基于图像投影序列的盲数字水印鲁棒检测方法*

金 聪[1,2,3+], 彭嘉雄[2]

[1](华中科技大学 图像识别与人工智能研究所,湖北 武汉 430074)

[2](华中师范大学 计算机科学系,湖北 武汉 430079)

[3](中国科学院 研究生院 信息安全国家重点实验室,北京 100039)

A Robust Detection Method of Blind Digital Watermark Based on Image Projective Sequence

JIN Cong[1,2,3+], PENG Jia-Xiong[2]

[1](State Key Laboratory of Education Ministry for Image Processing and Intelligent Control, Huazhong University of Science and Technology, Wuhan 430074, China)

[2](Department of Computer Science, Central China Normal University, Wuhan 430079, China)

[3](State Key Laboratory of Information Security, Graduate School, The Chinese Academy of Sciences, Beijing 100039, China)

+ Corresponding author: Phn: +86-27-62482305, Fax: +86-27-67868318, E-mail: jincong@mail.ccnu.edu.cn

Received 2003-06-06; Accepted 2004-11-03

Jin C, Peng JX. A robust detection method of blind digital watermark based on image projective sequence. *Journal of Software*, 2005,16(2):295–302. http://www.jos.org.cn/1000-9825/16/295.htm

Abstract: Blind digital watermarking, which can detect watermark without using the original image, is a key technique for practical intellectual property protecting systems and concealment correspondence systems. In this paper, a blind detection method for the digital image watermark is discussed. The theoretical research shows that the orthogonal projection sequence of a digital image is one-to-one correspondence with this digital image. By this conclusion, a kind of blind watermarking detector with good performance is designed and realized. To calculate the correlation value between the image and watermark, the pixel information of digital image is not adopted, but the orthogonal projection sequence of this image is adopted. Experimental results show that this watermark detector has not only the good robustness to Gaussian noise, but also the very strong resistant ability to translation and rotation attacks. Performance of this watermark detector is better than that of the general detector designed by using the pixel value information directly. The conclusions are useful for the research in the future.

Key words: digital watermark; image projective sequence; blind detection; geometrical attacks; robustness

摘 要: 检测时无须原始图像的盲数字水印是实用的数字产品版权保护系统和隐蔽通信系统的关键技术之一.理论研究证明,图像的正交投影序列与图像是一一对应的.利用此结论,设计并实现了一种具有良好性能的盲水印检测

* Supported by the National Natural Science Foundation of China under Grant No.F60085002 (国家自然科学基金); the Foundation of Department of Education of Hubei Province of China under Grant No.2003A012 (湖北省教育厅重点基金项目)

作者简介: **金聪**(1960－),女,上海人,教授,主要研究领域为信息安全;**彭嘉雄**(1934－),男,教授,博士生导师,主要研究领域为机器视觉,制导与控制.

器.该水印检测器的相关值不是采用像素值信息,而是采用图像的正交投影序列来计算的.实验结果表明,该水印检测器不仅对旋转、平移攻击有很强的抵抗能力,而且对随机高斯噪声也具有良好的鲁棒性.其性能优于一般的直接利用像素值设计的水印检测器.

关键词: 数字水印;图像投影序列;盲检测;几何攻击;鲁棒性

中图法分类号: TP309 **文献标识码**: A

在过去的几十年中,数字技术和数字媒体(数字声音、文本、图像和视频)深入到各行各业,广泛地应用于个人电脑和开放的网络环境中.随之而来的是,由于人们对原版文件可以进行无限制的任意编辑、修改、拷贝和散布,从而使得数字媒体易于处理,难以管理,其安全性无法得到保证.

一个通用的、在图像中隐藏秘密数据(以下称为水印)的模型可以描述为:嵌入的数据是希望秘密发送的消息,它常常隐藏于一幅公开的图像(称为原始图像)之中,从而产生隐秘图像.一个隐秘密钥用于控制隐藏过程,使得检测或恢复过程仅限于那些知道密钥的人(或者那些知道密钥起源的人).

