

一个完全基于混沌的数字图像认证方案

雷正桥

(重庆工业职业技术学院 计算机系, 重庆 401120)

摘 要: 基于混沌特性提出了一个新颖的数字图像认证方案. 首先利用分段线性混沌映射, 基于图像的特征信息, 生成查询表和二维猫映射的参数; 再利用猫映射对原始水印图像进行置乱预处理; 最后根据查询表和置乱后的水印完成水印嵌入工作. 而水印的提取和认证操作极为简便. 理论分析和仿真试验表明该方案安全高效、定位精确, 且具有简单、可行性好的特点.

关键词: 混沌; 图像认证; 图像特征; 篡改定位

中图分类号: TN918; TP309

文献标识码: A

文章编号: 1000-7180(2011)12-0049-05

An Entire Chaos-based Scheme for Digital Image Authentication

LEI Zheng-qiao

(Department of Computer, Chongqing Industry Polytechnic College, Chongqing 401120, China)

Abstract: By analyzing the limitation of the traditional image authentication schemes, a novel scheme entirely based on chaos is proposed for digital image authentication. A piecewise linear chaotic map is utilized to generate the look up table (LUT) and the parameter of two-dimensional Cat chaotic map, which is based on the image feature. The Cat map is used to pre-permutate the original watermark with diffusion mechanism. On the foundation of LUT and the diffused watermark, the embedding can be completed. While the watermark extraction and authentication are very simple. The performance analysis and simulation demonstrate that the whole scheme is secure, efficient, and practicable, with simple structure and strong ability of tamper localization.

Key words: chaos; image authentication; image feature; tamper localization

1 引言

多媒体技术的高速发展, 既给人们带来了巨大方便, 同时也引出了新的问题. 借助工具软件, 人们可以非常方便地对数字图像进行任意的修改. 如何认证法律证据图像或医疗图像等细节敏感图像的安全性, 已经成为一个非常迫切的问题.

在传统密码学中有关于信息认证的研究, 其基本思路是创建并保存一段原始文件的消息摘要 MD; 如果后来该文件发生了任何修改, 由于新文件的消息摘要 MD1 将会和原来的摘要 MD 不同, 从而可以鉴别原文件是否被修改. 但是这种作法没有充分利用数字图像自身的特点, 必须将相关的摘要

和图像分开保存, 而且无法准确地定位出图像被篡改的部分. 在文献[1]中, 数字图像 0 到 255 的灰度值被一个二值函数转换为 0 或 1, 水印是一个二维标识, 嵌入脆弱水印的过程就是通过修改图像的像素灰度使其对应的转换值与水印中相应的比特相同来实现的, 该方案具有良好的局部检测性能, 可以把认证过程具体到每一个像素. 但是该方案存在安全缺陷, 文献[2]对此做了详细分析.

混沌密码技术是现代密码学发展的一个重要成果, 已经成为当前信息安全领域的一个研究热点. 本文将数字混沌和数字水印技术结合应用到数字图像的实际认证活动中. 我们在文献[1-2]的基础上, 充分利用混沌的特性, 设计了一个安全高效、定位精确

的数字图像认证方案。

2 预备知识

2.1 混沌应用于信息安全领域的理论基础

混沌,作为一种普遍存在的复杂运动形式和自然现象,是在非线性动力系统中出现的一种确定性的、看起来毫无规律的类似随机过程。之所以混沌能被应用于信息安全领域,其理论基础包括:混沌系统对初始状态非常敏感;混沌系统是自相似的,它局部选取的混沌形态将和整体完全相似;混沌系统的动力学行为非常复杂,无法用概率统计的原理描述,也难以预测和重构;混沌系统具有遍历的特性;混沌的迭代过程是单向的,它每次迭代都会产生完全不同的结果,而对于同一个混沌系统,当其系统初始值和系统初始参数相同,则一定会得到完全一样的两个迭代序列;另外,具有确定性的混沌系统也易于用计算机来仿真实现。混沌系统具备的众多优秀性质,决定了它在信息安全领域广阔的应用前景^[3]。

