Computer Science and Application 计算机科学与应用, 2015, 5(8), 285-296
Published Online August 2015 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2015.58037

Hans汉斯

Design and Implementation of a Copyright Protection System Based on Digital Watermarking with Visual Cryptography

Chao Peng, Tiankai Sun, Dongrong Kong, Jianqiao Zhu

Department of Information and Electrical Engineering, Xuzhou Institute of Technology, Xuzhou Jiangsu
Email: ipengchao@126.com

Received: Sep. 3rd, 2015; accepted: Sep. 20th, 2015; published: Sep. 24th, 2015

Abstract

It is easy to copy digital works. When the copyright of a digital work is owned by multiple parties, the copyright issue that is not handled correctly will certainly cause various conflicts and commercial disputes. In this case, the copyright protection method that uses images containing visual cryptography and digital watermarks emerges. This method can verify the copyright owner without compromising visual effects. The visual cryptography technology is used to encrypt copyright information images as multiple cryptography files. Then a password image is embedded into the copyright image as an invisible watermark by the digital watermark algorithm. To restore and verify the copyright information, the watermark extract technology is used to extract original copyright information images from cryptography images whose quantity cannot be less than the threshold.

Keywords

Digital Rights Management, Visual Cryptography, Digital Watermarking

基于可视密码的数字水印版权保护系统的设计与实现

彭　超，孙天凯，孔冬荣，朱剑桥

徐州工程学院信电工程学院，江苏　徐州

文章引用: 彭超, 孙天凯, 孔冬荣, 朱剑桥. 基于可视密码的数字水印版权保护系统的设计与实现[J]. 计算机科学与应用, 2015, 5(8): 285-296. http://dx.doi.org/10.12677/csa.2015.58037

Email: ipengchao@126.com

收稿日期：2015年9月3日；录用日期：2015年9月20日；发布日期：2015年9月24日

摘　要

数字作品的拷贝较为容易，倘若多方拥有版权的数字作品在多用户合作之间，若其版权问题处理不当，势必会引起各种矛盾和商业纠纷等问题。设计一种结合可视密码、数字水印的图片版权保护方案，在不破坏视觉效果的前提下可以实现验证版权所有者。利用可视密码技术将版权信息图片加密为多份密码文件，用数字水印算法将其中一张密码图片以不可见水印嵌入版权图片中。还原时，采用水印提取技术提取出密码图，结合不少于权限值密码图恢复出原始版权信息图片来验证版权信息。

关键词

数字版权保护，可视密码，数字水印

1. 引言

近年来，数字图片侵权案频发，其中大部分涉及多用户的版权纠纷。合作有利于资源共享和生存发展，但是在合作过程中保障多方的共享机密和资源的安全至关重要。为了保护版权，部分作者或利益方采用了一些以牺牲作品质量为代价的方法，如添加版权标志等。然而这些标志易被篡改且破坏了作品，可行度差。因此，现在亟需寻找一种有效的、可靠的方法来解决多用户的图片版权保护问题。

本文根据可视密码(Visual Cryptography)和数字水印(Digital Watermarking)思想设计的多用户版权保护方案，利用 Java 技术实现[1] [2]，为验证图片的版权提供一个实用而又高效的平台。可视密码是针对秘密共享所提出的一种安全且隐蔽的算法，将秘密信息分发给持有者，凑齐一定数量后方可还原秘密。数字水印技术则应用于秘密标识，可将秘密信息嵌入到目标图像而不破坏原图像的视觉效果。将二者结合可实现图片的版权保护。

系统首先使用可视密码算法将版权信息按照需要生成可视密码，多个利益方各持有一个密码图片，然后利用数字水印技术将可视密码以不可见水印的形式嵌入需要保护版权的图片中。需要验证时，只需提取出图片中的可视密码，结合多方密码图片即可还原版权信息，验证版权。

2. 关键技术介绍

2.1. 可视密码算法

可视密码(Visual Cryptography)是一种从秘密共享中提出的信息隐藏技术[3] [4]。可视密码的解密结果是有意义的图像信息，所以它在解密时无需计算机的运算，只依靠人类的视觉进行解密。可视密码技术比传统的密码学技术安全性高，同时有具有隐蔽性，不易被察觉。同时可视密码的恢复较为简单，因此也具有通用性。可视密码技术是秘密共享中的一种新的重要技术，因此受到了广泛的关注，得到了快速的发展。

