基于带参数整数小波变换的脆弱水印

罗 永 成礼智 吴 翊 徐志宏
(国防科学技术大学理学院,长沙 410073)

摘 要 为了得到一种安全性更高,构造更简单的水印,提出了一种基于提升格式的带参数双正交整数小波的构造方法,并通过引入变型 Rijndael 密码构造出了一种 Hash 函数(记为 RH 算子),设计了带参数整数小波变换和 RH 算子相结合的脆弱数字水印。该方法在不需要原始图像和标准水印的条件下,就可以侦测到图像 1bit 的篡改,还可以对篡改区域进行定位。与现有基于小波变换的数字水印方法相比,带参数整数小波的使用,可以在减少计算复杂性的同时,提高水印的安全性,而变型的 Rijndael 密码的使用,则不仅提高了代码和电路共用率,而且降低了硬件实现的成本。大量的实验结果证明,该脆弱水印算法对篡改有极强的敏感性,且当小波参数不一致的情况下,则完全不能检测正确的水印信息。可见该脆弱水印算法具有广阔的应用前景。

关键词 脆弱水印 带参数整数小波变换 Rijndael 密码 Hash 函数
中图法分类号: TP309.7 **文献标识码**: A **文章编号**: 1006-8961(2004)09-1117-07

A Scheme of Weak Image Watermark Based on Integer Wavelets with Parameter

LUO Yong, CHENG Li-zhi, WU Yi, XU Zhi-hong
(*Science Institute, National University of Defense Technology, Changsha* 410073)

Abstract To design a securer and easier constructed watermark, the biorthogonal integer wavelets with parameter based on lifting scheme is constructed, and a Hash function is built by transmutative Rijndael code. A digital watermark is designed by integer wavelets with parameter combined with RH arithmetic operators. This watermark algorithm posed is a kind of weak algorithm. Without original image and standard watermark, it is shown to be most sensitive to distortion, that is even 1 bit of change to the picture can be sensed. And furthermore the region distorted can be easily oriented in this algorithm. Compared with the traditional digital watermark based on integer wavelets, the integer wavelets with parameter can reduce operation and increase security by changing the parameter. The integer wavelets with parameter not only simplify the calculation but also improve the security of the watermark. And the transmutative Rijndael code increases the availability ratio of code and circuit, which reduces the cost of hardware realization greatly. Lots of simulation results show that the weak watermark is sensitive to the distortion of the image. When the parameter in the wavelet is wrong, the watermark cannot be detected correctly. The weak watermark method presented in this paper has wide applications.

Keywords weak watermark, integers wavelets with parameter, Rijndael code, Hash function

1 引 言

随着信息时代的到来和数字技术、因特网的发展,互联网络已经成为发布信息的重要途径。由于各种形式的多媒体数字作品(图像、视频、音频等)开始通过网络对外发布,以及电子商务的日益普及,因此其版权保护以及防止数据被恶意的篡改成为一个迫切需要解决的问题[1,2]。为了避免开发商和使用者蒙受经济损失,近年来迅速发展起来的数字水印技术为版权保护提供了一种新的有效途径。数字水印的概念最早出现于 1994 年的国际图像处理会议上[3],它是一种在数字

基金项目:国家自然科学基金项目(10171109)
收稿日期:2003-11-07;改回日期:2004-04-28

信号中嵌入其他数据的技术[4,5]。

数字水印有很多种分类方法，按照数字水印对图像篡改的敏感性分类，可以分为脆弱数字水印和鲁棒性数字水印。其中脆弱数字水印对图像的篡改非常敏感，由于其可以检测出图像被改动，而不需要与原始图像做对照，因此脆弱水印通常应用于图像完整性检验、图像的篡改提示、监测重要的数据是否被恶意篡改（如票据的防伪）等领域。

本文的目的是设计一种高度敏感的脆弱数字水印，即首先构造出带参数双正交整数小波，然后再应用带参数整数小波变换、变型 Rijndael 密码和经典的密码学理论来设计水印算法。由于这种脆弱数字水印是将加密算法与图像处理技术相结合，因此算法可完全公开，使用者只要持有密钥和整数小波变换参数，就可以保证安全。应用带参数整数小波变换，主要有以下两个优点：一方面，由于整数小波变换能够在图像分解和重构过程中，使得图像损失为零，因此可提高嵌入水印图像质量；另一方面，利用参数变化，将其作为一个密码，可提高隐藏信息的安全性。