2.2 基于混沌映射设计散列函数的可行性

散列函数是一种特殊的单向函数,包括两类:带秘密密钥的散列函数和不带密钥的散列函数。不带密钥的散列函数也可被看作是仅有一个密钥的散列函数。

带密钥散列函数的定义如下:K-Hash 函数 $H(\cdot)$ 是一个散列函数族 $\{h_k: k \in K\}$, 对任意 $k \in K$, $h_k(M): \sum \rightarrow V_m$ 实现了消息集合 $\sum$ 中的任意长度的消息 M 被映射为长为 m 的消息摘要 $h_k(M)$, 如果:

(1) $h_k(M)$ 是密钥单向函数,即

① 如果 $k \in K$ 和 $M \in \sum$ 被给定, $h_k(M)$ 容易获得;

② 如果未知 k , 即使 $h_k(M)$ 被给定, M 也很难求出;

③ 如果未知 k , 即使 M 被给定, $h_k(M)$ 的求解也很困难。

(2) $h_k(M)$ 是抗密钥碰撞的函数,即:如果未知密钥 k , 希望得出 $M, M' \in \sum$, 满足 $M \neq M'$ 且 $h_k(M) = h_k(M')$, 将是困难的。

混沌序列,天生具有散列函数所要求的单向性,而且它的混乱和扩散性能良好,对密钥也非常敏感,因此,基于混沌映射设计出性能优秀的 Hash 函数是完全可能的。本文借鉴文献^[4]提出的基于变参数混沌映射构造单向 Hash 函数构造的思想,利用

混沌映射对图像的特征块进行“类散列”处理。

一维分段线性混沌映射定义为

$$X(t+1) = F_P(X(t)) =$$

$$\begin{cases} X(t)/P, 0 \leq X(t) < P \\ (X(t)-P)/(0.5-P), P \leq X(t) < 0.5 \\ (1-X(t)-P)/(0.5-P), \\ 0.5 \leq X(t) < 1-P \\ (1-X(t))/P, 1-P \leq X(t) \leq 1 \end{cases} \quad (1)$$

式中, $X \in [0, 1]$, $P \in (0, 0.5)$ 。该迭代系统是混沌的,其输出序列 $\{X(t)\}$ 在 $[0, 1]$ 上遍历,且具有良好的自相关特性呈 δ 形态。系统的不变分布函数 $f^*(x) = 1$, 可知系统在 $[0, 1]$ 上均匀分布。以上特性为构造单向 Hash 函数提供了有利的条件。

2.3 利用二维猫映射实现数字图像的高效置乱

文献^[5-6]提出对于图像信息加密需要重新设计一类适合其数据特点的算法,并利用 Baker 映射、标准映射和猫映射等复杂混沌系统实现了对数字图像的有效加密。本文借鉴这种思想,利用广义猫映射完成原始水印图像的位置置乱预处理。

二维猫映射定义为

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1 = C \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1 \quad (2)$$

猫映射除了具备混沌的一般属性,还有一些更重要的特性:行列式 $|C| = 1$, 表明它是一个没有吸引子且保面积的映射;而且,它还是一个一一映射,矩阵内的每一点将被唯一地变换到矩阵内的另一点。将猫映射作以下推广就成为广义猫映射:首先将相空间推广为 $\{0, 1, 2, \dots, N-1\}$;将方程推广为最一般的二维保面积方程:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N = C \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N \quad (3)$$

式中, a, b, c, d 为正整数,其保面积的性质要求 $|C| = ad - bc = 1$ 。由于广义猫映射系统中的系数都是整数,所以能很方便地利用它对图像进行处理。

