Computer Science and Application 计算机科学与应用, 2017, 7(10), 1002-1007
Published Online October 2017 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2017.710113

Hans汉斯

An Improved Algorithm Based on LSB

Yali Luo, Longjuan Wang*

College of Information Science and Technology, Hainan University, Haikou Hainan
Email: luoyali000@163.com, *juanywong@126.com

Received: Oct. 7th, 2017; accepted: Oct. 20th, 2017; published: Oct. 25th, 2017

Abstract

Information hiding is an important method to solve the problem of information security, and LSB algorithm is a common image information hiding method. Based on Logistic chaotic sequence, an improved LSB algorithm is proposed with the XOR operation to complete the encryption of embedded information. The simulation results show that the algorithm has good safety performance and can resist the pollution of salt and pepper noise. It is a kind of practical algorithm.

Keywords

Logistic, LSB, Security, Information Hiding

一种基于LSB的改进算法

骆雅丽，王隆娟*

海南大学，信息科学技术学院，海南 海口
Email: luoyali000@163.com, *juanywong@126.com

收稿日期：2017年10月7日；录用日期：2017年10月20日；发布日期：2017年10月25日

摘　要

信息隐藏是解决信息安全问题的一种重要手段，而LSB算法是一种常见的图像信息隐藏方法。本文在Logistic混沌序列的基础上，对LSB算法进行改进，用异或操作来完成对嵌入信息的加密。改进的算法经仿真试验验证，该算法安全性能较好，可以很好的抵御椒盐噪声的污染，是一种简单、实用性较好的算法。

*通讯作者。

文章引用: 骆雅丽, 王隆娟. 一种基于 LSB 的改进算法[J]. 计算机科学与应用, 2017, 7(10): 1002-1007.
DOI: 10.12677/csa.2017.710113

关键词

Logistic，LSB，安全性，信息隐藏

1. 引言

近年来，信息安全问题成为人们关注的热门问题[1]。信息隐藏则是其中一个热门研究点。随着网络的发展，信息传输变得简单便捷。但是在便利的同时也带来了新的问题：如何保障信息在传输过程中不遭受非法的窃取和篡改？如何保护电子媒体的知识产权？为了解决这些问题，信息隐藏逐渐发展起来。信息隐藏是 1996 年兴起的一门学科。在网络技术迅速发展的今天，信息隐藏技术的研究更具有现实意义。其基本特点有不可感知性，鲁棒性和隐藏容量。自上世纪 90 年代到现在，信息隐藏理论已经逐渐趋于成熟，并应用于数据保密通信、身份认证等众多领域。

数字水印[2]是信息隐藏中的一种方法。其主要的步骤是将水印信息通过一定的方式嵌入进载体(图像、音频、文本)中，而且不影响载体的使用价值，也不容易被探知或者修改。其主要特点有安全性、隐蔽性、鲁棒性和敏感性。LSB 算法则是一种基于空域的可以实现数字水印的简单算法。它嵌入方式简单，隐藏容量大，嵌入后的图片与原图在视觉上几乎没有差异。但是原始的 LSB 算法嵌入方式过于简单，鲁棒性较差，容易遭受噪声污染而导致水印信息被破坏。本文提出了一种基于 logistic 序列的改进的 LSB 算法，通过 logistics 序列，提升了秘钥的空间，通过隐藏信息与高位平面的异或，提高了算法的鲁棒性，较好的改善了普通空间域水印鲁棒性和安全性的问题。经仿真实验证明，算法简单实用，能抵抗部分噪声攻击。

2. 混沌序列

混沌序列是指在确定系统中不可预测的活动。其产生的序列对初值敏感，非周期。若是取一样的初值，可以很方便的复制出相同的序列。因此将混沌序列应用在加解密上，可以提高系统安全性和提高秘钥的搜索空间，且秘钥方便管理。

本文采用的混沌序列是 Logistic 混沌序列[3] [4]。Logistic 序列是由生态数学学家 R. May 首次提出的，是一种性能优良的伪随机序列。其映射公式为：

$$x(k+1)=u_0 x(k)(1-x(k)) \tag{1}$$

其中 $x(k)$ 在区间 $(0,1)$ 内，当 u_0 在区间 $(3.5699456,4]$ 时，序列处于混沌状态。此时产生的序列非周期，不收敛，而且对初值非常敏感。而当 $0<u_0<3.5699456$ 时，产生的序列呈周期性。

