

一种不携带隐秘信息的安全隐写模型

伍玉良,陈够喜,张鹏程,沈红雷
(中北大学 电子与计算机科学技术学院,山西 太原 030051)

摘 要: 基于数字图像的缩放算法,提出一种不携带隐秘信息的安全隐写模型.其利用缩放算法推演秘密信息,并非直接将秘密信息嵌入载体图像中.首先选取载体图像,通过相应放大算法将其放大到一定倍数,然后找出秘密图像与新图像中像素信息的相关性,最后再缩小为原图像大小进行传输.由于没有直接修改图像内容,其隐蔽性较好.实验证明,该方法实现简单,运算量小,安全性高,并且对嵌入的信息提取方便,满足隐藏信息的不可检测性,适应于图像隐藏通信.

关键词: 信息安全;图像缩放;像素信息;算法推演

中图分类号: TP391 **文献标识码:** A **文章编号:** 1000-7180(2011)12-0119-05

Security Steganographic Model for Non-carrying Secret Information

WU Yu-liang, CHEN Gou-xi, ZHANG Peng-cheng, SHEN Hong-lei
(School of Computer Science and Technology, North University of China, Taiyuan 030051, China)

Abstract: Proposing a security steganographic model which do not carry secret information based on digital image scaling. The secret information was deduced by using image scaling algorithm, rather than directly embedded in the carrier image. Firstly, selected the carrier image, zoomed it to a certain multiple through the appropriate algorithm, then found out the relevance of the pixel information between secret image and a new image, finally reduced to the original image size for transmission. Since the scheme did not directly modify the image content, the hidden performance was better. Experiments show that the method is simple, computation is safe, and embedded information is convenient to be extracted, meeting the non-detection of hidden information and adapting to image concealed communication.

Key words: information security; image scaling; pixel information; algorithm deduction

1 引言

信息隐藏是将待隐藏的信息通过一定的手段嵌入载体而不影响宿主信号的感觉效果和使用价值.最早的信息隐藏模型是由 Cox 提出来的^[1],认为信息隐藏中的数字水印可以看成是带边信息(密钥)的通信.但在目前实际的信息隐藏系统中,边信息并不是必需的.信息隐藏系统的通用模型如图 1 所示.基于香农信息熵和相对熵的安全约束条件还不能满足图像信息隐藏的相关性隐写分析^[2].因此,本文通过对图像像素信息的分析,提出了一种运用图像的缩

放实现隐秘通信的安全隐写模型.而是将信息源载体图像的像素值看作为一个参数值数据库,通过特定放大算法根据特定坐标的像素值求解出秘密信息图像的像素信息,然后缩小载体图像为原始大小进行传输,载体图像只是收发双方约定好的图像库中的一个普通图像,它本身是绝对安全的,不担心攻击者截获或是对其进行一系列的变换处理,真正达到不携带隐秘信息实现大容量、高安全、隐蔽性好的安全隐写的目的.

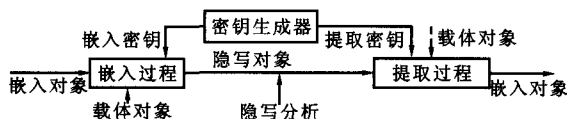


图1 信息隐藏的通用模型

2 信息隐藏的安全性

信息隐藏技术具有广泛的应用前景,要想进一步得到发展和实际应用,必须解决安全性问题. 本文给出相关信息隐藏的安全性定义如下.

定义1 指隐写分析者没有充分的信息证明经过传输信道的通信信息 C 中隐藏有秘密信息 $X^{[3]}$. 此类安全是所有安全隐蔽通信方案的前提,要求隐蔽通信满足不可检测性,如果隐写分析者可以检测到秘密信息的存在,可认为这种隐蔽方法是失败的. 在这种情况下,通信已经失去了隐蔽性.

定义2 指通信信息 C 受到主动攻击后依然能够正确接收到秘密信息. 隐藏方案广泛满足此类安全性.