可视密码的主要优点：

(1) 隐蔽性：加密后的图像是由杂乱无章的像素点构成的，肉眼无法直接识别，所以具有隐蔽性；

(2) 安全性：可视密码要求结合足够的密码图片才可以进行还原，在不满足此条件时，任何算法、手

段都无法进行还原操作；

(3) 秘密恢复的简单性：与其它密码算法不同，可视密码在恢复阶段无需复杂的运算，只要密码图片满足要求，即可迅速恢复出原始图像，具有较高的时间效率；

(4) 通用性：用户不用了解密码学的专业知识，可以无障碍地使用本技术。

可视密码存在的缺点：

(1) 图片清晰度及对比度损坏。这是可视密码的常见缺点。例如恢复后的图片较之原图存在比例和大小上的差异，或者在纵横比例和分辨率等方面出现视觉可见的失真；

(2) 在可视密码技术出现早期，只能加密与还原黑白二值图像，如需应用于常见的彩色或灰度图像，则需使用另外的算法结合较为成熟的适用于黑白二值图像的可视密码算法来加密和解密彩色和灰度图像，同时还需要考虑运算复杂度等问题；

(3) 可视密码的密码图像是无序的像素点构成的图像，因此在存储过程中容易受到损坏或者主动攻击；

(4) 在进行可视密码生成与恢复过程中，可能会遇到分发者或者参与者不诚实的问题，如伪造图片等欺骗行为。

2.2. 数字水印技术

数字水印技术(Digital Watermarking)在版权保护方面的主要手段是版权说明[5] [6]。具体做法通常是将版权说明文字或图片追加到数字图片中，可以有效地标识版权和进行靶向广告。强制去除版权图片会影响原图效果甚至破坏原图，因而数字水印技术可以限制和追踪盗版，避免盗版图片在互联网上的传播。

数字水印技术主要特点[7]：

1) 隐蔽性：嵌入到数字作品中的水印不会明显地影响图片的视觉效果；

2) 隐藏位置的安全性：图片文件格式转换时水印信息不会丢失。因为通常在数据中隐藏水印信息，而避免了在文件头中隐藏信息会在格式转换后丢失隐藏的水印信息；

3) 鲁棒性：在经历不同的处理过程后，水印图片依然能够被完整地提取出来或证明水印存在，如剪切、比例变换、信道噪声等。

数字水印技术存在缺点：

1) 目前数字水印技术还不够成熟，鲁棒性较差。导致水印信息很容易被破坏或破解。

2) 此外，数字水印是一种被动的技术，并不能防止产品被偷盗和复制。

3. 系统总体设计

3.1. 设计目标与原则

设计一个基于可视密码算法与数字水印技术的具有生成可视密码、嵌入与还原数字水印、验证图片版权归属权等功能的多用户版权保护系统。

基于可视密码算法及数字水印技术的特点，本设计方案应具有以下原则：

1) 保证图片质量。在对版权信息图片进行加密、恢复和验证的过程中，保证图片在对比度、大小比例等方面不受影响；

2) 可验证的结果。针对可能存在的参与者欺骗，提出验证方案：如果从被保护图片中提取出的水印图像被篡改，或者参与者个数不足，或者参与者提供的无效或伪造的密码图片，则无法重构得到正确的秘密版权信息；

3) 用户体验良好。人机交互体验优良的界面设计，没有繁琐的功能和选项，用户只需按照提示操作，就可以进行加水印保护图片和验证版权信息等，使得非专业人员使用起来轻松自如。