为了保证隐藏信息的安全，该算法还引入 Rijndael 密码[6]，并结合经典密码理论，构造出了基于 Rijndael 密码的 Hash 函数（记为 RH 算子），该函数可以将误差最大限度扩散，且扩散不会影响篡改区域的定位。区域的定位是通过检测 RH 逆变换之前的提取信息来进行，且定位只与错误信息的位置和小波滤波器长度有关。RH 算子使得篡改检测非常直观，如果检测出来的水印图像是噪声图像，则说明图像已经被篡改。同时为了保证水印方法的实用性，在不降低安全性的条件下，本文采用变型 Rijndeal 密码来提高代码的重用率，以减少硬件实现成本。

本脆弱水印算法可以完全公开，其采用的密钥长度为 128bit，并能抗密钥攻击。在不需要提供原始图像和标准水印的条件下，就可以检测到图像 1bit 的改动。

2 带参数整数小波构造方法

本文将设计的对称双正交 9-7 完全重构小波滤波器作为例子，其他类型的完全重构滤波器的构造方法类似。

由于消失矩条件是构造小波的必要条件[7~13]，因此，要获得对称双正交小波完全重构滤波器 $\{h,g,\tilde{h},\tilde{g}\}$，则消失矩条件是必要的。设 N 和 $\tilde{N}$ 分别表示小波和与它对偶的消失矩长度，也就是 $h_k(-1)=0,k=0,1,\cdots,N-1$ 和 $g_k(1)=0,k=0,1,\cdots,\tilde{N}-1$[9~11]。下文符号含义见文献[9,10]。

对 9-7 对称双正交小波完全重构滤波器，设 $h_k=h_{-k}$ 和 $\tilde{h}_k=\tilde{h}_{-k},k=0,1,2,3,4$[12]，有

$$\begin{cases}h_e(z)=h_0+h_2(z+z^{-1})+h_4(z^2+z^{-2})\\ h_o(z)=h_1(z+1)+h_3(z^2+z^{-1})\end{cases}\quad\text{和}$$

$$\begin{cases}g_e(z)=-\tilde{h}_o(z^{-1})=-[\tilde{h}_1(1+z^{-1})+\tilde{h}_3(z+z^{-2})]\\ g_o(z)=\tilde{h}_e(z^{-1})=\tilde{h}_0+\tilde{h}_2(z+z^{-1})\end{cases}\tag{1}$$

对于 h_3 取值，分以下两种情形讨论 9-7 滤波器的提升分解。

（1）当 $h_3\neq 0$ 时，应用 Euclidean 算法，可得到下面的提升结构

$$\begin{aligned}P(z)=\begin{bmatrix}h_e(z) & g_e(z)\\ h_o(z) & g_o(z)\end{bmatrix}=&\begin{pmatrix}1 & \alpha(1+z^{-1})\\ 0 & 1\end{pmatrix}\\ &\begin{pmatrix}1 & 0\\ \beta(1+z) & 1\end{pmatrix}\begin{pmatrix}1 & \gamma(1+z^{-1})\\ 0 & 1\end{pmatrix}\\ &\begin{pmatrix}1 & 0\\ \delta(1+z) & 1\end{pmatrix}\begin{pmatrix}\zeta & 0\\ 0 & \dfrac{1}{\zeta}\end{pmatrix}\end{aligned}\tag{2}$$

