

文章编号:1007-2780(2019)12-1210-08

基于二维串联调制耦合映射的 图像加密-秘密分享算法

王宛平¹, 李 冰^{2*}

(1. 河南质量工程职业学院现教中心, 河南 平顶山 467000; 2. 平顶山学院, 河南 平顶山 467000)

摘要:为了实现数字图像的分布式保密存储, 本文提出了一种图像加密-秘密分享算法。图像加密功能由 Logistic 映射和 ICMIC 映射串联构成的二维串联调制耦合映射(Two-dimensional cascade modulation coupling map, 2D-CMCM)产生的 4 个随机数序列控制图像的行/列置乱和扩散来实现。在已加密图像的秘密分享阶段, 使用基于拉格朗日多项式插值的 (3, 5) 门限秘密分享算法, 将已加密图像分为 5 份秘密子图。解密者只有获取不少于 3 份的秘密子图及二维串联调制耦合映射的密钥才能实现原始明文图像的无损重建。在安全性分析实验中, 本文所提出算法显示出了高度的抗攻击性; 在可逆性分析实验中, 秘密子图被证实可以实现原始明文图像的无损重构; 在执行效率测试实验中, 本文所提出算法的高执行效率也得到了验证。经过一系列实验, 本文所提出算法的高度实用性得到了证实。

关 键 词:混沌映射; 秘密分享; 图像加密

中图分类号: TP394.1; TH691.9 **文献标识码:** A **doi:** 10.3788/YJYXS20193412.1210

Image encryption-secret sharing algorithm based on two-dimensional cascade modulation coupling map

WANG Wan-ping¹, LI Bing^{2*}

(1. Henan Quality Polytechnic, Pingdingshan, 467000, China;

2. Pingdingshan University, Pingdingshan, 467000, China)

Abstract: In order to realize distributed secure storage of digital images, an image encryption-secret sharing algorithm is proposed in this paper. The image encryption function is completed by a sequence of four random numbers generated by a two-dimensional cascade modulation coupling map (2D-CMCM), which composed of a logistic map and an ICMIC map, including row/column scrambling and diffusion. In the secret sharing phase of the encrypted image, the encrypted image is divided into five secret subgraphs using a (3, 5) threshold secret sharing algorithm based on Lagrangian polynomial interpolation. The decryptor can obtain the lossless reconstruction of the original plaintext image only by acquiring no less than 3 secret subgraphs and secret keys. In the safety analysis experiment, the proposed algorithm shows a high degree of anti-aggression. In the reversibility analysis experiment, the secret subgraph is confirmed to achieve the lossless reconstruction of the original plaintext image. In the execution efficiency test, the high execution efficiency of the proposed algorithm is also verified.

收稿日期: 2019-08-16; 修订日期: 2019-09-19.

* 通信联系人, E-mail: Li-bing_0816@126.com

The a series of experiments con firmed the high practicability of the proposed algorithm.

Key words: chaotic map; secret sharing; image encryption

1 引言

随着多媒体技术及因特网的发展,数字图像在互联网中的收发越来越频繁,其存储总量也越来越多^[1-2]。近年来,一些针对数据云中心的网络攻击造成了一系列严重的损失,因此高价值数字图像在数据云中心的安全存储问题引发了广泛关注。针对这一问题,研究者们提出了一系列的解决方案。在图像抗破译方面,研究者们提出了图像加密^[3-4]、图像隐写^[5-6]等技术。在图像的抗破坏方面,研究者们提出了图像分布式存储^[7],图像秘密共享^[8-9]等技术。

