

基于带参数整数小波变换可见数字水印*

罗永⁺, 成礼智, 徐志宏, 吴翊

(国防科学技术大学 理学院, 湖南 长沙 410073)

A Visible Digital Watermark Based on Integer Wavelet Transform with Parameters

LUO Yong⁺, CHENG Li-Zhi, XU Zhi-Hong, WU Yi

(College of Science, National University of Defense Technology, Changsha 410073, China)

+ Corresponding author: Phn: +86-731-4215550, E-mail: yngluo@163.com

Received 2002-11-08; Accepted 2003-06-19

Luo Y, Cheng LZ, Xu ZH, Wu Y. A visible digital watermark based on integer wavelet transform with parameters. *Journal of Software*, 2004,15(2):238~249.

<http://www.jos.org.cn/1000-9825/15/238.htm>

Abstract: An Integer Wavelet Transform with parameters is firstly constructed and the transmutative Rijndael code is used to construct a Hash function, and then a visible digital watermark algorithm based on the Integer Wavelet Translation with parameters, Discrete Cosine Transform (DCT) and the Transmutative Rijndael encryption algorithm are presented. The change of parameters of the integer wavelet and the Hash function guarantees the security of the watermark which satisfies the public-key system. By theoretical analysis and numerous experiments, it is shown that a wide prospect for this algorithm can guarantee the quality of the image and the safety of the watermark.

Key words: image watermark; visual digital watermark; integer wavelet transform with parameter; Rijndael code; hash function

摘要: 构造出了带参数的整数小波,应用变型的 Rijndael 密码构造出了 Hash 函数.提出了一种基于带参数整数小波变换、离散余弦变换及变型 Rijndael 加密算法的可见数字水印算法.利用整数小波的参数变化,并结合 Hash 函数保证了水印的安全,同时使得该可见数字水印满足公开密码体制.通过理论分析和实验证明,该方法能够保证图像的质量和水印的安全,在版权保护方面具有广阔的应用前景.

关键词: 图像水印;可见数字水印;带参数整数小波变换;Rijndael 密码;Hash 函数

中图法分类号: TP309 文献标识码: A

* Supported by the National Natural Science Foundation of China under Grant No.10171109 (国家自然科学基金); the Defense Pre-Research Project of the 'Tenth Five-Year-Plan' of China (国家“十五”国防预研基金); the National High-Tech Research and Development Plan of China under Grant No.2001AA35040 (国家高技术研究发展计划(863))

作者简介: 罗永(1976—),男,湖南益阳人,博士生,主要研究领域为应用数学,信息安全,信号与图像处理;成礼智(1962—),男,博士,教授,博士生导师,主要研究领域为信息科学中新型算法与软件,小波变换与图像处理,应用数学;徐志宏(1977—),女,博士生,主要研究领域为工程力学,数值模拟;吴翊(1948—),男,教授,博士生导师,主要研究领域为应用数学,统计,数据处理.

随着信息时代的到来以及数字技术和国际互联网的发展,计算机网络已经成为发布信息的重要媒介.各种形式的多媒体数字作品(图像、视频、音频等)开始在互联网上发表,为了避免开发商蒙受巨大的经济损失,其版权保护成为一个迫切需要解决的问题^[1,2].近年来迅速发展起来的数字水印技术为解决该问题提供了一种新的有效途径^[2,3].

数字水印的概念最早出现于 1994 年的图像处理会议(ICIP'94)上^[3].数字水印(digital watermark)按照外观可以分为可见数字水印和不可见数字水印两类.不可见数字水印(invisible watermark)是指,在数字化的数据内容中嵌入不明显的记号,通过一些计算操作可以被检测或者被提取.其水印与源数据(如图像、音频、视频数据)紧密结合并隐藏其中,成为源数据不可分离的一部分.对图像而言,这种水印表现为不可见的标志.可见数字水印(visible watermark)是指,用一定含义的标志水印以可见的形式与源数据结合(称其为融合过程),将消除水印需要的数据隐藏到融合数据中,通过一些计算操作提取隐藏信息,消除水印并恢复源数据.对于图像而言,这种水印表现为一个可见的标志.

对可见数字水印进行研究是非常有意义的.由于不可见数字水印必须通过专门的检测软件才能够提取出来,人们不能凭借视觉来进行判断.另一方面,任何人都可以获取图像的全部信息,这对于许多方面的应用来说都是不合适的,例如,工程用的图纸、表格、云层遥感图像.非法用户在获取其中的重要信息以后,便可以将其删除,从而找不到盗版或侵权的痕迹.而数字水印却可以掩盖部分图像数据,能够防止非法用户获取部分重要信息,这些信息往往是至关重要的(如遥感图像的经纬度坐标、云层图像拍摄的坐标与时刻).总的说来,可见数字水印可以直观地表明版权,但是通过消除水印又可以使合法用户获得完整的数据.

图 1 是可见和不可见数字水印的比较,可以看出,它们的区别是明显的.对于图像而言,可见数字水印的水印标志是可见的(如图 1(c)所示),它将水印图像与原始图像进行融合.从本质上来讲,可见数字水印技术隐藏的并不是水印信息,而是被水印信息替换的那部分图像信息,也就是被遮蔽的子图像.它的目的是通过消除水印操作恢复出视觉上与原始图像一致的图像(如图 1(d)所示).然而,对于不可见数字水印,水印标志是不可见的(如图 1(e)所示).它隐藏的是数字水印信息,通过检测可以将隐含的水印提取出来(如图 1(f)所示).



Fig. 1 Comparison of visible and invisible digital watermark
图 1 可见和不可见数字水印比较

现在,对于数字水印的研究几乎全部集中在不可见数字水印方面^[2-4],对于可见数字水印技术,目前还没有见到文献报道.对于可见水印技术的研究主要有以下几个技术难题:(1) 信息量大.隐藏于图像中的信息实际上是被可见水印遮蔽的一部分子图像信息,信息量取决于原始图像的格式(一般为 256 色或真彩图像).(2) 还原子图像质量要求较高.隐藏的子图像信息还原时应该与整幅图像完整地对接,从视觉上看不出还原子图像与整体

图像的差异;(3) 如何保证嵌入可见数字水印的图像质量.由于嵌入信息量大,如何在保证安全性的前提下,减少信息在嵌入过程中对图像质量的破坏.