对于任何给定的系数 $h_k=h_{-k}$ 和 $\tilde{h}_k=\tilde{h}_{-k}$，式(1)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，即消失矩满足 $N=2$ 和 $\tilde{N}=4$[12]，就可得到

$$h^{(k)}(z)\big|_{z=-1}=0,k=0,1\quad\text{和}$$

$$g^{(k)}(z)\big|_{z=1}=0,k=0,1,2,3\tag{3}$$

比较式(1)和式(2)得到

$$\begin{aligned}h(z)=&\alpha\beta\gamma\delta\zeta(z^{-4}+z^4)+\beta\gamma\delta\zeta(z^{-3}+z^3)+\\ &\zeta(\alpha\beta+\alpha\delta+\gamma\delta+4\alpha\beta\gamma\delta)(z^{-2}+z^2)+\\ &\zeta(\beta+\delta+3\beta\gamma\delta)(z^{-1}+z)+\\ &\zeta(1+2\alpha\beta+2\alpha\delta+2\gamma\delta+6\alpha\beta\gamma\delta)\end{aligned}\tag{4}$$

$$\begin{aligned}\zeta g(z)=&\alpha\beta\gamma(z^{-4}+z^2)+\beta\gamma(z^{-3}+z)+\\ &(\alpha+\gamma+3\alpha\beta\gamma)(z^{-2}+1)+(1+2\beta\gamma)z^{-1}\end{aligned}$$

基于消失矩条件等式（式(3)）和归一化条件 $h(1)=2$，$\tilde{h}(1)=1$，即可得到下面包含 5 个方程的方程组：

$$\begin{cases}1+\delta(4\alpha+4\gamma-2)+2(2\alpha-1)\beta(1+4\gamma\delta)=0\\ 1+2\alpha+2\gamma+4\beta\gamma+8\alpha\beta\gamma=0\\ 2+6\alpha+6\gamma+16\beta\gamma+40\alpha\beta\gamma=0\\ [1+\delta(4\alpha+4\gamma+2)+2(2\alpha+1)\beta(4\gamma\delta+1)]\zeta=2\\ 1+(4\beta-2)\gamma-2\alpha(1+4\beta\gamma)=\zeta\end{cases}\tag{5}$$

该方程组的解能够表示为

$$\alpha=\frac{-2t+1}{4(t-1)},\beta=-(t-1)^2,\gamma=\frac{1}{4t(t-1)},\quad \delta=t^3-\frac{7}{4}t^2+t,\zeta=\frac{2}{t} \tag{6}$$

由式(3)到式(6),就可得到一个带有自由变量 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,还需要应用 Daubechies 不等式[7,10]来确定参数 t 的范围,即首先定义 $h_9(z)=\left(\frac{1+z^{-1}}{2}\right)^2F(z)$ 和 $\tilde{h}_7(z)=\left(\frac{1+z^{-1}}{2}\right)^4Q(z)$,这里 $F(z)$ 和 $Q(z)$ 都是包含参数 t 的多项式,然后将整数 k 作为常量,即可解下面关于参数 t 的不等式

$$B_k=\sup_{t\in\boldsymbol{R},|z|=1}|F(z)F(z^2)\cdots F(z^{2^{k-1}})|<2^{\frac{3}{2}},\quad \hat{B}_k=\sup_{t\in\boldsymbol{R},|z|=1}|Q(z)Q(z^2)\cdots Q(z^{2^{k-1}})|<2^{\frac{7}{2}} \tag{7}$$

当取 $k=40$ 时,为了满足不等式(式(7)),则 t 的取值范围是 $t\in[0.780,1)\cup(1,1.852]$。而基于式(3)到式(6)提供的系数,总能够获得双正交 9-7 小波。特别地,如果取 $t=1.230\,174$,就得到了著名的 CDF9-7 小波[10]。

(2) 当 $h_3=0$ 时,9-7 滤波器多相表示为

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

其相应提升分解为

$$P(z)=\begin{bmatrix}1 & -\frac{9}{16}(1+z^{-1})+\frac{1}{16}(z+z^{-2})\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ \frac{1}{4}(1+z) & 1\end{bmatrix}\begin{bmatrix}2 & 0\\ 0 & \frac{1}{2}\end{bmatrix} \tag{8}$$

由于 9-7 滤波器系数满足

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

因此式(9)实际上为一个 7-5 小波滤波器,其对应于式(6)中 $t=1$ 的情形。

从理论上来说,若 t 取不同的值,则其小波滤波器是不一样的,但是对于整数小波变换来说,由于变换以后的系数需要取整,因此一些误差可在取整的过程中去掉。当 Δt 过小,其实际的小波滤波器效果是一样的,这也是该方法的一个局限性。通过实验证明,由于只有当 $\Delta t>0.001\,2$ 时,整数小波滤波器才不一样(互异性),因此 $t\in[0.780,1.852]$ 中不同的整数小波滤波器实际上是有限个。只是当 $t=1$ 时,提升结构才都发生变化(见式(8))。