由于混沌映射对初始迭代值及系统参数的高度敏感性与图像加密算法所要求的高度密钥敏感性不谋而合,因此各种基于混沌映射的图像加密算法在实际中应用最为广泛。在现实场景中,为了避免存储设备的偶发故障而导致的图像数据丢失,图像的分布式备份存储是一种常用的手段。但这种冗余手段也会增加图像被窃取、篡改的风险。有鉴于此,部分研究者提出了 (k, n) 门限图像秘密分享技术,将图片通过秘密分享技术拆分成 n 份,任意 k 份便可以完整恢复出原始图像,但少于 k 份则不能得到任何原始图像中的有用信息。这种特性完美地解决了图像分布式存储的安全问题,因此得到了广泛应用。

为同时提高图像的抗破译能力和抗破坏能力,本文设计了一种新型的图像加密-秘密分享算法,在算法中,基于2D-CMCM的图像加密算法和基于拉格朗日插值的 (k, n) 门限秘密分享算法被合并使用,同时,在图像加密环节,本文通过已加密像素点参与加密新像素点的方式使算法具有了明文相关特性,这种特性进一步提升了算法的安全性。在安全性分析中,本文所提出算法显示出了高度的抗攻击性;在可逆性分析中,通过秘密分享产生的秘密子图被证实可以实现原始图像的无损重构;在执行效率测试实验中,本文所提出的算法的高执行效率也得到了验证。经过一系列实验,本文所提出算法的高度实用性得到了证实。

2 理论基础

2.1 2D-CMCM

文献[10]通过合并混沌映射串联架构^[11]和混沌映射闭环耦合架构^[12],提出了一种新型的串联调制耦合架构(Cascade modulation couple module, CMC)。该架构如公式(1)所示。

$$\begin{cases} x_{i+1} = F(f(y_i) \cdot G(k x_i)) \\ y_{i+1} = F((f(k x_i) \cdot G(y_i)) \end{cases}, \quad (1)$$

其中: f 为一个线性映射函数, G, F 分别为一个一维混沌映射。序列 $X = \{x_i, i = 0, 1, 2, \dots\}$ 和序列 $Y = \{y_i, i = 0, 1, 2, \dots\}$ 为该混沌映射架构所生成的两个混沌序列。 $k \in (0, +\infty)$ 为调制耦合参数。在该架构中,映射 G 的输出通过线性函数 f 进行调制,调制之后的输出作为混沌映射 F 的输入,其在各个阶段的输出构成混沌随机数序列。

Logistic映射^[13]和无限折叠迭代混沌映射^[14](Iterative chaotic map with infinite collapse, ICMIC)因优良的混沌性能,在密码学的各项应用中被广泛采用。这两个一维混沌映射的数学定义如公式(2)和(3)所示。

$$x_{i+1} = \alpha x_i (1 - x_i), \quad (2)$$

$$x_{i+1} = \sin\left(\frac{c}{x_i}\right), \quad (3)$$

其中: α 和 c 均为系统参数。当满足 $\alpha \in (0, 4]$ 时Logistic映射处于混沌状态,当满足 $c \in (0, +\infty)$ 时ICMIC处于混沌状态。在文献[10]中,线性映射函数被定义为 $f(x) = x + 3$,混沌映射 G, F 分别被定义为Logistic映射和ICMIC。其中ICMIC的系统参数 $c = 21$ 。通过此种方式设定的混沌映射被称为二维串联调制耦合映射(Two-dimensional cascade modulation coupling map, 2D-CMCM),如公式(4)所示。

$$\begin{cases} x_{i+1} = \sin(21 / ((y_i + 3) \cdot \alpha k x_i (1 - k x_i))) \\ y_{i+1} = \sin(21 / ((k x_i + 3) \cdot \alpha y_i (1 - y_i))) \end{cases}. \quad (4)$$

2.2 (k, n) 门限秘密分享

设待处理的密钥数据为 D , Shamir^[9]提出的

(k, n) 门限密钥秘密分享方案的实现流程如下所述:

步骤 1: 在一个均匀分布的区间内随机取 $k-1$ 个值 $a_1, a_2, \dots, a_{k-1}$, 令 $a_0 = D$, 构造 $k-1$ 阶多项式 $q(x) = a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1}$;

