图文信息技术

基于 Shamir 门限方案和 DWT 的图像盲水印算法

陈青，司旭
（上海理工大学，上海 200093）

摘要：目的 为了提高数字水印的抗剪切等方面的鲁棒性和不可见性，提出一种基于 Shamir 门限方案和 DWT 的图像盲水印算法。**方法** 首先将水印图像利用 Arnold 变换进行加密处理，然后对置乱后水印图像用 Shamir 门限方案进行分存，接着将原始图像进行分块，并对每块分别做二层离散小波分解，提取出相应的低频系数，通过叠加的方法将分存过后得到的子水印图像分别嵌入相对应的原始图像分块的低频系数中，最后合成图像，完成水印的嵌入。**结果** 实验结果显示，文中算法的不可见性较好，峰值信噪比均在 49 dB 以上，结构相似性接近于 1，并且在各种攻击下，水印 NC 始终大于 0.9。**结论** 文中算法对于剪切、JPEG 压缩和常见的噪声干扰等攻击表现出良好的鲁棒性，并且水印的提取过程无需用到原始图像，实现了水印的盲提取，在版权保护方面具有可行性。

关键词： Arnold 变换；Shamir 门限方案；水印分存；离散小波变换
中图分类号： TP391.41 **文献标识码：** A **文章编号：** 1001-3563(2021)11-0233-05
DOI： 10.19554/j.cnki.1001-3563.2021.11.034

Image Blind Watermarking Algorithm Based on Shamir Threshold Scheme and DWT

CHEN Qing, *SI Xu*
(University of Shanghai for Science and Technology, Shanghai 200093, China)

ABSTRACT: The paper aims to improve the robustness and invisibility of the digital watermarking, image blind watermarking algorithm based on Shamir threshold scheme and DWT is proposed. Firstly, after Arnold transformation of the watermark image was stored with Shamir threshold scheme. Then, the original image was divided into blocks and decomposed into two levels of wavelet, the corresponding low frequency coefficients were extracted, and then the separated watermark was embedded into the low frequency coefficients of the corresponding original image blocks by overlay method. Finally, the synthesized image completed watermarking embedding. The experimental results show that the algorithm has good invisibility, PSNR is above 49 dB, SSIM is close to 1, and the NC value of extracted watermarking is higher than 0.9 under various attacks. The algorithm demonstrates good robustness to shear, JPEG compression and common noise jamming attacks. And the extraction of the watermark does not need the original image. The algorithm achieves the blind extraction of the watermark and has realistic feasibility in copyright protection.

KEY WORDS: Arnold transformation; Shamir threshold scheme; watermarking sharing; discrete wavelet transform

随着科学技术的飞速发展以及互联网的广泛应用，数字化已成为当今社会发展的主流[1]。数字技术的发展在给人们带来巨大便利的同时，其副作用也随之而来。由于数字化信息具有易于存储、复制和传播的特点，因此容易被一些不法分子探知、窃取或者恶意篡改。这些行为严重侵害了原信息拥有者的数字版

收稿日期： 2020-12-04
基金项目： 上海理工大学国家级项目培育基金（16HJPY-MS06）
作者简介： 陈青（1962—），女，博士，上海理工大学副教授，主要研究方向为数字水印。

权，不仅给其带来了巨大的经济损失，也给信息安全造成强烈的冲击[2]。面对日益突出的信息安全问题，数字水印作为解决这类问题的有效手段已经引起人们的高度重视[3]。

数字水印通过在原始数据信息中嵌入水印来保证该信息的所有权，因此保证其安全性尤为重要[4]。在保密性方面，常用的水印嵌入及信息隐藏方案多是将秘密水印图像嵌入单一的图像载体中，这种方法操作简单，易于实现，但是会产生潜在的问题：如果原始图像在传输的过程数据受到攻击被破坏时，则嵌入其中的水印信息就可能无法恢复，或者只能恢复出其中的一部分；另一方面，如果将一份水印数据使用多个载体图像来嵌入时，则随着秘密数据副本的增多同样也会增加数据被截获及破解的可能性[5]。为了解决这些问题，国内外的研究者们开始尝试将传统密码学中门限秘密共享方案应用到数字水印的嵌入和提取过程中来。通过将其与数字水印技术相结合，对要隐藏的水印信息进行处理，提高了非法获取水印的难度，从而达到保护原始信息版权的目的，逐渐成为信息安全领域的研究热点[6]。