3　构造 Hash 函数

在当今电子商务迅猛发展的情况下,Rijndeal 密码[7]可以作为支持电子商务的关键性计算机安全工具。由于 Rijndael 密码没有使用其他密码的构成变换,同时 Rijndael 密码没有将其安全性建立在算术运算之间模糊的和不好理解的相互作用上,因此 2000 年 10 月,美国国家标准技术研究所推荐 Rijdael 作为高级加密标准。

Rijndael 密码加密、解密不一致有两点,即①加解密过程中使用不同的代码和表;②在硬件实现时,Rijndael 逆密码只能使用 Rijndael 密码的部分电路,而通过修改 Rijndael 算法中的 $m(x)$、$c(x)$ 和 $d(x)$,则不仅可使得 $c(x)$ 和 $d(x)$ 取相同的多项式,而且可使得加解密有更多的一致性,现已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,且统计性能更好[14]。

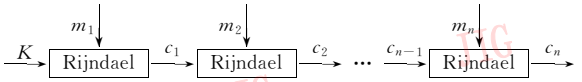
所谓 Hash 函数,即对于任意长度的信息 $\boldsymbol{M}$,若经过 Hash 函数运算后,压缩成固定长度的数据(比如 128bit),则它要求满足一定的条件[15]。

下面将用 Rijndael 加密算法来构造 Hash 函数。设水印图像为明文 $\boldsymbol{M}$,将它分为每组 128bit,设 $\boldsymbol{M}=m_1m_2m_3\cdots m_n$,$m_i$ 都是 128bit,$i=1,2,\cdots n$,最后一块若不满 128bit,则可以补以 0 或 1 符号串;设密钥为 K,长度为 128bit;设密文为 $\boldsymbol{C}=c_1c_2\cdots c_n$,则 Hash 函数构造方法如图 1 所示(其中 Rijndael^{-1} 表示 Rijndael 逆密码)。

由 Rijndael 构造的 Hash 函数,可以视为一个算子,记为 RH。在这里水印图可视为明文,记为 $\boldsymbol{P}$。众所周知,图像是一种二维信号,为了将由错误引起的扰动扩散到整个水印图 $\boldsymbol{P}$ 上面,就需要将水印做行、列两个方向的 RH 算子运算(如图 2 所示,RH^{-1} 表示 RH 逆变换)。

图 3 是对水印图进行错误敏感性试验。

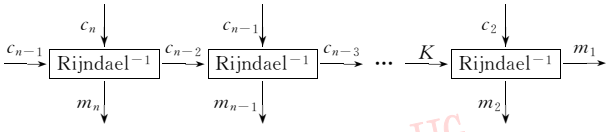
图 3(a)为原始水印图(64×64),图 3(b)为对原



①$k_1 \leftarrow k, i \leftarrow 1$；②$k_{i+1} \leftarrow \text{Rijndael}_{k_i}(m_i)$；

③若 $i<n$，则转步骤②，$c_i=\text{Rijndael}_{k_i}(m_i)$

(a) Rijndael 密码构造 Hash 函数正变换



①$k_n \leftarrow c_n, i \leftarrow n$；②$k_{i-1} \leftarrow \text{Rijndael}_{k_i}^{-1}(c_i)$；