3. LSB 算法

对于计算机来说，一幅图片就是由标记像素亮度的值组成的矩阵。其对于灰度图像，其取值范围在 0-255 内，取每一位像素值的 8 位二进制，可构成一个立体直方图。各个像素点的 8 位二进制位置相同的位形成一个平面，称为“位平面”。最高位平面代表了图像主要信息，而最低位平面一般是图像的冗余部分。在低平面的二进制成为“最低有效位”。LSB 算法首先将载体图像像素值和秘密信息转换为二进

制，利用秘密信息将载体图像的最低有效位进行替换，将加密后的信息再转为原进制，得到最终的隐秘图像。

LSB 具体替换流程：如要隐藏的二进制数值为[0100 0 1]，其载体信息如图 1 所示。用其替换掉原像素 8 位二进制的最低有效位。具体的算法流程如图 1。

LSB 算法算法简单，容易实现。由于是在低位平面上做替换，所以该算法具有良好的不可感知性。此外，该算法的隐藏容量较大，是一种实用性很高的算法。

4. 具体的改进算法流程

4.1. 嵌入算法

为了隐藏和加密传输信息，我们将用到 2 个一维的 Logistic 混沌序列，具体的操作流程如下：

步骤一：取初值 x_0, u_0， y_0, u_1 利用 Logistic 混沌序列映射公式，产生 2 个与待嵌入图像大小相等的一维混沌序列。将该混沌序列从小到大或者从大到小排列，并存储这 2 个序列在原数组中的位置信息，得到新的位置序列 orderX, orderY。

步骤二：对上述位置序列orderX做对 4 取余操作，再对取余结果加 5。得到 orderX′。具体的公式如下：

$$\text{orderX}'(1,\text{j}) = \text{mod}(\text{orderX}, 4) + 5 \tag{2}$$

该操作后， orderX′的取值范围为 5~8 之间的整数。接着将 orderX′进行升维操作，将其变成与嵌入图像大小一样的二维矩阵。

步骤三：选取载体图像 I，其大小为 $M \times N$，利用 orderX′数组，选取载体图像中 orderX′对应的位平面的值，得到 tmp_img。具体操作如下：

$$\text{tmp}_{\text{img(i,j)}} = \text{bitget}(\text{I}(\text{i},\text{j}), \text{orderX}'(\text{i},\text{j})) \tag{3}$$

其中 bitget 函数为获取某数二进制中的第 X 位。

步骤四：将上一步产生的 tmp_img 和待嵌入的信息进行异或得到加密的嵌入信息 encry_image。

步骤五：对 orderY 做对 2 取余操作，并在取余结果上加 1，得到 orderY′。具体操作如下：

$$\text{orderY}'(1,\text{j}) = \text{mod}(\text{orderY}, 2) + 1 \tag{4}$$

得到的 orderY′范围为 1 或者为 2。并将 orderY′做升维操作，将其变为与嵌入图像大小一样的二维矩阵。

步骤六：选取载体图像的第 $\text{orderY}'(\text{i},\text{j})$ 位平面，并将它的值替换为 encry_image(i,j)。如 $\text{orderY}'(\text{i},\text{j}) = 1$，则替换第 1 位平面，如果 $\text{orderY}'(\text{i},\text{j}) = 2$，则替换第 2 位平面。

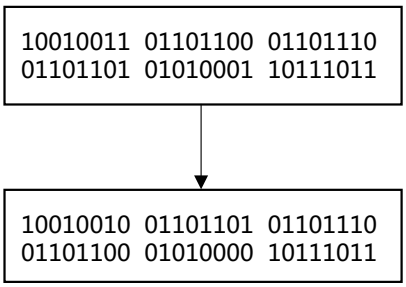


Figure 1. The algorithm flow
图 1. 算法流程

4.2. 提取算法

提取为嵌入算法的逆过程。具体过程如下：

步骤一：利用 x_0, u_0, y_0, u_1 计算出具体的混沌序列，在对其进行排序，得到相对应的 X，Y 顺序序列。对 X 序列做对 4 取余再加 5 操作，得到X’ 序列。对 Y 序列做对 2 取余再加 1 操作，得到 Y′ 序列。

