文章编号：2095-2163(2019)04-0315-05 中图分类号：TP309 文献标志码：A

面向 CALIC 的图像加密算法研究

张 淼，佟晓筠，张 华
（哈尔滨工业大学(威海) 计算机科学与技术学院，山东 威海 264209）

摘 要：将图像的加密和压缩结合在一起同步完成可以带来设计上的灵活和计算上的简化，同时也可以更好地保证安全性，为图像信息的安全高效存储和传输做出保障。基于 CALIC 良好的压缩效率，本文研究并设计了面向 CALIC 的图像加密算法。根据 CALIC 编码原理，算法实现在 CALIC 编码过程中的加密，主要包括 GAP 预测值的加密、最终残差的加密、明文像素的加密、熵编码码流的加密。实验结果表明面向 CALIC 的图像加密算法在压缩性能上取得较好效果的同时增加了安全性。

关键词：压缩加密联合；混沌；CALIC

Image encryption scheme for CALIC

ZHANG Miao, TONG Xiaojun, ZHANG Hua
(School of Computer Science and Technology, Harbin Institute of Technology at Weihai, Weihai Shandong 264209, China)

【Abstract】 Image encryption combined with image compression synchronously can result in the design flexibility and computational simplification. Moreover, encryption and compression are mixed together to ensure better security, and ensure secure and efficient image information storage and transmission. In terms of good compression performance of CALIC, image encryption scheme for CALIC is studied. Based on CALIC coding principle, the algorithm performs encryption in CALIC coding process, including encryption of gradient-adjusted prediction, encryption of final residual, encryption of two lines of pixels needed by prediction mode, and encryption of entropy coding bit stream. The experimental results show that the image encryption scheme for CALIC has better compression performance and security.

【Key words】 joint encryption and compression; chaos; CALIC

0 引 言

数字图像，作为现代通信领域重要的信息载体，其存储传输与安全性也被提出了更高的要求。图像的数据量庞大且存在冗余，为了提高存储和传输效率，对图像进行压缩显得非常必要。防止图像信息泄露提高安全性，一种非常有效的保护技术是图像加密技术。将图像的加密和压缩结合在一起同步完成，可以带来设计上的灵活和计算上的简化。同时，加密和压缩混合完成，可以更好地保证安全性。

混沌作为一种自由度很高的非线性动态系统，其运动轨道表现出的内随机性、遍历性和初值敏感性等特性，使得混沌系统相邻迭代点经有限次迭代后得到完全不同的序列。微小的变化引起不同计算结果的这种特性使得混沌密码可以满足传统密码在扩散、混淆和伪随机的重要需求。同时，混沌运动的确定性使得混沌应用于密码学的方法易于实现，其计算代价远小于其它传统密码的计算代价，非常适合大数据量的图像的加密处理。由于混沌的良好性质，一些基于混沌的图像加密算法已被提出[1-13]。

基于上下文的自适应无损编码(context-based, adaptive, lossless image Codec, CALIC)由 Wu 等人[14]于 1997 年提出。由于良好的压缩效率，CALIC 获得了广泛的关注。然而，CALIC 编码方法仅仅关注于压缩，并没有考虑安全性。本文基于混沌理论，研究并设计了面向 CALIC 的图像加密算法。通过研究与分析 CALIC 编码方法，在尽量保证压缩效率的同时，将加密嵌入到 CALIC 编码中，获得安全的 CALIC 编码。

1 Rabinovich 混沌系统与伪随机序列产生

Rabinovich 系统[15]是一个著名的三维混沌系

基金项目：2017 年威海市大学共建项目；信息保障技术重点实验室开放基金（KJ-17-004）。

作者简介：张 淼(1979-)，女，博士研究生，讲师，主要研究方向：混沌密码学、空间网络与信息安全；佟晓筠(1963-)，女，博士，教授，博士生导师，主要研究方向：混沌密码学、空间网络与信息安全、无线传感器网络安全；张 华(1978-)，男，硕士，讲师，主要研究方向：数据挖掘、机器学习、智能服务。

通讯作者：佟晓筠 Email：tong_xiaojun@163.com

收稿日期：2019-04-10

统,该系统有着复杂的动力学行为,与 Lorenz 系统关系密切,但并不拓扑等价,其方程如下:

$$\begin{cases} \dot{x} = hy - ax + yz; \\ \dot{y} = hx - by - xz; \\ \dot{z} = -dz + xy. \end{cases} \tag{1}$$