本文通过研究图像缩放实现秘密信息的传输,利用相应算法求解其中的有用像素信息,进而还原出秘密信息. 因为回避了直接向载体图像中嵌入秘密信息的问题,所以满足定义1. 对于定义2,可采取重发机制等方案解决.

3 图像缩放隐秘通信的描述

目前,信息隐藏技术利用人类感知特性,将秘密信息通过一定手段隐藏在载体中实现传输,但秘密信息实际仍被嵌入并存在于载体图像之中,存在被破译和提取的危险. 本文利用图像缩放特性,提出的信息隐藏模型如图2所示.

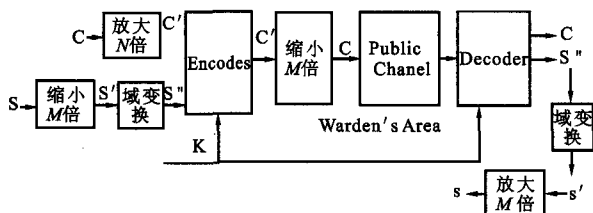


图2 信息隐藏模型

3.1 模型中的元素

秘密信息图像集为 $S = \{S_i^l \mid i = 1, 2, \dots, s\}$, l 是密图像素矩阵的维数, s 是密图的个数, $|S| = s$, $S_i^l = \{(S_{i1}, S_{i2}, \dots, S_{il}) \mid S_{ij} \in \{0, 1, \dots, 255\}, j = 1, 2, \dots, l\}$, 在不引起混淆的情况下, 将 S_i^l 简记为 S^l , $S^l \in S$. 同样, 载体图像来自同一集合 $C = \{C_i^c \mid i = 1, 2, \dots, c\}$, 提取出来的密图为 S' , 密钥空间用 $K =$

$\{K_i^k \mid i = 1, 2, \dots, k\}$ 表示.

3.2 模型中的定义

模型可能引起各种各样的攻击, 不只影响到系统的容量, 还影响到检测出的秘密信息与原始秘密信息的相似程度, 有的应用环境要求秘密信息被正确无误地提取出来, 并且安全性基于密钥的保密性. 本模型只要检测出的密图与原始秘密图像基本相似, 能够辨认, 且系统的安全性基于算法的保密性. 为了更准确描述该隐写模型, 给出如下定义.

定义3 信息隐藏系统: 假设 T_r 是域变换器, E_n 是编码器, D_m 是检码器, 则该系统是一个三元组 $\Gamma_s = (T_r, E_n, D_m)$.

定义4 假设 t_r 是信息隐藏域(空间域和变换域)变换算法, S' 是秘密图像缩小后所得新图像, S'' 是经过域变换后所得图像. 若变换过程 $T_r: S' \xrightarrow[t_r]{t_r} S''$ 成立, 则域变换器 T_r 是一个三元组 $T_r = (t_r, S', S'')$.

定义5 假设图像缩放算法是 f_n , 载体图像为 C , 秘密图像进行域变换后所得新图像为 S' , 密钥为 K , 载体图像经放大处理后的携密图像为 C' . 则五元组 $E_n = (f_n, C, S', K, C')$ 是一个编码器, 嵌入过程可表示为 $f_n: C \times S' \times K \rightarrow C'$ 或者 $f_n(C, S', K) = C'$.

如果为纯隐写系统, 则 K 为空, 此时嵌入过程可表示为 $f_n(C, S') = C'$.

定义6 假设图像缩放算法为 ϕ_m , 经过预处理的秘密图像为 S' , 密钥为 K . 则三元组 $D_m = (\phi_m, S', K)$ 是一个检码器, 检测过程可表示为 $D_m: \phi_m \times S' \times k \rightarrow S$. 检测过程可不需要预处理图像, 检测过程可进一步简化为 $\phi_m(K) = S$.

Warden 无论主动或被动攻击, 秘密信息的安全性均是当务之急. 使隐写分析人员无法检测出载体 C 中携带隐秘信息, 该模型满足如下基本条件:

(1) 已知 $P(C' \mid CSK) = 0$, 已知 C, S, K 的情况下, 可确定 C', S' ;

(2) 已知 $P(S \mid C'K) = 0$, 已知 C', K 的情况下, 可以确定 S ;

(3) 已知 $P(S \mid S'K) = 0$, 已知 S', K 的情况下, 可以确定 S .