3 方案设计

3.1 方案描述

Yeung-Mintzer 原始方案^[1]:首先,在密钥的控制下,一个查询表 LUT 被生成,该密钥与图像是没有关系的。一旦查询表生成,就相当于一个二值转换函数 $f: \{0, 1, \dots, 255\} \rightarrow \{0, 1\}$, 可以实现将图像的灰度值 0 到 255 转换为 0 或 1 的值。待嵌入的水印

b 是一个和原图大小相同的二值图像,在水印嵌入过程中,利用查询表 LUT 来控制图像像素值 $I(i, j)$ 的修改,使得修改后的图像灰度值 $I(i, j)'$ 在查找表中的映射值正好等于二值水印图像,即: $b(i, j) = f(I(i, j)')$ 。但是,下面的攻击方法可以攻破这个方案:(1) 水印 b 和转换函数 f 被估计出来:因为对于每一幅已嵌入水印的图像,其特定的位置 (i, j) 将一定对应相同的水印标识比特 $b(i, j)$,如果攻击者掌握了足够多的已嵌入水印图像,就完全可以确定出查询表 LUT 和映射函数,从而可以估计出水印 b 。(2) 拼贴攻击:如果攻击者获得了足够多的已嵌入水印图像,通过测试这些图像可以获得一组图像局部块,这些块可以通过认证,而攻击者如果将这些图像的局部块拼贴起来,并保持其在图像中的位置不变,就可以伪造出新的嵌入水印的图像,而该伪造图像可通过认证。

经过分析,我们认为这两种攻击之所以可以成功,关键是因为即使是不同的嵌入水印图像,它们在图像的固定位置上嵌入的信息是相同的,改进的思路是必须使局部位置的嵌入信息随图像的不同而改变。

我们的方案:在图像中选取重要的局部像素块作为其图像特征,不失一般性,本文选取位于图像中间的 8×8 的局部块 $\{I_n, n = 1, \dots, N\}$,共 $N = 64$ 个像素。在一些特殊应用中,还可以根据需要选用其他图像特征。秘密取定分段线性混沌映射的初值 X_0 、 $H_0 \in [0, 1]$ 作为密钥 K 。在算法中引入了 CBC 模式,在迭代过程中根据上一次的迭代值和不同位置的图像灰度值来动态确定混沌方程的参数 P ;通过 $1^{st} \sim N^{th}$ 、 $(N+1)^{th} \sim 2N^{th}$ 、 $(2N+1)^{th} \sim 3N^{th}$ 和 $(3N+1)^{th} \sim 4N^{th}$ 这 4 个单元共 256 次迭代,使得最终迭代值与图像特征的所有像素紧密相关。算法具体描述如下:

(1) 依次将待处理图像特征块的灰度值线性变换为 $0 \sim 1$ 之间的数。这样整个特征块将得到一个大数组,记为 C ,数组长度即特征块的像素数 $N = 64$ 。

(2) 分段线性混沌映射的迭代过程如下:

1^{st} : $P_1 = (C_1 + H_0)/4 \in [0, 0.5)$, $X_1 = F_{P_1}(X_0) \in [0, 1]$;

$2^{nd} \sim N^{th}$: $P_i = (C_i + X_{i-1})/4 \in [0, 0.5)$, $X_i = F_{P_i}(X_{i-1}) \in [0, 1]$;

$(N+1)^{th}$: $P_{N+1} = (C_N + X_N)/4 \in [0, 0.5)$, $X_{N+1} = F_{P_{N+1}}(X_N) \in [0, 1]$;

$(N+2)^{th} \sim 2N^{th}$: $P_i = (C_{(2N-i+1)} + X_{i-1})/4 \in [0, 0.5)$, $X_i = F_{P_i}(X_{i-1}) \in [0, 1]$;

$(2N+1)^{th}$: $P_{2N+1} = (C_1 + H_0)/4 \in [0, 0.5)$, $X_i = F_{P_{2N+1}}(X_{i-1}) \in [0, 1]$;

