基于混沌映射的压缩图像加密算法

邱 劲[1,2] 王 平[2]
(重庆大学计算机学院 重庆 400044)[1] (西南大学计算机与信息科学学院 重庆 400715)[2]

摘 要 在分析现有DCT系数加密算法安全性的基础上,提出了一个空域加密和频域加密相结合的JPEG压缩图像加密算法。理论分析与计算机仿真实验表明,该算法具有很好的加密效果,对压缩算法的压缩效率影响很小,能充分满足压缩图像加密算法的要求。

关键词 图像加密,混沌映射,密码学
中图法分类号 TN918 **文献标识码** A

Encryption Algorithm for Compressed Image Based on Chaotic Maps

QIU Jing[1,2] WANG Ping[2]
(College of Computer Science, University of Chonqing, Chongqing 400044, China)[1]
(College of Computer and Information Science, Southwest University, Chongqing 400715, China)[2]

Abstract We proposed an encryption scheme for the compressed image. In the scheme, the image data is first encrypted in space domain and then is encrypted in frequency domain. The proposed scheme can not only achieve high security but also guarantee the efficiency of the compression algorithm.

Keywords Image encryption, Chaotic map, Cryptography

1 引言

随着Internet的日益普及和广泛应用,越来越多的多媒体数据通过网络传输。多媒体数据对网络的带宽有很高的要求,而在网络中传输多媒体数据时,一般采用各种压缩算法来减轻其对带宽的要求。当使用加密算法对通过网络传输的多媒体数据加密时,不仅要考虑安全性,还需考虑多媒体数据的格式兼容性、对压缩效率的影响等问题。

加密算法可以分别使用在图像压缩编码前、图像压缩编码后或压缩算法中。根据加密算法的使用位置,可以将针对压缩图像的加密算法分为独立于压缩的加密算法和压缩加密联合算法[1]。在图像压缩编码前或图像压缩编码后,对图像加密的算法称为独立于压缩的加密算法。将加密算法和压缩算法相结合的方式称为压缩加密联合算法。如果在压缩编码前加密图像数据,由于加密后的数据几乎不存在冗余,因此图像的压缩效率会受到很大的影响。此外,如果采用有损压缩算法,将导致在解密时遇到困难。由于图像压缩编码后具有一定的编码结构和语法,因此采用在图像压缩编码后加密的方式可能会导致数据格式的兼容性问题。近年来,研究人员提出了许多针对JPEG图像的压缩加密联合算法。在这类算法中,主要是针对量化后的DCT系数和熵编码加密[2-4]。Zigzag置乱算法和符号位随机改动算法是两种比较典型的DCT系数加密算法。

文献[5]指出Zigzag置乱算法对压缩算法的效率影响很大,恶劣情况下可以导致加密后的文件增加46%左右。算法中使用的置乱操作不能抵抗已知明文攻击和选择明文攻击。在文献[3]中,提出一种随机改动DCT系数符号位的加密方法。该方法实现简单,也不会影响压缩算法的压缩效率。但研究表明,这种方法是不安全的,攻击者只需要将DC系数置为某个常量,然后将AC系数全部改为正值就可以重构原图的细节[6]。

在DCT系数中,DC系数代表了图像的平均亮度,而在AC系数中含有图像纹理、边缘信息以及图像的一些细节。为了防止图像细节的泄漏,对AC系数的加密显得尤为重要。AC系数的取值集中在[-1,1]之间,并且高频AC系数趋于零,当使用伪随机序列对其进行掩盖或使用置乱算法对其置乱时,对压缩算法的压缩效率有很大的影响。此外,由于JPEG子块间具有很强的相关性,在一个8×8子块内的加密操作并不能很好地破坏子块间的相关性,因此需要把在空域上的加密算法和频域上的加密算法相结合,才能达到满意的加密效果。

根据上面的分析和研究,将空域加密算法和频域加密算法相结合,提出一种JPEG灰度图像加密算法。在空域上,使用基于猫映射的置乱算法将明文图像按块的方式进行置乱,块的大小和JPEG子块大小相同。在频域上,根据伪随机序列修改DCT系数的符号位。此外,使用取值为1和-1的伪随机序列对非零AC系数进行掩盖。理论分析与计算机仿真实验表明,算法具有很好的加密效果,对压缩算法的压缩效率影响很小,能充分满足压缩图像加密算法的要求。

