文章编号:1000－2367(2016)02－0157－06 DOI:10.16366/j.cnki.1000－2367.2016.02.028

# 基于 DWT-DCT 灰度图像小阴影尺寸的 VSS 加密技术

李 伟[a],孙云娟[b],刘玉芳[a]

(河南师范大学 a.物理与电子工程学院;b.新联学院,河南 新乡 453007)

**摘 要**:提出了灰度图像的最新的(2,$n$)可视加密共享技术方案(VSS).它是基于频域的分析方法,该方法利用 DWT 以及 DWT-DCT 高性能的压缩比,计算效率高,恢复图像误差小,并且避免了较大的传统阴影尺寸.实验结果证实了该方法的有效性,即重构了高质量的原始图像,且产生了小尺寸的灰度阴影.

**关键词**:DWT; DCT; Shamir 方案;可视加密共享方案

**中图分类号**:TP317 **文献标志码**:A

灰度图像的可视加密共享技术在最近阶段已经发展起来.传统方案典型的问题是计算的复杂性,以及传输的高成本和存储量的高成本问题.文献[1]中提出的(2,$n$)的方案适用于二进制图像,利用简单的布尔运算并且无像素扩展;文献[2]中的($k$,$n$)方案适用于二进制图像、灰度图像、彩色图像,利用矩阵扩展算法对于 VSS 提出了一个基本的构建;文献[3]中的(2,2)方案采用了误差扩散算法和图像聚类技术,具有小的阴影尺寸和较低的计算复杂性;文献[4]提出了一个适合灰度图像的尺寸不变 VSS 方案;文献[5]中提出的方案,阴影尺寸比较清晰,文献[6]中给出了一个计算成本特别低的方案;文献[7]中利用 DWT 变换进行频域分析,但由于模块尺寸 $m$ 较大时,向量量化及模块截断编码所产生的误差大,因此恢复出的图像与原始图像产生较大的误差.本文应用频域分析方法,利用 DWT 以及 DWT-DCT 的高性能压缩比,提出了新的(2,n)可视加密共享方案,计算效率高,并且产生较小的阴影尺寸,可以恢复出高性能的原始图像.

## 1 基本理论

1) Shamir 方案. 1979 年 Shamir 提出了基于多项式内插方法的($k$,$n$) 阈值方案[8].该方案中将所要加密的数据 $s$ 分成 $n$ 份,每一份称为一个 share,或一个阴影 shadow.它是基于任一有限 $GF(q)$ 域中 $k-1$ 阶共享多项式产生,即:

$$f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}, \tag{1}$$

其中 $q$ 为质数,$s = f(0) = a_0$,其它系数在该域中随机选择.份 $s_i = f(i)$ 被指为加密数据的第 $i$ 份构成.

为了恢复加密数据 $s$,至少需要 $n$ 份当中的任意 $k$ 份.首先必须获得多项式 $f(x)$ 的系数,这些系数来自于拉格朗日内插公式:

$$l_i = \prod_{\substack{1 \le j \le k \\ i \ne j}} \frac{x - x_j}{x_i - x_j}, \tag{2}$$

则即可产生 $k-1$ 阶共享多项式:

$$f(x) = \sum_{i=1}^{k} (s_i \times l_i) \ (q \text{ 为模}), \tag{3}$$

最后可以恢复数据 $s = f(0)$.下面给出 Shamir 方案步骤.

加密数据 $s$ 的 $n$ 份构建(已知加密数据 $s$,$k$, $n$ $1 \le k \le n$):

**收稿日期**:2014-12-27;**修回日期**:2015-12-13.

**基金项目**:国家自然科学基金(61127012)

**第 1 作者简介(通信作者)**:李 伟(1967－),男,河南新乡人,河南师范大学讲师,研究方向为数字图像处理、模式识别、水印技术、安全技术等,E-mail:weiwei19671028@126.com.

**步骤 1** 在有限 $GF(q)$ 域中,定义一个 $k-1$ 阶 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1}$ 共享多项式,其中 $s=a_0$,其他系数在该域中任意选择,$q$ 为质数.

**步骤 2** 计算出 $s_i=f(i)$,$i=1,2,\cdots,n$ 即可获得加密数据 $s$ 的 $n$ 份构成$(i,s_i)$.

数据 $s$ 的恢复步骤:

**步骤 1** 根据公式(3) 计算多项式 $f(x)$ 的系数.

**步骤 2** 根据 $s=f(0)$ 恢复数据.

该方案的鲁棒性在于暴露 $k-1$ 份都不会危机密钥,同时若 $n-k$ 份丢失或损坏,还可以恢复加密数据.该方案可以抵挡任何不当行为的攻击,以达到分散风险和容忍入侵的目的,保证信息的安全性和可靠性.