③若 $i>0$，则转步骤②，$m_i=\text{Rijndael}_{k_i}^{-1}(c_i)$

(b) Rijndael^{-1}密码构造 Hash 函数逆变换

图 1 Hash 函数构造

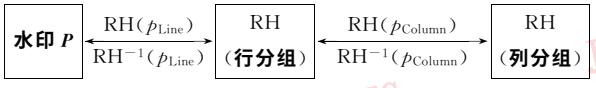


图 2 采用 RH 算子加解密水印示意图

(a) 原始水印 (b) RH 变换图 (c) RH 逆变换图 (d) 篡改 1bit 后 RH 逆变换图

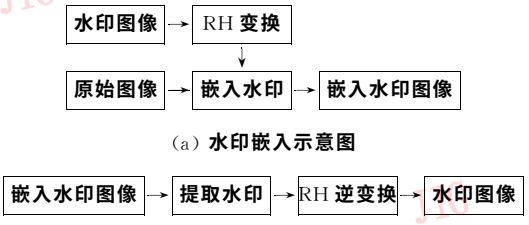
图 3 水印对 1 bit 错误敏感实验

始水印图做行和列两个方向的 RH 变换后得到的图像，此时的水印图已经接近于一幅随机噪声图像了。图 3(c)为图 3(b)的还原图，由该图可以看出，RH 变换与 RH 逆变换构成了完全重构函数对。如果修改图 3(b)中的一位，再分别做列与行的 RH 逆变换，就得到了图 3(d)。从实验结果可以看出，微小的改动(1bit)带来的是还原图的剧烈变化，可见该水印对错误有极强的敏感性。

4 图像水印的嵌入和检测

图 4 是图像水印的嵌入和提取过程示意图，其水印的检测过程不需要原始图像和标准的水印，只需要提供带参数小波变换的参数 t 和 RH 算子的密钥就可以了，然后通过提取水印就可以知道图像是否被篡改，而且可以统计出错误点的数量。

设原始图像 $F(u,v)\in\mathbf{Z}(u\in[0,n]\bigcap\mathbf{Z},v\in[0,m]\bigcap\mathbf{Z}$，其中 n,m 分别为图像的宽度和高度，$\mathbf{Z}$ 为整数集合)，则图像的多级小波分解系数为 $W_F(u,v)\in\mathbf{Z}$。当将图像数据 $F(u,v)$ 改动为 $\hat{F}(u,v)$ ($\hat{F}(u,v)\neq F(u,v)$)时，由于整数小波变换是一种一一映射关系，因此必定有 $W_F(u,v)\neq\hat{W}_F(u,v)$。一般将于浮点小波变换系数记为 $W_F^{\text{float}}(u,v)\in\mathbf{R}$，但当将图像数据 $F(u,v)$ 改为 $\hat{F}(u,v)$ ($\hat{F}(u,v)\neq F(u,v)$)时，则不一定满足$[W_F^{\text{float}}(u,v)]\neq[\hat{W}_F^{\text{float}}(u,v)]$([ ]表示取整运算)。对于浮点小波变换而言，在取整的过程中，由于改动图像带来的小波系数的误差很有可能在系数取整的过程中给略去了，因此选择整数小波变换来对图像进行频域化和设计脆弱水印，就可以大大提高水印对篡改的敏感性。



(a) 水印嵌入示意图

(b) 水印提取示意图

图 4 水印图像嵌入和提取过程

设水印 P 做 RH 变换后的系数为 $R(p)_i(i=0,1,2,3,\cdots,q)$($q$ 为水印数据长度，单位是 bit，$R(p)_i$ 表示水印 P 经过 RH 变换以后的第 i bit 信息，取 0 或 1)，图像的整数小波变换系数为 $W_F(u,v)$，则对于任意一个(x_i,y_i)，其 $W_F(x_i,y_i)$可修改为

$$\hat{W}_F(x_i,y_i)=\text{sgn}(W_F(x_i,y_j))\times\{|[W_F(x_i,y_i)\backslash e]\times e|+\frac{e}{2}R(p)_i\}$$

(“\”代表整除，e 为修正偏差值)

在检测信息时，

如果$\hat{W}_F(x_i,y_i)\text{mod}e\geqslant e/2, R(p)_i=1$；

如果$\hat{W}_F(x_i,y_i)\text{mod}e<e/2, R(p)_i=0$；

为了提高水印敏感性，在嵌入脆弱水印的过程中，由于是采用嵌入小波系数最低位($e=2$)的方法来嵌入水印，即对所有的小波系数都嵌入一位的水印信息，因此一幅图像可以包含多个水印图像。除了 RH 算子的密钥以外，整数小波的参数也是一个重要数据，固它可以由版权所有者持有，若没有这个参数，同样也不能正确检测水印。