条件概率 P , 其值为 0 表示 Warden 判断 C' 不含密, 否则含密. Warden 已知 C, C' 可能检测出 C' 是否含有秘密信息. 因而, 应尽量使 Warden 不能轻易获得 C' . 其原理是将秘密图像上的点 (u, v) 映射到

载体图像上的点 (x,y) ,然后将 (u,v) 处的像素值取为 (x,y) 处的像素值,当 (x,y) 不是格点时,秘密图像在 (u,v) 处的像素值可用 (x,y) 临近若干格点处的像素值计算求得.其工作原理如下:

(1) 将载体图像放大 N 倍,根据双线性插值算法求出未知坐标点 (x,y) 的像素值 P_{xy} ;

(2) 将秘密图像缩小 M 倍,对所得新图像进行DCT变换、滤波、量化等预处理,去除冗余信息.从左到右,从上到下找出其中的各个坐标点 (i,j) 的非零像素值 Q_{ij} ;

(3) 找出放大后载体图像中与缩小以及DCT、量化等预处理后秘密图像各坐标点非零像素值相等的坐标点;

(4) 结合第3步中找出的点坐标以及可推算出其像素值的四周A、B、C、D坐标和相应放大、缩小倍数,建立形如 $(M,N),(X_A,X_B,X_C,X_D,Y_A,Y_B,Y_C,Y_D),(m,n)$ 的密钥.其中, M,N 是缩放系数, $X_A,X_B,X_C,X_D,Y_A,Y_B,Y_C,Y_D$,分别是可求出 (i,j) 坐标点像素的A、B、C、D四点的坐标 $(X_A,Y_A),(X_B,Y_B),(X_C,Y_C),(X_D,Y_D)$, $m \times n$ 是原秘密图像的大小.

提取秘密信息图像时,根据密钥计算出非零像素点的值,依据其中包含的坐标点整理出像素矩阵,进行反余弦变换等步骤还原出缩小后的秘密信息图像,再放大 M 倍得到更准确的秘密信息图像.

3.3 模型中的算法

插值算法对于图像缩放比例较小情形,缩小0.5倍以上或放大3.0倍以下对任何图像都是可以接受的^[4].设置坐标通过反向变换得到浮点坐标为 $(i+u,j+v)$,其中 u,v 为 $[0,1]$ 区间的浮点数, i,j 均为大于等于零的整数,则这个目的像素的值 $f(i+u,j+v)$ 可由原载体图像中坐标为 $(i,j),(i+1,j),(i,j+1),(i+1,j+1)$ 所对应的周围四个像素的值计算求得,即: $f(i+u,j+v) = (1-u)(1-v)f(i,j) + (1-u)vf(i,j+1) + u(1-v)f(i+1,j) + uvf(i+1,j+1)$,其中 $f(i,j)$ 表示原图像 (i,j) 处的像素值^[5],依此类推.

如图3所示,已知 $(0,0),(0,1),(1,0),(1,1)$ 四点的256级灰度值,可以由灰度值 $f(0,0),f(1,0)$ 在 X 线性方向上求出 $(X,0)$ 点的灰度 $f(X,0)$ 值,由灰度值 $f(0,1),f(1,1)$ 在 X 方向上线性插值可求出 $(X,1)$ 点的灰度 $f(X,1)$ 值,最后由 $(X,0)$ 和 $(X,1)$ 处的灰度值 $f(x,0),f(x,1)$ 在 Y 方向上线性插值可求得 (X,Y) 点的灰度值 $f(X,Y)$.