为了具体说明该方法步骤,现给出一例子:已知 $s=206$,选择 $n=6$,$k=3$.

加密数据 $s$ 的 $n$ 份构建:

**步骤 1** 任意选择两个随机数 $r=n/m$,且令 $f(x)$. 于是构造一个多项式函数:$a_0=s$,模为 257.

**步骤 2** 计算加密数据的 6 份构成:

$\{i,f(i)\}=\{(1,209),(2,143),(3,8),(4,61),(5,45),(6,217)\}$,其中$(i,f(i))$ 为其第 $i$ 个阴影数据$s_i$.

数据 $s$ 的恢复步骤:

从 6 份数据中随机选择 3 个数据:(2,143),(4,61),(5,45).

**步骤 1** 计算拉格朗日基多项式:

$$l_1=\frac{x-x_2}{x_1-x_2}\cdot\frac{x-x_3}{x_1-x_3}=\frac{x-4}{2-4}\cdot\frac{x-5}{2-5}=\frac{x-4}{-2}\cdot\frac{x-5}{-3},$$

$$l_2=\frac{x-x_2}{x_2-x_1}\cdot\frac{x-x_3}{x_2-x_3}=\frac{x-2}{4-2}\cdot\frac{x-5}{4-5}=\frac{x-2}{2}\cdot\frac{x-5}{-1},$$

$$l_3=\frac{x-x_1}{x_3-x_1}\cdot\frac{x-x_2}{x_3-x_3}=\frac{x-2}{5-2}\cdot\frac{x-4}{5-4}=\frac{x-2}{3}\cdot\frac{x-4}{1},$$

则构造的拉格朗日内插多项式:

$$f(x)=\sum_{i=1}^{3}s_i\cdot l_i=143\cdot l_1+61\cdot l_2+45\cdot l_3=94x^2+166x+206,\text{模为 }257.$$

**步骤 2** 获得加密数据 $s=f(0)=206$.

2) 离散小波变换(DWT)和离散余弦变换(DCT). 离散小波变换已经成功用于纯数学领域以及应用科学领域.小波变换非常容易分析信号的瞬时特性和频谱特性,并且表示非平稳信号非常灵活.为了计算灰度图像的一阶两维 DWT,首先按行计算该图像的一维 DWT,其次再按列计算图像的一维 DWT,最后得出图像的 4 个子带分量:LL,LH,HL,HH. LL 为原始图像的低频分量,其余 3 个分量为原始图像的高频分量.如果再继续将 LL 分量分解,可得到原始图像的二阶 DWT.若将 LL 分量进行离散余弦变换,即 DWT-DCT 变换,设定不同的阈值,抛弃低能量频率分量,并且可以得到可观的压缩比.由于 DWT 和 DCT 的高性能压缩比,这使得它广泛地应用于数字图像处理和数据压缩中[9-10].

图像可视加密共享方案的主要目标是产生一个可接受质量的重构图像,并且生成一个足够小尺寸的阴影图像,计算效率要高.在可得到的小波中,Haar 小波具有算法简单,计算成本低,并且具有其他小波高的压缩比性能.选择 Haar 小波作为图像加密的首选小波.

## 2 提出的方法

假设原始图像尺寸大小为 $n\times n$ 像素,且 $n$ 为 2 的整数次幂,将其划分成 $m\times m$ 像素的子模块,$m$ 也为 2 的整数次幂,且 $m<n$. 非常显然原始图像可以划分成 $r\times r$ 个子模块,其中 $r=n/m$.

将每一个子模块图像,大小为 $m\times m$ 像素,进行二维 DWT 变换分解.每一模块可以分解成 4 个子带分量,即 LL,LH,HL,HH.再将 LL 分量进行 DWT 变换,即二 阶 DWT 变换.若将 LL 分量进行 DCT 变换,即 DWT-DCT 变换.小波变换和离散余弦变换具有高性能的压缩比,并且能恢复出高质量的图像.变化不同的数据压缩率,进行分析处理.数据压缩率越高,生成的阴影图形越小.