$(2N+2)^{th} \sim 3N^{th}$: $P_i = (C_{(i-2N)} + X_{i-1})/4 \in [0, 0.5)$, $X_i = F_{P_i}(X_{i-1}) \in [0, 1]$;

$(3N+1)^{th}$: $P_{3N+1} = (C_N + X_{3N})/4 \in [0, 0.5)$, $X_{3N+1} = F_{P_{3N+1}}(X_N) \in [0, 1]$;

$(3N+2)^{th} \sim 4N^{th}$: $P_i = (C_{(4N-i+1)} + X_{i-1})/4 \in [0, 0.5)$, $X_i = F_{P_i}(X_{i-1}) \in [0, 1]$ 。

(3) 将迭代结果序列 $X_n \{n = 1, \dots, 4N\}$ 按下式转化为查询表 $LUT(n) \{n = 1, \dots, 4N\}$;取出 X_{4N} 经线性变换转化为二进制数后,直接从小数部分中抽取 18 bit,作为下一步猫映射所需的参数。

$$LUT(i) = \begin{cases} 0, & X_i \in [0.25, 0.75] \\ 1, & X_i \in [0, 0.25) \cup (0.75, 1] \end{cases} \quad (4)$$

(4) 用猫映射对原始水印 b 进行位置置乱预处理成为待嵌入水印 bb :

水印图像被作为广义猫映射的初始值,开始进行迭代置乱,需要先保证映射的独立参数 a, b, c, d 被指定。为了既便于软件实现,又保持保面积的性质要求 $|C| = ad - bc = 1$,采用的方案是分别取 $a, b, c, d = 1$,各自对应 4 种参数取法:

$$\begin{pmatrix} 1 & b \\ c & bc+1 \end{pmatrix}, \begin{pmatrix} a & 1 \\ ad-1 & d \end{pmatrix}, \begin{pmatrix} a & ad-1 \\ 1 & d \end{pmatrix}, \begin{pmatrix} bc+1 & b \\ c & 1 \end{pmatrix}$$

每种取法有两个独立的参数。将(3)中取出的 18 bit 中的 1~2 bit 用来确定是取这 4 种参数方式中的哪一个;剩下的 3~10 bit 和 11~18 bit 分别代表其中两个独立参数的值。至于迭代的次数可以暂时取为一个定值 2。

(5) 根据查询表 LUT 和置乱后的水印 bb 来改变原图的灰度值,嵌入水印:

设图像的 (i, j) 像素处需嵌入水印比特 $bb(i, j)$,则修改图像的灰度 $I(i, j)$ 使得 $bb(i, j) = LUT(I(i, j))$,其中 $I(i, j)$ 是修改后的像素灰度值,且须保证对像素的修改应使 $I(i, j)$ 和 $bb(i, j)$ 的距离最小。

(6) 保证图像特征 $\{I_n, n = 1, \dots, N\}$ 不变,完成其他所有像素的修改。

(7) 水印提取及认证:

提取水印必须具有密钥 K 。用和嵌入水印时相同

的方法产生 LUT, 根据待认证图像的像素 $III(i, j)$ 和查询表 LUT 即可提取出图 1(b) 中所嵌入的水印 bb , 并与真实的水印 bb 进行客观的比较. 整个过程逐个像素地进行. 如果存在不同的比特, 我们就用灰度值 255 (即一个白点) 来表示图像中被篡改的位置. 最后, 根据白点的数量多少和分布位置, 就能够实现对该图像被修改的程度及局部位置的判断和定位.

3.2 方案性能分析

3.2.1 安全性分析

本方案把整个算法的安全性建立在密钥 K 的安全性上, 完全符合现代密码学的基本观点. 先利用分段线性混沌映射, 基于图像的特征信息, 生成查询表 LUT 和二维猫映射的参数; 再利用猫映射对原始水印图像进行置乱预处理; 最后根据 LUT 和置乱后的水印完成水印嵌入工作; 而水印的提取和认证操作非常简单.

