文章编号 1004-924X(2002)03-0253-04

一种改进的敏感数字水印技术

李 涛,孟庆海,徐 彤
(大连91550部队, 辽宁 大连 116023)

摘要:首先介绍了数字水印的基本原理并对图像数字水印技术进行了总结,然后提出了一种改进的基于离散Haar小波变换和量化编码的敏感数字水印技术。针对原技术的缺陷,在改进技术中,离散Haar小波变换没有进行归一化处理;此外,对量化函数和水印嵌入公式进行了修改。理论和实验证明,这些改进使得该敏感数字水印技术可以更容易地实现,消除了原有的缺陷。最后,结合纠错编码技术提出了一种在验证水印时无需原水印信息的方法。

关 键 词:离散小波变换;敏感数字水印;纠错编码;数据安全
中图分类号:TP391 文献标识码:A

1 引 言

随着数字化的发展,各种信息都以数字化的电子信息形式生成、存储、交换和使用,可以很方便地复制、修改。数字化给人们带来方便的同时也带来了新的问题,如版权保护。数字水印技术是对数字化信息进行版权保护的很有发展前途的技术。数字化的信息包括声音、图像、图形等数据信息形式,对不同形式的信息,数字水印的方法也不同。

所谓数字水印就是在数字化的数据内容中嵌入特定记号。目前主要从密码学、信号处理及通信等三个角度对数字水印技术进行研究。从密码学的角度看,数字水印技术是由信息隐藏或掩盖技术发展而来的。数字水印大致可以分为健壮的数字水印(Robust copyright marking)和敏感的数字水印(Fragile watermarking)。所谓健壮的数字水印是指不管被嵌入数字水印信息的数字信息经过什么处理,只要不影响该数字信息的正常使用,都可以从中提取并确认数字水印的真实性,主要用于所有权确认。而敏感的数字水印是指只要被嵌入数字水印信息的数字信息发生变化,都将影响提取的数字水印,主要用于完整性确认。数字水印技术按人的感觉还可以分为可见水印(Visible watermarking)和不可见水印(Imperceptible watermarking)两种。

2 图像水印的一般方法

嵌入数字水印的一般系统框图如图1所示。对于一个给定的图像(X)、水印信息(I)和密钥K,水印嵌入的过程可以一般描述为$Y=f(I,X,K)$,其中Y为水印处理后的图像。在某些算法中,嵌入图像中的实际水印信息可能与图像、密钥有关,即实际水印信息$W=f_0(I,K,X)$。这样,水印嵌入的过程可以一般描述为$Y=f_1(X,W)$。

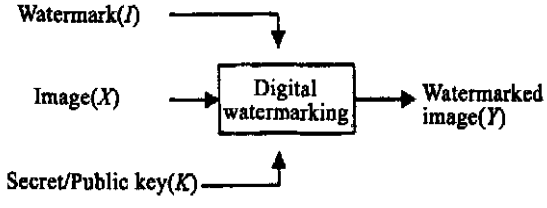

图1 数字水印的一般性嵌入框图

Fig. 1 Generic digital watermarking scheme.

对图像中的数字水印检测技术可以分为要求原图的和不要求原图的,要求水印信息的与不要求水印信息的。对数字水印的检测一般系统框图如图2所示。既不要求原图也不要求原水印信息

收稿日期:2001-10-24;修订日期:2002-03-11

的检测过程可以描述为 $I^* = g(K, X^*)$, 其中 I^* 为提取的水印信息或水印信息的有无。需要原图和原水印信息的检测过程可以描述为: $I^* = g(K, X, X^*, I)$。不需要原图但需要原水印信息的检测过程可以描述为: $I^* = g(K, X^*, I)$。作为商业应用, 对图像中的数字水印检测技术应当是既不要求原图也不要求原水印信息, 直接由用户提供的检测控制方法如密钥或其他信息等从待测图像中提取水印信息或检测水印的有无[1]。

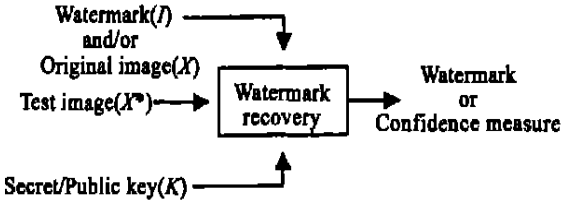

图2　数字水印的一般性检测框图

Fig. 2　Generic watermark recovery scheme.