本文提出的可见数字水印方法从以下几个方面来解决上述问题:(1) 为了解决隐藏信息的信息量大的问题,本文提出的可见数字水印方法对隐藏子图像采用 DCT(discrete cosine transform)变换作有损压缩处理;(2) 对子图像选取合适的压缩比,保证子图像的质量,保持恢复图像的整体性;(3) 嵌入隐藏的信息肯定会破坏图像的品质,为了使这种破坏减到最小,采用带参数整数小波变换对融合图像作变换,将变换部分的能量损失减少为 0,选择适当的强度嵌入压缩子图信息,保证抗攻击性的同时兼顾图像的质量.

应用带参数的整数小波变换,主要有两方面的优点:一方面,整数小波变换能够在图像分解和重构过程中,使得图像损失为 0,这样可以提高嵌入水印图像的质量;另一方面,带参数整数小波变换,利用参数的变化,可以将参数作为一个密码,提高了隐藏信息的安全性和灵活性.本文第 1 节详细地介绍了带参数整数小波变换的构造方法.

为了进一步保证隐藏信息的安全,引入变型的 Rijndael 密码^[5],可以将水印加密的算法完全公开.这种数字水印满足公开密码体制.2000 年 10 月,美国国家标准技术研究所(NIST)推荐 Rijndael 作为高级加密标准(AES).由于 Rijndael 密码加/解密是不一致的,在加/解密过程中使用不同的代码和表;在硬件实现时,Rijndael 逆密码只能使用 Rijndael 密码的部分电路.通过修改 Rijndael 算法中的 $m(x)$, $c(x)$ 和 $d(x)$,使 $c(x)$ 和 $d(x)$ 取相同的多项式,使得加/解密有更多的一致性,并且从理论上证明这种修改不影响其抗差分能力和抗 Square 攻击的能力^[6].

本文第 1 节主要介绍变换理论.第 2 节介绍加密算法理论.第 3 节介绍可见数字水印的嵌入与消除.第 4 节对可见数字水印作安全性分析.第 5 节是该方法的实验测试以及与传统可见标志的比较.第 6 节是对该方法的总体评价与应用前景展望.

1 带参数整数小波变换和加密算法理论

在图像压缩理论中,DCT 变换占据了重要的地位,无论是静态图像还是动态视频的压缩都用到了 DCT(JPEG,MPEG).它的优点是运算简单、速度快.可逆的整数小波变换(IntDWT)^[7](从整数映射到整数)在图像压缩方面有重要的应用.整数小波变换的优点在于图像变换无损,其已经被推荐为新一代压缩标准 JPEG2000 的无损压缩算法.它可以保证图像在变换部分能量损失为 0.带参数整数小波带有一个自由变量,在一定范围内都构成小波.这样,就可以将参数作为密码来提高水印的安全性和灵活性.

1.1 一般的小波提升

本文仅考虑 FIR(有限长滤波器)滤波器 $h = \{h_k\}_{k=k_1}^{k_2}$, 它的 Z 变换是一个 Laurent 多项式,满足 $h(z) = \sum_{k=k_1}^{k_2} h_k z^{-k}$.

设双正交滤波器 $\{h, g, \tilde{h}, \tilde{g}\}$ 是双正交完全重构(PR)滤波器,那么完全重构(PR)条件为^[8]

$$h(z)\tilde{h}(z^{-1}) + g(z)\tilde{g}(z^{-1}) = 1, h(z)\tilde{h}(-z^{-1}) + g(z)\tilde{g}(-z^{-1}) = 0.$$

当 $h = \tilde{h}$ 且 $g = \tilde{g}$ 时, $\{h, g, \tilde{h}, \tilde{g}\}$ 构成了正交滤波器组.在给定的完全重构(PR)条件下,新的双正交滤波器 $\{h, g^{\text{new}}, \tilde{h}^{\text{new}}, \tilde{g}^{\text{new}}\}$ 能够通过下面的被称为提升的算术运算得到:

$$g^{\text{new}}(z) = g(z) + h(z)s(z^2), \tilde{h}^{\text{new}}(z) = \tilde{h}(z) - \tilde{g}(z)s(z^2), \quad (1)$$

这里 $s(z)$ 是一个 Laurent 多项式.类似地,对偶提升可以描述为

$$h^{\text{new}}(z) = h(z) - g(z)\tilde{s}(z^2), \tilde{g}^{\text{new}}(z) = \tilde{g}(z) + \tilde{h}(z)\tilde{s}(z^2), \quad (2)$$

这里 $\tilde{s}(z)$ 是另一个 Laurent 多项式.基于已知的滤波器 $\{h, g, \tilde{h}, \tilde{g}\}$, 我们选择适当的 $s(z)$ 和 $\tilde{s}(z)$, 就可以构造出新的性质优良的双正交完全重构滤波器 $\{h^{\text{new}}, g^{\text{new}}, \tilde{h}^{\text{new}}, \tilde{g}^{\text{new}}\}$.它们可以有更大的消失矩和更大的滤波器长度.

另一方面,通过一个多项式来表示一个滤波器 $h: h(z) = h_e(z^2) + z^{-1}h_o(z^2)$, 这里 $h_e(z) = \sum_k h_{2k}z^{-k}$ 包含了偶数项系数, $h_o(z) = \sum_k h_{2k+1}z^{-k}$ 包含了奇数项系数.我们能够用一个多相矩阵^[7]来表示这个滤波器对 (h, g) :

$$P(z) = \begin{bmatrix} h_e(z) & h_o(z) \\ g_e(z) & g_o(z) \end{bmatrix}.$$

显然,由上面的等式,等式(1)能够等价地写为下面的矩阵形式:

$$P^{\text{new}}(z) = \begin{bmatrix} 1 & 0 \\ s(z) & 1 \end{bmatrix} P(z), \tilde{P}^{\text{new}}(z) = \begin{bmatrix} 1 & -s(z^{-1}) \\ 0 & 1 \end{bmatrix} \tilde{P}(z) \quad (3)$$

1.2 应用提升理论构造对称双正交小波滤波器

我们将设计双正交小波对称 9-7 完全重构滤波器作为例子,其他类型的完全重构滤波器的构造方法类似.