步骤二：选取嵌入秘密信息的图像 H。选取 $H(i, j)$ 像素二进制位中对应的 $Y'(i, j)$ 位数值，储存为 tmp_low 矩阵。

步骤三：提取出嵌入秘密信息的 H 图像对应的像素值 $H(i, j)$ 的 $X'(i, j)$ 位，存储为 tmp_high 矩阵。

步骤四：遍历 tmp_low，将 tmp_low(i,j)的值与 tmp_high(I,j)的值相异或，异或结果则是嵌入的信息。

5. 实验结果及分析

5.1. 视觉性能分析

不可感知性[5]是指嵌入秘密信息后的伪装载体应不使源载体质量显著下降，并且视觉效果也无明显变化。在仿真实验中，采用 256 × 256 的 Lena 图像为隐藏载体，分别了嵌入图像大小为 150 × 148 和 256 × 256 的二值图像。其结果如图 2 和图 3 所示。分别对比图 2(c)和图 2(d)以及图 3(c)和图 3(d)可以发现被嵌入信息的图像和载体图像在视觉上并没有差别。对比图 2(c)和图 2(d)以及图 3(c)和图 3(d)，发现提出出来的嵌入图像和原始隐藏图像在视觉上也没有差异，说明该算法有较好的不可感知性。

为了评价图像的隐蔽性，我们采用峰值信噪比来衡量原图像与嵌入图像的区别，峰值信噪比是一个表示信号最大可能功率和影响它的表示精度的破坏性噪声功率的比值的工程术语。一般 PSNR 计算数值越大，表示失真越少。其中具体计算公式如下：

$$\mathrm{PSNR} = 20\log_{10}\frac{\mathrm{MAX}}{\sqrt{\mathrm{MSE}}} \tag{5}$$

其中 MAX 表示图像点颜色的最大值，MSE 表示图像间的均方差。分别计算嵌入大小图像为 150 × 148 和 256 × 256 的峰值信噪比，具体结果如表 1 所示。

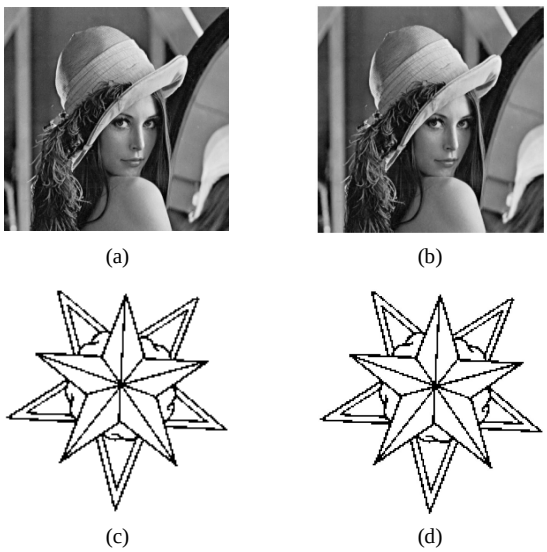
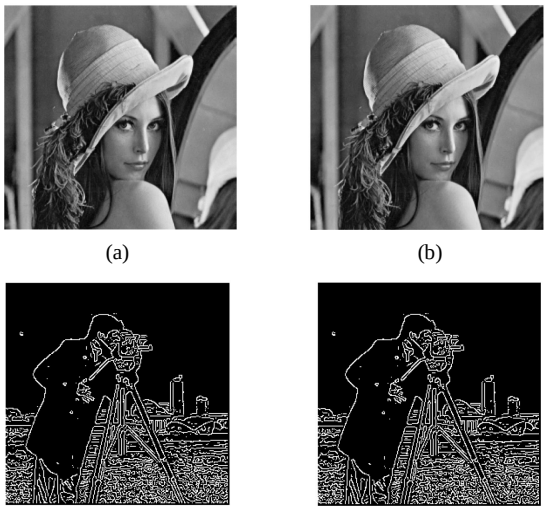


Figure 2. Embedded image (150 × 148) and original image. (a) Watermarked image; (b) Original image; (c) Recovered watermark; (d) The original watermark

图 2. 嵌入图像(150 × 148)和原始图像。(a) 水印图像；(b) 原始图像；(c) 嵌入水印；(d) 原始水印



(a) (b)

(c) (d)

Figure 3. Embedded image (256 × 256) and original image. (a) Watermarked image; (b) Original image; (c) Recovered watermark; (d) The original watermark
图 3. 嵌入图像(256 × 256)和原始图像。(a) 水印图像；(b) 原始图像；(c) 嵌入水印；(d) 原始水印

Table 1. Embeds the peak signal to noise ratio of different images
表 1. 嵌入大小不同图像的峰值信噪比

嵌入图像大小	150 × 148	256 × 256
PSNR	51.8856	47.1567

一般认为当峰值信噪比大于 35 db 时，图像在视觉上不会有太大的差异。从峰值信噪比的数值计算结果来看，该算法的 PSNR 值大于 35 db，图像有较好的隐藏效果。