文中提出一种基于Shamir门限方案和DWT的图像盲水印算法。该算法首先对原始载体图像进行 2×2 分块，接着将经过 Arnold 置乱后的水印图像利用 Shamir 门限方案对其进行分存加密，使加密后水印的数量与原始图像块数相同。然后对每块原始图像进行二级小波分解，选择逼近子图系数，对其进行修改，再将相对应块数的水印嵌入其中，最后进行图像的合成，完成水印的嵌入过程。

1 基本原理

1.1 Arnold 变换

Arnold 变换是一种比较常见的图像置乱算法，对 $N\times N$ 的二维图像进行 Arnold 变换，可表示为[7]：

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\, N) \quad x, y \in \{0,1,\cdots,N-1\} \tag{1}$$

式中：a，b 为正整数；(x, y)为原图像像素的坐标；(x', y')为变换后新图像像素的坐标。

Arnold 变换的逆变换为：

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ab+1 & -a \\ -b & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} (\mathrm{mod}\, N) \tag{2}$$

1.2 离散小波变换

DWT 是一种对图像数据进行时间-频率变换的常用方法，它具有时域、频域表征信号局部特征的能力[8]。经过小波分解后的图像具有很好的方向选择性，并且与人的视觉特性十分相符。利用人类视觉系统的掩蔽特性，将水印嵌入图像的纹理和边缘等区域，而不易被察觉[8]。对图像进行小波变换后，图像的纹理、边缘等信息主要表现在 HH，HL 和 LH 细节子带中一些比较大的系数上，而低频子带（LL）则包含图像的主要特征[9]。由此可知，将水印信息嵌入经过修改后的图像某些系数中，可以达到良好的嵌入效果[10]。根据 Weber 定律[11]，图像的对比度与其背景信号的幅度成正比，由于低频系数的幅值一般远大于高频系数，低频子带中含有较大的感觉容量，因此水印信息常常被嵌入图像小波的低频子带中，得到图像的鲁棒性较好。

1.3 Shamir 秘密共享方案

秘密门限共享[12—13]的思想是：为了确保秘密信息 M 的安全性，在开始保存时将其分成 n 份，且这 n 份之间的交集为空集，这 n 份中任意的一份都可称之为原信息 M 的子秘密或者子密钥，然后将其分别交给 n 个人去保管，要求任意 t（$t_0 \leqslant t \leqslant n$，$t_0$ 为该方案固有的阈值）个人将自己得到的子密钥合在一起可以无损地推导出秘密信息 M，而少于 t 个子密钥则无法恢复处秘密 M。这种方案也称之为(t, n)门限共享方案，简称门限方案，t 为门限值。以色列著名的密码学专家 Shamir 提出了一种基于拉格朗日插值法的秘密门限共享方案[14]。

在有限域 $GP(q)$中，有 $q>n$，要想将密钥 M 交由 n 个人保管，则需先分成 n 份，要求随意选取 $t(t \leqslant n)$ 个人将他们手中的子密钥合在一起可以得到密钥 M。这可以通过随机选取 $t-1$ 个整数 $b_1, b_2, \cdots, b_{t-1}$，$0 \leqslant b_j \leqslant q-1 (1 \leqslant j \leqslant t-1)$，用来构造出一个 $t-1$ 次多项式：