通过对提取的信息进行统计，出现概率低的信息就是错误信息，设滤波器的长度为(d,l)，则只需对第 1 层小波系数出现的错误信息 $E_{x,y}((x,y)$是错误点坐标)进行判断(其他层小波系数都可由第 1 层小波系数直接或间接计算得到)即可。设 $r=\max\{d,l\}$，定

义篡改矩阵 $\boldsymbol{U}_{x,y}=[x-(r-1)/2,x+(r-1)/2]\times[y-(r-1)/2,y+r-1)/2]$,设 $\{\boldsymbol{U}_{x_i,y_i}\}(i=0,\cdots,t)$ 为篡改矩阵集合,则篡改区域定义为 $\bigcup_{i=0,\cdots,t}\boldsymbol{U}_{x_i,y_i}$。由于此时还没有进行 RH 逆变换,因此篡改区域的定位与 RH 算子的扩散无关,篡改区域的确定只与错误信息的位置和小波滤波器的长度有关。

5　实验与比较

为了验证本文算法的效果,首先选取 RH 算子对水印做行和列运算的密钥,其长度为 128bit;然后对(64×64)的二值水印图做 RH 变换,并将变换后的数据嵌入到图像中;最后分析图像在嵌入水印以后的质量以及水印对篡改的敏感性。对图像质量采用峰值信噪比(PSNR)来进行评价。

图 5 演示了标准图 Lena 嵌入和提取水印的试验。图 5(a)为嵌入的水印图像,实验中采用的是同一幅水印图像多次嵌入的方式,当然也可以是不同的水印图像。图 5(b)为嵌入了水印以后的 Lena 图像,图 5(c)为从图 5(b)中提取出来的所有水印。小波参数为 $t=1.25$,嵌入水印后 Lena 图像的 $PSNR$ 为 44.923dB。可见这种脆弱水印能满足不可见性的要求。表 1 列出了在不同的参数下,几种标准图像嵌入水印以后图像的质量。

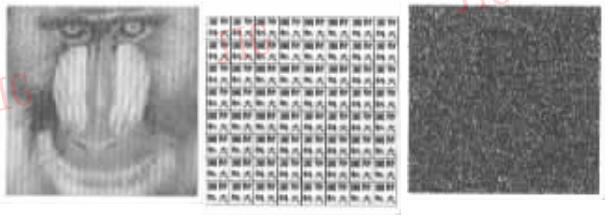
(a) 水印图　(b) 嵌入水印后的"Lena"图　　(c) 提取出来的水印

图 5　水印嵌入与提取实验

表 1　几种标准图像采用不同的参数 t 时嵌入水印以后图像质量(峰值信噪比)比较　　单位:dB

	$t=1.230\,174$	$t=1.25$	$t=1$	$t=1.4$
Lena	45.537	44.923	43.719	42.417
Barb	45.513	44.896	43.773	42.419
Boat	45.526	44.958	43.400	42.124
Goldhill	45.562	44.854	43.726	42.470
Mandrill	45.522	44.887	43.706	42.444

从上面的实验可以看出,在不同的参数下,图像质量虽有所差异,但是嵌入水印以后的图像质量都很高($PSNR>40$dB),可满足水印不可见性的要求。当嵌入和提取的过程中所选取的参数 t 不一致时(这种不一致是有限的,试验证明,$\Delta t>0.0012$ 时,才可以满足整数小波滤波器互异的要求),就会出现如图 6(c)所示的情况,即其提取出来的水印是噪声图像。



(a) 嵌入水印后的狒狒图($t=1.25$)　(b) 提取的水印($t=1.25$)　(c) 提取的水印($t=1$)