式中, x, y, z 为实数变量;当 $a = 4, b = d = 1$, $4.84 \leqslant h \leqslant h_0, h_0 \geqslant 4.92$ 时系统处于混沌状态。

给定系统初值,利用 Rabinovich 混沌系统(1)得到 3 组混沌序列 $\{x_n\}$、$\{y_n\}$ 和 $\{z_n\}$ ($n = 1, 2, \cdots$)。由于上述得到的混沌序列是浮点数,因此为了得到二元序列,必须离散化混沌序列 $\{x_n\}$, $\{y_n\}$ 和 $\{z_n\}$。对于每一个序列,获得其小数部分。以 $\{x_n\}$ 为例,即

$$x'_n = x_n - \lfloor x_n \rfloor, \tag{2}$$

其中, $\lfloor x \rfloor$ 表示对 x 向下取整。对于序列 $\{y_n\}$, $\{z_n\}$,可做同样的操作得到 $\{y'_n\}$ 和 $\{z'_n\}$。以 $\{x'_n\}$ 为例,量化小数部分得到整数序列 key_{1n}。

$$key_{in} = \mathrm{mod}(shiftR(\lfloor x'_n \times 10^P \rfloor, 7), N), \tag{3}$$

其中, P 代表计算机精度, N 取 256。$shiftR(x, y)$ 代表对 x 无符号右移 y 位, $n = 1,2,3,\cdots$, $i = 1,2,3$。对于序列 $\{y'_n\}$ 和 $\{z'_n\}$,做同样的处理,得到整数序列 key_{2n}, key_{3n}。最后,伪随机序列按如下方式产生:

$$key1 = key_{1n}, \tag{4}$$

$$key2 = key_{2n}, \tag{5}$$

$$key3 = key_{3n}. \tag{6}$$

其中, $key1$, $key2$, 和 $key3$ 为最后产生的伪随机序列。

2 CALIC 算法原理

CALIC 是一种顺序编码,其编码和解码都是以光栅扫描的顺序扫描一次图像。CALIC 编码过程使用预测和上下文模板,仅仅涉及编码像素的前两扫描行。因此编码和解码算法仅需要一个能存放 2 行像素的简单的 2 行缓冲区。CALIC 编码器的原理描述如图 1 所示。解码过程是编码过程的逆。CALIC 是对称的,即编码器和解码器具有相同的时间和空间复杂度。

从图 1 中可以看出,CALIC 具有 2 种工作模式:二值模式和连续色调模式。根据当前像素的上下文,2 种模式在编码过程中自动选择,对用户是透明的。在连续色调模式下,系统包括 4 个主要部分:梯度自适应预测器(GAP)、上下文选择和量化、预测误差上下文建模、预测误差熵编码。