2 JPEG压缩图像加密算法

明文图像置乱

到稿日期:2011-08-13 返修日期:2011-11-10
邱 劲 博士生,主要研究方向为信息安全;王 平 博士,主要研究方向为语义网。

将明文图像按 8×8 方式分成 $N\times N$ 个子块。使用基于猫映射的置乱算法对 $N\times N$ 个子块的位置重新排列。子块的新位置计算如下：

$$\begin{pmatrix} i' \\ j' \end{pmatrix}=\begin{pmatrix} 1 & b \\ a & ab+1 \end{pmatrix}^{M}\begin{pmatrix} i \\ j \end{pmatrix} \bmod N-1 \quad (1)$$

式中，(i,j)为子块的编号，$0\leqslant i,j\leqslant N-1$。控制参数 a,b 和迭代次数 M 为密钥。如果 a,b 满足 $ab=2N-4$，则式(1)的周期 $T=2N$[7]。

DCT 系数加密

①使用伪随机序列发生器生成二进制随机序列 $b_1,b_2,\cdots,b_n$，对每个 JPEG 子块中的 DC 系数和 AC 系数，按如下规则修改其符号位。

$$d=d\times(-1)^{b_i} \quad (2)$$

②使用伪随机序列发生器生成二进制随机序列 $s_1,s_2,\cdots,s_n$，对所有非零系数 AC，按如下方式变更。

$$ac_i=ac_i+2\times s_i-1 \quad (3)$$

解密算法与加密算法原理相同，是加密过程的逆运算。

DCT 系数解密

①使用与加密过程相同的密钥生成二进制伪随机序列，对每个 JPEG 子块中的 DC 系数和 AC 系数，使用与加密过程相同的规则修改其符号位。

②生成与加密过程相同的二进制伪随机序列 $s_1,s_2,\cdots,s_n$，对所有非零系数 AC，按如下方式处理。

$$ac_i=ac_i-(2\times s_i-1) \quad (4)$$

明文图像恢复

根据控制参数 a,b 和迭代次数 M，使用猫映射的逆运算恢复各子块的位置，从而恢复明文图像。

3 性能分析

3.1 安全性分析

与数字图像相关的一类特定攻击手段称为感知攻击(perceptual attack)，即攻击者不需要解密全部图像数据，仅仅通过图像泄露出的一些信息就能够理解图像的内容。针对 JPEG 图像加密算法，典型的攻击方法是提取 DC 系数或 AC 系数来重构图像[6]。例如，将所有 DC 系数置为某个常数，仅使用 AC 系数就能观察到图像的细节，如图 1 所示。因此，为了掩盖图像细节的泄露，很多加密算法对 AC 系数使用伪随机序列掩盖和位置置乱的加密方式。AC 系数的分布类似于拉普拉斯分布[8]，如图 2 所示。其中大部分值集中在以 0 为中心的区域内，且在一个 JPEG 子块中，不为零的 AC 系数几乎集中在 AC 系数序列的前半部分。上述两点给攻击者提供了很好的线索，他们可以通过将 AC 系数的前若干位置为 1 的方式来观察图像的情况。造成上述 AC 系数加密困难的原因是图像像素之间存在很强的相关性，这种相关性即使在 JPEG 的子块之间也存在，这是 JPEG 能够压缩图像的基础所在。因此，在一个 JPEG 子块内的置乱操作不足以破坏这种相关性，从而造成图像信息的泄漏。

在我们提出的加密方案中，首先在空域上使用置乱算法来破坏块间的相关性。考虑到对压缩算法的影响，在空域上的置乱是采用基于 8×8 的块置乱，在频域上，通过对符号位的随机改动来增强算法的安全性。当加密后的图像的 DC 系数被置为某个常数后，加密图像 AC 系数呈现图 3 所示的效果。通过对比图 1 和图 3 可以观察到加密图像没有泄漏图像的细节信息。针对 AC 系数的分布特点，使用值为 1 和−1 的伪随机序列对非零 AC 系数进行加密，以模糊图像的细节。

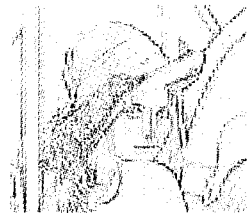

图 1 lena 图 AC 系数效果

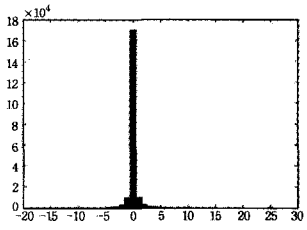

图 2 bridge 图 AC 系数的直方图

另一种常见攻击方式是单独提取 DC 系数来重构图像。图 4 是提取加密后的 lena 图的 DC 系数重构的图像。可以观察到，该图不能获得关于明文图像内容的相关信息。