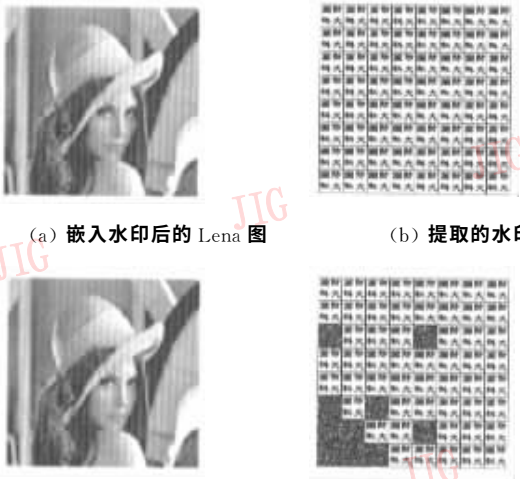
图 6　嵌入与提取选取的参数 t 不一致提取的水印

由于这种脆弱数字水印方法是采用带参数整数小波变换,并且小波变换的参数是保密的,因此如果对小波系数进行篡改,同样会被脆弱水印侦测出来,图 7 的实验证明了这一点。

(a) 嵌入水印后的房屋图($t=1.25$)　(b) 篡改后的小波系数图($t=1$)　(c) 从篡改图中提取的水印

图 7　篡改小波系数实验

下面通过图 8 的实验来验证水印对篡改的敏感性。图 8(c)为图 8(a)中的一个像素点篡改一位以后的结果图,图 8(d)为从图 8(c)中提取出来的水印。



(a) 嵌入水印后的 Lena 图　(b) 提取的水印

(c) 篡改 1 位后的 Lena 图像　(d) 提取的水印

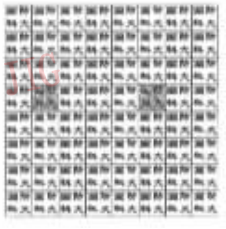
图 8　水印对图像篡改的敏感实验

由该实验可以看出部分水印图像是一幅噪声图像，由此可见，这种脆弱水印对篡改极度敏感，并且可最直观地将篡改反映出来，同时可以统计出错误信息的数量。

通过上面的实验可以看出，这种脆弱水印对图像篡改有极强的敏感性，这种敏感性来源于 RH 算子对误差的扩散能力，以及整数小波变换——映射的性能。下面将不采用 RH 算子，而直接用 Rijndael 密码加密水印来做对照实验（如图 9 所示）。

(a) 嵌入水印后的图像

(b) 篡改 1 位的嵌入水印后图像



(c) 提取的水印

图 9 Rijndael 行列加密水印实验

从图 9 的实验可以看出，如果直接对水印图像做行列方向的 Rijndael 加密，则它的误差扩散能力明显比 RH 算子弱。由图 9(c)可见，两个变化的水印仍然是可以辨识的。表 2 列出了对嵌入水印的标准图随机篡改 1～6bit 时，水印侦测到的错误信息的数量。

从表 2 可以看出，该算法不需要原始图像和标准的水印，只要图像被篡改就一定能够被水印侦测到，但是篡改对于水印的影响与篡改的图像像素点的位置有关。从表 2 中可以看出，当图像被篡改 1bit 时，从有的图像(Mandrill、Barb)侦测到的错误信息只有 2 个，而从有些图像(Boat)侦测到的错误点数量达到了 17 个，但是有一点却是肯定的，就是随着篡改位数的增加，水印侦测到的错误点的数量也在不断增加。

表 2 从篡改后水印图像中侦测到的错误信息数量

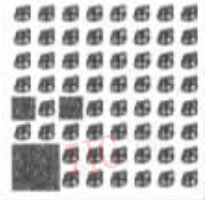
单位：个

	1 bit	2 bit	3 bit	4 bit	5 bit	6 bit
Lena	13	28	36	38	43	46
Barb	2	12	14	33	34	54
Boat	17	21	27	31	34	38
Goldhill	4	8	11	17	21	24
Mandrill	2	12	32	34	59	71

图 10 是脆弱水印对篡改区域定位的试验结果。

(a) 嵌入水印后的图像

(b) 篡改 1 位的嵌入水印后的图像



(c) 提取的水印

(d) 篡改区域定位

图 10 篡改区域定位试验

6 结 论

本文提出了一种基于带参数整数小波变换、变型 Rijndael 密码和 Hash 函数的脆弱数字水印算法，不仅构造出带参数整数小波变换，并通过改变小波参数来提高水印的安全性。由于满足整数小波互异性要求的参数 t 是有限的，因此这种提高是有限的，但通过引入变型的 Rijndael 密码，使得加解密过程一致，不仅可提高代码和电路共用率，而且减少了硬件实现成本。另外，还构造出 RH 算子，并应用到该水印算法中，使得图像篡改能够直观地被检测出来。本水印算法只需提供小波变换参数 t 和 RH 算子密钥，就可以侦测出图像 1bit 改动，并且可以对篡改区域定位。

