

结合混沌的小波变换数字水印技术

李明 廖晓峰

(重庆大学计算机学院 重庆 400044)

摘要 本文结合了混沌系统与小波变换实现了数字图像水印的嵌入。利用混沌系统产生的混沌序列对灰度水印图像进行调制,置乱;对待处理图像进行多级小波分解,将调制置乱后的水印按位拆分为八个二值平面,分别嵌入各层的小波系数中,从而实现水印鲁棒性和不可见性的较好结合。

关键词 混沌,小波变换,数字水印

A New Method for Digital Watermarking of Wavelet Transform Combined Chaos

LI Ming LIAO Xiao-Feng

(College of Computer, Chongqing University, Chongqing 400044)

Abstract This paper realizes embedded watermarking which is consisted of chaotic system and wavelet transform. This method is composed of two steps. First use chaotic sequence to modulate and disorder grayed watermark. Second, decompose the image by wavelet transform, then dismantle the watermark and embed into the parameter of wavelet. So the robustness and invisibility of watermarking realized.

Keywords Chaos, Wavelet transform, Digital watermarking

数字水印技术^[1]是用来解决数字多媒体中版权问题和内容认证的主要工具。关于数字图像的水印技术^[2~5]是当前数字水印技术的主要研究内容。一般情况下数字图像水印应满足两方面要求:1. 加入水印不应导致原图过多失真,水印应不可见。2. 水印应具有鲁棒性,能够抵御一定的破坏。良好的水印技术应尽量地实现鲁棒性(Robustness)和不可见性的结合。小波是 MPEG-4 及 JPEG-2000 压缩标准^[6]的核心技术,基于小波域的水印算法^[7,8]可以防止由于 JPEG-2000 有损压缩而造成水印消除;可以利用信源编码领域对图像失真的可见性研究成果来控制水印的嵌入位置和强度;可以实现压缩域直接嵌入水印。此外,利用小波多分辨率分析可以更好地控制水印在宿主中的分布,更好地解决鲁棒性和可见性之间的矛盾。而混沌系统则具有对初值的敏感性和良好的伪随机性,混沌系统所产生的混沌序列可用来对水印图像进行调制、置乱,从而加强了水印的随机性和安全性,并具有一定的抗破坏能力。

本文结合混沌系统,利用小波变换实现了灰度数字图像水印的嵌入。灰度图像比二值图像具有更大的信息量,其可辨识性也优于二值图像,因此具有更大的实际意义。本文的第 1 部分介绍所选取的混沌系统,并利用混沌系统产生混沌序列对水印图像进行调制、置乱。第 2 部分对原始图像进行多层小波分解,并实现水印的嵌入。第 3 部分进行嵌入后水印的提取,并进行抗攻击测试。最后是对全文的总结。

1 原始水印的处理

1.1 混沌系统

混沌现象是非线性确定系统中的一种类似随机的过程,把两个十分相近的初值代入同一个混沌函数进行迭代运算,经过一定阶段的运算后,数值序列变得毫不相关。它隶属于

确定性系统却难于预测,隐含于复杂系统却又不可分解,看似混乱无序,实则颇有规律。混沌系统具有高度不可预测性,看似随机性,对初始条件和参数敏感等特点。

目前广泛研究的一维混沌系统是 Logistic 映射,即

$$x_{k+1} = \mu x_k (1 - x_k) \quad (1)$$

其中, $0 \leq \mu \leq 4$ 是分支参数, $x_k \in (0, 1)$ 。当 $3.5699456 \dots < \mu \leq 4$ 时,该系统处于混沌状态。Logistic 映射的另一种形式为

$$x_{k+1} = 1 - \mu x_k^2 \quad (2)$$

其中, $\lambda \in [0, 2]$, $x_k \in (-1, 1)$, 当 $1.40115 < \lambda < 2$ 时系统处于混沌状态。本文即采取(2)式的混沌系统。该系统具有计算简单,混沌性好等特点。

1.2 水印图像的调制,置乱

我们选择嵌入的原始水印图像为 64×64 的 8 位 256 阶灰度图。对于(2)式的混沌系统,我们可以任选符合条件的初值和参数。如选取 $x_0 = 0.873624$, $\mu = 1.9$, 生成 64×64 长度的混沌伪随机序列。对其舍弃小数点后 4 位以前的数字,形成新的浮点序列,其分布范围应在 $0.000 \dots$ 到 $0.999 \dots$ 之间,对其乘以 256, 向下取整,即得到灰度分布在 0 到 255 之间的灰度图像,其可采用异或的方式作用于原始水印图像,得到调制的水印图像。

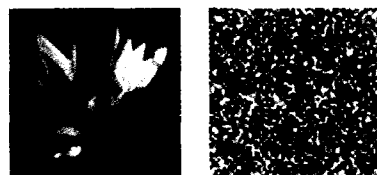


图 1. 原始水印和调制后的水印

再取不同的初值和系数,和上述类似的方法生成多个 $64 \times 64 \times 2$ 大小的置乱矩阵(与上面不同的是值分布在 1 到

64 间,即乘以 64 向下取整后加 1),利用得到的置乱矩阵对调制后的水印进行置乱,设水印为 $Mark(64 \times 64)$,一个置乱矩阵为 $Matrix(64 \times 64 \times 2)$,则 $Mark(i, j)$ 与 $Mark((Matrix(i, j, 1), Matrix(i, j, 2)))$ 对换。经过数轮置换可得到充分置乱后的水印。