$$M_k = g(x_k) = (M + b_1 x_k + \cdots + b_{t-1} x_k^{t-1}) \bmod q \tag{3}$$

在多项式（3）中需遵循以下几个条件。

1）t 和 k 是不大于 n 的正整数。

2）$b_1, b_2, \cdots, b_{t-1}$是在 $GP(q)$随机选取的整数。

3）每个选定的 x_k 代表各个参与者的公开 ID 号，不能重复。带入式（3）计算出对应的 $g(x_k)$值。

然后将子密钥 M_k 及编号 k 交给用户 B_k，即用户 B_k 获得序列号对(k, B_k)。当有任意 t 个人或者以上的用户相结合，即用户 $B_1, B_2, \cdots, B_t$ 分别交出了各自的序列号对(t, M_t)，则这时可以利用 Lagrange 插值公式[15]：

$$g^*(x) = \sum_i^t M_i \prod_{j=1, i \neq j}^{t} \frac{x - x_j}{x_i - x_j} \bmod(q) \tag{4}$$

得到 $t-1$ 次多项式。由于 $g^*(x)=g(x)$，因此原密钥 M 得以恢复：$M=g(0)=g^*(0)$。

使用式（4）恢复共享秘密 M 时，必须要有 t 个或者以上的参与者相联合，即提供至少 t 份子秘密；当只有 $m(m<t)$份子秘密时，无法确定 $g(x)$，因此恢复不出来秘密信息 M。

2　水印算法

2.1　水印的预处理

读入 $m\times n$ 的二值水印图像 W，并利用式（1）对其进行 γ 次 Arnold 置乱处理，处理结果见图 1。文中取置乱次数 γ=6，水印尺寸为 64×64。

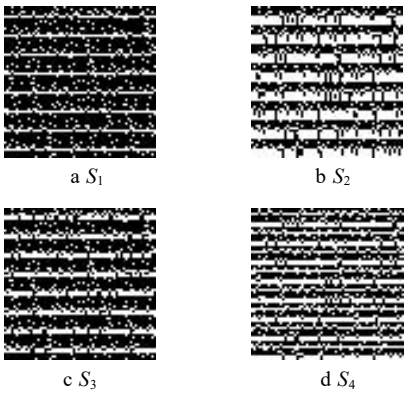
对置乱后的水印图像矩阵以 8 bit 为一组转化为十进制数据，这样得到转化后的十进制数据 $M_i(1\leqslant i\leqslant\lceil m\times n/8\rceil)$($\lceil\rceil$为向上取整符号)处于(0, q−1)之间。构造门限素数 q，因为将水印矩阵分组转化为十进制数据 $M_i\in[0,255]$，而素数 q 是大于 M_i 的最小素数，所以 q 取 257。

构造(3,4)的门限共享体系，即 t=3, n=4。确定一个二次多项式 $u_j=g_j(x_j)=(M_i+b_1x_j+b_2x_j^2)\bmod q(1\leqslant j\leqslant 4)$。$M_i$ 为步骤 2 中得到的数据，b_1 和 b_2 为随意整数，文中 b_1=1, b_2=2。

分别取 4 个大小不同的 x_j 带入上述多项式，得到十进制数组 u_1, u_2, u_3, u_4，再将 u_j 转化为二进制数后就得到分存后的 4 块子水印图像 S_1, S_2, S_3, S_4，见图 2。

a 水印图像　　b Arnold 变换图像

图 1　水印图像和 Arnold 变换图像
Fig.1 Watermark image and Arnold transform image



a S_1　　b S_2

c S_3　　d S_4

图 2　子水印图像
Fig.2 Shadow watermark image

2.2　水印的嵌入算法

1）载体图像分块。读入大小为 512×512 载体图像 I，并将其分成 4 块。

2）小波分解。对 4 块分别进行二级小波分解，得到不同分辨率下的细节子图 HL_i, LH_i, HH_i（i=1, 2）和逼近子图 LL_2,其低频子图系数为 $A_j(j$=1,2,3,4)

3）水印叠加嵌入。将 4 幅子水印图像 $S_j(j$=1,2,3,4)依次按照水印叠加嵌入的方法将其嵌入逼近子图系数 A_j 中，即 $A'_j=A_j+c*S_j$，其中 c 为嵌入强度，实验中取 c=0.1。

