一类二值图像快速加密算法的压缩性能分析

周　庆　　廖晓峰　　胡　月
(重庆大学计算机学院　重庆　400030)

摘　要：近年来，多媒体加密技术得到了广泛的研究，但是现有算法在分析加密算法的压缩性能时主要采用定性分析和实验检验的方式，未能实现对压缩性能的量化分析和控制，从而限制了该技术的应用。该文分别就 MH 编码，Huffman 编码和自适应算术编码 3 种不同的编码方式，对一类常用的二值图像快速加密算法的压缩性能进行了定量分析。实验结果表明该文给出的压缩性能预测公式是准确的。

关键词：图像加密；快速加密；二值图像；MH 编码
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2009)08-2015-04

Compression Performance Analysis of a Sort of Fast Binary Image Encryption Algorithms

Zhou Qing　　Liao Xiao-feng　　Hu Yue
(*Institution of Computer Science*, *Chongqing University*, *Chongqing* 400030, *China*)

Abstract: Multimedia encryption algorithms are widely studied in recent years. However, the performances of those algorithms are usually checked by qualitative analysis and simulations. In this paper, the compression performance of a sort of encryption algorithms for binary image is analyzed quantitatively using information theories. It shows that those algorithms are good at performances including security, speed, compression ratio, robustness and format-compliance, and therefore suitable for practical use.

Key words: Image encryption; Fast encryption; Binary Image; MH coding

1　引言

现代通信和计算技术的飞速发展使得多媒体技术被广泛用于人们的生活中，涉及军事、政治、教育、医疗、商业和娱乐等多个领域。在这些领域中，涉及个人隐私、商业利益乃至国家安全的多媒体数据都需要进行加密。最直接的加密方法是将多媒体对象(图像、音频、视频等)当作普通的二进制数据，并采用传统的加密标准如 DES 或 AES 进行加密。由于多媒体数据量通常很庞大，这种方法的加密速度很慢。为此研究者们提出了多媒体加密技术，利用多媒体的特性如时间性、空间性、感知差异性和可压缩性来提高加密速度[1]。根据研究方法的不同，多媒体加密技术可分为空域置乱技术、选择加密技术、熵编码加密技术等种类[2−4]。由于加密通常会降低加密算法的压缩性能，而多媒体的数据量很大，因此多媒体加密算法的压缩性能是研究者关心的重要指标。然而，目前多媒体加密技术对压缩性能主要采用定性分析的方式，未进行定量分析。

本文的研究对象为二值图像，它是最简单的一种多媒体形式，较为复杂的灰度图像和彩色图像也可分解成多幅二值图像。本文采用概率论和信息论方法对此类加密算法的压缩性能进行了定量分析，并就 MH 编码、Huffman 编码和自适应算术编码 3 种编码算法分别作了详细的讨论。

2008-09-22 收到，2009-03-13 改回
国家自然科学基金(60573047，60703035)资助课题

2　采用 MH 编码的二值图像快速加密算法的压缩性能分析

2.1 MH编码介绍

MH 编码(Modified Huffman)，是 CCITT(国际电报电话咨询委员会)建议的一种传真机压缩编码国际标准，目前仍在绝大多数三类传真机上使用。MH 编码具有压缩率高、实施成本低、抗干扰能力强的优点[5]，其编码规则主要包括以下几个内容：