已有的很多数字水印方法往往对隐藏水印技术的鲁棒性[1−3]进行大量的研究,但基本上集中在抵抗 JPEG 压缩、添加的高斯噪声、低通滤波等操作方面,而对特殊的攻击诸如几何变换常常被忽略,尤其对盲水印检测更是困难重重.对于非盲水印检测问题,人们可以通过将受到攻击的隐秘图像与原始图像比较估计出几何变换的参数,之后进行反变换,从而达到恢复像素同步的目的.对于盲水印检测问题,由于没有原始图像作参考,因此上述方法不能实现.然而,作为数字图像处理的工具,裁剪、旋转、伸缩以及平移等是最常见的操作,而经典盲数字水印技术却正是对这些几何变换缺少鲁棒性.因此有必要对具有抵抗几何攻击性能的盲数字水印算法进行研究.

经典的几何变换一般是将诸如旋转、平移、裁剪、伸缩以及它们的组合施加在隐秘图像上,这些变换是在整幅图像上实施的.很多几何变换可以很方便地用数学形式表示出来.为了精确地检测水印,检测器必须具有被嵌入水印的全部位置信息.但在不使用原始图像的前提下,要实现这个要求是非常困难的.由于对数字图像做几何变换是一件轻而易举的事,而几何变换后所得图像与原始图像在像素坐标上已不同步,因此熟知的相关运算不能使用.已有的抗几何攻击数字水印算法[4−6]都是把图像看作是像素的阵列,因此,一旦图像受到了几何攻击,图像中的水印在不知道受到何种攻击的情况下就不能被检测出来,因为此时同步已失去.

没有原始图像作参考,要确认采用了哪种几何变换的一个基本解决方法是对被测试图像所有可能采用的几何变换一一进行检测.这种处理方法将使计算量飞速上升.例如,如果我们只考虑旋转和伸缩操作的组合(伸缩是使隐秘图像的大小从 50%~200%),粗略估计计算量将增加 5.4×10^4 倍.因此,采用穷举法是不明智的.

目前存在的绝大多数数字水印算法基本上采用加性扩展频谱技术.从视觉角度考虑,水印信号与原始图像信号相比要小得多.为了检测水印,水印检测器通常采用统计方法,例如匹配滤波器等.而采用这种方法,是否同步是检测能否成功的关键.

近年来,新提出的克服几何变换的数字水印方法很多[7,8],但本质上都是把图像看作是像素阵列.目前,尚不存在能够抵抗一般几何变换的数字水印技术.

本文首先分析了图像的正交投影序列与图像之间的关系,证明了在一定条件下它们是一一对应的.利用此结论,我们在设计水印检测器时,不再使用像素值信息来计算归一化相关值,而是利用图像的正交投影序列来计算.通过实验可以证明,这种水印检测器不仅对旋转、平移攻击有很强的抵抗能力,而且对随机高斯噪声也具有很好的鲁棒性.

1 方法描述

已有的盲水印检测技术基本上是将研究重点放在水印嵌入方法上.为了达到抗几何攻击以及盲水印检测的目的,本文并不是将研究重点放在水印嵌入方法的设计上,现有的水印嵌入方法完全可以继续使用,不同的是,我们的水印检测器计算归一化相关值不是采用像素值信息,而是采用图像的正交投影序列.这种水印检测器

设计方法尚未见报道.

为此,我们首先讨论数字图像与其正交投影序列之间的关系问题.

数字图像 $I(x,y)$的 $p+q$ 阶几何矩[9]定义为

$$M_{pq}=\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}x^p y^q I(x,y)\mathrm{d}x\mathrm{d}y \tag{1}$$

这里,$p,q=0,1,2,\ldots$,可以证明,若 $I(x,y)$分段连续且只在有限区域内取非零值,无穷序列$\{M_{pq}\}$与 $I(x,y)$是一一对应的[10].$I(x,y)$是 m 行 n 列的数字图像,记 $m\times n=N$.当通过式(1)计算积分时,在有限区域外的部分可补充定义 $I(x,y)=0$.

设 H 是一个 Hibert 空间, $\{g_i(x,y)\}_{i=1}^{\infty}$ 是这个空间的规范正交基,则

$$\iint_A g_i(x,y)g_j(x,y)\mathrm{d}x\mathrm{d}y=\begin{cases}0, & i\neq j\\ 1, & i=j\end{cases}.$$

设 $I(x,y)\in H$,且为平方可积函数,定义

$$\alpha_i=\alpha(g_i(x,y))_A=\iint_A I(x,y)g_i(x,y)\mathrm{d}x\mathrm{d}y,\ i=1,2,\ldots \tag{2}$$

α_i 是 $I(x,y)$关于这组基的坐标,即正交投影.