3.2. 系统组成与功能

本系统通过对可视密码算法和数字水印技术的合理结合，实现对版权信息的多重保护。系统分为版权信息加密与版权信息验证两大模块。

系统功能有：

(1) 版权信息加密模块：

1) 版权信息(以图片形式)与版权图片的上传；

2) 版权信息图片的可视密码加密；

3) 基于可视密码的数字水印的生成；

4) 版权图片的数字水印嵌入等。

(2) 版权信息验证模块：

1) 数字水印的提取；

2) 基于可视密码的版权信息图片的恢复；

3) 根据恢复的版权信息进行版权验证。

3.3. 系统总体实现流程

系统总体实现流程图如图 1 所示。

版权信息加密模块实现流程见图 2，版权信息验证模块实现流程见图 3。

4. 主要算法

4.1. 数字水印生成与提取

离散余弦变换(Discrete Cosine Transform, DCT)与傅里叶变换紧密相关，是一种正交变换的方法。这种算法的原理是：首先对图像进行离散余弦变换，然后对变换域的系数嵌入水印，最后再进行 DCT 逆变换得到嵌入水印后的图像。如果直接进行二维图像的 DCT 变换，工作量非常大(以 8 × 8 的图像分块为例，进行 DCT 和 IDCT 需求 1024 次乘法和 896 次加法)。为了加快变换的速度，人们根据 DCT 变换的对称性和正交性，提出了快速 DCT 变换算法(FDCT) [8]。

水印嵌入的步骤：首先提取原始图像中的 r 层分量 rPixeles 及 secret 水印图像 wPixels，对 rPixels 进行 8 × 8 分块，进行 FDCT 变换，将得到的结果存入 dblk。最后，在 dblk 中频位置加入水印(如果 wPixels 是 1 则加一个系数 d，否则减 d)。

水印提取的步骤：获得原始图像的 r 层分量 oRPixeles 和水印的嵌入图像 mRPixels，对 oRPixeles 和 mRPixeles 进行 8 × 8 分块，并进行快速 DCT 变换，得 odblk 和 mdblk。比较 odblk 和 mdblk 嵌入水印的 5 个位置系数大小，如果 mdblk 大则水印信息为 1，相反为 0。

4.2. 秘密图像分享 Lagrange 插值多项式方案

实数域 Lagrange 插值多项式方案[9]。

参考 Shamir 提出的实数域的 Lagrange 插值算法，基于该算法，本文假设秘密 y 的参与者为 n，秘密 y 的还原门限值为 k。可以根据下列公式实现对消息的生成和分发：

$$F\left(x_i\right)=y+m_1x_i+m_2x_i^2+\cdots+m_{k-1}x_i^{k-1} \tag{1}$$

满足以下条件：

a) k 应该是不大于 n 的整数。

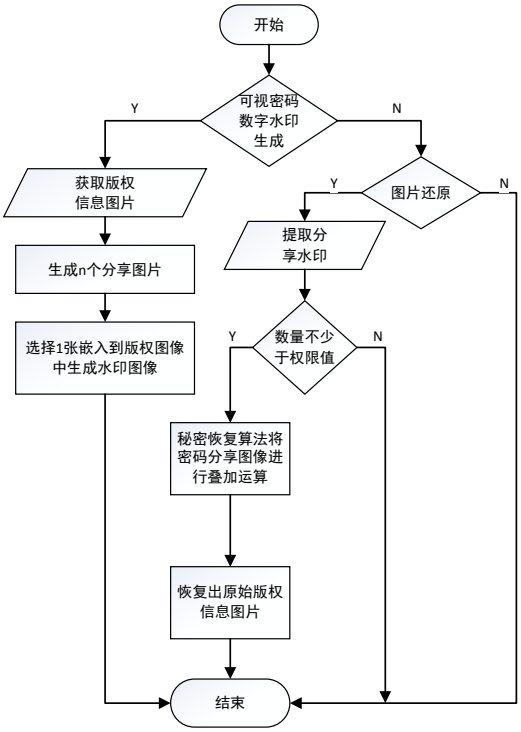

Figure 1. Overall implementation flow chart of the system
图 1. 系统总体实现流程图

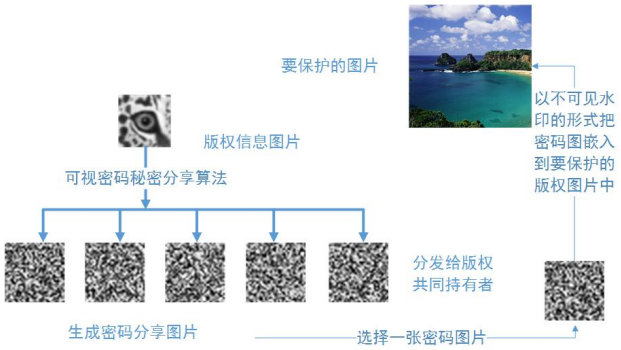

Figure 2. Implementation flow chart of encrypting copyright information module
图 2. 版权信息加密模块实现流程