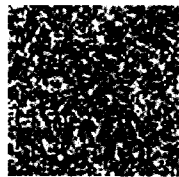


图 2 置乱后的水印

2 水印嵌入方案

2.1 原始图像的小波分解

选取的原始图像为 512×512 的 8 位灰度 lena 图,如图 3 所示。



图 3 原始图像

设原图为 $lena(512 \times 512)$,将原图各像素点的 0 到 255 间的灰度整数转化为 0 到 1 之间的浮点数,即 $lena(i, j) = lena(i, j) / 255$,以便于进行小波变换。本文中采用小波基 db1 对 lena 图进行三级二维小波变换分解^[9],每层产生 4 组的小波系数,即:逼近信号 cA,水平细节信号 cH,垂直细节信号 cV,对角细节信号 cD。其中 cD 即是我们选择进行水印嵌入的区域,各层的 cD 信号分别为 cD1 (256×256)、cD2 (128×128)、cD3 (64×64)。

2.2 水印的嵌入

我们按位将调制置乱后的水印图像按位拆分为 8 个 2 值平面图。其总的信息量为 $64 \times 64 \times 8 \text{ byte}$ 。通常嵌入较高层小波系数的水印抗破坏能力强,但越高层其系数个数越少,所能嵌入的信息也越少,故而我们将高位信息嵌入到较高的层上,低位信息镶嵌到较低的层上,即最高的第 8 位嵌入到 cD3,第 7、6、5、4 位嵌入到 cD2,第 3、2、1 位嵌入到 cD1。

通常使用伪随机序列决定水印的嵌入位置,但是有可能出现嵌入同一个点的情况,故而一般要记录嵌入的位置,或做标记以防止重复嵌入。本文则采取混沌序列置乱系数矩阵然后顺序嵌入水印再还原置乱的矩阵的方法,具体置乱方法与上文提到的图像置乱方法一致。

水印具体嵌入操作为保留嵌入位置的小波系数到小数点后 1 位,1 位以后舍弃,若要嵌入的 2 值信息为 0 则减去 0.025,为 1 则加上 0.025。在提取时则对系数乘以 10,对其 4 舍 5 入,若 4 舍 5 入后的结果小于系数值则认为该位为 0,否

则为 1。对系数进行嵌入修改后,还原置乱的系数矩阵,然后进行反变换重构,得到嵌入水印后的图像。



图 4 嵌入水印后的图像

3 水印的检测

3.1 水印的提取

对嵌入水印后的图像进行 3 层小波分解,根据置乱矩阵重排各层 cD 系数矩阵,提取嵌入的水印的各个位信息,进行置乱恢复,调制恢复,即得到提取出的水印图。



图 5 提取出的水印图

3.2 抗攻击测试



图 6 剪切



图 7 JPEG 压缩



图 8 中值滤波

结论 本文所提出的灰度水印镶嵌方式能够在基本不破坏原图视觉效果的情况下实现水印的嵌入, 嵌入的水印具有不可见性, 并能被较好地提取出来。而且对剪切、JPEG 压缩、滤波等操作有一定的抵抗能力, 有一定的实用价值。

参 考 文 献

- 1 Van Schyndel R G, et al. A digital watermark. In: Proc. of ICIP 94, 1994, 2: 86~89
- 2 Tirkel A, Randkin G, Vanschyndel R, Ho W, et al. Electronics watermark. In: Proceedings DICTA 1993, December 1993. 666~

- 3 Bender W, Gruhl D, Morimoto N. Techniques for data hiding. In: Proceedings of the SPIE, Storage and Retrieval for Image and Video Databases III, Vol. 2420, San Jose, CA, Feb. 1995. The Society for imaging Science and Technology and SPIE, The International Society for optical Engineering, SPIE
- 4 Koch E, Zhao J. Towards robust and hidden image copyright labeling. In: IEEE workshop on Nonlinear Signal and Image Processing, Neos Marouaras, Greece, June 1995. 123~132
- 5 Cox I. J, Killian J, Leighton F T, et al. Secure Spread Spectrum Watermarking for multimedia. IEEE Trans. On Image Processing, 1997, 6(12): 1673~1687
- 6 International Organization for Standardization. Information Technology-JPEG 2000 Image Coding System, ISO/IEC 15444, July 2002
- 7 Kundur D, Hatainakos D. A robust digital image watermarking method using wavelet-based fusion. In: Proc. of ICIP 97, 1997, 1: 544~547
- 8 Xia X G, Boncelet C G, Arce C R. Wavelet transform based watermark for digital images. OPTICS EXPRESS, 1998, 3(12): 497~1998
- 9 孙兆林编著. Matlab6. x 图像处理. 清华大学出版社

(上接第 218 页)