数字水印信息一般分为伪随机信号和确定性信息。伪随机信号可以是白噪声、高斯噪声或随机二进制信号等, 它们用于区分图像的拥有者。确定性信息可以是任何形式的代表版权的信息, 在嵌入时都转换成二进制信息。对这两类的数字水印信息的验证方法也不同, 对伪随机信号主要是通过相关检测进行, 而对确定性信息则是进行精确比较统计分析进行。

数字水印嵌入的方法很多, 可以是加法或自适应加法, 另外还可以采用数字通信技术中的数字编码。数字水印的嵌入可以以像素为单位, 也可以以块为单位进行。数字水印的嵌入算法应当是公开的, 但控制嵌入过程的参数或密钥应当保密。嵌入控制可以采用各种保密算法, 如公钥加密算法、单向函数加密(HASH)算法、混沌算法等。

嵌入水印可以在空域或变换域进行, 变换域包括离散傅里叶变换(DFT)、离散余弦变换(DCT)、小波变换(DWT)等。

有发展前途的健壮数字水印算法应当是结合人类视觉特性, 针对图像的特征如物体的轮廓、纹理或其它特点, 进行数字水印信息的嵌入。这样, 只要图像没有受到影响图像正常使用的处理或图像的特征没有受到破坏, 都可以进行数字水印的提取或验证, 保证了数字水印的健壮性。

3　基于Haar小波变换的敏感数字水印方法

图像在存储、传输过程中, 可以很容易地修改。这样, 有时需要对图像的真伪进行鉴别验证, 检验图像是否发生修改及修改的范围。虽然数字签名技术可以进行数据的完整性保障工作, 但那需要进行公钥管理和签名管理。利用敏感数字水印技术检测图像的真伪则很容易。在文献[2]中, D. Kundur 等人给出了一种基于 Haar[6] 小波变换和量化编码的敏感数字水印方法, 但该方法有一定的缺陷。为此, 我们对该方法进行了改进, 提出了一种改进的数字水印算法, 如下所述。

3.1　水印嵌入算法

1) 输入给定数据

原图像 $f(m, m)$, 其大小为 $M \times M$, 像素颜色值或灰度值可以为8位或更多;

数字水印数据 $W(i)$, 其中 $i = 1, \ldots, N_w$, 其值为0或1;

数字水印的密码 $\mathrm{ckey}(i)$, 其值为0或1, 可以由给定的密钥采用混沌算法或单向函数加密算法产生, 其中 $i = 1, \ldots, N_w$。如不输入水印密码, 则取水印密码全为0。

2) 选择嵌入水印参数

小波分解级数 L;

嵌入水印的区域: 在低频近似区或横向、纵向及对角线分量区嵌加水印;

量化及嵌入水印信息的幅度 $\mathrm{d}Q$ (正整数);

3) 生成有效水印数据

$W_1(i) = W(i) \oplus \mathrm{ckey}(i)$。

4) 对原图像进行 L 级 Haar 小波分解

小波分解后得到其横向、纵向及对角线分量, 还有图像的低频信息, 小波信息定义为 $f_{L,K}(m, m)$, 其中 K 可以为 H(代表横向分量信息)、V(代表纵向分量信息)、D(代表对角线分量信息)及 A(代表低频近似信息)。

5) 嵌入水印

对于每个要嵌入水印的小波信息, 进行如下处理:

①量化

量化函数定义为 $D(f_{L,K}(m, m))$。量化规则为: 如果 $f_{L,K}(m, m)/\mathrm{d}Q$ 是奇数, 则

$D(f_{L,K}(m,m))=1$; 如果$f_{L,K}(m,m)/\mathrm{d}Q$ 是偶数或者是 0, 则 $D(f_{L,K}(m,m))=0$。

在程序实现时, 首先进行 $abs(f_{L,K}(m,m))/\mathrm{d}Q$ 的整数运算, 设结果为整数 N, 然后判断 Nmod2 的结果, 如果是 0, 则 $D(f_{L,K}(m,m))=0$; 如果 Nmod2 的结果是 1, 则 $D(f_{L,K}(m,m))=1$。