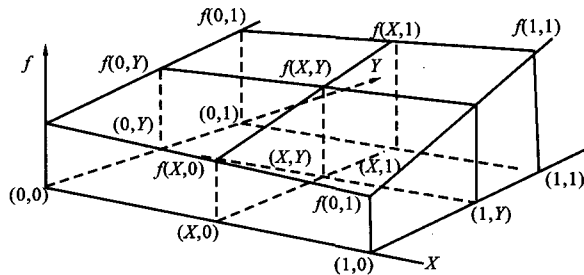


图3 双线性插值原理

4 图像的缩放

图像可看作是平面区域上的二元函数 $Z = (X,Y)$, $X,Y \in R$.在绝大多数情况下区域 R 是一个矩形,一般具有相关性,像素信息为 $F(X,Y)$.在图像被数字化后, $Z = (X,Y)$ 相应于一个矩阵,其元素所对应自变量取值即为图像的诸像素点灰度值 $F(X,Y) \in (0,1,\dots,255)$.对于彩色图像而言,可以取作混合矩阵,每个像素灰度级与红、绿、蓝3基色有关,可用 P_R, P_G, P_B 矩阵表示.也可由一个三维矩阵表示.

设 (u,v) 为原图像上的点, (x,y) 为目标图像上的点,则 (u,v) 处的颜色值与 (x,y) 处的颜色值对应起来 $(u,v) \leftrightarrow (x,y)$,并具有以下关系:

$x = X(u,v), y = Y(u,v)$, (由 (u,v) 计算对应点 (x,y)) (1)

$u = U(x,y), v = V(x,y)$, (由 (x,y) 反求对应点 (u,v)) (2)

式中, $X(u,v), Y(u,v)$ 或 $U(x,y), V(x,y)$ 均为变换.由式(1)对应的变换称作向前映射法也叫像素移交法(pixel carry-over),而由式(2)对应的变换称作向后映射法也叫像素填充法(pixel filling)^[6].

4.1 图像的放大

当把一个小图像放大的时候,可以依据原来相邻像素点的色彩值,按照放大倍数找到新像素点的位置并进行对应的填充,但是它们之间存在大量的像素点的色彩值却是不可知的,需要进行估算.

图像放大有很多不同的算法,关键在于选用何种插值方式运用于未知像素.最临近点插值算法(Nearest Neighbor)、双线性插值算法(Bilinear Interpolation)、双立方插值算法(Bicubic Interpolation)和自适应样条插值算法(S-Spline)^[7]是几种常见算法.最临近点插值算法令未知点 P 的像素值等于欧氏距离最近的已知点像素值.双线性插值算法是对最临近点插值算法的一种改进.双立方插值算法与双线性插值算法类似,对于放大后未

知像素点 P , 将对其影响的范围扩大到邻近的 16 个像素点, 依据对 P 点的远近影响进行插值计算. S-Spline 采用了一种自适应技术, 不仅依靠该像素点在图像中的位置, 还会考虑实际图像的像素信息.

最邻近插值算法最简单速度也最快, 但会带来明显的失真. 双立方插值算法和自适应样条插值算法处理效果好, 但计算量大, 复杂度高, 耗时长. 双线性差值算法缩放后图像质量高, 不会出现像素值不连续的情况, 视觉效果较好, 速度适中^[8]. 经对比分析, 本文实验拟采用双线性插值算法. 其做法是将放大后未知像素点 P 的位置换算到原始影像上, 用离 P 点最近的四个点的像素值加权求得, 其示意图如图 4 所示.

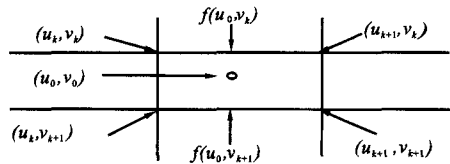


图 4 双线性插值算法示意图

设 (u_0, v_k) 是要插值点的坐标, 其具体的算法分三步:

第一步, 从 $f(u_k, v_k)$ 及 $f(u_{k+1}, v_k)$ 求 $f(u_0, v_k)$;

第二步, 从 $f(u_k, v_{k+1})$ 及 $f(u_{k+1}, v_{k+1})$ 求 $f(u_0, v_{k+1})$;

第三步, 从 $f(u_0, v_k)$ 及 $f(u_0, v_{k+1})$ 求 $f(u_0, v_0)$.