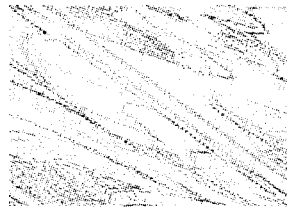

图 3 加密后 lena 图 AC 系数效果

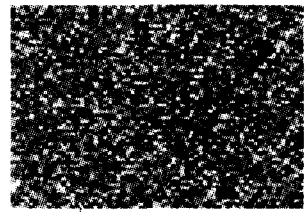

图 4 加密后 lena 图 DC 系数效果

对不同图像的加密结果如图 5 所示。可以看到，经过加密的图像基本无法辨认，达到了很好的加密效果。

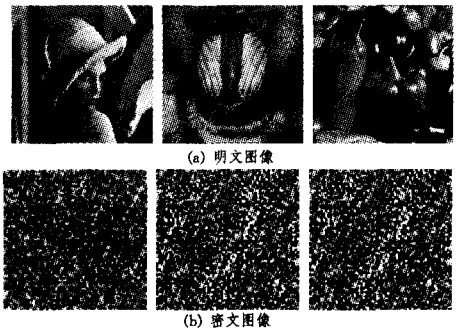

图 5 明文图像和密文图像

3.2 加密算法对压缩率的影响

我们提出的加密算法主要由 3 个操作构成：在空域上的置乱操作、在频域上的符号位随机改动操作以及对非零系数 AC 的加密操作。JPEG 的编码方式决定了对符号位的改动不影响压缩算法的效率。加密算法对压缩效率的影响主要是在空域上的置乱操作和对非零系数 AC 的加密操作。由于采用与 JPEG 相同的分块方式，并且以块为单位做置乱变化，因此与未置乱图像相比，DCT 系数没有变化。但 DC 系数采用差分编码方式，当置乱操作改变了块之间的相关性时，差值会增加，从而增加编码的长度。当使用值为 1 和−1 的伪随机序列对非零 AC 系数加密时，可能会增加 AC 编码的长度，但这种增长是在可控的范围内。另一方面，这种操作也存在减小编码长度的可能。例如，操作将最后一个非零系数 AC 去掉或将系数 AC 的值向 0 点靠拢。加密后图像的增长率如表 1 所列。可以看到，加密后图像的增长率在可接受的范围内。

表 1　压缩图像以及加密压缩图像大小

图像名称	原始图像大小(kB)	不加密压缩图像大小(kB)	加密压缩图像大小(kB)	加密后图像增长率(%)
Lena	256	20.8	21.8	4.8
Baboon	256	45	46.3	2.8
Peppers	256	21.3	22.8	3.2
cameraman	256	18.6	20.5	10.2
Jetplane	256	22	24	9.1
crowd	256	28.4	29.6	4.2
bridge	256	40.6	41.9	3.2
lake	256	28.4	29.9	5.3
portofino	256	23.6	25.5	8.1
boats	256	24	25.7	7.1

3.3　格式兼容型

使用 JPEG 压缩算法生成的文件具有标准的语法结构，以便解码器能正确理解图像数据。错误的语法结构可能会导致解码器的崩溃，因此加密后的数据最好能保持压缩文件的特有语法格式。JPEG 文件由图像开始 SOI(Start of Image)标记、APP0 标记(Marker)、APPn 标记(Markers)等 8 个部分组成。在我们提出的算法中，只针对图像数据加密，没有修改 JPEG 文件的数据头和标记信息，因而具有格式兼容性。

3.4　加密速度

加密算法主要包括 3 个部分，即 DC 系数、AC 系数的加密和在空域上的置乱操作。对于 AC 系数和 DC 系数的加密只涉及简单的加法、异或以及赋值运算，因此加密速度非常快。此外 AC 系数的个数一般在图像像素个数的 5%～15%以下，DC 系数和块置乱各占 1/64，因此总的加密量只占图像像素个数的 8%～18%。

结束语　在分析现有的 DCT 系数加密算法安全性的基础上，提出了一个空域加密和频域加密相结合的 JPEG 压缩图像加密算法。理论分析与计算机仿真实验表明，算法具有很好的加密效果，对压缩算法的压缩效率影响很小，能充分满足压缩图像加密算法的要求。