步骤 2: 代入 $\{x_1=1, x_2=2, \dots, x_n=n, n > k\}$ 到多项式 $q(x)$, 得到 n 个函数值点对 $(x_1, y_1), (x_2, y_2), (x_3, y_3), \dots, (x_n, y_n)$;

步骤 3: 根据拉格朗日插值公式构造的唯一性^[15], 通过任意 k 个函数值点对构造 $k-1$ 阶拉格朗日插值多项式 $q'(x)$, $q'(x)$ 的常数项就是密钥数据 D 。

3 图像加密-秘密共享方案设计

本文所设计的基于 2D-CMCM 和 (k, n) 门限秘密分享技术的图像加密-秘密共享方案包含 3 个部分: 图像加密模块、图像秘密分享模块和图像重构模块。

3.1 图像加密模块算法设计

图像加密模块的输入为原始图像及如图 1 所示的密钥对, 输出为类似噪声图像的加密图像。本模块的运行流程如图 2 中加密模块所示。设原始图像为 $I_{M \times N}$, 生成加密图像的详细步骤如下所述:

步骤 1: 设置密钥对 $\{x_0, y_0, k, \alpha\}$, 通过 2D-CMCM 产生两个长度分别为 $2M$ 和 $2N$ 的混沌随机数序列 $X = \{x_0, x_1, \dots, x_{2M-1}\}$ 和 $Y = \{y_0, y_1, \dots, y_{2N-1}\}$;

步骤 2: 将随机数序列 X 分为两个子随机数序列: $X_1 = \{x_0, x_1, \dots, x_{M-1}\}$ 和 $X_2 = \{x_M, x_{M+1}, \dots, x_{2M-1}\}$; 将随机数序列 Y 分为两个子随机数序列: $Y_1 = \{y_0, y_1, \dots, y_{N-1}\}$ 和 $Y_2 = \{y_N, y_{N+1}, \dots, y_{2N-1}\}$;

步骤 3: 将 X_1 (Y_1) 按升序排列并将 $x_{i,i=0,2,\dots,M-1}$ ($y_{j,j=0,2,\dots,N-1}$) 的排列序号数作为待加密图像对应的第 i 行 (j 列) 像素下 (右) 移的行 (列) 数, 通过该过程完成图像的行 (列) 置乱, 生成图像 I_1 ;

步骤 4: 使用 X_2 (Y_2) 中元素, 按照公式 (5), 生成 X'_2 (Y'_2)

$$\begin{cases} X'_2(i) = X_2(i) \times 100, i=1, 2, \dots, M \\ Y'_2(j) = Y_2(j) \times 100, j=1, 2, \dots, N. \end{cases} \quad (5)$$

步骤 5: 将 I_1 的第一列与 X'_2 中各元素进行与或运算, 完成列扩散, 生成 $I'_1(i, 1) (i=1, 2, \dots, M)$ 。从 I_1 的第二列开始, 每一列元素与 X'_2 中各元素以及上一次列扩散生成的新列进行与或运算, 完成列扩散, 生成 $I'_1(i, j) (i=1, 2, \dots, M; j=2, 3, \dots, N)$ 。然后将 I'_1 的第一行与 Y'_2 中各元素进行与或运算, 完成行扩散, 生成 $I_2(1, j) (j=1, 2, \dots, N)$ 。从 I'_1 的第二行开始, 每一行元素与 Y'_2 中各元素以及上一次行扩散生成的新行进行与或运算, 完成行扩散, 生成 $I_2(i, j) (i=2, 3, \dots, M; j=1, 2, \dots, N)$ 。