无穷序列 $\{\alpha_i\}_{i=1}^{\infty}$ 是否与 $I(x,y)$有一一对应关系?因为由任意无穷序列 $\{\alpha_i\}_{i=1}^{\infty}$ 并不能保证一定存在函数 $I(x,y)$,使得 $I(x,y)$满足式(2),故一般无一一对应关系.但如果 $\{\alpha_i\}_{i=1}^{\infty}$ 满足一定的条件,则这种一一对应关系是存在的.这就是下述定理的结论.

定理. 如果函数项级数 $\sum_{j=1}^{\infty}\alpha_j g_j(x,y)$ 一致收敛,则存在唯一的函数 $I(x,y)$满足式(2).

证明:令 $I(x,y)=\sum_{j=1}^{\infty}\alpha_j g_j(x,y)$.由级数的一致收敛性可知,$I(x,y)$存在,且

$$\iint_A I(x,y)g_i(x,y)\mathrm{d}x\mathrm{d}y=\iint_A g_i(x,y)\left\{\sum_{j=1}^{\infty}\alpha_j g_i(x,y)\right\}\mathrm{d}x\mathrm{d}y,\ i=1,2,\ldots$$

交换积分与求和次序,并且利用函数系的规范正交性,得到

$$\iint_A I(x,y)g_i(x,y)\mathrm{d}x\mathrm{d}y=\alpha_i,\ i=1,2,\ldots$$

即这样确定的 $I(x,y)$满足式(2).下面证明唯一性.

设 $I_1(x,y)\neq I_2(x,y),\ (x,y)\in A$,但两函数对应的投影序列相同,则有

$$\alpha_i=\iint_A I_1(x,y)g_i(x,y)\mathrm{d}x\mathrm{d}y,\ \alpha_i=\iint_A I_2(x,y)g_i(x,y)\mathrm{d}x\mathrm{d}y,\ i=1,2,\ldots$$

两式相减得到 $\iint_A g_i(x,y)\{I_1(x,y)-I_2(x,y)\}\mathrm{d}x\mathrm{d}y=0,\ i=1,2,\ldots$ 由基的完备性[10]得知, $I_1(x,y)=I_2(x,y),(x,\ y)\in A$.这与假设矛盾,故唯一性成立. □

因此,在定理的条件下,利用一般的完备正交基 $\{g_i(x,y)\}_{i=1}^{\infty}$ 获得的正交投影序列 $\{\alpha_i\}_{i=1}^{\infty}$ 与 $I(x,\ y)$一一对应.从而可知无穷序列 $\{\alpha_i\}_{i=1}^{\infty}$ 是图像 $I(x,\ y)$的特征序列.

由于只能取 $\{g_i(x,y)\}_{i=1}^{\infty}$ 的有限项进行研究,所以可以将 $\{g_i(x,y)\}_{i=1}^{\infty}$ 表示为两个互不相交的子集的并,令

$$S=\{g_i(x,y)\}_{i=1}^{N},\ \overline{S}=\{g_i(x,y)\}_{i=N+1}^{\infty}.$$

我们只在 S 上研究数字水印问题,相应的正交投影也只取前 N 个.

本文中,水印嵌入取乘法嵌入规则:

$$J(x,y)=I(x,y)+\omega\cdot I(x,y)\cdot W(x,y),x=0,1,\ldots,m-1;y=0,1,\ldots,n-1 \tag{3}$$

其中, ω 是水印嵌入强度因子.

以下记水印 $W(x,y)$,隐秘图像 $J(x,y)$的有限投影序列分别为 $\boldsymbol{w}=\{w_i\}_{i=1}^{N}$,$\boldsymbol{\beta}=\{\beta_i\}_{i=1}^{N}$,而隐秘图像 $J(x,y)$受到攻击

后所得图像 $\tilde{J}(x,y)$ 的有限投影序列是 $\boldsymbol{\gamma}=\{\gamma_i\}_{i=1}^{N}$.

利用图像有限投影序列进行水印检测,按如下的归一化相关运算方法:

$$c=\frac{\sum_{i=1}^{N}w_i\gamma_i}{\sqrt{\sum_{i=1}^{N}w_i^2}\sqrt{\sum_{i=1}^{N}\gamma_i^2}} \tag{4}$$

如果 $c\geq\rho$,则判断 $\tilde{J}(x,y)$ 嵌入了水印 W,否则判断 $\tilde{J}(x,y)$ 中没有嵌入水印 W.其中, ρ 是预先给定的阈值.