②嵌入水印信息

如果 $D(f_{L,K}(m,m))$ 不等于 $W_1(i)$, 则

$$f_{L,k}(m,m)=\begin{cases}f_{L,k}(m,m)-\mathrm{d}Q, & \text{if } f_{L,k}(m,m)\geqslant \mathrm{d}Q\\ f_{L,k}(m,m)+\mathrm{d}Q, & \text{if } \mathrm{d}Q>f_{L,k}(m,m)\geqslant 0\\ f_{L,k}(m,m)-\mathrm{d}Q, & \text{if } 0>f_{L,k}(m,m)>-\mathrm{d}Q\\ f_{L,k}(m,m)+\mathrm{d}Q, & \text{if } f_{L,k}(m,m)\leqslant -\mathrm{d}Q,\end{cases}\quad(1)$$

如果 $D(f_{L,k}(m,m))$ 等于 $W_1(i)$, 则不对 $f_{L,k}(m,m)$ 做任何处理。

嵌入水印信息的过程, 可以使得对嵌入水印信息后的图像的 $f_{L,k}(m,m)$ 值重新进行量化的结果数据就是有效水印 $W_1(i)$, 即 $D(f_{L,k}(m,m))=W_1(i)$。

例如:

设 $\mathrm{d}Q=4$, 水印信息 $W_1(i)=0$, $f_{L,K}(m,m)=1$, 则 $D(f_{L,K}(m,m))=0$, 则不对 $f_{L,K}(m,m)$ 进行任何处理; 如果水印信息 $W_1(i)=1$, 则 $f_{L,K}(m,m)=f_{L,K}(m,m)+\mathrm{d}Q=5$, 使得 $D(f_{L,K}(m,m))=1$; 同理可证, $f_{L,K}(m,m)=-1$ 的情况亦是正确的。

设 $\mathrm{d}Q=4$, 水印信息 $W_1(i)=0$, $f_{L,K}(m,m)=5$, 则 $D(f_{L,K}(m,m))=1$, 则 $f_{L,K}(m,m)=f_{L,K}(m,m)-\mathrm{d}Q=1$, 使得 $D(f_{L,K}(m,m))=0$; 如果水印信息 $W_1(i)=1$, 则不对 $f_{L,K}(m,m)$ 进行任何处理; 同理可证, $f_{L,K}(m,m)=-5$ 的情况亦是正确的。

6) 对嵌入水印数据的小波数据做小波逆变换, 得到水印后的图像。

3.2　水印提取认证算法

相关数据及量化函数定义如 3.1。

1) 给出 $\mathrm{d}Q$ 值、小波变换的级数、嵌入水印的位置及数字水印的密码。

2) 对待测图像进行小波变换。

3) 从选定的小波信息中提取数字水印信息并利用数字水印的密码进行解密, 提取实际水印信息的公式为 $W'(i)=D(f_{L,k}(m,m))\oplus \mathrm{key}(i)$。

4) 将提取的数字水印信息 $W'(i)$ 与原水印信息 $W(i)$ 相比较, 确定图像是否发生变化, 从而估计图像被修改的程度。

在文献[2] 中, 公式(1) 为如下形式:

$$f_{L,k}(m,m)=\begin{cases}f_{L,k}(m,m)-\mathrm{d}Q, & \text{if } f_{L,k}(m,m)>0\\ f_{L,k}(m,m)+\mathrm{d}Q, & \text{if } f_{L,k}(m,m)\leqslant 0,\end{cases}\quad(2)$$

在文献[2] 中, 量化规则定义为: 如果 $f_{L,K}(m,m)/\mathrm{d}Q$ 是奇数, 则 $D(f_{L,K}(m,m))=1$; 如果 $f_{L,K}(m,m)/\mathrm{d}Q$ 是偶数, 则 $D(f_{L,K}(m,m))=0$。该规则没有考虑 $f_{L,K}(m,m)/\mathrm{d}Q$ 等于 0 的情况。

此外, 在文献[2] 中, 其 Haar 小波变换进行了归一化处理。如果进行归一化处理, 则由于计算机舍入误差的影响, 实际实现时在一定情况下不能提取正确的水印信息。为此, 本文中的 Haar 小波变换不进行归一化处理。

在实践中, 如果按照原来的量化规则利用公式(2) 进行处理, 在一定情况下不能正确提取水印。例如, 当 $\mathrm{d}Q>f_{L,k}(m,m)>-\mathrm{d}Q$ 时, 量化函数的结果为 0, 既不是偶数也不是奇数, 所以也就不能正确提取水印信息。本文的改进使得该方法更加有效, 适用范围更广。