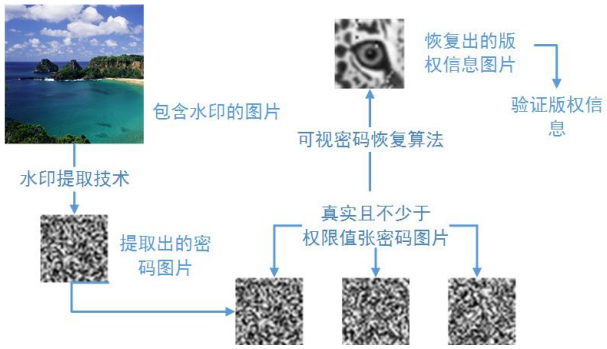

Figure 3. Implementation flow chart of deciphering copyright information module
图 3. 版权信息验证模块实现流程

b) 随机地选取$(k-1)$个整数：$m_1, m_2, \cdots, m_{k-1}$。

c) 每个参与者都持有一个公开且不重复的 ID，设 ID 为 x_i。

d) 为每个参与者选定一个 x_i；

e) 将计算结果$\left(x_i, F\left(x_i\right)\right)$分发给每个参与者。

为安全起见，在上述过程结束后，可以丢弃 $m_i\left(i=1,2,\cdots,k-1\right)$ 的值，因为在重构时，这些值可以在重构秘密 y 的过程中，也得到重构。

从 n 个分享的子秘密中，任意选取不少于 k 个秘密份额的恢复过程：

(a) 根据 k 个秘密份额，构造如下所示的方程组：

$$\begin{cases} F\left(x_1\right)=y+m_1x_1+m_2x_1^2+\cdots+m_{k-1}x_1^{k-1} \\ F\left(x_2\right)=y+m_1x_2+m_2x_2^2+\cdots+m_{k-1}x_2^{k-1} \\ \cdots \\ F\left(x_k\right)=y+m_1x_k+m_2x_k^2+\cdots+m_{k-1}x_k^{k-1} \end{cases} \tag{2}$$

(b) 依据 Lagrange 插值算法，计算得到未知变量和 y，因此可以表示方程(2)中的$(k-1)$次多项式为：

$$\begin{aligned} F\left(x\right)=&F\left(x_1\right)\frac{\left(x-x_2\right)\left(x-x_3\right)\cdots\left(x-x_k\right)}{\left(x_1-x_2\right)\left(x_1-x_3\right)\cdots\left(x_1-x_k\right)}+F\left(x_2\right)\frac{\left(x-x_1\right)\left(x-x_3\right)\cdots\left(x-x_k\right)}{\left(x_2-x_1\right)\left(x_2-x_3\right)\cdots\left(x_2-x_k\right)} \\ &+\ldots+F\left(x_k\right)\frac{\left(x-x_2\right)\left(x-x_3\right)\cdots\left(x-x_k\right)}{\left(x_k-x_2\right)\left(x_k-x_3\right)\cdots\left(x_k-x_{k-1}\right)} \end{aligned} \tag{3}$$

可得 $y=F\left(0\right)$，其具体计算如下：

$$\begin{aligned} F\left(x\right)=y=F\left(0\right)=\left(-1\right)^{k-1}\Bigg[&F(x_1)\frac{x_2x_3\ldots x_k}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_k)} \\ &+F\left(x_2\right)\frac{x_1x_3\cdots x_k}{\left(x_2-x_1\right)\left(x_2-x_3\right)\cdots\left(x_2-x_k\right))} \\ &+\ldots+F\left(x_k\right)\frac{x_1x_2\cdots x_k}{\left(x_k-x_2\right)\left(x_k-x_3\right)\cdots\left(x_k-x_{k-1}\right)}\Bigg] \end{aligned} \tag{4}$$

根据上述公式，只有联合不少于 k 个参与者，才可以重构得出秘密 y，而当参与者的数目少于 k 个时，则无法重构得到秘密 y。

2) 有限域 Lagrange 插值多项式[10]