Fourier 变换[10]在图像信号处理方面有许多优点,但是计算机运算时,实、虚部分开运算使之运算速度受到影响.由于 Walsh 函数系[11]是一个完备的规范正交基,因此可以取作计算投影的基.又由于每一个 Walsh 函数取值恒为 1 或−1,不像 DFT 和 DCT 那样要用到复数乘法,而且核矩阵产生容易,所以计算简单,运算速度可以大大提高.

从排列次序上分,Walsh 函数可以有 3 种产生方法,本文采用 Hadamard 矩阵的方法生成 Walsh 函数.利用所生成的一元 Walsh 函数系,按下面顺序排列二元 Walsh 函数系

Walsh(0,x) Walsh(0,y), Walsh(0,x) Walsh(1,y),…,Walsh(0,x) Walsh(n−1,y),

Walsh(1,x) Walsh(0,y), Walsh(1,x) Walsh(1,y),…,Walsh(1,x) Walsh(n−1,y),

… … …

Walsh(m−1,x) Walsh(0,y),Walsh(m−1,x) Walsh(1,y),…,Walsh(m−1,x) Walsh(n−1,y).

共产生 $m\times n$ 个二元 Walsh 函数.对于给定的图像,将计算得到的正交投影序列按照二元 Walsh 函数系的排列方式排成矩阵,可以得到此图像的投影矩阵.此时生成的投影矩阵与图像大小相同.当然,如果图像比较大,可以不取这样多的二元 Walsh 函数.具体使用时,可以根据具体情况来确定.

2 实验结果及讨论

本实验要考察利用图像投影序列来实现盲水印检测的鲁棒性问题.图 1 是大小为 512×512 的灰度图像,将其作为原始图像.随机生成 1 000 个服从高斯分布的随机矩阵 W_i,i=1,2,…,1000,其中 W_{500} 是数字水印,每一个 W_i 都是 m 行 n 列的矩阵,与原始图像有相同大小.图 2 是取 ω=0.03 时将 W_{500} 嵌入图 1 时所获得的隐秘图像.

Fig.1 The original image

图 1 原始图像

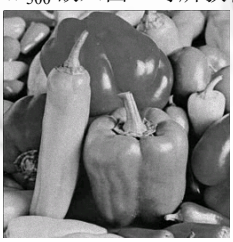


Fig.2 The watermarked image (ω=0.03)

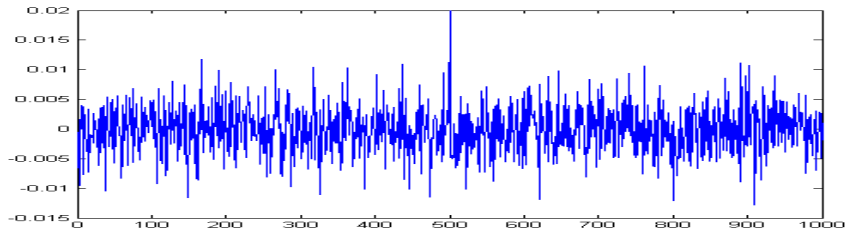
图 2 隐秘图像(ω=0.03)

2.1 两种方法性能测试

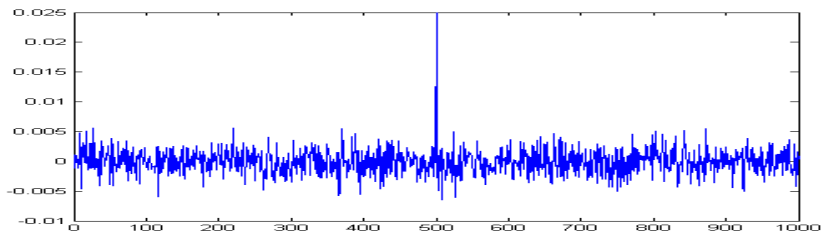
对于水印检测问题,我们分别用隐秘图像像素值(以下称为检测器 1)和图像投影序列(以下称为检测器 2)来计算与数字水印的归一化相关值.对于数字图像,式(2)为

$$\alpha_{ij}=\sum_{k=0}^{m-1}\sum_{l=0}^{n-1}I(k,l)Walsh(i,k)Walsh(j,l),\ i=0,1,...,m-1;\ j=0,1,...,n-1.$$

这里要注意到,在计算相关值时,隐秘图像与水印图像要么同时采用图像投影序列,要么同时都不采用图像投影序列.图 3(a)是检测器 1 的输出结果,图 3(b)是检测器 2 的输出结果,在 500 的输出位置上都形成了峰值.因此,两个检测器都可以成功地对水印进行检测,但比较而言,检测器 2 的性能要优于检测器 1,因为检测器 2 的阈值选择范围比检测器 1 大得多,这可以保证有较低的虚警概率.