消失矩条件是构造小波的必要条件^[4,8-13].因此,获得对称双正交小波完全重构滤波器 $\{h, g, \tilde{h}, \tilde{g}\}$, 消失矩条件是必要的. 设 N 和 \tilde{N} 分别表示小波及其对偶的消失矩长度,也就是 $h^{(k)}(-1) = 0, k = 0, 1, \dots, N-1$ 和 $g^{(k)}(1) = 0, k = 0, 1, \dots, \tilde{N}-1$ ^[4,8,12,14,15].

对于 9-7 对称双正交完全重构小波滤波器,设 $h_k = h_{-k}$ 和 $\tilde{h}_k = \tilde{h}_{-k}, k = 0, 1, 2, 3, 4$ ^[8], 得到:

$$\begin{cases} h_e(z) = h_0 + h_2(z+z^{-1}) + h_4(z^2+z^{-2}) \\ h_o(z) = h_1(z+1) + h_3(z^2+z^{-1}) \end{cases}, \begin{cases} g_e(z) = -\tilde{h}_o(z^{-1}) = -[\tilde{h}_1(1+z^{-1}) + \tilde{h}_3(z+z^{-2})] \\ g_o(z) = \tilde{h}_e(z^{-1}) = \tilde{h}_0 + \tilde{h}_2(z+z^{-1}) \end{cases}.$$

下面对于 h_3 取值,分两种情形讨论 9-7 滤波器的提升分解.

A. 当 $h_3 \neq 0$ 时,应用 Euclidean 算法,得到下面的提升结构:

$$P(z) = \begin{bmatrix} h_e(z) & g_e(z) \\ h_o(z) & g_o(z) \end{bmatrix} = \begin{bmatrix} 1 & s_0(1+z^{-1}) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ s_1(1+z) & 1 \end{bmatrix} \begin{bmatrix} 1 & s_2(1+z^{-1}) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ s_3(1+z) & 1 \end{bmatrix} \begin{bmatrix} t_3 & 0 \\ 0 & \frac{1}{t_3} \end{bmatrix} \quad (4)$$

对于任意给定的系数 $h_k = h_{-k}$ 和 $\tilde{h}_k = \tilde{h}_{-k}$, 式(4)并不是构成小波的充分条件. 为了获得 9-7 小波滤波器,还需要引入一个新的条件:消失矩满足 $N = 2$ 和 $\tilde{N} = 4$ ^[8], 我们得到:

$$h^{(k)}(z)|_{z=-1} = 0, \quad k = 0, 1; \quad g^{(k)}(z)|_{z=1} = 0, \quad k = 0, 1, 2, 3 \quad (5)$$

式(4)可以等价于下面的形式:

$$P(z) = \begin{pmatrix} 1 & \alpha(1+z^{-1}) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \beta(1+z) & 1 \end{pmatrix} \begin{pmatrix} 1 & \gamma(1+z^{-1}) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \delta(1+z) & 1 \end{pmatrix} \begin{pmatrix} \zeta & 0 \\ 0 & \frac{1}{\zeta} \end{pmatrix} \quad (6)$$

比较式(4)和式(6)得到:

$$\begin{cases} h(z) = \alpha\beta\gamma\delta\zeta(z^{-4} + z^4) + \beta\gamma\delta\zeta(z^{-3} + z^3) + \zeta(\alpha\beta + \alpha\delta + \gamma\delta + 4\alpha\beta\gamma\delta)(z^{-2} + z^2) + \zeta(\beta + \delta + 3\beta\gamma\delta)(z^{-1} + z) + \zeta(1 + 2\alpha\beta + 2\alpha\delta + 2\gamma\delta + 6\alpha\beta\gamma\delta) \\ \zeta g(z) = \alpha\beta\gamma(z^{-4} + z^2) + \beta\gamma(z^{-3} + z) + (\alpha + \gamma + 3\alpha\beta\gamma)(z^{-2} + 1) + (1 + 2\beta\gamma)z^{-1} \end{cases} \quad (7)$$

基于消失矩条件等式(5)和归一化条件 $h(1) = 2, \tilde{h}(1) = 1$, 得到下面包含 5 个方程的方程组:

$$\begin{cases} 1 + \delta(4\alpha + 4\gamma - 2) + 2(2\alpha - 1)\beta(1 + 4\gamma\delta) = 0 \\ 1 + 2\alpha + 2\gamma + 4\beta\gamma + 8\alpha\beta\gamma = 0 \\ 2 + 6\alpha + 6\gamma + 16\beta\gamma + 40\alpha\beta\gamma = 0 \\ [1 + \delta(4\alpha + 4\gamma + 2) + 2(2\alpha + 1)\beta(4\gamma\delta + 1)]\zeta = 2 \\ 1 + (4\beta - 2)\gamma - 2\alpha(1 + 4\beta\gamma) = \zeta \end{cases} \quad (8)$$

方程的解能够表示为

$$\alpha = \frac{-2t+1}{4(t-1)}, \quad \beta = -(t-1)^2, \quad \gamma = \frac{1}{4t(t-1)}, \quad \delta = t^3 - \frac{7}{4}t^2 + t, \quad \zeta = \frac{2}{t} \quad (9)$$

从式(6)~式(9),得到了一个带有自由变量 t 的双正交 9-7 完全重构滤波器.

为了得到双正交 9-7 小波滤波器,需要应用 Daubechies 不等式^[9,13]来确定参数 t 的范围. 首先,定义

$h_0(z) = (\frac{1+z^{-1}}{2})^2 F(z)$ 和 $\tilde{h}_7(z) = (\frac{1+z^{-1}}{2})^4 Q(z)$, 这里 $F(z)$ 和 $Q(z)$ 都是包含参数 t 的多项式. 对于整数 k , 解下面的

不等式:

$$B_k = \text{Sup}_{t \in R, |z|=1} |F(z)F(z^2)...F(z^{2^{k-1}})| < 2^{\frac{3}{2}}, \bar{B}_k = \text{Sup}_{t \in R, |z|=1} |Q(z)Q(z^2)...Q(z^{2^{k-1}})| < 2^{\frac{7}{2}} \quad (10)$$