4）调整逼近子图系数。A_j^*=round(A'_j/d)*d，round 为四舍五入运算，d 为量化系数，实验中取 d=0.1555。

5）小波重构与载体图像合成。对嵌入水印的图像进行二级小波重构并合成，最后得到嵌入水印后图像 IG。

6）生成并保存密钥 K。K_j=xor(mod(A_j^*,2), S_j)，xor 为异或操作，mod 为取余。

2.3　水印的提取算法

水印的提取是水印的嵌入过程的逆过程，具体步骤如下所述。

1）对含水印图像 IG 分块后再进行二级小波分解，得到其低频子带系数为 A_j。

2）计算 A_j^*=round(A_j/d) *d。

3）利用密钥 K 提取子水印图像：S_j = xor (mod(A_j^*, 2), K_j)。

4）任意选择 4 块提取出的子水印图像中的 3 块，就可以恢复出原始的水印。即已知 S_o, S_p, S_q ($i\leq o<p<q\leq$ 4) 3 块子水印，根据 2.1 节内容将其转换成十进制数 U_o, U_p, U_q，那么可以利用 Lagrange 插值公式：

$$h(x)=u_o\frac{(x-p)(x-q)}{(o-p)(o-q)}+u_p\frac{(x-o)(x-q)}{(p-o)(p-q)}+u_q\frac{(x-o)(x-p)}{(q-o)(q-p)}\bmod q \tag{5}$$

求出 $h(0)=\dfrac{pqu_o}{(o-p)(o-q)}+\dfrac{oqu_p}{(p-o)(p-q)}+\dfrac{opu_q}{(q-o)(q-p)}\bmod q=M'$，再将其转换为二进制即为置乱后的水印图像 W'。

5）对 W'进行 T–γ 次 Arnold 置乱，即可恢复出原水印图像 W，其中 T 为水印的置乱周期。文中选择的水印图像为 64×64 的二值图像，其 Arnold 置乱周期 T=48。

3　实验结果与分析

文中提出的算法以 Matlab R2014a 为运行平台，选取 512×512 的 Lena，Pepper，Baboon 和 Airplane 灰度图像作为载体图像，选取 64×64 的 usst 二值图像作为水印图像进行实验，分别进行水印的不可感知性能和鲁棒性能测试。

3.1　不可见性分析

由于载体图像在嵌入水印之后可能存在部分失

真，因此选择峰值信噪比（Peak Signal-To-Noise, PSNR）来定量评价嵌入水印后图像的质量。当含水印图像在受到各种各样攻击时，会在一定程度上使得图像内部结构遭到破坏，从而导致提取出的水印图像与原始的水印图像有所不同，为此用归一化相关系数（Normalized Cross-correlation, NC）来定量衡量受到攻击后提取的水印和原始水印的相似度。除此之外，还用结构相似性（Structural Similarity，SSIM）来更加准确地衡量水印嵌入前后图像相似度。给定 2 个图像 x，y，其结构相似性 SSIM 定义为：

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{5}$$

式中：μ_x 为 x 的平均值；μ_y 为 y 的平均值；σ_x^2 为 x 的方差；σ_y^2 为 y 的方差；σ_{xy} 为 x 和 y 的协方差；$c_1=(k_1L)^2$，$c_2=(k_2L)^2$ 为维持稳定的常数；L 为像素值的动态范围，实验中取 255；$k_1=0.01$，$k_2=0.03$。

对 4 个不同的载体图像分别进行嵌入和无攻击提取水印操作，结果见表 1。通过表 1 可以看出，在未受到攻击的情况下，提取水印的 NC 值都为 1，表明水印都可以被无损地提取出来。通过仔细地观察载体图像和含水印图像可以发现，嵌入水印后图像质量没有明显视觉差别，几乎感觉不到水印的嵌入；图像的 PSNR 全都在 49 dB 以上，而且 SSIM 都在 0.99 以上，接近于 1。另外将文中算法与文献[7]和文献[8]中的算法相比较，PSNR 的值均高于文献[7]和文献[8]，表明文中算法具有很好的不可见性。