将变换后的系数作为加密数据 $s$，按照 Shamir 的$(k,n)$方案生成加密数据 $s$ 的 $n$ 份构成. 在 $GF(q)$域中，构造一个 $k-1$ 阶多项式 $f(x)$，$a_0=s$，其他系数任选，且选择模 $q=257$，数据 $s$ 的 $n$ 份构成：$\{1,f(1)\}$，$\{2,f(2)\}$，…，$\{n,f(n)\}$，即生成了 $n$ 个阴影图形. 根据 Shamir 方案，如果至少知道 $n$ 份中的 $k$ 份，则由拉格朗日基函数构建拉格朗日内插多项式，令 $x=0$，即可恢复原来的加密数据：$s=f(0)$.

将恢复出来的数据按照 IDWT 二阶求逆(或 IDCT-IDWT 变换)，可得到 r×r 个子模块原始图像. 图 1 画出了该方法的框图.

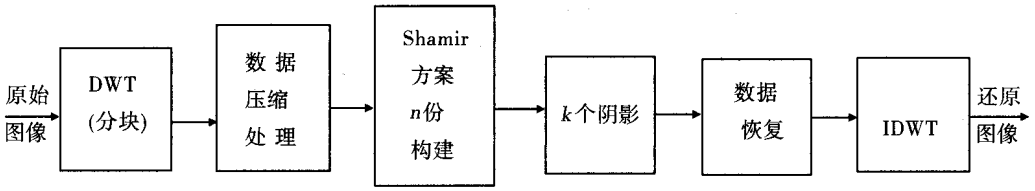



图1 所提出方法的框图

## 3　实验仿真

本文仿真环境为 MATLAB7.0，所选图像为 JPEG 照片图像，像素大小为 256×256($n=256$)，按照大小为 $m\times m$ 像素的子模块进行划分(选择 m=64)，整幅图像可以划分为 4×4 个子模块. 为了方便表示，采用元胞数组表示图像矩阵，共计16 个元胞数组. 为了提高计算效率采用 Haar 小波. 将每一个子模块进行二维 DWT 变换，分解出 4 个子带：LL，LH，HL，HH. 对于每一个数据，按照$(2,n)$加密方案，生成该数据的 $n$ 个 share，形成 $n$ 个阴影图形. 压缩率增加，所产生的阴影图形越小. 本文中选择 $n=5$，$k=2$，多项式系数 $a_1=94$. 数据恢复必须获得至少 2 个阴影图形，才能够恢复出原来的数据. 按照 IDWT 算法做逆变换恢复原始图像.

如果抛弃 3 个高频子带，仅仅保留 LL 分量，数据压缩率为 4:1，share 的图形相应变为未压缩时的 1/4. 如果将 LL 子带再进行 DWT 分解(即二阶 DWT)，抛弃高频分量，仅仅保留低频分量，数据压缩率为16∶1，share 的图形尺寸变为未压缩时的 1/16. 若将 LL 分量进行 DCT 变换，设定不同的阈值，可以得到大约 8∶1、12∶1、16∶1 等不同的压缩率，相应的 share 的图形尺寸随着压缩率的增加而变小. 图 2(a)为 256×256 像素的 JPEG 原始图像，图 2(b)为 DWT 数据压缩率 4∶1 时恢复的图像，图 2(c)为 DWT 数据压缩率为 16∶1时恢复的图像，(d)、(e)、(f)分别为 DWT-DCT 变换 8∶1、12∶1、16∶1 等不同压缩率时恢复的图像. 为了方便比较，图 3(a)、(b)、(c)给出了 DWT-DCT 变换数据压缩率为 8∶1、12∶1、16∶1 时的 share 图形，该阴影图形取自模块 cell{3,2}. 随着压缩率的增加，白点数目明显减少(黑点量值为 0)，阴影图形尺寸大小(白点面积)显著减少.

## 4　性能分析

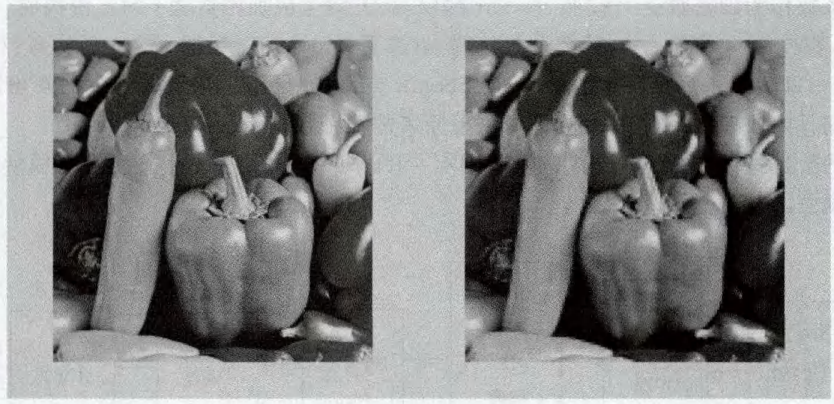
VSS 加密方案的性能可以通过重构图像的质量反映出来. 灰度图像的质量可由峰值信噪比和相关系数指标来衡量[11-12]. 峰值信噪比(PSNR)的定义如下：