当 $k=40$ 时,得到当 $t \in [0.780,1) \cup (1,1.852]$,满足式(10).基于式(6)~式(9)提供的系数,我们总能够获得双正交 9-7 小波.特别地,如果取 $t = 1.230174$,就得到了著名的 CDF9-7 小波.注意到 CDF9-7 小波的系数全是无理数,为了使运算简单,选择 CDF9-7 小波的一种近似来代替它.如果选取 $t = 1.25$,那么 9-7 小波的系数就是

$$\left. \begin{aligned} \{h(0), h(1), h(2), h(3), h(4)\} &= \frac{1}{10} \left\{ \frac{190}{16}, \frac{86}{16}, -\frac{24}{16}, -\frac{6}{16}, \frac{9}{16} \right\} \\ \{\tilde{h}(0), \tilde{h}(1), \tilde{h}(2), \tilde{h}(3)\} &= \left\{ \frac{18}{32}, \frac{19}{64}, -\frac{1}{32}, -\frac{3}{64} \right\}, h(-k) = h(k), \tilde{h}(-k) = \tilde{h}(k) \end{aligned} \right\} \quad (11)$$

对照 CDF9-7 小波,式(11)给出的小波系数得以大大简化,而且实现了整数变换.

B. $h_3 = 0$,此时,9-7 滤波器多相表示为

$$\begin{cases} h_e(z) = h_0 + h_2(z + z^{-1}) + h_4(z^2 + z^{-2}) \\ h_o(z) = h_1(z + 1) \end{cases}$$

相应提升分解为

$$P(z) = \begin{bmatrix} 1 & -\frac{9}{16}(1+z^{-1}) + \frac{1}{16}(z+z^{-2}) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \frac{1}{4}(1+z) & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{bmatrix} \quad (12)$$

9-7 滤波器系数满足:

$$\begin{cases} h_0 = \frac{23}{32}, & h_1 = h_{-1} = \frac{1}{4}, & h_2 = h_{-2} = -\frac{1}{8}, & h_3 = h_{-3} = 0, & h_4 = h_{-4} = \frac{1}{64} \\ \tilde{h}_0 = \frac{1}{2}, & \tilde{h}_1 = \tilde{h}_{-1} = \frac{9}{32}, & \tilde{h}_2 = \tilde{h}_{-2} = 0, & \tilde{h}_3 = \tilde{h}_{-3} = -\frac{1}{32} \end{cases} \quad (13)$$

式(13)实际上是一个 7-5 小波滤波器,对应于式(9)中 $t = 1$ 的情形.

1.3 带参数整数小波变换应用于图像的分解和重构

小波变换可达到时域和频域局部化的时-频分析方法.在图像处理研究中,小波变换是一种非常有价值的工具,已经被广泛应用于图像压缩.图像通过小波变换被分解为 4 个子带图:水平和垂直方向的低频子带图 LL、水平方向的低频和垂直方向的高频子带图 LH、水平方向的高频和垂直方向的低频子带图 HL 以及水平和垂直方向的高频子带图 HH.若对子带图 LL 再进行小波分解,又可以得到更低分辨率的 4 个子带图像,如此反复,可对数字图像进行多级小波分解.如图 2 所示,原始图像作二级小波分解得到图 2(b).

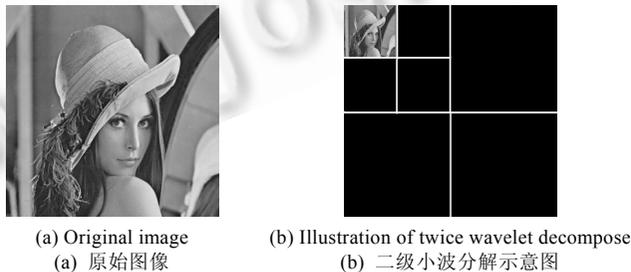


Fig.2 Illustration of wavelet decompose

图 2 小波分解示意图

基于提升结构的第二代小波理论在提高运算速度和保证图像无损变换方面取得了成功.我们知道,计算机在处理浮点运算时,由于数据类型存储位数是有限的,对超过存储位的数据采用的是截断处理,可以证明这种截断是不可逆的,因此图像在变换过程中会产生损失.引入整数小波变换就可以保证图像在进行小波变换和重构过程中不存在能量损失.带参数的整数小波变换则可以进一步提高数字水印的安全性和灵活性.图 3 显示了在

不同参数 t 下,9-7 整数小波分解以后的无损重构图像.



Fig.3 Reconstructed lossless image with different parameters t

图 3 不同参数 t 下的无损重构图

2 变型的 Rijndael 密码构造 Hash 函数

在当今电子商务迅猛发展的情况下,Rijndael 密码^[5]可以作为支持电子商务的关键性计算机安全工具. Rijndael 是一种迭代分组密码,它采用的是代替/置换网格(SPN).Rijndael 的圈函数由 4 层组成,第 1 层(字节替换)为非线性层,一个 8×8 的 S-盒应用于每一个字节;第 2 层(行移位变换)和第 3 层(列混合)是线性混合层, 4×4 的阵列按行位移,按列混合;在第 4 层(加圈密钥交换),子密钥异或到阵列的每个字节.

2.1 字节替换(ByteSub)

首先,GF(2^8)中取元素 a 的乘法逆.在所有的可逆变换中,它不是最好的变换.根据分组密码的设计原则,并且参考 E2 密码设计中的同构变换 $a^e, e=127$,将有限域上的逆元映射变为幂函数映射,即将求逆变换变成求 127 次幂(解密求 127 次根);其次,替换原有的仿射变换矩阵.两个矩阵首行向量分别为 $(1,0,0,0,1,1,1,1)$ 和 $(0,1,0,0,1,1,1,1)$,其余各行向量依次向右循环一位.

2.2 列混合变换(MixColumn)

在列混合中,为了使加/解密共用部分电路和代码,选择了一种比较好的 $c(x)=d(x)$ 算法,而它没有明显的缺陷.经过大量的实验仿真,选取 $c(x)=d(x)=3+x+2x^2+x^3$,它不仅简单,而且性质好.

经过上面的算法变型,可以证明这种变型不会降低 Rijndael 密码的安全性^[6].它所带来的好处是,加/解密达到了一致.在软件和硬件实现过程中,可以共用更多的代码和电路.