由分发者选择一个素数 p，p 既大于最大可能的秘密，也大于秘密分享的个数。在分发分享秘密前，由分发者随机构造一个多项式，其次数为 $m-1$。

如，分发者可以构造一个(3,n)门限方案(即：3 个秘密份额可以重构 M)，则任意的二次多项式为：

$$F\left(x\right)=\left(ax^2+bx+M\right)\bmod p \tag{5}$$

其中随机选择的系数 a 和 b 为随机整数，必须保密，p 是比任何一个系数都大的随机机素数，且公布 p；M 是消息。分发者可以通过公式(5)得到秘密份额如下：

$$k_i=F\left(x_i\right) \tag{6}$$

不失一般性，可以将在 $x=1$ 处的值作为第一个份额，第二个份额取可以在 $x=2$ 处的取值，由此类推。

由以上多项式结构可以看出(如图 4)，多项式(5)具有三个未知系数 a，b，M，若是参与者持有任意 3

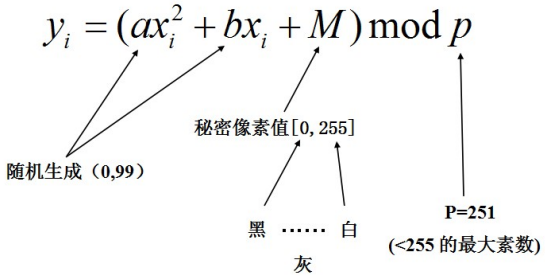

Figure 4. Coefficient sketch map of discretional composited quadratic polynomial
图 4. 任意构成的二次多项式系数示意图

个或 3 个以上的秘密份额，就可以重构出该多项式，从而得到了多项式的三个未知数，从而重构了秘密信息 M。但是若是少于 3 个秘密份额则不能重构该多项式，从而也不能重构出秘密消息 M。以下给一个具体实例说明：

假设 M = 11，我们构造(3,5)门限方案，设定素数为 13，从该方案可以看出，5 个参与者中的任何 3 个就能重构得到 M，公式如下(7 和 8 为随机选择)：

$$F(x) = \left(7x^2 + 8x + M\right) \bmod 13 \tag{7}$$

5 个秘密份额：

$$\begin{cases} k_1 = F(1) = 7\times1^2 + 8\times1 + 11 \equiv 0 \pmod{13} \\ k_2 = F(2) = 7\times2^2 + 8\times2 + 11 \equiv 3 \pmod{13} \\ k_3 = F(3) = 7\times3^2 + 8\times3 + 11 \equiv 7 \pmod{13} \\ k_4 = F(4) = 7\times4^2 + 8\times4 + 11 \equiv 12 \pmod{13} \\ k_5 = F(5) = 7\times5^2 + 8\times5 + 11 \equiv 5 \pmod{13} \end{cases} \tag{8}$$

随机选择 5 个秘密份额中的 3 个(比如)，可以得到以下方程组，解线性方案组：

$$\begin{cases} 3 = a\times2^2 + b\times2 + M \pmod{13} \\ 7 = a\times3^2 + b\times3 + M \pmod{13} \\ 5 = a\times4^2 + b\times4 + M \pmod{13} \end{cases} \tag{9}$$

解得：和 M = 11。从而重构了秘密信息 M。

从该方案可以看出，如果多项式系数随机地选择，若是少于门限值 t 个参与者想重构得到秘密信息 M，即使他们有无限的计算能力，也未必能得到除消息长度的任何关于秘密消息的任何信息。该方案很像一个一次一密的乱码本，任何想通过穷举搜索都是不可能得到消息的任何信息。

5. 系统测试与分析

5.1. 系统方法与标准

(1) 系统测试方法

在图形界面中运行本系统，

1) 可视密码技术将版权信息图片加密成多份灰度密码图片；

2) 数字水印算法生成不可见水印嵌入版权图片中；

3) 还原版权信息图片时，水印提取出灰度密码图片；

4) 利用可视密码秘密图片恢复算法，用不少于权限值 t 张密码图片，还原得到版权信息图片。

若以上四个步骤都运行成功，则本系统测试通过，否则，测试失败。

(2) 测试环境(见表 1)。

5.2. 测试过程

(1) 测试准备

假定 4 人拥有版权，在验证时需要 2 人同时提供各自持有的版权信息可视密码。因此，需要生成 5 张秘密分享图片，其中一张(系统默认第一张)作为水印嵌入至要保护的图片中，剩余 4 张分发给四名版权持有者。准备要保护的图片(如图 5)、版权信息图片(如图 6)。