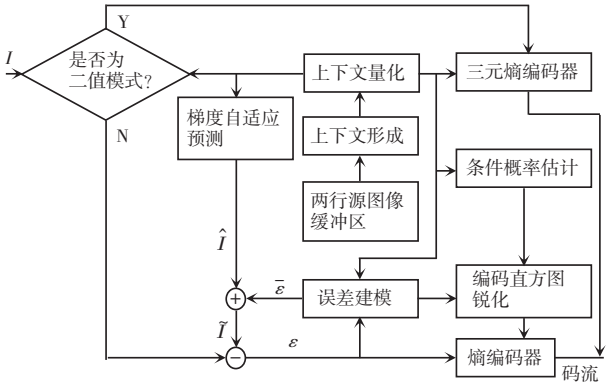

图 1 CALIC 编码器的原理描述

Fig. 1 Schematic description of CALIC's encoder

3 加密方法设计

通过分析 CALIC 编码原理,将加密嵌入到 CALIC 编码中,形成安全的 CALIC 编码,算法流程如图 2 所示。

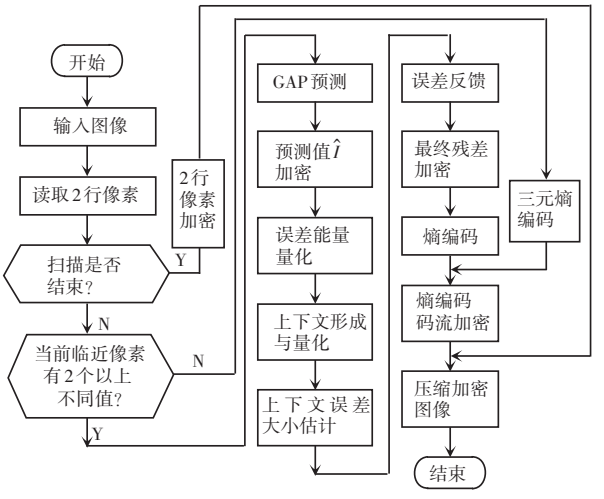

图 2 安全的 CALIC 编码流程图

Fig. 2 Flow chart of secure CALIC

由图 2 可知,在 CALIC 编码过程中,实现了 4 处加密,分别是 GAP 预测值加密、最终残差加密、2 行像素加密和熵编码码流加密。

3.1 明文像素加密

作为编码初始值的图像前 2 行像素值在编码结束后要写入文件中。由于这 2 行像素值不涉及后续的压缩编码操作,因此采用扩散置乱结构对其加密。

设 2 行像素为图像 X,其像素序列 $pixseq$ 长度为 l,如下所示:

$$pixseq = \{p(1), p(2), \ldots, p(l)\}, \tag{7}$$

其中，$p(i)$ 为第 i 个像素值，$i \in [1,l]$。每个像素值由 8 比特组成，$p(i)$ 从高位到低位可表示为：

$$p(i) = \{b_{i8}, b_{i7}, b_{i6}, b_{i5}, b_{i4}, b_{i3}, b_{i2}, b_{i1}\}, \quad (8)$$

其中，b_{ij} 表示第 i 个像素的第 j 位。$b_{ij} \in \{0, 1\}$。将每 4 个像素值 $p(i)$ 的高 4 比特 $\{b_{i8}, b_{i7}, b_{i6}, b_{i5}\}$ 组成一组，低 4 比特 $\{b_{i4}, b_{i3}, b_{i2}, b_{i1}\}$ 组成一组，如图 3 所示。然后按照 16 比特的高 4 比特和 16 比特的低 4 比特穿插排列，如图 4 所示。

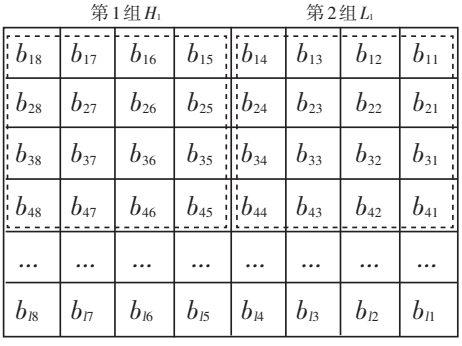

图 3　比特组构成

Fig. 3　Bit groups construction

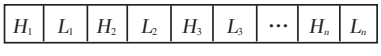

图 4　比特组排列

Fig. 4　Bit groups arrangement

对每个 16 比特的比特组使用猫映射进行比特级置乱：

$$\begin{pmatrix} x'_{i+1} \\ y'_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod 4, \quad (9)$$

式中，控制参数 p 和 q 由混沌系统(1) 产生，每一组置乱用的 p_i，q_i 产生方法如下：

$$p_i = (fabs(x_{1000+i}) \times 10^{14}) \bmod 4, \quad (10)$$

$$q_i = (fabs(y_{1000+i}) \times 10^{14}) \bmod 4, \quad (11)$$

其中，x_{2000+i} 和 y_{2000+i} 分别是混沌系统(1) x 和 y 迭代第(2000 + i) 次取值，i 为组号。

对比特组内置乱后的像素值进行扩散操作，具体操作如下：

$$\begin{cases} c_{Hi} = (mH_i + key1(i) + c_{L(i-1)}) \bmod (2^{16}); \\ c_{Li} = (mL_i + key2(i) + c_{H(i-1)}) \bmod (2^{16}). \end{cases} \quad (12)$$

其中，mH_i 代表比特组穿插排列后的第 i 个高 4 比特组，mL_i 代表比特组穿插排列后的第 i 个低 4 比特组。$key1(i)$ 和 $key2(i)$ 分别为密钥流 $key1$ 和 $key2$ 相应的 2 字节值。

最后对扩散后的像素值进行组间置乱，迭代混沌系统(1) 获得混沌序列 $Y = \{y_i, i = 1,2,\cdots,n\}$。对混沌序列 Y 进行排序，得到排序后的序列 $S = \{s_i, i = 1, 2, \cdots, n\}$。得到转换序列 $T = \{t(i), i = 1, 2, \cdots, n\}$，使得 $t(i)$ 的值等于 s_i。将第 i 组移动到第 $t(i)$ 组的位置。