2.3 Rijndael 加密算法构造加密算子

根据图像压缩的原理,将图像变换系数量化、编码以后仍然可以还原出较好的图像(JPEG 压缩,小波图像压缩).在自然图像压缩过程中,对于变换系数来说,舍弃一部分(高频)或者修改一些系数值,仍然可以还原出可以接受的图像^[4].因此,即使非法用户获取了隐藏子图的一些变换系数,仍然可以粗略地还原出隐藏子图.为了解决部分还原的问题,本文用 Rijndael 加密算法构造了 Hash 函数以加密变换系数.提取加密数据如果有一位出错,解密算子就会将错误扩散到整个隐藏子图 DCT 系数中.

所谓 Hash 函数^[4,16],即对于任意长度的信息 m ,经过 Hash 函数运算以后,压缩成固定长度的数据,比如 128 比特,要求满足:

- (1) 已知 Hash 函数的输出,要求它的输入是困难的,即已知 $c = Hash(m)$,求 m 是困难的.
- (2) 已知 m ,计算 $Hash(m)$ 是容易的.
- (3) 已知 $c_1 = Hash(m)$,构造 m_2 ,使得 $Hash(m_2) = c_1$ 是困难的.
- (4) $c = Hash(m)$, c 的每一比特都与 m 的每一比特相关,并有高度的敏感性.即每改变 m 的一个比特,都将对 c 产生巨大的影响.

下面用 Rijndael 加密算法来构造 Hash 函数.设压缩数据为明文 m ,将它分为每组 128 比特,设

$$m = m_1 m_2 m_3 \dots m_n,$$

m_i 都是 128 比特, $i=1,2,\dots,n$,最后一块若不满 128,可以补上 0 或 1 符号串.设密钥为 k ,长度为 128 比特.

设密文 C 有

$$C = c_1c_2\dots c_n,$$

由 Rijndael 加密算法构造 Hash 函数正变换(如图 4(a)所示):

- S1. $k_1 \leftarrow k, i \leftarrow 1;$
- S2. $k_{i+1} \leftarrow \text{Rijndael}_{k_i}(m_i);$
- S3. 若 $i < n$, 则转 S2, $c_i = \text{Rijndael}_{k_i}(m_i);$

由 Rijndael 加密算法构造 Hash 函数逆变换(如图 4(b)所示):

- T1. $k_n \leftarrow c_n, i \leftarrow n;$
- T2. $k_{i-1} \leftarrow \text{Rijndael}^{-1}_{k_i}(c_i);$
- T3. 若 $i > 0$, 则转 T2, $m_i = \text{Rijndael}^{-1}_{k_i}(c_i).$

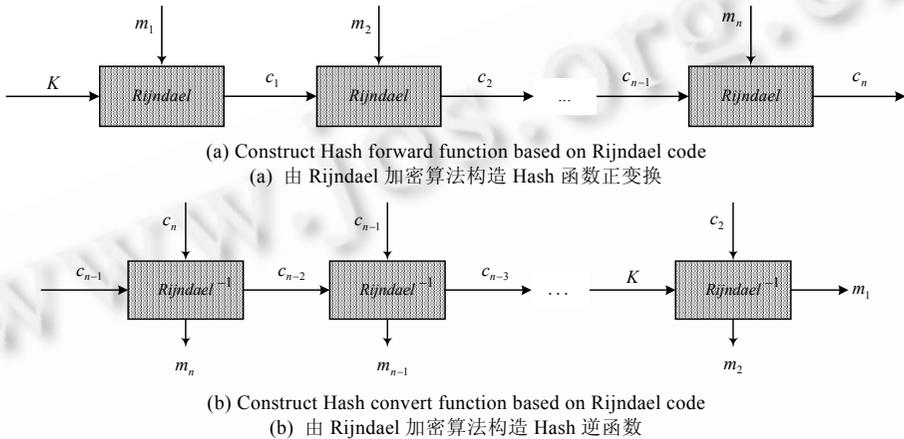


Fig.4 Construct Hash function based on Rijndael code

图 4 由 Rijndael 加密算法构造 Hash 函数

3 可见数字水印的嵌入与消除

3.1 隐藏子图的压缩方法

引入 JPEG 对静态图像压缩的一些思想,将隐藏子图图像进行分块(8×8),然后对每个小块作 DCT 变换,选取低频变换系数.注意,这里没有引入量化、编码过程,有以下几个原因:(1) 引入量化表,进行游程编码和熵编码,就需要储存很多的参数信息,由于隐藏图像数据少,压缩以后参数信息过多,压缩效果并不好;(2) 处理太复杂,压缩以后的数据长度不确定,不便于嵌入与提取.

图 5 给出了隐藏子图压缩方法.

3.2 压缩数据加密算法

由 Rijndael 构造的 Hash 函数可以作为隐藏子图压缩数据的加密算子,记为 RH . 设隐藏子图图像经过压缩以后转化为二进制数据流 p . 为了在还原隐藏子图过程中反映出任何破坏,首先对二进制数据分组,转化成 $L \times L$ 的矩阵(L 表示每行包含压缩数据的二进制位数). L 与 Rijndael 密钥长度 S 有如下关系:

$$L = \frac{S}{2^k}, k=0,1,2,3,\dots$$

如 Rijndael 的密钥长度为 128 位,则 L 可以取值 128,64,32,...,不足的在数据流后面补 0.

这样就可以从行、列两个方向来作 RH 算子运算,达到数据加密的效果,如图 6 所示.