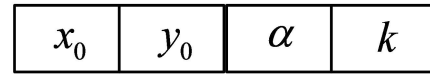


图 1 密钥对结构

Fig.1 Structure of secret keys

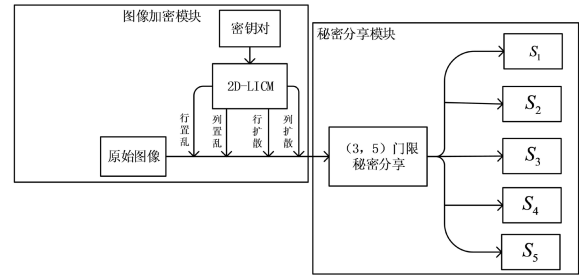


图 2 图像加密及秘密分享模块运行流程

Fig. 2 Running process of image encryption and secret sharing module

3.2 图像秘密分享模块算法设计

图像秘密分享模块的输入为加密图像 I_2 , 输出为 5 幅类似噪声图像的秘密子图: S_1, S_2, S_3, S_4, S_5 。首先构造函数 $q(x) = a_0 + a_1x + a_2x^2$, 将 a_0 的值依次设为 I_2 中各像素值, 剩余的两个系数 a_1 和 a_2 从区间 $[0, 255]$ 中任意取得。代入 $x_{i,i=1,2,\dots,5}$ 到 $q(x)$ 中, 生成 $q(x_{i,i=1,2,\dots,5})$ 。按照 a_0 在 I_2 中的行列位置, 将 $q(x_{i,i=1,2,\dots,5})$ 作为图像 $S_{i,i=1,2,\dots,5}$ 中对应位置的像素。

3.3 图像重构模块算法设计

在原始图像重构步骤中, 只需任意 3 幅秘密子图便可以完整复原原始图像, 但少于 3 幅秘密子图将不能得到任何信息。该模块的详细运行流程如下所述:

步骤 1: 获取任意 3 幅不同的秘密子图:

$S_{i1,i1=1,2,\dots,5}$, $S_{i2,i2=1,2,\dots,5}$ 和 $S_{i3,i3=1,2,\dots,5}$ 。然后遍历 3 幅子图中的各像素值,通过构造 3 阶拉格朗日插值公式得到其常数项,将常数项作为图像 I_2 中对应位置的像素值;

步骤 2:通过密钥对 $\{x_0, y_0, k, \alpha\}$ 驱动 2D-CMCM,生成与秘密分享阶段相同的 4 个随机数序列 X_1, X_2, Y_1 和 Y_2 ;

步骤 3:通过步骤 2 生成的 4 个随机数序列分别完成行和列的逆向置乱(扩散)操作,生成原始图像。

4 算法性能分析

以图片数据集 textures 中图片作为测试样本,本小节展示了本算法在一系列图像安全算法评价指标上的测试结果,这些指标包括:明文敏感性、密文鲁棒性、峰值信噪比(Peak Signal to Noise Ratio, PSNR)和算法执行速度。同时,为了验证本文所提出算法的安全性和执行效率,将几种常见的图像加密算法^[3-4,10]与本文所提出的算法进行了比较。本小节包含的所有测试程序均使用 Eclipse 编译环境运行。所使用计算机的主要配置如下:Windows10, 64 位;Core-i7 8809 G, 3.1 GHz;64 G 内存。

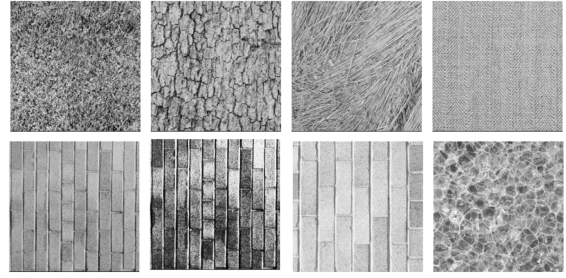
图片数据集 textures 中部分样本图片如图 3(a)所示。使用本文所提出的算法对 textures 数据集中图片进行处理,生成的部分秘密子图如图 3(b)所示,经过本文算法完成重构之后得到的部分重构图像如图 3(c)所示。