5.2. 安全分析

数字水印安全性[6]数是指字水印系统应该对非法提取具有很强的免疫力，对抗未授权的删除、嵌入和检测，从而保护数字产品。一般都使用密码术的经典算法来保证密钥的安全。而混沌系统有着对初始条件特别敏感的特点。对由混沌系统，选取差异及其微小的初值，经过长时间计算后，仍然可以输出完全不相同的结果。因此，利用混沌系统可以很好的提高系统的安全性。

该算法引入了两个一维的 Logistic 混沌序列，由于该混沌序列对初值的敏感性。即使 2 个差异甚小的初值序列，仍然不可以提取出最终的嵌入信息。如图 4 所示，其初值与原初值相差了 10^{-9} 最终的提取结果并不能显示出任何有关原图的信息。证明了该算法的安全性较高。可以进一步提高 LSB 算法的安全性及秘钥的空间容量，更便于在信息安全领域利用。

5.3. 鲁棒性分析

鲁棒性[7]是指数字水印中被保护的信息经过某种改动后，比如传输、过滤操作、重新采样、编码、有损压缩等，嵌入的信息应保持其完整性，不能被轻易地去除，并以一定的正确概率被检测到。

噪声污染对图像的质量会产生不可磨灭的影响。本文对嵌入水印信息的图像做椒盐噪声污染，再提取对应的水印信息。提取结果如图 5 所示。从恢复的水印可以看出，加密图像虽然经过噪声的污染，但是利用该种改进算法而提取的结果与原加密信息几乎一致，证明该算法能较好的抵抗噪声污染，鲁棒性较好。

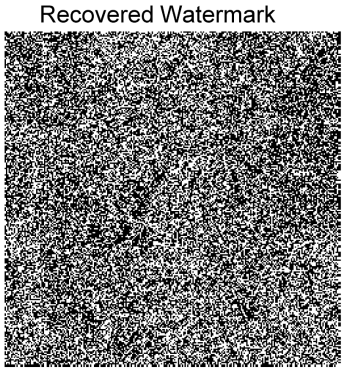


Figure 4. The initial value of 10^{-9} extracted from the embedded information
图 4. 与初值相差 10^{-9} 提取出的嵌入信息

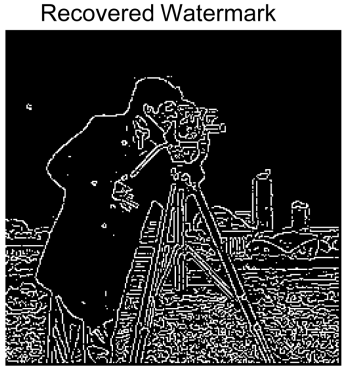


Figure 5. The embedded image is extracted from the embedded image which does the salt and pepper noise treatment
图 5. 对嵌入图像做椒盐噪声处理后所提取的嵌入图像

6. 结语

本文基于 Logistic 混沌序列，利用取余和亦或运算，提出了一种改进的 LSB 算法。经仿真实验验证，该算法的高效简单，不可感知性良好，安全性能高，而且该算法对于抵御椒盐噪声污染，效果极好。

基金项目

海南省自然基金项目(617079)，国家自然基金项目(61462023)。

参考文献 (References)

[1] 马文姬, 张煜林. 传统 LSB 图像隐藏算法的优化研究[J]. 电子产品世界, 2016, 23(9): 61-63.
[2] 马小燕, 丁伟. 数字水印在网络作品版权保护中的应用[J]. 甘肃科技纵横, 2017, 46(2): 20-22.
[3] 陈志刚, 梁涤青, 邓小鸿, 张颖. Logistic 混沌映射性能分析与改进[J]. 电子与信息学报, 2016, 38(6): 1547-1551.
[4] 张永红, 张博. 基于 Logistic 混沌系统的图像加密算法研究[J]. 计算机应用研究, 2015, 32(6): 1770-1773.
[5] 刘玄玄, 王晓红. 基于视觉显著图的数字水印算法[J]. 光学技术, 2016, 42(3): 260-263.
[6] 孙森. 信息隐藏的应用及其安全性研究[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2015.
[7] 泰克瑞. 图像信息隐藏关键技术研究[D]: [博士学位论文]. 长沙: 中南大学, 2013.

知网检索的两种方式：

1. 打开知网页面 http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD
   下拉列表框选择：[ISSN]，输入期刊 ISSN：2161-8801，即可查询
2. 打开知网首页 http://cnki.net/
   左侧“国际文献总库”进入，输入文章标题，即可查询

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：csa@hanspub.org