前文已经指出, Yeung-Mintzer 原始方案易被攻击的根本原因是因为不同的嵌入水印图像在图像的固定位置上含有相同的嵌入信息. 在本方案中, 由图像特征的唯一性和混沌系统的初值 (密钥) 敏感性、单向性等众多特性, 可以确保在不同图像的固定位置上需要嵌入的水印图像是无法事先确定的. 而正是这种不确定性, 使得攻击者能够进行的修改一定是随机的, 所以每个像素被成功攻击的概率为 $1/2$, 要想伪造 M 个嵌入水印的像素, 其成功概率将下降为 $(1/2)^M$. 而要想正确地估计出水印 b 和映射函数 f 是完全不可能的.

3.2.2 篡改定位能力分析

由上面的分析可知, 如果一个像素被修改, 该点被检测出来的概率是 $1/2$, 也就是说, 一幅嵌入水印的图像一旦被篡改, 理论上将有 50% 的篡改点会被检测出来, 而且这些被检测出的篡改点将会非常随机地分布在篡改区域, 使得篡改区域的轮廓十分明显, 所以本方案的篡改定位能力很好.

3.2.3 效率分析

本方案的主要功能都建立在混沌方程的迭代上, 计算简单, 容易实现. 在对图像数据进行处理时, 充分利用了它的二维存储特点, 确保了整个系统的高效率.

3.3 实验结果

用 Matlab 仿真实现本方案, 类似文献[2], 作了相应的实验测试, 所得结果如下.

尺寸为 256×256 的灰度 Lena 图像和原始二值水印图像被用于本实验中, 如图 1(a) 和图 1(b) 所

示; 图 1(c) 所示的则是预处理置乱以后的水印图像; 嵌入水印后的图像如图 1(d) 所示. 特征区域是位于图像中间的 8×8 块. 嵌入水印后的图像峰值性噪比 (PSNR) 高于 50 dB, 与原始图像在视觉上觉察不出差异.

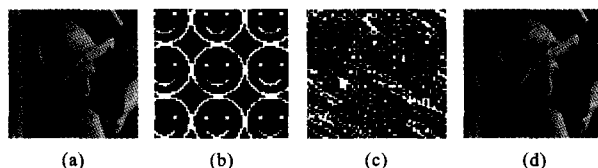


图 1 水印仿真实例

嵌入水印后的图像的攻击可以被分为两种:

I 类攻击: 图像被篡改的位置完全不会重合于作为图像特征的局部块的情况. 如图 2(a) 所示, 用圆环附近某像素的灰度值替代圆环上所有像素的灰度; 检测结果如图 2(b) 所示, 其中白点代表被篡改过的像素, 可见尽管篡改很细微, 仍可很准确地将其检测出来.



(a) I 型攻击所篡改的嵌入水印后的 Lena 图像 (b) 检测出图中被修改的位置

图 2 I 型攻击检测

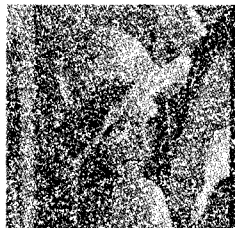
II 类攻击: 图像被篡改的位置部分重合于作为图像特征的局部块. 由于混沌系统对初始状态极度敏感, 当我们利用分段线性混沌映射对图像的特征块进行散列处理时, 如果图像特征块有任何微小修改, 将导致根据迭代结果序列所生成的查询表 LUT 和猫映射的参数完全不同. 比如: 在密钥 K 取为初值 $X_0 = 0.232\ 323$, $H_0 = 0.858\ 485$ 的条件下, 若将图像特征块中的像素灰度值 $I(125, 125)$ 从原来的 193 改为 192, 则 LUT 中发生改变的有 137 项; 而从 X_{4N} 小数部分中抽取的 18 bit 数据从原来的 111010001100010010 改变为 10111110111101100, 即: 原来的猫映射采用第 4 种参数方式, 其中参数 $b = 163$, $c = 18$; 而后来的猫映射将采用第 3 种参数方式, 其中参数 $a = 251$, $b = 236$.