4.2 图像的缩小

设原图像大小为 $M \times N$, 缩小为 $K_1 M \times K_2 N$, ($K_1 < 1, K_2 < 1$). 算法步骤如下:

(1) 设旧图像是 $F(i, j), i = 1, 2, \dots, M, j = 1, 2, \dots, N$;

新图像是 $I(x, y), x = 1, 2, \dots, K_1 M, y = 1, 2, \dots, K_2 N$;

(2) $I(x, y) = F(C_1 * i, C_2 * j); C_1 = 1/K_1, C_2 = 1/K_2$.

由于 $I(x, y) \in (0, 1), \forall C_i \in Z$, 要用插值处理.

5 性能分析

5.1 信息隐藏容量

本模型由载体图像的像素值通过图像缩放算法推算出秘密图像信息, 因此载图像体包含的像素信息越丰富, 则隐藏的秘密信息量也越大. 通过图像的放大可以实现像素信息量的急速增长, 对于双线性

插值算法, 新填充像素个数可由 $(n+1)^2 - 4(n$ 是放大倍数) 求得, 如放大 2、3、4 倍时填充个数分别为为 5、12、21. 反推得到原载体图像的坐标, 放大 2 倍的情形如表 1 所示.

表 1 图像放大 2 倍像素填充值

坐标 (u, v)	$(1/2, 0)$	$(0, 1/2)$	$(1/2, 1/2)$	$(1, 1/2)$	$(1/2, 1)$
计算范围	$(0, 255)$	$(0, 255)$	$(0, 255)$	$(0, 255)$	$(0, 255)$
取值范围	$(0, 255)$	$(0, 255)$	$(0, 255)$	$(0, 255)$	$(0, 255)$

计算所得像素值的范围可能超出, 所有大于 255 的值均取作 255.

5.2 安全性分析

本模型利用图像的缩放算法实现秘密信息的传输, 并非真正将秘密信息嵌入到图像载体中, 只是将其作为通信载体, 通过算法求解出秘图的像素信息, 进而还原出原始秘密信息图像, 并且允许还原的图像在不影响可读性的前提下有一定程度的失真. 那么无论攻击者对载体图像内容作如何改动, 我们隐藏的信息也不会丢失. 即可不考虑其自身失真, 可抵抗隐写分析攻击.

6 实验结果与分析

选择灰度级均为 256, 大小 256×256 的 cameraman 作为秘密图像, 标准 512×512 大小的 lena 作为载体图像. 按双线性插值法, 将秘图缩小 2 倍得到大小为 128×128 的图 5(a); 将载体图像放大 2 倍, 得到大小为 1024×1024 的图 5(b).

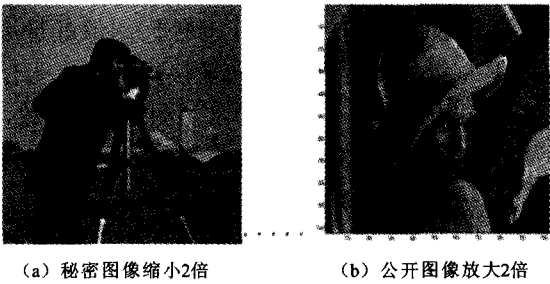


图 5 原始图像缩放处理

对缩小 2 倍的秘密图像 8×8 分块后进行 DCT 变换并进行二值掩膜运算得到部分像素矩阵如图 6 所示.

对载体图像中相应像素值进行计算求得一与密图相对应的像素矩阵, 对其进行逆余弦变换, 再利用双线性插值算法将逆离散余弦变换结果放大 2 倍, 分别得到图 7(a)、(b).