(2) 版权信息加密模块

测试步骤：

a) 进入可视密码水印生成界面；

b) 打开需要分享的版权信息图片；

c) 点击选择输入多用户 ID；

d) 选择多个加密分享图像的保存地址，如图 7；

Table 1. Test environment
表 1. 测试环境

	项目	配置
硬件环境	CPU	Intel Pentium 4 主频 2.4 GHz
	内存	4 GB
	操作系统	Windows 8.1
	网络连接	无
软件环境	开发工具	NetBeans 8.0、JDK1.7.0_45

Figure 5. Image to be protected
图 5. 要保护的图片

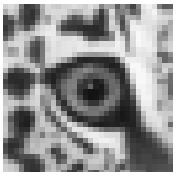

Figure 6. Image of copyright information
图 6. 版权信息图片

e) 点击“开始生成”按钮；

f) 可视密码及嵌入了水印的版权图片生成成功，如图 8。

嵌入水印的版权图片在视觉上与原始图片没有区别，不影响视觉效果，可以在互联网上分享、传播。可视密码图片由版权所有者持有。下面测试验证版权的过程。

(3) 版权信息验证模块

a) 进入还原图像界面，选择水印图片和原始图片；

b) 选择加密的版权密码图像(个数大于权限值)；

c) 选择恢复图像的保存位置，如图 9；

d) 点击“开始还原”按钮；

e) 还原版权信息图片成功，如图 10。

(4) 可验证功能

本小节测试环节有：

a) 选择还原图片个数小于权限值(测试结果如图 11，左一为还原出的版权信息，左二为原始版权信息)。

b) 选择还原图片中存在虚假图片，结果无法恢复出源图片(测试结果如图 12)。

5.3. 性能测试

(1) 方案的优势

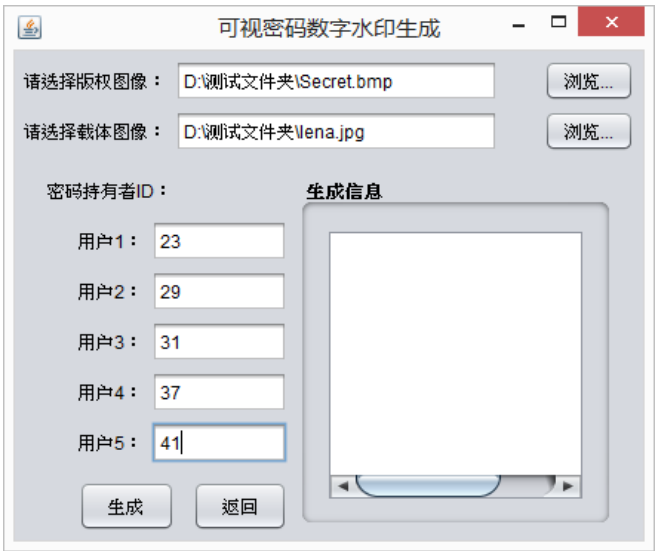

Figure 7. Settings of encrypting copyright information
图 7. 加密信息设置

Figure 8. Result generated
图 8. 生成结果

Figure 9. Settings of deciphering copyright information
图 9. 设置解密信息

Figure 10. Recovered image of copyright information
图 10. 还原出的版权信息图片

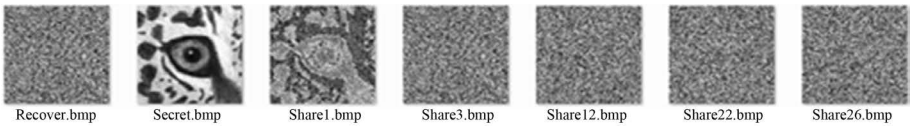

Figure 11. The wrong image (third from the left) recovered by deficient cryptogram images
图 11. 还原图片个数小于权限值(左三)