实验和理论都证明, 增大 $\mathrm{d}Q$, 则提高了嵌入水印的强壮性。但如果 $\mathrm{d}Q$ 太大, 则会造成有些图像数据溢出, 图像质量下降, 从而不能正确提取和认证水印。此外, 在细节信息中嵌入的水印比在低频近似信息中嵌入的水印敏感; 在低阶小波信息中嵌入的水印比在高阶小波信息中嵌入的水印敏感。所以, 应当根据需要选择 $\mathrm{d}Q$ 的大小和嵌入水印的位置。作者对 $\mathrm{d}Q$ 为 1、2、3 的情况都进行过实验, 实验表明: 随着 $\mathrm{d}Q$ 的增大, 水印的可见性越强。

3.3　纠错编码的使用

纠错编码早期是用于数字通信中, 为了增强通信的健壮性, 在原始数字信息中增加纠错信息,

以便能够检错和纠错。比较简单的纠错编码有奇偶校验码、行列监督码、恒比码及正反码等。

为了能够在没有原数字水印的情况下检测图像是否被修改,在将数字水印信息嵌入到图像之前,先将水印信息采用某种纠错编码方式进行纠错编码,然后再将其嵌入到图像中。在提取数字水印信息后,利用纠错编码检查数字水印信息是否改变或纠错。这样,就可以在没有原数字水印信息的情况下,确定图像是否改变,而不必关心数字水印信息是什么,因为数字水印信息已经体现在纠错编码中。

4 结束语

本文提出了一种改进的用于检测图像真伪或是否发生篡改的敏感数字水印方法。针对在验证数字水印信息时需要原数字水印信息,本文还提出在将数字水印嵌入图像之前,先将数字水印信息进行纠错编码,在提取水印信息后利用纠错编码直接验证有效性。这样,实现了不需要原数字水印信息就可以检验水印和图像是否发生变化。

参考文献:

[1] Petitcolas F A P, Anderson R J, Kuhn M G. Information Hiding[A]. *Proceedings of the IEEE* [C] 1999, 87(7): 1062-1078.

[2] Kundur D, Hatzinakos. Digital Watermarking for Telltale Tamper Proofing and Authentication[A]. *Proceedings of the IEEE* [C]. 1999, 87(7): 1167-1180.

[3] Deepa K, Dimitrios H. Digital watermarking using multiresolution wavelet decomposition [A]. *In International Conference on Acoustic, Speech and Signal Processing (ICASP)* [C]. Seattle, Washington, USA, IEEE, 1998, 5: 2969-2972.

[4] Hartung F, Kutter M. Multimedia Watermarking Techniques[A]. *Proceedings of the IEEE* [C]. 1999, (7): 1079-1107.

[5] Hwang M S, Chang C C, Hwang K F. A Watermarking Technique based on One Way Hash Function[A]. *IEEE Transaction on Consumer Electronics* [C]. 1999, 45(2): 286-294.

[6] Stollnitz E J, DeRose T D, Salesin D H. Wavelets for Computer Graphics: A Primer, Part 1[A]. *IEEE Computer Graphics and Applications* [C]. 1995, 15(3): 76-84.

[7] Hwang R W. *A Robust Algorithm for Information Hiding in Digital Pictures* [EB/OL]. http://nif.www.media.edu/Data Hiding/index.html. 1999.

[8] 王新梅,肖 国镇. 纠错码[M]. 西安:西安电子科技大学出版社, 1991.

[9] Bruce Schneier, 吴世忠. 应用密码学[M]. 北京:机械工业出版社, 2000.

Improved fragile watermark technique

LI Tao, MENG Qing_hai, XU Tong

(91550 *Unit of PLA, Dalian* 116023, *China*)

Abstract: This paper firstly introduces the principle of watermark and summarizes the techniques of image watermark. Then an improved fragile watermark technique is presented, where Haar wavelet transform does not involve normalization, and quantization function is mended, watermark embedding equation is also improved. With these improvements, the watermark technique does work precisely. Using the error control code, fragile watermark detection can be done without original watermark.

Key words: discrete wavelet transform; fragile watermark; error control code; data security

作者简介:李涛(1963-),男,辽宁大连人,博士,工程师,研究领域包括信息安全、测控技术等。