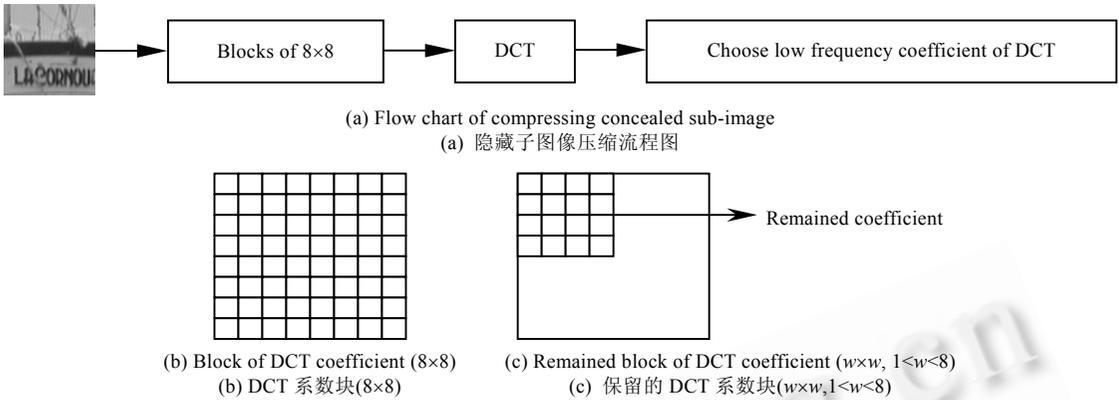


Fig.5 Illustration of compressing concealed sub-image

图 5 隐藏子图压缩示意图

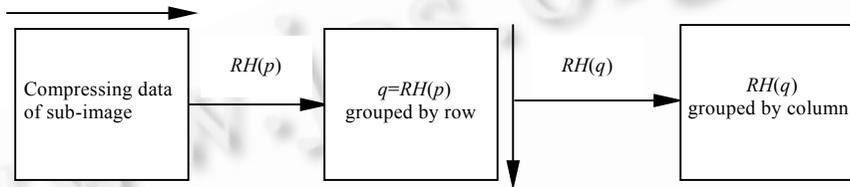


Fig.6 Illustration of encrypting sub-image compressed data

图 6 加密隐藏子图压缩数据示意图

3.3 可见水印嵌入、提取方法

下面描述可见数字水印的嵌入和消除过程,如图 7 和图 8 所示.

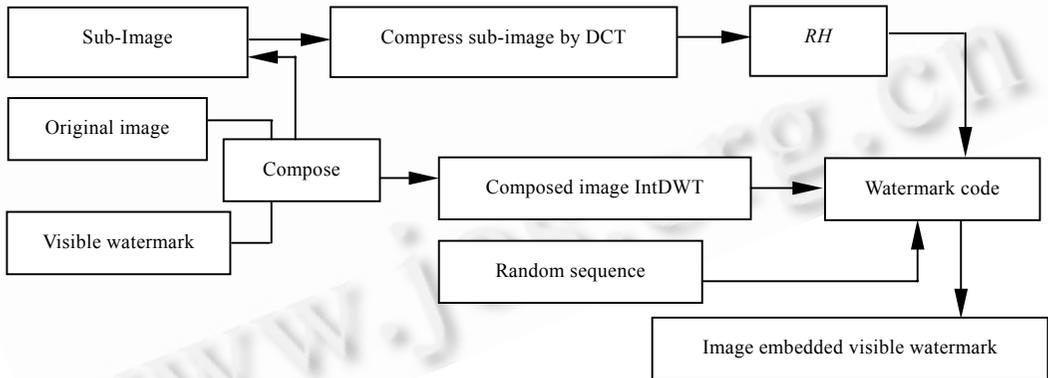


Fig.7 Flow chart of embedding visible digital watermark

图 7 可见数字水印嵌入流程图

设原始图像与可见数字水印合成图为 $F(u, v) \in Z(u \in [0, n] \cap Z, v \in [0, m] \cap Z)$, 其中 n, m 分别为图像的宽度和高度, Z 为整数集合, 图像的多级小波分解系数为 $IntW_F(u, v) \in Z(u \in [0, n] \cap Z, v \in [0, m] \cap Z)$, 其中 n, m 分别为图像的宽度和高度, Z 为整数集合.

设压缩加密以后的隐藏图像数据流 p 作 RH 变换后的系数为 $RH(p)_i (i = 0, 1, 2, 3, \dots, p)$ ($RH(p)_i$ 表示 1bit 信息 0 或 1), 图像的整数小波系数 $IntW_F(u, v)$.

嵌入信息: 对于每个 (x_i, y_i) , 修改 $IntW_F(x_i, y_i)$,

如果 $\text{Int}W_F(x_i, y_i) \bmod e > \frac{e}{2}$, $RH(p)_i = 0$, $\text{Int}W_F(x_i, y_i)' = \text{Int}W_F(x_i, y_i) + \frac{e}{2}$;

如果 $\text{Int}W_F(x_i, y_i) \bmod e > \frac{e}{2}$, $RH(p)_i = 1$, $\text{Int}W_F(x_i, y_i)' = \text{Int}W_F(x_i, y_i)$;

如果 $\text{Int}W_F(x_i, y_i) \bmod e < \frac{e}{2}$, $RH(p)_i = 1$, $\text{Int}W_F(x_i, y_i)' = \text{Int}W_F(x_i, y_i) - \frac{e}{2}$;

如果 $\text{Int}W_F(x_i, y_i) \bmod e < \frac{e}{2}$, $RH(p)_i = 0$, $\text{Int}W_F(x_i, y_i)' = \text{Int}W_F(x_i, y_i)$.

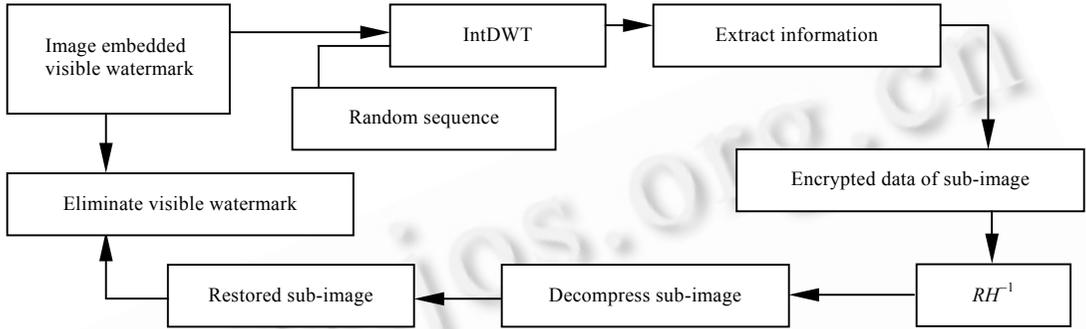


Fig.8 Flow chart of eliminating visible digital watermark

图8 可见数字水印消除流程图

检测信息:在检测信息时,只需要求解:

如果 $\text{Int}W_F(x_i, y_i)' \bmod e > \frac{e}{2}$, $RH(p)_i = 1$;

如果 $\text{Int}W_F(x_i, y_i)' \bmod e < \frac{e}{2}$, $RH(p)_i = 0$.