(a) Output result of detector 1
(a) 检测器 1 的输出结果



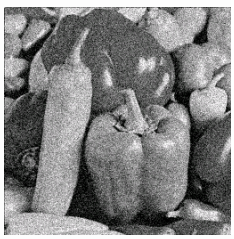
(b) Output result of detector 2
(b) 检测器 2 的输出结果

Fig.3 Comparison of the output results of two detectors

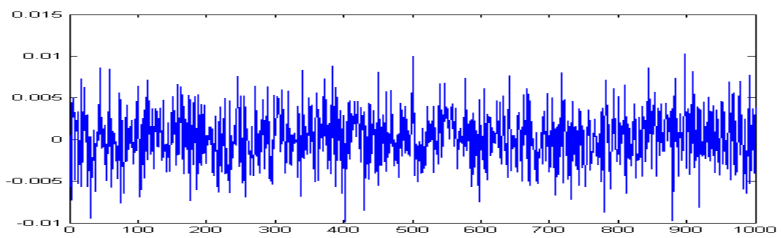
图 3 两种检测器检测结果的比较

2.2 抗噪声攻击测试

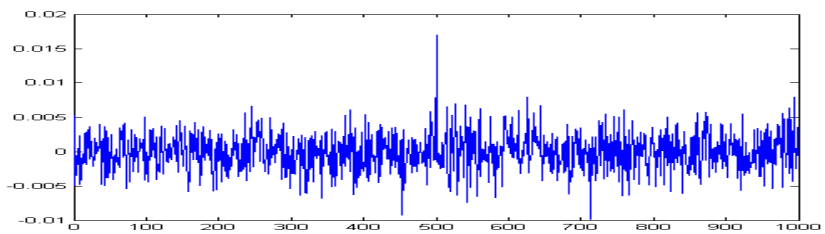
图 4(a)是在图 2 中添加均值为 0,方差为 0.01 的高斯噪声后的结果.我们仍利用两种检测器分别对受到高斯噪声(均值为 0,方差为 0.01)攻击的隐秘图像及不含水印且受到同样攻击的图像进行检测,其检测结果如图 4(b)和图 4(c)所示.



(a) The watermarked image attacked by the Gaussian noise
(a) 受到高斯噪声攻击后的隐秘图像



(b) Output result of detector 1
(b) 检测器 1 的输出结果



(c) Output result of detector 2
(c) 检测器 2 的输出结果

Fig.4 Comparison of the output results attacked by the Gaussian noise of two detectors

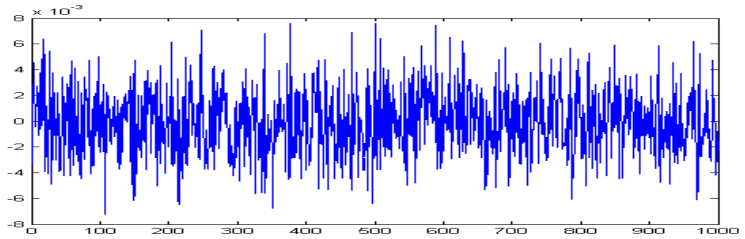
图 4 受到高斯噪声攻击后两种检测器检测结果的比较

从图 4(b)和图 4(c)可见,检测器 1 不能正确地检测出水印,而检测器 2 在 500 的输出位置上形成了较高的峰值.这表明,检测器 2 对噪声干扰不敏感,具有较强的抗干扰能力.这是由于图像的投影特征是图像的积分特征,而图像的积分运算具有平滑作用,因此对噪声具有抵抗能力.