4.1 安全性分析

4.1.1 明文敏感性分析

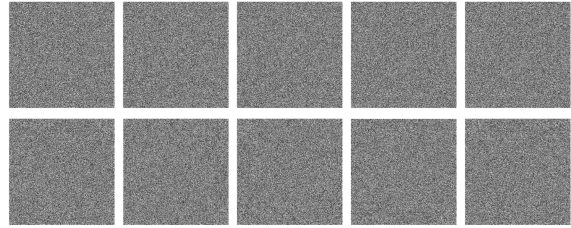
明文敏感性分析的目的在于衡量算法对明文攻击和选择性明文攻击这两种最常见的图像攻击方式的抵抗能力。当明文发生微小变化时,若使用同一对密钥加密原明文图像和变化后的明文图像所得到的两幅密文图像有显著差异,则该加密方案的明文敏感性强。

以数据集 textures 中图片作为测试图片,每张图片随机选择一个像素点将像素值置为 0 得到新测试图片,两张图片使用本文算法与参与比较的几种算法分别进行加密-秘密分享处理,计算原



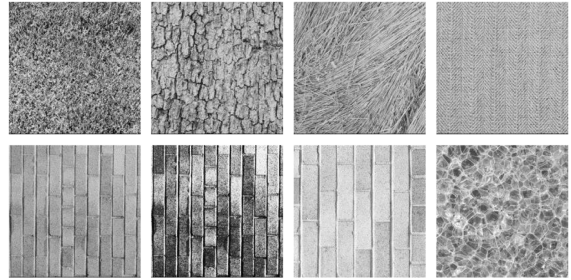
(a)数据集 textures 中部分样本图片

(a)Part of sample images in dataset textures



(b)数据集 textures 中部分秘密子图

(b)Partial secret subgraphs in dataset textures



(c)图像重构之后得到的部分重构图像

(c)Part of the reconstructed images

图 3 部分样本图片、秘密子图及重构图像。

Fig.3 Part of sample images, secret subgraphs and reconstructed images.

测试图片得到的 5 幅秘密子图和新测试图片得到的 5 幅秘密子图之间的平均 NPCR(Number of pixels change rate),部分图片的实验结果列于表 1。在理想情况下,两幅完全不同的图像之间的 NPCR 约为 99.6094%。设有两幅尺寸均为 $M \times N$ 的图像 P, P' ,NPCR 的定义如公式(6)所示。

$$\text{NPCR}(P, P') = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N D(P_{i,j} - P'_{i,j}) \times 100\%, \quad (6)$$

其中 $D(x) = \begin{cases} 0, & x=0 \\ 1, & x \neq 0 \end{cases}$ 。

表 1 部分样本图片的 NPCR 测试结果
Tab.1 NPCR test results for some images

图片名	NPCR/%			
	本文算法	文献[3]	文献[4]	文献[10]
1.1.01	97.740 4	96.543 6	96.248 6	97.154 8
1.1.02	97.055 1	96.872 5	95.573 9	97.068 9
1.1.03	98.143 7	96.445 6	96.315 9	97.027 0
1.1.04	98.541 8	97.038 9	98.476 0	97.710 6
1.2.01	97.925 8	97.716 8	95.010 5	96.103 0
1.2.02	98.520 0	97.007 7	97.891 2	96.036 7
1.3.01	97.832 7	96.257 1	97.013 9	96.248 3
1.3.02	97.206 6	95.036 7	97.015 9	97.530 7
1.3.03	98.770 5	96.964 0	98.753 1	97.258 2

通过表 1 可以看出,相比于 3 种参考算法,本文所提出的算法测出的 NPCR 指标更接近理想值,说明当测试图像发生微小变化时,通过本文所提出算法进行加密-秘密分享之后生成的秘密子图与原始测试图对应的秘密子图之间具有显著差异,两者近似完全不相关。因此,相比于 3 种参考算法,本文所提出算法具有更高的明文敏感性,对明文攻击和选择性明文攻击具有很强的抵抗能力。