$$\mathrm{PSNR}=10\lg\frac{255\times 255}{\sum_{i,j}(I(i,j)-I_R(i,j))^2},$$

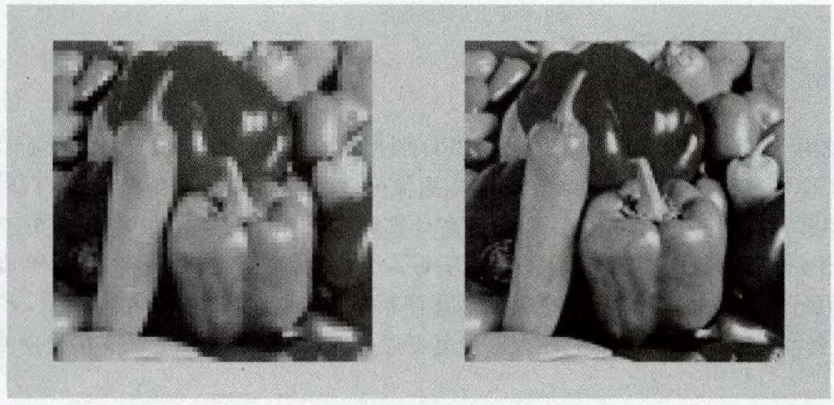
其中：$I(i,j)$ 为原始图像，$I_R(i,j)$ 为重构图像. 相关系数的定义为：

$$\rho=\frac{\sum_{i,j}(I(i,j)-m)(I_R(i,j)-m_R)}{\sqrt{\sum_{i,j}(I(i,j)-m)^2}\sqrt{\sum_{i,j}(I_R(i,j)-m_R)^2}},$$

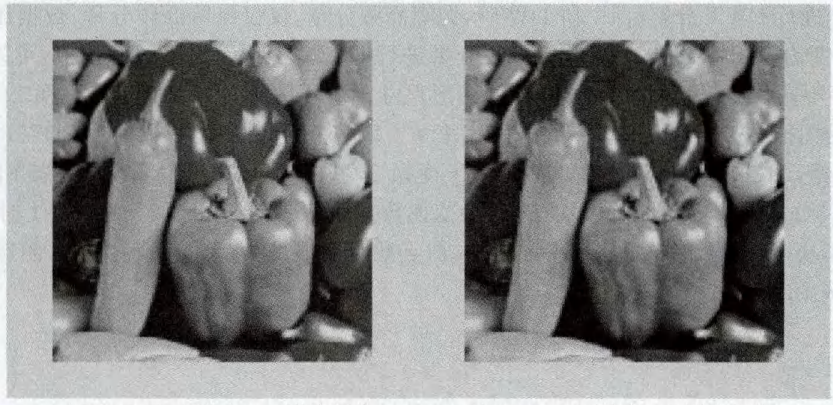
其中：$m$ 为 $I(i,j)$ 的均值，$m_R$ 为 $I_R(i,j)$ 的均值.



(a) 原始图像 (b)DWT压缩率4:1时恢复图像



(c)DWT压缩率16:1时恢复图像 (d)DWT-DCT压缩率8:1时恢复图像



(e)DWT-DCT压缩率12:1时恢复图像 (f)DWT-DCT压缩率16:1时恢复图像

图2 原始图像和恢复后的图像

**表 1 DWT 压缩率为 4:1 和 16:1 情况下相关系数和 PSNR 值**

| 压缩率 | 4∶1 | 16∶1 |
|---|---|---|
| PSNR/dB | −24.8008 | −26.0791 |
| 相关系数 | 0.9537 | 0.9368 |