(1)传真内容可看作一个二值图像，由多条扫描线组成；

(2)对每个扫描线进行行程编码；

(3)对各行程进行 Huffman 编码，Huffman 表的内容是固定的；

(4)为了便于收发同步，规定在每行结束时添加一个结束符，当文档结束时添加 6 个结束符。

2.2 加密算法及实验

采用 MH 编码的二值图像快速加密算法过程非常简单，由两个步骤组成：

(1)对二值图像的像素进行随机排列；

(2)对排列后的图像采用 MH 编码。

本文采用该算法对 3 个典型的传真文档(分别为中文文档、英文文档和程序流程图)进行加密，其压缩性能的理论分析和实验结果在 2.3 节给出。

2.3 压缩性能分析

评价加密算法的压缩性能可采用压缩比作为指标：

$$C = n_1/n_2 \tag{1}$$

其中 n_2 表示压缩后的数据量(本文以比特为单位)，n_1 表示压缩前的数据量。为了归一化处理，也可采用相对冗余来表示压缩性能[6]：

$$R = 1 - 1/C \tag{2}$$

其中 C 由式(1)定义，本文采用式(2)作为加密算法的压缩性能指标。为计算相对冗余，必须先求出加密后白色和黑色行程的分布。设明文图像有 N 个像素，其中白色像素占全体像素的比例为 $p(0\leqslant p\leqslant 1)$，黑色像素的比例为 $q=1-p$；为简化讨论，不妨设加密后的图像各像素 X_i 呈独立同分布，且分布为

$$P\{X_i = a\} = \begin{cases} p, & a = 1 \\ q, & a = 0 \\ 0, & \text{其它} \end{cases} \tag{3}$$

引理 1 设加密后图像各像素的分布由式(3)定义，则长度为 t 的白色行程在所有非零的白色行程中出现的概率为

$$w_t = qp^{t-1} \tag{4}$$

长度为 t 的黑色行程在所有黑色行程中出现的概率为

$$b_t = pq^{t-1} \tag{5}$$

证明略。

图 1 给出了一个中文文档加密后零行程和壹行程的实际分布与式(4)和式(5)给出的理论值的对比。

从图 1 可以看出，式(4)和式(5)预测出的零行程和壹行程分布与实际值非常吻合。

引理 2 设加密后图像各像素的分布由式(1)定义，则黑色行程和白色行程的个数 n_0 和 n_1 的数学期望为

$$E(n_0) = E(n_1) = Npq \tag{6}$$

证明略。

定理 1 设加密后图像各像素的分布由式(1)定义，则加密后长度为 t 的白色行程个数的数学期望等于：

$$W_t = Nq^2p^t \tag{7}$$

黑色行程个数的数学期望等于：

$$B_t = Np^2q^t \tag{8}$$

证明 由引理 1 和引理 2 容易推出定理 1。

由定理 1 可推出图像经加密和 MH 编码后的比特数：

$$N' = W + B = \sum_t W_tU_t + \sum_t B_tV_t \tag{9}$$

其中 W 和 B 为白色和黑色行程编码后的比特数，U_t 和 V_t 分别表示长度为 t 的白色或黑色行程经 MH 编码后的比特数。

实验表明，当 t 的取值范围为 1 到 128 时，式(9)能够对 MH 编码后的比特数进行非常准确的预测。但是式(9)的计算较复杂，考虑到大多数扫描文档中白色像素所占比例 p 的取值满足 $0.85\leqslant p\leqslant 0.95$(参见文献[5] Table III)，可对式(7)进行简化。其中

$$\begin{aligned} W &= \sum_t W_tU_t = 5\sum_t W_t + \sum_t W_t(U_t - 5) \\ &\approx 5Npq + \sum_t W_t(U_t - 5) \end{aligned}$$

当 $0.85\leqslant p\leqslant 0.95$ 时，$\sum_t W_t(U_t-5)$ 可由直线 $0.7N(p-0.87)$ 近似逼近，又因为黑色行程的长度超过 6 的概率极小，故式(9)可简化为

$$N' = W + B \approx 5Npq + 0.7N(p-0.87) + \sum_{t=1}^{6} B_tV_t \tag{10}$$

表 1 显示了图 1 中的 3 个文档经加密和 MH 编码后的相对冗余以及根据式(10)给出的理论值之间的对比。该表说明式(10)可以精确地预测典型的传真文档加密后的相对冗余。

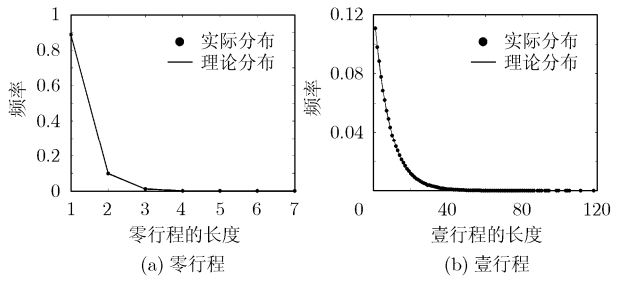

图 1 一个中文文档加密后零行程和壹行程分布的理论值与实际值

表 1 各文档加密后相对冗余的实际值以及由式(10)给出的理论值

	中文文档	英文文档	程序流程图
p	0.8892	0.9167	0.9453
理论值	0.2021	0.3539	0.5277
实际值	0.2015	0.3552	0.5290