- 2 Freeman H. Computer processing of line-drawing images. Computing Surveys, 1974, 6(1): 57~97
- 3 <http://202.119.109.14/jpkc/jiaoan/Chinese/kjsjgg.htm>
- 4 Zahn C T, Roskies R Z. Fourier Descriptors for Plane Closed Curves. IEEE Trans on Computers, 1972, 21(3): 269~281
- 5 Rauber T W. Two-dimension Shape Description; [Tech Rep]. Gruninova-RT-10-94. Universidade Nova de Lisboa, Lisboa, Portugal, 1994
- 6 Rui Y, She A C, Huang T S. A Modified Fourier Descriptor for Shape Matching in MARS. In: Chang S K, ed. Image Databases and Multimedia Search, Series on Software Engineering and Knowledge Engineering, World Scientific Publishing House in Singapore, 1998, 8: 165~180
- 7 Mokhtarian F, Abbasi S, Kittler J. Robust and Efficient Shape Indexing through Curvature Scale Space. In: Proc. British Machine Vision Conference, 1996. 53~62

- 8 Zibreira C, Pereira F. A study of similarity measures for a turning angles-based shape descriptor. In: Proc. Conf. on Telecommunications - ConfTele, Figueira da Foz-Portugal, April 2001
- 9 Kim W Y, Kim Y S. A region-based shape descriptor using Zernike moments. Signal Processing: Image Communication, 2000, 16(1-2): 95~102
- 10 Kim H K, Kim J D. Region-based shape descriptor invariant to rotation, scale and translation. Signal Processing: Image Communication, 2000, 16(1-2): 87~93
- 11 Hu M K. Visual pattern recognition by moment invariants. IRE Transactions on information theory, 1962, IT-8: 179~187
- 12 Khotanzad A, Hong Y H. Invariant Image Recognition by Zernike Moments. IEEE Trans on Pattern Analysis and Machine Intelligence, 1990, 12(5): 489~497
- 13 Chang S-F, Sikon T, Puri A. Overview of MPEG-7 standard. IEEE Trans Circuits and System for Video Technology, 2001, 11(6): 688~695

(上接第 228 页)

$\{x_{k+3}, x_k\} \leq (2n-7)/3$, 矛盾。
 当 $d(x) = (n-6)/3$ 时, $|N(x_{k+1})| \geq (2n-6)/3 - |N(x)| + |\{x_k\}| \geq (n+2)/3$, 其后 $|N(x_{j+1}) \cup N(x)| \leq |V(G)| - |N(x_{k+1}) \setminus \{x_{k-1}, x_k\}| - |\{x, x_{j+1}, x_{i+1}, x_{i+2}\}| \leq (2n-7)/3$, 矛盾。

子情况 3.2.2: $V(G_1) = \{x\}$

此时, 综合上面所有情况有 $(n-6)/3 \leq d(x) = 3 \leq (n-3)/3$, 有 $12 \leq d(x) \leq 15$ 。则 $\min\{|j-i|, |k-i|, |i-k|\} \leq 4$, 不妨认为 $|j-i| \leq 4$ 。当 $|j-i| \leq 3$ 时, 则易有更长圈, 矛盾。当 $|j-i| = 4$ 时, x_{i+2} 至多和 x_{i+1}, x_{k-1} 相邻, 从而 $|N(x) \cup N(x_{i+2})| \leq |\{x_i, x_j, x_k, x_{i+1}, x_{k-1}\}| = 5 \leq (2n-7)/3$, 矛盾。

至此, 完成定理的证明。

参 考 文 献

- 1 Swamy M N S, Thulasiraman K. 图论、网络与算法[M]. 北京: 高等教育出版社, 1988

- 2 Gould R J. Updating the Hamiltonian problem-A survey[J]. J. Graph Theory, 1991, 15(2): 121~157
- 3 赵克文, 柳柏濂. A neighborhood condition for ertives at distance two implying hamiltonicity[J]. Soochow Journal of Mathematics, 2006, 32(1): 171~177
- 4 Chen Guantao, Jacobson M S, Kézdy A E, et al. Tough enough chordal graphs are Hamiltonian[J]. Networks, 1998, 31(1): 29~38
- 5 Lai Hongjian, Yang Xiaofan, Evans D J, et al. Generalized honeycomb torus is Hamiltonian[J]. Inform. Process. Lett., 2004, 92(1): 31~37
- 6 Hsu H C, Li T K, Hsu L H, et al. Fault Hamiltonicity and Fault Hamiltonian Connectivity of the Arrangement Graphs[J]. IEEE Trans. on Computers, 2004, 53(1): 39~53
- 7 赵克文, Lai Hongjian, Shao Yehong. New sufficient condition for hamiltonian graphs[J]. Applied Mathematics Letters, (已接受, 见杂志网上的本文 [http://dx. doi. org/10.1016/j. aml. 2005. 10. 024](http://dx.doi.org/10.1016/j.aml.2005.10.024))
- 8 赵克文, Gould R J. A new sufficient condition for hamiltonian graphs[J]. Arkiv for matematik, 2006, 42(2): 299~308