嵌入小波系数可以采取伪随机选取的方法^[4],提取过程就只需再现这个序列就可以了.有一个问题要解决,即在随机生成 $\{(x_i, y_i)\}$ 时,会出现重复的情况,即

$$\exists i \neq j, (x_i, y_i) = (x_j, y_j),$$

为了解决这个问题,可以建立一个临时表,在信息嵌入的过程中,记录每一个嵌入位置 (x_i, y_i) . 对于生成的 (x_i, y_i) , 要对照表内的元素,如果存在,则跳过 (x_i, y_i) , 即水印信息点,不嵌入在 (x_i, y_i) , 也就是说,保证每个 $RH(p)_i$ 嵌入在不同的位置上.并且,临时表不需要保存.在提取信息时同样建立临时表,按照同样的原则再现 $\{(x_i, y_i)\}$ 即可.

4 安全性分析

对于非法用户来说,嵌入可见数字水印的图像已经标明了版权,并且水印将原始图像的一部分遮蔽了,这对于他来说有两种情况:

(1) 嵌入可见数字水印的图像对非法用户来说是毫无意义的,因为可见数字水印遮蔽了图像的重要信息(如卫星云图的经纬度坐标、时刻信息).在水印嵌入方法公开的前提下,合法的用户只有拥有消除可见水印的密钥才能还原完整的图像,获取这些重要信息.

(2) 非法用户仍然可以勉强使用,如果不对图像数据作很大的破坏(将嵌入可见数字水印的局部图像剪切掉),可见数字水印是去不掉的.可见数字水印可以明显地标明合法的版权.

对于可见数字水印而言,其目的是防止非法用户获取完整的图像信息.只有合法的用户在拥有密钥的前提下,才能够得到消除了可见数字水印的图像.当然,如果可见数字水印遮蔽的是图像的重要部分,非法用户只要获取这些图像的参数信息就拥有了图像的使用价值.也就是说,仅获取部分隐藏子图信息,就可以获取图像的使用价值.例如卫星云图,可见数字水印将经纬度、时间信息遮蔽以后,非法用户得到了部分隐藏子图压缩系数,还

原出来的隐藏子图虽然质量很差,但是仍然可以用肉眼观察出参数信息,那么这张卫星云层图对他来说就是有价值的.因此可以看出,数字水印的抗攻击性能和不可见数字水印是不一样的.

本方法由 Rijndael 加密算法构造的 Hash 函数来对隐藏子图的压缩数据进行加密,可以保证:如果获取的隐藏子图加密压缩数据信息有 1bit 错误,那么解密压缩数据就全部错误.有了这样的处理,非法用户是完全不能够获取任何隐藏子图的信息的.可以得出结论:这种可见数字水印是高度安全的.

图 9 显示的是隐藏图对错误的敏感性实验.

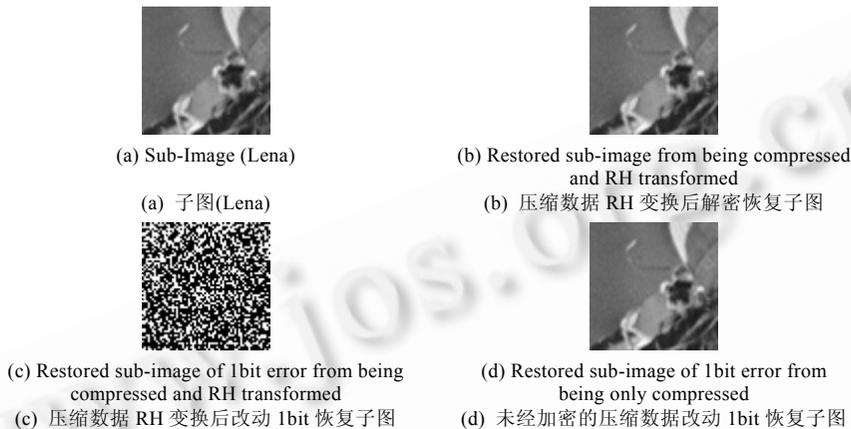


Fig.9 Test of RH transformation with 1bit changed

图 9 RH 变换对 1 位错敏感实验

图 9(a)为被隐藏的子图像(64×64 灰度图),图 9(b)为图 9(a)压缩数据 RH 加密后进行 RH^{-1} 解密恢复图.可以看出, RH 与 RH^{-1} 构成了完全重构函数对.图 9(c)为图 9(a)的压缩数据作 RH 加密后,将其改动 1bit,再通过 RH^{-1} 变换的解压缩恢复图.此时的水印图已经接近于 1 幅噪声图像了.从实验结果可以看出,1 位错已经影响到了整个隐藏子图.微小的改动带来的是恢复图的剧烈变化,这表明 RH 变换对错误有极强的敏感性.图 9(d)为未经 RH 加密,对图 9(a)的压缩数据改动 1bit 后的解压缩恢复图.可以看出,图 9(d)的质量仍然是很高的.对比图 9(c)和图 9(d)可以看出,虽然同样是改动 1bit,但是还原出来的隐藏子图却相差甚远.这明显地证明了 RH 算子有很高的安全性,可以完全保证隐藏子图的安全.

5 实验与比较

以往的图像水印技术都是仅仅将一个可以标明版权的标志融合到原图像中(我们将其称为标志水印),例如 Photoshop 软件就有这样的功能.这种嵌入了标志的图像即使是嵌入者本人都无法恢复出源数据.因为引入了信息隐藏的概念,本文提出的可见数字水印方法与标志水印是有本质区别的.可见数字水印技术可以恢复出原数据,因此能够应用在更广阔的领域.

图 10 是可见数字与标志水印的比较研究.图 10(c)是嵌入标志水印图,图 10(d)是嵌入可见数字水印图.可以看出,传统的标志水印与可见数字水印在外观上是相似的.但是它们还存在着本质的区别:传统的标志水印将原图像破坏以后就不能够恢复破坏的信息了;可见数字水印技术将可见水印嵌入到原图像以后,将替换出来的原图像数据经过压缩以后隐藏到融合图像中去(如图 10(d)所示),我们可以通过提取自身隐藏的这部分信息,恢复出原图像(如图 10(e)所示).当然,这个过程给原图像带来了一定的破坏,但是这种破坏是轻微的(人的视觉分辨不出来).从后面的实验结果可以看出,恢复图像 PSNR>40db,恢复的隐藏子图与整个图像非常吻合.