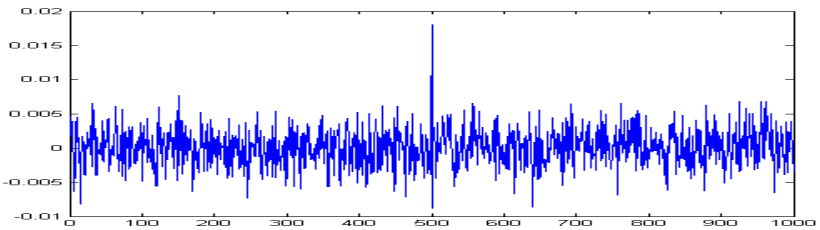
2.3 抗旋转攻击测试

图 5(a)是将图 2 旋转 5º 后的结果.利用两种检测器分别对受到旋转(这里旋转 5º)攻击的隐秘图像及不含水印且受到同样攻击的图像进行检测,其检测结果如图 5(b)和图 5(c)所示.

(a) The watermarked image attacked by rotating 5 degrees
(a) 受到旋转攻击后的隐秘图像



(b) Output result of detector 1
(b) 检测器 1 的输出结果



(c) Output result of detector 2
(c) 检测器 2 的输出结果

Fig.5 Comparison of the output results rotating 5 degrees of two detectors

图 5 旋转 5° 后两种检测器检测结果的比较

从图 5(b)和图 5(c)可见,检测器 1 不能正确地检测出水印,而检测器 2 在 500 的输出位置上形成了较高的峰值.这表明,检测器 2 对旋转攻击不敏感,具有较强的抗旋转能力.这是由于图像的投影特征是图像自身的内在特征,它不依赖于像素的位置而存在,因此对旋转攻击不敏感.

2.4 抗平移攻击测试

图 6(a)是将图 2 分别向右、向下平移 3 个像素后的结果.利用两种检测器分别对受到平移(这里分别向右、向下平移 3 个像素)攻击的隐秘图像和不含水印且受到同样攻击的图像进行检测,其检测结果如图 6(b)和图 6(c)所示.

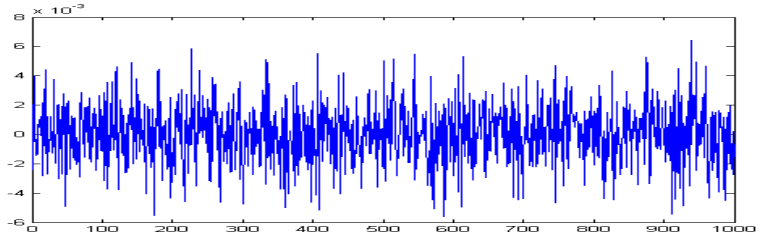
可见,检测器 1 不能正确地检测出水印,而检测器 2 在 500 的输出位置上形成了较高的峰值.这表明,检测器 2 对平移攻击不敏感,具有较强的抗平移能力.其原因与检测器 2 具有较强的抗旋转攻击能力相同.

2.5 抗其他攻击测试

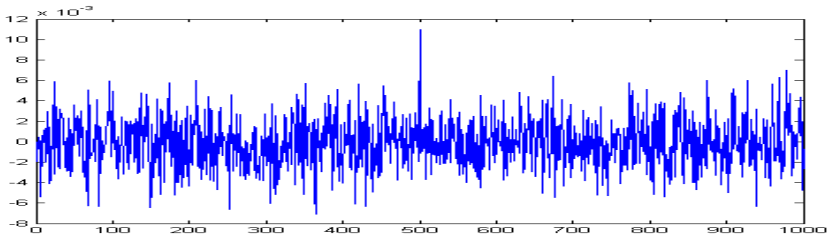
对于两种检测器,我们还进行了其他的攻击测试,主要有均值滤波、JPEG 压缩等.通过测试我们发现,对于这几种攻击,利用两种检测器都不能进行正确的检测.这表明,利用图像投影序列进行水印检测,在抗均值滤波、JPEG 压缩攻击方面,并不比检测器 1 优越.

为了验证新算法在抵抗几何攻击和高斯噪声能力方面的有效性,除上述实验外,我们从 USC-SIPI[12]图像库中另取多幅图像,将它们分别作为原始图像进行与上述相同的实验,实验结果表明,新算法在抵抗几何攻击和高斯噪声能力方面仍具有良好的鲁棒性.

(a) The watermarked image attacked by translating
(a) 受到平移攻击后的隐秘图像



(b) Output result of detector 1
(b) 检测器 1 的输出结果



(c) Output result of detector 2
(c) 检测器 2 的输出结果

Fig.6 Comparison of the output results by translating of two detectors
图 6 平移后两种检测器检测结果的比较

3 结 论

与以往水印检测器的设计方法不同,本文中不采用图像的像素信息,而是利用图像的正交投影序列来实现归一化相关运算,从而部分地实现水印的盲检测.通过实验可以发现,利用图像的正交投影序列来计算归一化相关值,这种水印检测器对高斯噪声攻击、旋转攻击以及平移攻击具有良好的鲁棒性.这为我们进一步设计更好的水印检测器提供了一个新的思路.