最终, 检测结果将非常明显地表明篡改过的嵌入水印图像已不具有完整性. 如图 3(a) 所示, 仅仅将图 1(d) 中图像特征区域某一像素灰度值加上 1; 检测结果见图 3(b), 其中的白点即检测出的被修改

位置,类似于随机噪声。



(a) II型攻击所篡改的嵌入水印后的Lena图像



(b) 检测出图中被修改的位置

图3 II型攻击检测

4 结束语

本文利用数字混沌特性,建立起图像自身特征信息与图像水印的预处理、嵌入、提取等过程的复杂联系,提出了一个新颖的数字图像认证方案.该方案具有简单、高效、篡改定位精确、安全可行的特点。

参考文献:

- [1] Yeung M, Mintzer F. An invisible watermarking tech-

nique for image verification[C]// Proc. ICIP'97. Santa Barbara, California, 1997:680-683.

- [2] 钟桦,刘芳,焦李成. 基于图像特征的易损水印技术[J]. 电子与信息学报,2003,23(11):1482-1487.
- [3] 姜楠,杨日璟,袁克杰,等. 基于置乱排序的身份认证协议研究[J]. 微电子学与计算机,2010,27(6):1-4.
- [4] Xiao Di, Liao Xiaofeng, Deng Shaojiang. One-way Hash function construction based on the chaotic map with changeable-parameter[J]. Chaos, solitons and fractals, 2005, 24(1):65-71.
- [5] 仲兴荣,刘家胜,黄贤武. 一种基于混沌猫映射的图像加密算法[J]. 微电子学与计算机,2007,24(12):131-133.
- [6] 盛苏英,吴新华. 一种新的图像加密算法研究与应用[J]. 微电子学与计算机,2011,28(2):124-128.

作者简介:

雷正桥 男,(1971-),硕士研究生,讲师.研究方向为网络安全.

(上接第48页)

需求,又大大提升了系统开发效率,对Web信息管理系统查询系统开发具有重要的应用价值。

5 结束语

目前,作为油田生产信息管理系统的一个系统已投入使用.通用动态查询系统的应用大大提高了数据查询的灵活性,为自动化管理生产数据提供了有力的保障.同时,基于多表的通用动态查询控件实现,提高了系统的开发效率与可维护性.有待于进一步研究的工作是设计开发基于自定义控件的通用动态查询系统实现,进一步提高控件的应用价值。

参考文献:

- [1] 冯少丽. 管理信息系统在企业中的应用现状及存在问题浅析[J]. 化学工程与装备,2009(1):12-13.
- [2] 王豫,谷建华,张海辉. 一种新的企业服务总线架构设计方案[J]. 微电子学与计算机,2007,24(3):105-107.

- [3] 刘军,阳小华,杨星. 基于B/S模式的通用型组合查询组件的设计[J]. 微计算机信息,2006,22(2):256-258.
- [4] Roger S Pressman. Software engineering: a practitioner's approach[M]. 6th ed. New York:McGraw-Hill Science/Engineering/Math,2004.
- [5] 刘婕,张琳,温才斌,等. ASP.NET 2.0+SQL Server 动态网站开发从基础到实践[M]. 北京:电子工业出版社,2007.
- [6] 柴华,周兴社,杨刚,等. 基于企业服务总线的信息共享交换平台研究[J]. 微电子学与计算机,2008,25(4):116-120.

作者简介:

李竹林 女,(1972-),博士,副教授.研究方向为数字图像处理.

许 淳 男,硕士.研究方向为并行数据处理.

田云娜 女,硕士,讲师.研究方向为软件理论.