3　采用 Huffman 或自适应算术编码的二值图像加密算法

3.1 采用Huffman编码的二值图像加密算法

尽管基于 MH 编码的图像加密算法对于加密传真文档具有许多优点，但仍然存在两个主要的缺陷：

(1)MH 编码使用固定的 Huffman 表，当二值图像中白色像素的比例大于 0.85 时，加密算法具有较好的压缩效果。但是对于普通二值图像，该 Huffman 表不能最优地反映出行程的概率分布，从而减小了加密图像的压缩性能；

(2)MH 编码每加密一行像素都要传输一次结束符，大大降低了普通二值图像的压缩率。

这些缺陷说明，基于 MH 编码的图像加密算法移植到普通二值图像上需要改进。考虑到普通二值图像的应用平台主要为计算机，改进算法在原算法的基础上作了两点修改，一是采用自定义的 Huffman 表，二是不使用结束符。

3.2 压缩性能

改进算法的相对冗余决定于加密后数据的比特数。显然，经改进算法加密后白色和黑色行程个数的数学期望与原算法相同，均由式(7)和式(8)给出；关键在于求出白色和黑色行程的平均编码长度。在理想情况下，符号的平均编码长度近似等于符号的信息熵。

引理 3　设加密后图像各像素的分布由式(3)定义，则经改进算法加密后黑色行程和白色行程的信息熵 h_0 和 h_1 分别为

$$\left.\begin{aligned} h_0 &= H(p)/p \\ h_1 &= H(p)/q \end{aligned}\right\} \tag{11}$$

其中 H 表示熵函数。

证明略。

定理 2　设加密后图像各像素的分布由式(3)定义，则加密后的相对冗余等于：

$$R = 1 - H(p) \tag{12}$$

证明　经熵编码后序列的比特数为

$$\begin{aligned} E(n) &= E(n_1)h_1 + E(n_0)h_0 \\ &= Npq \cdot H(p)/q + Npq \cdot H(p)/p \\ &= N \cdot H(p) \end{aligned} \tag{13}$$

故相对冗余 $R = 1 - E(n)/N = 1 - H(p)$。　　证毕

为了检验式(12)的正确性，我们选用美国南加利福尼亚大学建议的 15 幅典型的数字图像[7]的最高位平面作为二值图像，包括了 Baboon(第 2 幅)和 Lena(第 11 幅)等常见图像。表 2 列出了各图像加密后压缩率的实际值与式(12)预测的理论值的对比，可以看出对于某些图像(如第 1、5、10 和 14 幅图)其预测值与实际值还存在较大的误差(大于 6%)。

分析表明，主要的预测误差源自行程分布的不平衡。以'Airplane'(序号为 1 的图像)为例，比特 1 所占的概率约为 80%，由式(5)可知加密后绝大多数零行程的长度小于 3。由于 Huffman 树是单符号编码，当多数符号的值都集中到一两个符号时 Huffman 的编码效率很低，其相对冗余接近 0。因此当比特 1 或比特 0 的频率较高时，加密后的压缩率可由式(14)近似表示：

$$R = \begin{cases} 1 - pH(p) - q, & p \geq 0.5 \\ 1 - qH(p) - p, & p < 0.5 \end{cases} \tag{14}$$

表 3 列出了 15 幅图像加密后实际的压缩率以及由式(14)预测的理论值。从表 3 中可以看出式(14)可以很准确地预测出改进算法的压缩率。

3.3 采用自适应算术编码的二值图像加密算法

对比式(14)和式(12)可以发现采用 Huffman 编码进行加密的压缩性能与理想的压缩性能还存在较大的差距。为了接近理想的压缩性能，可以采用新的编码方法来代替 Huffman 这种单符号编码算法。表 4 列出了采用算术编码后前 7 幅图像相对冗余的实际值与式(12)之间的对比。