3.2　熵编码码流加密

这里对熵编码码流进行加密提供最后一层安全保护以增强安全性。熵编码码流不涉及后续的压缩编码操作，因此采用扩散置乱结构对其加密。

首先，执行扩散操作，码流以 2 个字节为单位进行处理。具体扩散公式如下：

$$c_i = ((m_i \oplus key1(i)) + key3(i) + c_{i-1}) \bmod (2^{16}). \quad (13)$$

其中，$key1(i)$ 和 $key3(i)$ 为密钥流 $key1$ 和 $key3$ 相应的 2 字节数据。

然后进行置乱操作，迭代混沌系统(1) 获得混沌序列 $Z = \{z_i, i = 1,2,\cdots,n\}$。对混沌序列 Z 进行排序，得到排序后的序列 $S = \{s_i, i = 1, 2, \cdots, n\}$。得到转换序列 $T = \{t(i), i = 1, 2, \cdots, n\}$，使得 $t(i)$ 的值等于 s_i。将第 i 组移动到第 $t(i)$ 组的位置。

3.3　GAP 预测值与最终残差加密

GAP 预测值是编码过程中根据当前像素生成的初始预测值，后续的上下文选择和量化、预测误差的上下文建模都要使用该预测值。为了不对后续的操作造成较大影响从而影响压缩性能，GAP 预测值的加密操作不能过于复杂。同时 GAP 预测值是在编码过程中一个一个按顺序产生的，如果执行置乱加密将增加空间复杂度。因此只对 GAP 预测值执行替换加密。

残差的结果最终要执行熵编码，因此最终残差的加密操作也不能过于复杂而导致压缩性能下降。同时，最终残差结果也是一个一个顺序产生，且其数量只有在算法结束才能确定。因此，对最终残差执行置乱加密将增加算法的空间复杂度和时间复杂度。在这里仅对最终残差执行替换加密。加密方法如下：

$$c_i = m_i \oplus key2(i). \quad (14)$$

其中，c_i 表示密文；m_i 表示明文；$key2(i)$ 表示密钥流 $key2$ 相应的一个字节。

4　实验和讨论

4.1　实验结果

算法的实验环境为 3.19 GHz 处理器，2 GB 内存，MATLAB 2012R。选取 USC-SIPI 数据库中的标准图像进行测试，图 5 给出了 3 幅 512×512 的灰度图像 Lena、Barbara 和 Baboon 的重构图像。

(a) Lena (b) 重构的 Lena (c) Barbara (d) 重构的 Barbara (e) Baboon (f) 重构的 Baboon

(a) Lena (b) Reconstructed lena (c) Barbara (d) Reconstructed Barbara (e) Baboon (f) Reconstructed Baboon

图 5 原始图像和重构图像

Fig. 5 Original and reconstructed image

4.2 压缩性能评估

表 1 列出原始没有添加加密的 CALIC 算法的压缩比,及添加加密的安全的 CALIC 的压缩比。从表中结果可以看出,添加加密后对原有 CALIC 算法的压缩性能的影响较小。

表 1 压缩性能

Tab. 1 The compression performance for different images

图像	Lena	Babara	Baboon
原始 CALIC	4.28	4.66	6.00
安全的 CALIC	4.65	5.38	6.23

4.3 密钥空间分析

系统包括置乱密钥和扩散密钥,均取混沌系统的初始值(x_0, y_0, z_0)。因此置乱密钥和扩散密钥各含 3 个变量。根据 IEEE 754-2008 标准,采用双精度(binary64)类型存储,8 个字节表示 1 个双精度数。因此密钥空间为 2^{384}。该加密算法的密钥空间为 2^{384}。显然在目前的计算能力下,该密钥空间足够大,可以抵抗穷举攻击。

4.4 信息熵分析

密文信息熵测试结果见表 2。从表中看出,密文的信息熵接近理想值 8,说明密文随机性很好。

表 2 密文信息熵

Tab. 2 Information entropy of the encrypted code stream

图像	信息熵
Lena	7.982
Baboon	7.991
Barbara	7.992

5 结束语

针对 CALIC 虽具有良好的图像无损压缩特性,而没有考虑安全性的问题,研究了面向 CALIC 的图像加密算法。首先,基于混沌的良好性质,利用三维混沌系统 Rabinovich 产生伪随机序列。其次,研究了 CALIC 无损压缩原理。在 CALIC 压缩编码的过程中加入加密算法,实现面向 CALIC 的图像加密过程。面向 CALIC 的图像加密方法主要体现在 4 个方面:GAP 预测值的加密、最终残差的加密、明文像素的加密、熵编码码流的加密。根据加密处 CALIC 编码的特点,设计了适合于 4 个编码位置的、对压缩性能影响最小的加密算法。