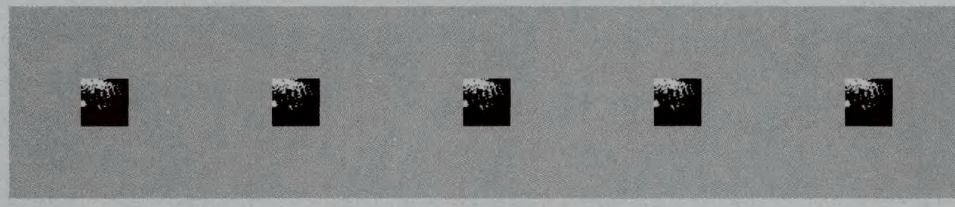
**表 2 二阶 DWT 和 DWT-DCT 压缩率为 16∶1 情况下相关系数和 PSNR 值**

| 压缩率 | 二阶 DWT 压缩率 16∶1 | DWT-DCT 压缩率 16∶1 |
|---|---|---|
| PSNR/dB | −26.0791 | −24.8196 |
| 相关系数 | 0.9368 | 0.9533 |

表 1 给出 DWT 压缩率为 4∶1 和 16∶1 情况下相关系数和 PSNR 值. 由表可以看出压缩率越大，相关系数变得越小，PSNR 值同时变小，恢复图像质量降低. 表 2 为同一压缩率下，DWT 和 DWT-DCT 的相关系数和 PSNR 值. 由表 2 可以看出，在同一压缩率下 DWT-DCT 压缩性能优于 DWT 压缩.

(a)DWT-DCT变换数据压缩率8:1时的 share图形

(b)DWT-DCT变换数据压缩率12:1时的share图形



(c)DWT-DCT变换数据压缩率16:1时的share图形

图3 DWT-DCT变换不同数据压缩率时的share图形

## 5 结　论

本文所提出的灰度图像$(2,n)$可视加密共享技术方案，实验仿真说明了该方法的有效性：选择 Haar 小波使得计算效率提高，DWT 以及 DWT-DCT 高性能的压缩比，产生了小尺寸的阴影图形，并且重构了高质量的原始图像.

## 参 考 文 献


[1] Wang Daoshun, Zhang Lei, Ma Ning, et al. Two secret sharing schemes based Boolean operation[J]. Pattern Recognition, 2007, 40(10): 2776-2785.

[2] Wang Daoshun, Yi Feng, Liu Xiaobo. On general construction for extended visual cryptography schemes[J]. Pattern Recognition, 2009, 42(11): 3071-3082.

[3] Chang Chinchen, Lin Chiachen, Le T, et al. Sharing a verifiable secret image using two shadows[J]. Pattern Recognition, 2009, 42(11): 3097-3114.

[4] Lee Chengchi, Chen Honghao, Liu Huangting, et al. A new visual cryptography with multi-level encoding[J]. Journal of Visual Languages & computing, 2014, 25(3): 243-250.

[5] Yang Chingnung, Yang Yaoyu. New extended visual cryptography schemes with clearer shadow images[J]. Information Sciences, 2014, 271(18): P243-263.

[6] Kamel Mohamed Faraoun. A novel fast and provably secure (t, n)-threshold secret sharing construction for digital images[J]. Journal of Information Security and Applications, 2014, 19(6): 331-340.

[7] Le T, Hoang Ngan, Lin Chiachen, et al. A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for graycvale image[J]. Digtal signal processing, 2011, 21(6): 734-745.

[8] Shamir A. How to share a secret[J]. Communication of ACM,1979,22(11):612-613.
[9] Boggess A, Narcowich FJ. A First Course in Wavelets with Fourier Analysis[M]. 北京:电子工业出版社(国外引进教材),2002.
[10] Charles K. An introduction to wavelets[M]. 北京:人民邮电出版社,2009
[11] Gonzalez R C, Woods R E. DigitalImage Processing(Second Edition)[M]. 北京:电子工业出版社(国外引进教材),2007.
[12] Davies E R. Machine Vision Theory, Algorithms, Practicalities(Third Edition)[M]. 北京:人民邮电出版社,2009.

# The Small Shadow Size Visual Sharing Scheme Based on DWT-DCT for Grayscale Image

LI Wei[a], SUN Yunjuan[b], LIU Yufang[a]

(a. College of Physics and Electronic Engineering; b. College of Xinlian, Henan Normal University, Xinxiang 453007, China)

**Abstract**: The paper is a new VSS scheme with $(2,n)$ method. The scheme is based on analysis method in frequency domain, it uses high performance ratio of compression for DWT and DWT-DCT, it owns high computation efficiency, and the error is small about the restoration image, it advoids traditional larger shadow size. The result of simulations shows the effectiveness of the methods, or, the original image has been resconstructed in high quality and it generates smaller shadow size.

**Keywords**: DWT; DCT; Shamir scheme; Visual secret share scheme