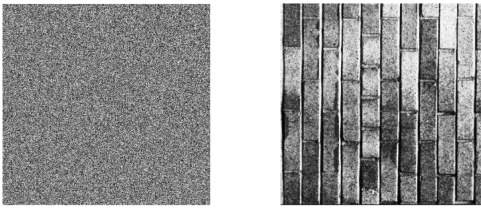
4.1.2 密文鲁棒性分析

密文图像在保存时往往会遭受数据损失攻击,具有较强鲁棒性的图像保密算法可以在密文图像部分受损的情况下恢复出具有较高可视性的原始图像。通过人为将加密得到的密文图像中部分像素点置 0(数量为总像素点总数的 1%, 2%, 4%),然后进行秘密分享生成秘密子图,最后观察重构图像的可视性,算法的抗数据损失攻击能力也得到了测试。部分图片的测试结果见图 4。

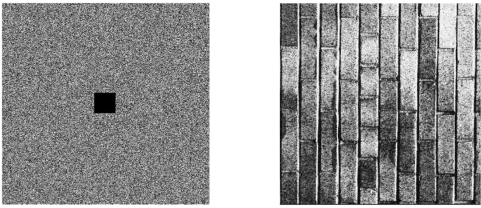
通过图 4(b~d)可以看出,密文图像中部分数据的损失让密文图像被污染,这导致了重构图像的可视性下降,但解密者仍可以从中获取绝大多数有用信息。因此,本文所提出的算法具有较强的抗数据损失攻击能力。

4.2 可逆性分析

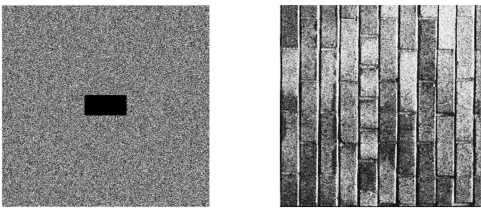
峰值信噪比(Peak Signal to Noise Ratio, PSNR)这个指标经常被用于检验数字图像加密算法是否能高质量地恢复加密图,峰值信噪比越



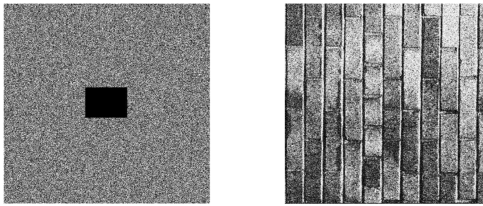
(a)密文图像及其对应的重建图像
(a) Encrypted image and its decrypted image



(b)包含 1% 数据损失的密文图像及其对应的重建图像
(b) Encrypted image with 1% data loss and its decrypted image



(c)包含 2% 数据损失的密文图像及其对应的重建图像
(c) Encrypted image with 2% data loss and its decrypted image



(d)包含 4% 数据损失的密文图像及其对应的重建图像
(d) Encrypted image with 4% data loss and its decrypted image

图 4 密文图像鲁棒性分析实验结果

Fig.4 Experimental results ciphertext image robustness analysis

高,说明被重构出的图像越接近原始图像。PSNR 定义如公式(7)所示。

$$K_{\text{PSNR}} = 10 \times \lg \frac{255^2}{K_{\text{MSE}}} \text{dB}, \quad (7)$$

其中 K_{MSE} 为均方根误差 (Mean Square Error)。设明文图像大小为 $M \times N$, 明文图像和从秘密子图中得到的重构图像第 i 行第 j 列像素值分别为 $p_{i,j}$ 和 $p'_{i,j}$ 。 K_{MSE} 的定义如 (8) 所示。

$$K_{\text{MSE}} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (p_{i,j} - p'_{i,j})^2. \quad (8)$$

部分样本图片的 PSNR 测试结果列于表 2。由表 2 可知, 本文所提出的算法重建出的图像与原始明文图像间的不相同像素点数目在 2 个以内, 远少于另外几种参考算法, 表明本文所提出的算法具有更高的图像可逆性, 通过秘密子图能几乎完整地恢复出原始明文图像。