最后对算法的压缩性能、安全性能进行了分析。在压缩性能上取得了好的效果。在安全性上,通过对密钥空间、密文信息熵的分析测试证明了算法的安全性。

参考文献

[1] MIRZAEI O, YAGHOOBI M, IRAN H. A new image encryption method: Parallel sub-image encryption with hyper chaos [J]. Nonlinear Dynamics, 2012,67(1):557-566.

[2] ZHANG W, WONG K W, YU H, et al. Asymmetric color image encryption using the intrinsic features of bit distributions [J]. Commun Nonlinear Sci Numer Simul, 2013,18:584-600.

[3] ZHANG Yingqian, WANG Xingyuan. Analysis and improvement of a chaos-based Symmetric image encryption scheme using a bit-level permutation[J]. Nonlinear Dynamics, 2014,77(3): 687-698.

[4] LIU Hongjun, WANG Xingyuan. Color image encryption using spatial bit-level permutation and high-dimension chaotic system [J]. Optics Communications,2011,284(16/17):3895-3903.

[5] TENG Lin, WANG Xinyuan. A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive [J]. Optics Communications, 2012,285(20):4048-4054.

[6] XU Lu, LI Zhi, LI Jian, et al. A novel bit-level image encryption algorithm based on chaotic maps [J]. Optics and Lasers in Engineering, 2016,78:17-25.

[7] ZHANG Wei, WONG K W, YU Hai, et al. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion[J]. Communications in Nonlinear Science and Numerical Simulation, 2013,18(8):2066-2080.

[8] KUMAR A, GHOSE M K. Extended substitution-diffusion based image cipher using chaotic standard map[J]. Communication in Nonlinear Science and Numerical Simulation, 2011, 16(1): 372-382.

[9] WANG Xinyuan, TENG Lin. An image blocks encryption algorithm based on spatiotemporal chaos[J]. Nonlinear Dynamics, 2012, 67(1): 365-371.

[10] LIU Hongjun, WANG Xingyuan, KADIR A. Image encryption using DNA complementary rule and chaotic maps s[J]. Applied

Soft Computing，2012，12(5)：1457-1466.
[11] CHAI Xiuli，CHEN Yiran，BROYDE L. A novel chaos-based image encryption algorithm using DNA sequence operations[J]. Optics and Lasers in Engineering，2017，88：197-213.
[12] BIGDELI N，FARID Y，AFSHAR K. A novel image encryption/decryption scheme based on chaotic neural networks [J]. Engineering Applications of Artificial Intelligence，2012，25(4)：753-765.
[13] SABERIKAMARPOSHTI M，MOHAMMAD D，RAHIM M S M，et al. Using 3-cell chaotic map for image encryption based on biological operations[J]. Nonlinear Dynamics，2014，75(3)：407-416.
[14] WU Xiaolin，MEMON N D. Context-based，adaptive，lossless image coding[J]. IEEE Transcations on communications，1997，45(4)：437-444.
[15] Cheng Chen，Jinlong Cao and Xiang Zhang. The topological structure of the Rabinovich system having an invariant algebraic surface[J]. Nonlinearity，2008，21(2)：211-220.

(上接第 314 页)

图 4　域代码

Fig. 4　Domain code

4　结束语

在邮件合并中，灵活运用域，可以让邮件合并的功能如虎添翼。本文中只使用了域其中的一部分功能，其它比如照片域[3]、数值域等等在邮件合并中也可能会用上，对图形图像、数值、文本等数据均能批量处理，对用户而言，节省了时间、减少了工作量、提高了效率。

参考文献

[1] 张红艳，杨勇. 邮件合并中嵌套式 Word 域“If…Then…Else…”的运用[J]. 办公自动化，2010(4)：36-38.
[2] 朱克武. Word 邮件合并在 VB 编程中的应用 [J]. 计算机与现化化，2012(6)：204-207，211.
[3] 孙传庆，李国芳，朱正平. 域 INCLUDE PICTURE 在 Word 2003 邮件合并中的应用研究[J]. 自动化与仪器仪表，2011(2)：20-21.