3.2 鲁棒性分析

在图像的印刷和传输过程中，会受到各种各样攻击，常见的攻击包括在保存图像时进行的压缩和剪切，以及在传输途径的过程中引入的噪声等。为了测试含水印图像在不同的攻击情况下的鲁棒性，对其进行剪切、添加噪声、JPEG 压缩及中值滤波等信号的攻击，然后提取水印，并将其与文献[10]和文献[16]中算法提取的水印 NC 值相比较，结果见表 2。

根据表 2 的实验结果可得知，文中算法在受到各种攻击的情况下，仍然能很好地提取出水印，并且水印的 NC 值始终保持在 0.92 以上，高于文献[10]和文献[16]的水印算法的 NC 值，因此在对于常规的攻击具有较好的鲁棒性。特别对于剪切攻击，从表 2 结果可以看出，当对含水印图像进行不超过 1/4 的剪切时，提取水印的 NC 值都为 1，表示可以完整地恢复出全部的水印信息，可以有效地抵挡剪切方面的攻击，在这方面较文献[10]和[16]的鲁棒性有了很大的提升。由此通过数据的对比，文中算法对剪切、噪声、JPEG 压缩及滤波等方面的攻击具有较好的鲁棒性。

表 1 原始图像和含水印图像

Tab. 1 Original image and watermarked image

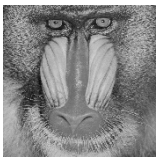
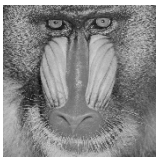
载体图像	含水印图像	提取的水印	NC	SSIM	PSNR/dB		
					文中算法	文献[7]	文献[10]
			1	0.9963	49.5106	47.6649	37.1851
			1	0.9987	49.1084	46.6143	36.8880
			1	0.9980	49.2278	45.5163	37.0499
			1	0.9998	53.3395	—	—

表 2　攻击实验结果
Tab.2 Results of attack experiment

攻击参数	提取的水印	NC 值		
		文中算法	文献[10]	文献[16]
1/16 剪切		1	0.9216	—
1/4 剪切		1	0.8203	0.9521
JPEG 压缩 (Q = 80)		0.9633	0.9497	0.9161
JPEG 压缩 (Q = 20)		0.9206	—	0.8671
椒盐噪声 0.01		0.9886	0.7326	0.9386
高斯噪声 0.01		0.9659	0.9544	0.9033
中值滤波(3×3)		0.9565	0.9847	0.9368
高斯低通滤波 (3×3)		0.9937	0.9435	—

4　结语

文中以 Shamir 秘密门限共享方案和 DWT 理论为基础，提出一种可以有效抵抗剪切攻击的数字水印算法。利用 Arnold 变换对水印图像进行加密后，再进行分存处理，起到了二次加密的作用，提高了算法的安全性。当且仅当获得 t 份子水印时，原始数字水印才得以恢复。因为该算法把一份水印分成多份，同时提高了水印的嵌入量。实验结果表明，该算法嵌入水印后的图像其不可见性较好，对于剪切、JPEG 压缩和常见的噪声干扰等攻击表现出良好的鲁棒性。

参考文献：

[1] SUNESH R, RAMA K. A Novel and Efficient Blind Image Watermarking in Transform Domain[J]. Procedia Computer Science, 2020, 167: 1505—1514.

[2] LEE Y S, SEO Y H, KIM D W. Digital Blind Watermarking Based on Depth Variation Prediction Map and DWT for DIBR Free-Viewpoint Image[J]. Signal Processing: Image Communication, 2018, 70: 104—113.

[3] POONAM S, SHAIFALI M A. A DWT-SVD Based Robust Digital Watermarking for Digital Images[J]. Procedia Computer Science, 2018, 132: 1441—1448.