表 2 部分样本的 PSNR 测试结果

Tab.2 PSNR test results of partial samples

图片名	PSNR/dB			
	本文算法	文献[3]	文献[4]	文献[10]
1.1.01	84.58	35.15	43.86	51.68
1.1.02	87.18	35.85	41.24	52.37
1.1.03	86.31	36.12	42.36	52.16

表 3 部分图片执行效率测试结果

Tab.3 Execution efficiency of partial samples

图片名	加密-秘密分享耗时/s				图像重构耗时/s			
	本文算法	文献[3]	文献[4]	文献[10]	本文算法	文献[3]	文献[4]	文献[10]
1.1.01	0.29	1.25	2.64	0.78	0.21	0.37	0.74	0.64
1.1.02	0.38	1.21	2.54	0.74	0.11	0.38	0.75	0.71
1.1.03	0.32	1.22	2.67	0.75	0.17	0.37	0.74	0.75
1.1.04	0.11	1.26	2.53	0.76	0.25	0.34	0.76	0.68
1.2.01	0.34	1.27	2.41	0.74	0.11	0.36	0.73	0.73
1.2.02	0.29	1.27	2.34	0.75	0.20	0.37	0.74	0.72
1.3.01	0.39	1.28	2.36	0.78	0.10	0.36	0.76	0.64
01.3.02	0.18	1.23	2.38	0.81	0.22	0.37	0.79	0.64
1.3.03	0.32	1.22	2.39	0.80	0.14	0.35	0.82	0.81

续 表

图片名	PSNR/dB			
	本文算法	文献[3]	文献[4]	文献[10]
1.1.04	84.10	35.54	41.28	52.75
1.2.01	81.58	35.24	42.95	52.96
1.2.02	83.99	36.61	41.25	53.21
1.3.01	85.12	36.37	41.67	54.30
1.3.02	85.08	35.49	41.04	52.61
1.3.03	83.00	36.02	43.36	53.67

4.3 执行效率分析

为了实现海量图片的实时性加密-秘密分享及原始图像重建, 每幅图像的加密-秘密分享时间及图像重建时间必须尽可能短。以数据集 textures 中图像作为测试样例, 本算法与另外几种参与比较的算法的加密-秘密分享消耗时间及图像重建时间列于表 3。通过表 3 可以看出, 使用本文所提出算法时, 每幅图像完成加密-秘密分享及重建的总消耗时间均不超过 0.5 s, 因此本文所提出的算法能够实现海量图片的实时分布式秘密存储。

5 结 论

为了实现数字图像的分布式保密存储,本文提出了一种图像加密-秘密分享算法。图像加密包含行/列置乱和扩散两个步骤,使用2D-CMCM产生的4个随机数序列完成,通过在行扩散阶段使用已加密像素点参与扩散,本文算法的安全性进一步得到了提高。在对图像加密得到的密文图像进行秘密分享的阶段,使用基于拉格朗日多项式插值的(3,5)门限秘密分享算法,通过带入5个

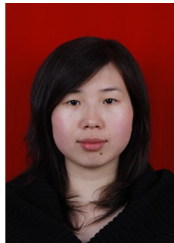
不同的整数值到多项式,将密文图像分为5份秘密子图。解密者只有在获取不少于3份的秘密子图及密钥的情况下才能实现原始图像的无损重建。在安全性分析实验中,本文所提出算法显示出了高度的抗明文/选择性明文攻击能力和抗数据损失攻击能力;在可逆性分析中,秘密子图被证实可以实现原始明文图像的无损重构,重构出的图像与原始明文图像的差异不超过2个像素点;在执行效率测试实验中,本文所提出算法的高执行效率也得到了验证。经过一系列实验,本文所提出算法的高度实用性得到了证实。

参 考 文 献:

- [1] MIGLIORINI D, MINGOZZI E, VALLATI C. Performance evaluation of H.264/SVC video streaming over mobile WiMAX [J]. *Computer Networks*, 2011, 55(15): 3578-3591.
- [2] PRAVEENKUMAR P, PRIYA P C, AVILA J, *et al.* Tamper proofing identification and authenticated DICOM image transmission using wireless channels and CR network [J]. *Wireless Personal Communications*, 2017, 97(4): 5573-5595.
- [3] KEKRE H B, SARODE T, HALARNKAR P N. Partial image scrambling using Walsh sequency in sinusoidal wavelet transform domain [M]//BERRETTI S, THAMPI S M, SRIVASTAVA P R. *Intelligent Systems Technologies and Applications: Volume 1*. Cham: Springer, 2015: 471-484.
- [4] SONG C Y, QIAO Y L. A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos [J]. *Entropy*, 2015, 17(10): 6954-6968.
- [5] 雷正桥,肖迪.基于空域可恢复信息隐藏的图像安全人工退化算法[J]. *计算机科学*, 2015, 42(3): 162-166.
LEI Z Q, XIAO D. Artificial image security degradation algorithm based on invertible information hiding in spatial domain [J]. *Computer Science*, 2015, 42(3): 162-166. (in Chinese)
- [6] 穆晓芳,邓红霞,李晓宾,等.基于人工蜂群算法的两阶段图像隐写分析算法[J]. *计算机科学*, 2019, 46(6): 174-179.
MU X F, DENG H X, LI X B, *et al.* Two-phase image steganalysis algorithm based on artificial bee colony algorithm [J]. *Computer Science*, 2019, 46(6): 174-179. (in Chinese)
- [7] 刘松.基于分布式的海量图片数据存储系统的设计与实现[D].深圳:深圳大学, 2016.
LIU X. Based on the distributed mass image data storage system in the research and design [D]. Shenzhen: Shenzhen University, 2016. (in Chinese)
- [8] LIU Y X, YANG C N, WU C M, *et al.* Threshold changeable secret image sharing scheme based on interpolation polynomial [J]. *Multimedia Tools and Applications*, 2019, 78(13): 18653-18667.
- [9] LI P, YANG C N, ZHOU Z L. Essential secret image sharing scheme with the same size of shadows [J]. *Digital Signal Processing*, 2016, 50: 51-60.
- [10] CAO C, SUN K H, LIU W H. A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map [J]. *Signal Processing*, 2018, 143: 122-133.
- [11] HUA Z Y, ZHOU Y C, CHEN C L P. A new series-wound framework for generating 1D chaotic maps [C]// *Proceedings of 2013 IEEE Digital Signal Processing and Signal Processing Education Meeting (DSP/SPE)*. Napa, CA, USA: IEEE, 2013: 118-123.
- [12] LIU W H, SUN K H, ZHU C X. A fast image encryption algorithm based on chaotic map [J]. *Optics and Lasers in Engineering*, 2016, 84: 26-36.
- [13] MAY B R. Simple mathematical models with very complicated dynamics [J]. *Nature*, 1976, 261(5560): 459-467.
- [14] HE D, HE C, JIANG L G, *et al.* Chaotic characteristics of a one-dimensional iterative map with infinite collapses

- [J]. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 2001, 48(7): 900-906.
- [15] ASMA F. Finite element model updating using Lagrange interpolation [J]. *Mechanics and Mechanical Engineering*, 2019, 23(1): 228-232.

作者简介:



王宛平(1983—),女,河南南阳人,硕士,2012年于郑州大学获得硕士学位,主要从事软件工程、计算机图形图像等方面的研究。E-mail: wangwanping0809@163.com



李冰(1979—),男,河南新蔡人,硕士,2018年于南京理工大学获得硕士学位,主要从事软件工程、 workflow 技术等方面的研究。E-mail: Li_bing_0816@126.com