参 考 文 献

[1] Liu F W, Koenig H. A survey of video encryption algorithms [J]. Computers & Security, 2010, 29(1): 3-15

[2] Tang L. Methods for encrypting and decrypting MPEG video data efficiently[C]// Proceedings of the fourth ACM international on multimedia. 1996: 219-229

[3] Shi C, Bhargava B. A Fast MPEG Video Encryption Algorithm [C]// Proc. of ACM Multimedia'98. 1998: 81-88

[4] Xie D, Kuo C-C J. Multimedia encryption with joint randomized entropy coding and rotation in partitioned bitstream[J]. EURASIP Journal on Information Security January, 2007, 2007(1): 1-12

[5] Qiao L T, Klara N. Comparison of MPEG encryption algorithm [J]. Comput & Graphics, 1988, 22(4): 437-448

[6] Wu C, Kuo C. Design of integrated multimedia compression and encryption systems [J]. IEEE Transactions on Multimedia, 2005, 7(5): 828-39

[7] Chen Fei, Liao Xiao-feng, et al. Period Distribution Analysis of Matrix Transformations[C]// Submitted to Signal Processing. 2011

[8] Lam E Y, Goodman J W. A Mathematical Analysis of the DCT Coefficient Distributions for Images [J]. IEEE Trans. on Image Processing, 2000, 9(10): 1661-1666

[9] 何波，罗龙艳，肖迪. 迭代混沌映射的 S 盒构造方法[J]. 重庆邮电大学学报：自然科学版，2010，22(1)：89-93

(上接第 15 页)

[54] Lu H, Plataniotics K N, Venetsanopoulos A N. Boosting discriminate learners for gait recognition using MPCA features[J]. EURASIP J. Image and Video Processing, 2009, 11

[55] Kellokumpu V, et al. Dynamic textures for human movement recognition[C]//CIVR 2010. Xi'an, 2010: 470-476

[56] Wang L, Tan T, Ning H, et al. Fusion of static and dynamic body biometrics for gait recognition[J]. IEEE Transactions on Circuits and Systems for Video, 2004, 14(12): 149-158

[57] Bazin A, Nixon M. Probabilistic combination of static and dynamic gait features for verification[C]// Proc. BTHI2005 Conf. Orlando, Apr. 2005: 23-30

[58] Veres G V, Gordon L, Carter J N, et al. What image information is important in silhouette-based gait recognition [C] // Proc. CSCCVPR. Washington DC, 2004: 776-782

[59] Wagg D K, Nixon M S. Automated markless extraction of walking people using deformable contour models[J]. Computer Animation and Virtual Worlds, 2004, 15(3): 399-406

[60] Nandini C, RaviKumar C N. An approach to gait recognition[C]// Biometrics and Security Technologies. 2008: 1-3

[61] Shakhnarovich G, Darrell T. On probabilistic combination of face and gait cues for identification[C]// Proc. Int. Conf. Automatic Face and Gesture Recognition. 2002: 169-174

[62] Kale A, et al. Fusion of gait and face for human identification [C] // Proc. Int. Conf. Acoustics, Speech, and Signal Processing. 2004

[63] Geng X, et al. Adaptive fusion of gait and face for human identification in video[C]// IEEE Workshop on Applications of Computer Vision. 2008: 1-6

[64] Kusakunniran W, et al. Multiple views gait recognition using view transformation model based on optimized gait energy image[C]// ICCV Workshops. 2009: 1058-1064

[65] Kusakunniran W, et al. Cross-view and multi-view gait recognitions based on view transformation model using multi-layer perceptron[Z]. Pattern recognition letters. doi: 10. 1016/j. patrec. 2011, 4: 14

[66] Liu N, Lu J, Tan Y P. Joint subspace learning for view-invariant gait recognition [J]. IEEE Signal Processing Letters, 2011, 18 (7): 431-434

[67] BenAbdelkader C, Davis L. Detection of people carrying objects: a motion-based recognition approach[C]// Proc. Int. Conf. Automatic Face and Gesture Recognition. 2002: 378-383

[68] Lee H, Hong S, Kim E. An efficient gait recognition with backpack removal[C]// EURASIP J. Advances in Signal Processing. 2009: 1-7

[69] http://www.cbsr.ia.ac.cn/china/Gait%20Databases%20CH.asp