References:

[1] Wu YT, Shih FY. An adjusted-purpose digital watermarking technique. Pattern Recognition, 2004,37(12):2349−2359.

[2] Cox IJ, Killian J, Leighton T, Shamoon T. Secure spread spectrum watermarking for multimedia. IEEE Trans. on Image Processing, 1997,6(12):1673−1687.

[3] Barni M, Bartolini F, Furon T. A general framework for robust watermarking security. Signal Processing, 2003,83(10):2069−2084.

[4] Bas P, Chassery JM, Macq B. Geometrically invariant watermarking using feature points. IEEE Trans. on Image Processing, 2002,11(9):1014−1028.

[5] Deguillaume S, Voloshynovskiy S, Pun T. Secure hybrid robust watermarking resistant against tampering and copy attack. Signal Processing, 2003,83(10):2133−2170.

[6] Lin PL. Robust transparent image watermarking system with spatial mechanisms. Journal of Systems and Software, 2000, 50(2):107−116.

[7] Kim BS, Choi JG, Park CH, Won JU, Kwak DM, Oh SK, Koh CR. Robust digital image watermarking method against geometrical attacks. Real-Time Imaging, 2003,9(2):139−149.

[8] Baudry S, Nguyen P, Maître H. Optimal decoding for watermarks subject to geometrical attacks. Signal Processing: Image Communication, 2003,18(4):297−307.

[9] Heikkilä J. Pattern matching with affine moment descriptors. Pattern Recognition, 2004,37(9):1825−1834.

[10] Gelman L, Braun S. The optimal usage of the fourier transform for pattern recognition. Mechanical Systems and Signal Processing, 2001,15(3):641−645.

[11] Harmuth HF. Applications of walsh functions in communications, IEEE Spectrum, 1969,6(11):82−91.

[12] http://umunhum.stanford.edu/~morf/ss/UWB_CDROM_1/PAPERS/WALSHFCT.PDF

[13] USC-SIPI Image Database. 1977. http://sipi.usc.edu/services/database/Database.html

第 2 届全国 Web 信息系统及其应用会议(WISA 2005)

征 文 通 知

全国 Web 信息系统及其应用会议(WISA)是中国计算机学会电子政务与办公自动化专委会主办的系列会议。WISA2005 将于 2005 年 8 月 5 日~7 日在沈阳召开。会议将在 Web 技术、信息系统、电子政务与办公自动化等方面进行深入广泛的学术交流。会议期间除进行会议论文交流外，还将邀请著名学者作特邀报告。本次会议还将评选大会优秀论文和优秀学生论文。

一、征文范围(包括但不限于)

Web 信息挖掘与检索
语义 Web 与智能 Web
Web 与网格计算
Web 与数据库技术
XML 与半结构化数据管理
Web 信息系统环境与基础
Web 应用框架和体系结构
Web 与信息系统安全性
Web 信息系统开发工具
Web 系统度量与分析技术
Web 站点逆向工程与维护技术
Web 测试与 Web 应用的质量保证
多媒体数据管理
工作流模型
组件与中间件技术
代理技术及信息管理
自动文本索引与分类技术
决策支持与分析技术
电子政务与电子商务框架及应用
电子政务与办公自动化发展现状与趋势

二、来稿要求

1．本次会议只接受 Email 投稿。

2．中英文稿均可，一般不超过 6000 字，为了便于出版论文集，来稿必须附中英文摘要、关键词、资助基金与主要参考文献，注明作者及主要联系人姓名、工作单位、详细通信地址（包括 Email 地址）与作者简介。稿件要求采用 WORD 或 PDF 格式。

三、联系信息

1．论文投稿地址： 中国人民大学信息学院 孟小峰 刘青(qliu@ruc.edu.cn)

2．会务情况： 东北大学信息学院软件所 于戈 赵志滨(zhaozb@mail.neu.edu.cn)

3．大会网站：http://www.neu.edu.cn/wisa2005

四、重要日期

1．征 文 截 止 日 期：2005 年 4 月 5 日

2．录用通知发出日期：2005 年 4 月 30 日

3．正式论文提交日期：2005 年 5 月 20 日