为了开发出真正商业化、实用性的水印技术，本方法必须与经典的密码理论以及高级加密算法相结合。这样在算法完全公开的前提下，只要持有密钥和小波变换参数就可以保证安全；另一个方面，由于整数小波运算量小，且 Rijndael 密码结构简单，因而为开发硬件降低了成本。由于脆弱水印可以应用在许多领域，因此可以预见，其具有很大的应用前景。

参 考 文 献

1 Chang C C, Wu T C. Remote password authentication with smart cards[J]. IEE Proceedings-E, 1991, **138**(3):165～168.

2 Voyatzis G, Ipitas I. The use of watermarks in protection of digital multimedia products[J]. Proceedings of IEEE, 1999, **87**(7):1197～1207.

3 Van R G, Tirkel A Z, Osborne C F. A digital watermark[A]. In: Proceedings of IEEE International Conference on Image Processing[C], Austin, TX, USA, 1994, **2**:86～90.

4 Tsai J M, Yu K Y, Chen Y Z. Joint wavelet and spatial transformation for digital watermarking[J]. IEEE Transactions on Consumer Electronics, 2000, **46**(1):241～245.

5 Wu C F, Hsieh W S. Digital watermarking using zero-tree of DCT[J]. IEEE Transactions on Consumer Electronics, 2000, **46**(1):87～93.

6 Daeman J, Rijmen V. AES Proposal: Rijndael[R]. Document Version 2, 1999.

7 Calderbank R, Daubechies I, Sweldens W, *et al*. Wavelet transforms that map integers to integers[J]. Journal of Applied Computational Harmonics Analysis, 1998, **5**(3): 32～369.

8 Mallat S G. Multiresolution approximation and wavelet orthogonal base of $L^2(R)$[J]. Transactions of the American Mathematics Society, 1989, **315**(1):69～87.

9 Daubechies I. Orthonormal bases of compactly supported wavelets[J]. Communications on Pure and Applied Mathematics, 1988, **41**(7):909～996.

10 Cohen A, Daubechies I, Feauveau J C. Bi-orthogonal bases of compactly supported wavelets[J]. Communications on Pure and Applied Mathematics, 1992, **45**(1):485～560.

11 Vetterli M, Herley C. Wavelets and filter banks: Theory and design[J]. IEEE Transactions on Signal Processing, 1992, **40**(9):2207～2232.

12 Sweldens W. The lifting scheme: a new philosophy in biorthogonal wavelet constructions[A]. In: Laine A F, Unser M editors. Proceedings of SPIE Wavelet Applications in Signal and Image Processing Ⅲ[C], New York: SPIE, 1995, **2569**:68～79.

13 Daubechies I, Sweldens W. Factoring wavelet transforms into lifting step[J]. Journal of Fourier Analysis' and Applications, 1998, **4**(3):247～269.

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

15 Merkle R C. One way hash functions and DES[A]. In: Brassard G, ed. Advances in Cryptology, CRYPTO'89. Lecture Notes in Computer Science[C], Heidelberg: Springer-Verlag, 1990, **435**:428～466.

罗　永　1976 年生,现为国防科技大学博士研究生,2001 年获国防科技大学硕士学位。主要研究领域为应用数学、信息安全、信息伪装、信号与图像处理等。参与多项国家“863”和自然科学基金项目的研究。发表论文多篇,其中三篇被 SCI 和 EI 检索。

E-mail:yngluo@163.com

成礼智　1962 年生,教授,2002 年获国防科技大学博士学位,现为国防科技大学博士生导师。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、应用数学等。申请多项国家“863”和自然科学基金项目的研究。发表论文 60 多篇,其中 20 多篇被 SCI 和 EI 检索。

吴　翊　1948 年生,教授,现为国防科技大学博士生导师。主要研究领域为应用数学、统计和数据处理。申请并主持多项国家“863”项目的研究。

徐志宏　1977 年生,现为国防科技大学博士研究生,2001 年获国防科技大学硕士学位。主要研究领域为工程力学、数值模拟等。