表 2　各图像加密后压缩性能的实际值与式(12)预测的理论值的对比

图像索引	1	2	5	7	10	12	14	15
理论值	0.3053	0.0013	0.3397	0.9091	0.3430	0.0021	0.2888	0.0013
实际值	0.2418	0.0001	0.2774	0.8996	0.2813	0.0000	0.2269	0.0001
误差	−0.0635	−0.0012	−0.0623	−0.0095	−0.0617	−0.0021	−0.0619	−0.0012

表 3　各图像加密后压缩率的实际值与式(14)预测的理论值的误差

图像索引	1	2	3	4	5	6	7	平均值
理论值	0.2483	0.0007	0.8528	0.5487	0.2816	0.0224	0.8986	0.2521
实际值	0.2418	0.0001	0.8555	0.5475	0.2774	0.0007	0.8996	0.2493
误差	−0.0065	−0.0006	0.0027	−0.0012	−0.0042	−0.0217	0.0010	−0.0029

表 4 各图像加密后压缩性能的实际值与式(12)预测的理论值的对比

图像索引	1	2	3	4	5	6	7	平均值
理论值	0.3053	0.0013	0.8686	0.5966	0.3397	0.0366	0.9091	0.2773
实际值	0.3039	0.0003	0.8478	0.5883	0.3342	0.0331	0.8978	0.2731
误差	−0.0014	−0.001	−0.0208	−0.0083	−0.0055	−0.0035	−0.0113	−0.0042

从表 4 可以看出若采用合适的熵编码算法，式(12)可以非常准确地预测加密后图像的相对冗余。另一方面，比较表 3 和表 4 中压缩性能的实际值可以看出采用自适应算术编码的加密算法具有更高的压缩性能。

4 结束语

本文主要研究了一类二值图像快速加密方法的压缩性能。现有的多媒体加密技术在研究加密性能时主要采用定性分析和实验检验的方式，本文则利用信息论方法对加密算法的压缩性能作了定量分析，分别给出了基于 MH 编码，Huffman 编码和自适应算术编码 3 种加密算法的压缩性能的预测公式。实验结果表明，本文推导出的 3 种压缩性能理论公式能准确地给出 3 种加密算法的压缩性能。此外，这类算法在安全性、加密效率和鲁棒性方面也有很好的表现，可用于二值图像的安全通信。

本文的研究对象仅限于二值图像，但是本文采用的研究方法可以推广到其它类型的多媒体类型(如 JPEG 和 MPEG 标准)，这是我们下一步的研究内容。

参 考 文 献

[1] Lian Shiguo. Multimedia Content Encryption–Techniques and Apllications. Boca Raton,Florida: CRC Press, 2008, Chapter 1.

[2] 陈帅, 钟先信, 石军锋, 朱士永. 基于离散数字混沌序列的图像加密. 电子与信息学报, 2007, 29(4): 898–900.
Chen S, Zhong X X, Shi J F, and Zhu S Y. Image encryption through discrete digital chaotic sequence. *Journal of Electronics & Information Technology*, 2007, 29(4): 898–900.

[3] Zeng W and Lei S. Efficient frequency domain selective scrambling of digital video. *IEEE Transactions on Multimedia*, 2003, 5(1): 118–129.

[4] Grangetto M, Magli E, and Olmo G. Multimedia selective encryption by means of randomized arithmetic coding. *IEEE Transactions on Multimedia*, 2006, 8(5): 905–917.

[5] Hunter R and Robinson A H. International digital facsimile coding standards. *Proceedings of IEEE*, 1980, 68(7): 854–867.

[6] Gonzalez C and Woods E. Digital Image Processing. 2nd Edition, Prentice Hall, Englewood Cliffs, 2002, Chapter 8.

[7] University of Southern California. The USC-SIPI image database: version 5, http://sipi.usc.edu/database, 2008.

周 庆： 男，1979 年生，博士，讲师，CCF 会员，研究领域为多媒体信息安全技术.

廖晓峰： 男，1964 年生，博士，教授，主要研究领域为信息安全与计算智能技术.

胡 月： 女，1979 年生，博士，讲师，研究领域为密码学技术.