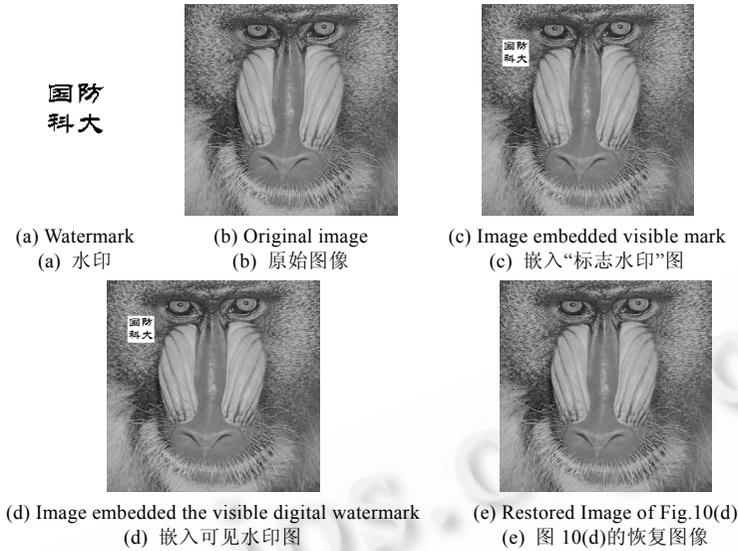


Fig.10 Comparison of the visible digital watermark and visible mark

图 10 可见数字水印与标志水印的区别

图 11 提供了一组可见数字水印实验.我们通过对标准图像 boat,baboon,barb 进行实验,图像的尺寸都是 512×512 ,嵌入的水印尺寸为 64×64 (单位是像素),分别取不同的参数 $t=1.230174, t=1.25, t=1$,结果表明,可见数字水印方法恢复出来的图像质量很高($e=8$)(PSNR=50.35, 40.36, 49.17),PSNR 都在 40db 以上(当两图像的 PSNR 大于 40db 时,人眼是不能够分辨出差别的),boat 和 barb 两幅图像更是达到 50db 左右.Baboon 恢复图质量比 boat 和 barb 要低,这主要是由于 baboon 包含的图像细节比较多,在频域中表现为高频系数较大,隐藏信息过程对这些系数破坏以后对恢复图像质量影响较大.



Fig.11 Experiment to test the quality of restored image with visible watermark when $t = 1.230174$

图 11 可见数字水印方法恢复图像质量实验 $t = 1.230174$

6 结 论

本文引入了带参数整数小波变换和离散余弦变换,实现了一种可见数字水印技术.这种数字水印技术不同于传统的嵌入可见标志,它利用信息隐藏技术将可见数字水印遮蔽的图像信息隐藏到融合图像中.这种可见数字水印可以消除,原图像被高质量地还原出来(PSNR>40db).我们采用变型的 Rijndael 加密算法构造出了 Hash 函数,对隐藏子图的压缩数据进行加密.这样,可以将 1bit 错误扩散到所有的压缩子图数据,最大限度地保证隐藏子图的安全.

References:

[1] Chang CC, Wu TC. Remote password authentication with smart cards. IEE Proceedings-e, 1991,138(3):165~168.

- [2] Voyatzis G, Ipitias I. The use of watermarks in protection of digital multimedia products. Proc. of the IEEE, 1999,87(7): 1197~1207.
- [3] van Schyndel RG, Tirkel AZ, Osborne CF. A digital watermark. In: Proc. of the ICIP'94, Vol 2. 1994. 86~90.
- [4] Hwang MS, Chang CC, Hwang KF. A watermarking technique based on one-way hash functions. IEEE Trans. on Consumer Electronics, 1999,45(2):286~294.
- [5] Daeman J, Rijmen V. AES Proposal: Rijndael. Document Version 2, 1999.
- [6] Feng GZ, Li C, Duo L. Transmutative Rijndael with the differential and statistical characteristics. Acta Electronica Sinica, 2002, 30(10):1544~1546 (in Chinese with English abstract).
- [7] Daubechies I, Sweldens W. Factoring wavelet transforms into lifting step. Journal of Fourier Analysis' and Applications, 1998,4(3):247~269.
- [8] Daubechies I. Orthonormal bases of compactly supported wavelets. Communications on Pure and Applied Mathematics, 1988,41(7):909~996.
- [9] Calderbank AR, Daubechies I, Sweldens W, Yeo B-L. Wavelet transforms that map integers to integers. Applied and Computational Harmonic Analysis, 1998,5(3):332~369.
- [10] Jayant N, Johnston J, Safranek R. Signal compression based on models of human perception. Proc. of the IEEE, 1993,81(10): 1385~1410.
- [11] Shen K, Delp EJ. Wavelet based rate scalable video compression. IEEE Trans. on CAS for Video Technology, 1999,9(1):109~122.
- [12] Mallat SG. Multiresolution approximation and wavelet orthogonal base of $L^2(R)$. Trans. of the American Mathematical Society, 1989,315(1):69~87.
- [13] Cohen A, Daubechies I, Feauveau J. Bi-Orthogonal bases of compactly supported wavelets. Communications on Pure and Applied Mathematics, 1992,45(5):485~560.
- [14] Vetterli M, Herley C. Wavelets and filters banks: Theory and design. IEEE Trans. on Signal Processing, 1992,40(9):2207~2232.
- [15] Sweldens W. The lifting scheme: A new philosophy in biorthogonal wavelet constructions. In: Laine AF, Unser M, eds. Wavelet Applications in Signal and Image Processing III. New York: SPIE, 1995. 68~79.
- [16] Merkle R. One way hash functions and DES. In: Brassard G, ed. Advances in Cryptology, CRYPTO'89. Lecture Notes in Computer Science Vol.435, Springer-Verlag, 1989. 428~466.

附中文参考文献:

- [6] 冯国柱,李超,多磊.变型的 Rijndael 及其差分和统计特性.电子学报,2002,30(10):1544~1546.