[4] YUAN Shen, MAGAYANE D A, LIU Xue-mei, et al. Blind Watermarking Scheme Based on Computational Ghost Imaging in Wavelet Domain[J]. Optics Communications, 2021, 482: 123—129.

[5] CRESCENZO G D. Essential Secret Image Sharing Scheme with Small and Equal Sized Shadows[J]. Signal Processing: Image Communication, 2020, 87: 186—196.

[6] YOGESH M, LAXMI S, HIMANSHU S. Secure and Efficient Arithmetic-Based Multi-Secret Image Sharing Scheme Using Universal Share[J]. Journal of Information Security and Applications, 2019, 47: 267—274.

[7] 张帅，杨雪霞. 一种基于 DWT—DCT 的数字图像盲水印算法[J]. 现代计算机, 2020(24): 33—36.
ZHANG Shuai, YANG Xue-xia. A Blind Watermarking Algorithm for Digital Image Based on DWT-DCT[J]. Modern Computer, 2019(24): 33—36.

[8] 周广州，陈青，熊蒙，等. 一种基于 Harris 特征点和 DWT—SVD 的图像盲水印算法[J]. 包装工程, 2016, 37(19): 191—194.
ZHOU Guang-zhou, CHEN Qing, XIONG Meng, et al. An Image Watermarking Algorithm Based on Harris Feature Points and DWT-SVD[J]. Packaging Engineering, 2016, 37(19): 191—194.

[9] 雷蕾. 基于变换域的数字图像水印算法研究[D]. 长春: 吉林大学, 2013: 38—49.
LEI Lei. Research of Digital Image Watermarking Algorithm Based on Transformation Domain[D]. Changchun: Jilin University, 2013: 38—49.

[10] 席光伟，余丽群. 基于混沌映射的 DCT 域鲁棒图像水印算法[J]. 计算机时代, 2020(12): 10—13.
XI Guang-wei, YU Li-qun. A Robust Image Watermarking Algorithm Based on DCT and Chaotic Mapping[J]. Computer Era, 2020(12): 10—13.

[11] JEROEN B, IOSEPH A H, RAFAEL P. Weber's Law: A Mechanistic Foundation after Two Centuries[J]. Trends in Cognitive Sciences, 2019, 23(11): 906—908.

[12] 牛少彰，钮心忻，杨义先，等. 基于拉格朗日插值公式的数字水印分存算法[J]. 北京邮电大学学报, 2003, 26(3): 8—11.
NIU Shao-zhang, NIU Xin-xin, YANG Yi-xian, et al. Digital Watermarking Sharing Algorithm Based on Lagrange Interpolation Formula[J]. Journal of Beijing University of Posts and Telecommunications, 2003, 26(3): 8—11.

[13] LEIN H, XIA Zhe, LIU Yi-ning, et al. Secret Sharing with Secure Secret Reconstruction[J]. Information Sciences, 2020, 519: 1—8.

[14] 谭亦夫，李子臣. 基于 Shamir 门限秘密分享的图像可视加密算法[J]. 网络与信息安全学报, 2018, 4(7): 69—76.
TAN Yi-fu, LI Zi-chen. Image Visualization Encryption Algorithm Based on Shamir Threshold Secret Key Sharing[J]. Chinese Journal of Network and Information Security, 2018, 4(7): 69—76.

[15] YAN Xue-hu, LIU Lin-tao, LU Yu-liang, et al. Security Analysis and Classification of Image Secret Sharing[J]. Journal of Information Security and Applications, 2019, 47: 208—216.

[16] 钱言玉，吴友情. 一种基于多数字基整数的数字水印分存算法[J]. 计算机应用与软件, 2016, 33(11): 317—320.
QIAN Yan-yu, WU You-qing. A Watermarking Sharing Scheme Based on Multiple-Based Number[J]. Computer Applications and Software, 2016, 33(11): 317—320.