $a=4$ 的敏感性,利用偏差量 $\Delta t=10^{-15}$ 对 a 进行变动,形成错误密钥 $a=4+10^{-15}$,其余参数不变。利用正确密钥 $a=4$ 与错误密钥 $a=4+10^{-15}$ 对图9完成复原,并测试了 a 的均方差(mean square error,MSE)曲线[13]。实验结果如图10所示。由密钥敏感性测试数据可知,即使密钥被攻击者进行穷举试探,哪怕 a 出现 10^{-15} 这样微小的偏差时,攻击者仍然是不能获得初始明文,见图10(c)、(d)所示;只有输入正确密钥 $a=4$ 时,方能完成解密操作,输出明文,如图10(a)、(b)所示。另外,根据图10(e)所示的MSE曲线可知,一旦密钥发生变动,其MSE发生了突变。该实验数据显示了所提双图像加密技术不但能够较好地隐秘明文信息,而且迎合了雪崩原则。主要是因为所提加密技术的扩散操作与置乱图像的像素位置密切相关,提高了算法的动态性,从而增强了扩散过程的随机性。

(a) 解密图像1 (b) 解密图像2



(c) 错误密钥的解密图像 (d) 错误密钥的解密图像2



(e) MSE 曲线测试

图 10　本文算法的密钥敏感性测试

4　结　论

为了对两幅图像完成同步加密，本文提出了系数融合模型与锯齿填充的双图像加密算法。通过利用离散余弦变换 DCT 与 Zigzag 扫描机制，获取输入明文的系数矩阵，建立明文系数融合模型，将两个明文矩阵转换成融合矩阵，借助逆向离散余弦变换，获取复合图像；随后，设计锯齿填充曲线，对复合图像的像素位置进行扰乱，形成置乱图像；并改进了引力模型，对置乱图像进行扩散，改变其灰度值。实验结果验证了所提算法的有效性与安全性。

参 考 文 献

[1] 涂正武，金聪. 适用于 Android 手机的像素异或图像分块加密算法[J]. 电子测量技术，2015，38(10)：46-52.

[2] 邱应强，余轮. 基于整数变换的图像可逆水印方法[J]. 电子测量与仪器学报，2015，29(1)：92-98.

[3] 王浩，李玉，秘明睿. 一种基于监督机制的工业物联网安全数据融合方法[J]. 仪器仪表学报，2014，34(4)：817-824.

[4] HUA T X，CHEN J M，PEI D J，et al. Quantum image encryption algorithm based on image correlation decomposition[J]. International Journal of Theoretical Physics，2015，54(2)：526-537.

[5] 浩明. 基于多个混沌系统和位运算的图像加密算法[J]. 实验室研究与探索，2015，34(3)：35-39.

[6] 宋鑫超，苏庆堂，赵永升. 内联时延混沌映射耦合 Lorenz 系统的图像加密算法[J]. 计算机工程与设计，2016，37(7)：1757-1761.

[7] ZHANG X P，ZHAO ZH M. Chaos-based image encryption with total shuffling and bidirectional diffusion[J]. Nonlinear Dynamics，2014，75(75)：319-330.

[8] LI P，CORNER B，PAQUETTE S. Shape analysis of female torsos based on discrete cosine transform[J]. International Journal of Clothing Science and Technology，2015，27(5)：677-691.

[9] CHANG W L. Efficient bit rate control method for distributed video coding system[J]. EURASIP Journal on Advances in Signal Processing，2012，6 (1)：1-12.

[10] 胡亦，王琳娜，朱恭生. 锯齿空间填充曲线耦合压缩感知的彩图灰度化实时加密算法[J]. 激光杂志，2015，6(2)：12-18.

[11] 郭静博，孙琼琼. 改进的引力模型耦合明文像素相关交叉机制的图像加密算法[J]. 包装工程，2016，7(13)：165-172

[12] 孙玉峰，陈建华. 基于万有引力模型的图像置乱新方法[J]. 福州大学学报：自然科学版，2006，34(1)：47-50.

[13] 孙光民，王晨阳. 一种基于改进 SIFT 的图像检索算法[J]. 国外电子测量技术，2016，12(8)：32-37.

[14] WANG X Y，WANG Q. A novel image encryption algorithm based on dynamic S-boxes constructed by chaos[J]. Nonlinear Dynamics，2014，75(3)：567-576.

[15] CARAGATA D，TUTANESCU I. On the security of a new image encryption scheme based on a chaotic function[J]. Signal，Image and Video Processing，2014，8(4)：641-646.

作 者 简 介

闫娜，1982 年出生，硕士，讲师，主要研究方向为图像处理、信息安全、计算机应用。
E-mail：yann1982xcj@163.com