本方法简单可行, 在把握所还原的秘密图像不失可读性的前提下, 很好的实现了不携带隐秘信息

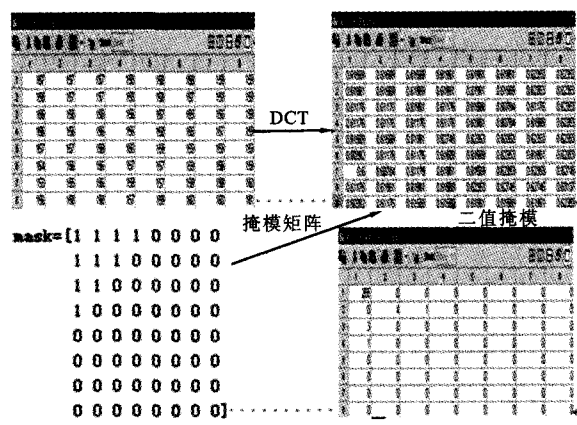


图6 像素矩阵变换

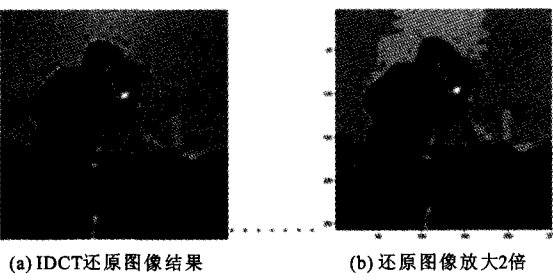


图7 还原图像结果

的安全隐写. 本实验将二维灰度秘密图像进行传输, 载体可看作是三个二维矩阵, 这样, 相关灰度矩阵的选取方案就有 3^2 种. 若秘密图像是RGB图像, 那么相关灰度矩阵的分配方案就有 3^3 种. 除容量和安全性外还具备如下特点.

(1)灵活性. 首先, 以简洁为前提, 秘图可做不同的预处理, 得出不同的结果, 载体图像上相应像素信息点的选取具有很大的灵活性; 其次, 图像只作为载体, 所以可任意选取, 甚至可以根据需要, 对其作域变换、量化等一系列操作, 再进行缩放, 使其和秘密图像具有更大的相关性.

(2)可扩展性. 理论上可将任何秘图隐藏其中; 图像缩放算法的改进和扩展, 为像素值的推演提供了更广阔的空间; 各种图像处理手段使载体图像本身可具备比原图像更大的信息量, 保证还原的秘密图像的质量.

7 结束语

本模型提供一种区别于传统意义的信息隐藏思路. 由于双线性插值低通滤波的性质, 一定程度上会造成高频分量受损, 可能会使图像轮廓略微变得模糊. 因此, 可以将此方法与其他更加成熟的缩放算法相结合来实现更加准确的秘密图像信息的传递.

参考文献:

[1] Cox I, Miller M, Mckellips A. Watermarking as communications with side information[J]. Proceedings of the IEEE, 1999, 87(7): 1127—1141.

[2] 丁一军, 郑雪峰. 一种图像隐蔽通信的安全模型[J]. 计算机科学, 2010, 27(2): 120—122.

[3] 林代茂, 胡岚. 广义信息隐藏技术的安全问题[J]. 中山大学学报, 2004, 43(2): 14—16.

[4] 王耀南, 李树涛, 毛建旭. 计算机图像处理与识别技术[M]. 北京: 高教育出版社, 2000.

[5] 王森, 杨克俭. 基于双线性插值的图像缩放算法的研究与实现[J]. 计算机应用, 2008, 27(7): 44—45.

[6] 贾永红. 数字图像处理[M]. 武汉: 武汉大学出版社, 2003.

[7] 王东鹤, 何昕, 魏仲慧, 等. 一种基于细化边缘的图像放大方法[J]. 微电子学与计算机, 2010, 27(2): 122—126.

[8] 廖汝鹏, 蔡泽锋, 闻晓晨, 等. 一种图像缩放的简化双线性插值电路[J]. 微电子学与计算机, 2009, 26(12): 136—138.

作者简介:

伍玉良 男, (1985—), 硕士研究生. 研究方向为信息隐藏、嵌入式系统.

陈够喜 男, (1966—), 副教授, 博士研究生, 硕士生导师. 研究方向为信息隐藏和图像处理.

张鹏程 男, (1981—), 硕士研究生, 研究方向为信息隐藏.

沈红雷 男, (1982—), 硕士研究生, 研究方向为信息隐藏、嵌入式系统.