Figure 12. The wrong image recovered by false cryptogram image
图 12. 存在虚假图片的测试结果

a) 在秘密共享中，多秘密能够被同步重构；

b) 没有合法身份的参与者，即提供伪造分享信息的参与者无法参与还原过程获得原始图片。具有合法身份的参与者可以方便地通过本文所设计的系统获得原始图片；

c) 只要满足参与者数量大于权限值，即可通过重构算法获得原始图片，而当参与者数量不足时，无法获得原始图片。

(2) 计算复杂性

通过上述分析可以得出，本文所设计的系统的主要时间消耗是在验证和恢复阶段(见表 2)。

由于本文提出的方案是基于 LFSR 公钥秘密系统：每个参与者选择 e_i 作为他自己的秘密 Shadow，e_i 是私钥，公布 $S_{e_i}(a,b)$。

6. 总结与展望

6.1. 工作总结

针对多用户版权保护的问题，本文将可视密码技术与数字水印技术相结合，利用 JAVA 技术设计出

Table 2. Computational complexity analysis
表 2. 计算复杂性分析

是否具有可验证性	Yes
分发者无法成功欺诈	Yes
可以有效进行重构和验证	Yes
基于不同的公钥系统安全性	LFSR
密钥长度(1024 位安全级别)	340
公钥长度(1024 位安全级别)	340
Shadow 可以被重用(成员离开或加入)	Yes
Shadow 可以多次被用	Yes
时间复杂性($k > t$)	$O(t^2)$

了一套基于可视密码的数字水印版权保护系统。通过对测试的结果整理和分析可知，本文所设计的算法在功能上能够满足一定的安全性，并且在时间上和空间上均具有较高的效率。因此，本文设计的基于可视密码的多用户水印版权保护方案不论是理论上还是实践上都有着积极的意义。

本文在彩色图像的可视密码分享方案具体实现上，用到了较多的数论方法，实用价值很高应用范围十分广阔。

6.2. 创新点

本文的创新之处在于：

①传统的数字水印算法直接嵌入明文信息，容易被检测或移动，本文提出的方案将明文信息通过可视密码算法加密，弥补了目前广泛使用的数字水印产品容易被破解的不足。

②将引入可视密码技术，为同时给多用户提供多重水印提供了可能。这样拓宽了数字水印技术的应用范围。有效地解决了信息安全中多人共享一个秘密而缺乏有效的保护机制的问题，避免了一人保存密钥而造成的密钥损失或恶意泄露密钥问题。

③通过数字水印提取技术及可视密码图片恢复算法重新得到版权信息图片可以有效的判断所有权的归属，以便确认数字产品的所有权或跟踪侵权行为。

6.3. 应用前景

可视密码与数字水印都是关于隐藏(或嵌入)信息于图片中的算法，但是它们却有着完全不同的意义。可视密码算法把秘密图片通过分发给参与者实现秘密分享。数字水印则是为了隐藏信息，不是为了秘密分享，好的数字水印算法可以讲信息以难以察觉的方法隐藏到载体中。

在侵权现象越发严重的当下，寻求一个能够在合作过程中保障利益双发或多方的共享保密机制越发重要。本方案可以保护多用户的版权，进而有效的避免引起不必要的利益矛盾和商业纠纷等问题。本方案数字水印与可视密码技术相结合，对于版权保护的完善及我国电子商务、电子政务的建设方面等具有广阔的市场前景。

6.4. 不足

本文设计和实现的基于可视密码的数字水印版权保护系统，经过大量的测试后，系统都能够正常进行加密、解密操作，视觉效果上没有误差。同时对于欺骗行为，如伪造密码图片、少于权限值张密码图

片等均无法恢复出原始图像。

本文仍有许多方面都需要进一步完善。首先，本文所提出的方案目前只适用于位图图像的分享与恢复。其次由于小于 255 的最大素数为 251，导致 R、G、B 值大于 255 的像素无法正确恢复。最后图像大小与分享速度关系不是很大，但稍大的图恢复速度会比较慢，彩色图更慢。本文接下来的研究重点将会放在提高算法处理效率以及扩展算法的功能上。在效率方面，尽量在恢复速度上进一步提高；在功能扩展方面，尽量做到实行对所有格式图像都支持，且在恢复时进行恢复者的身份认证。

基金项目

江苏省科技创新基金(BC2010056)；徐州市科技计划项目(XM13B126)徐州工程学院青年基金(XKY 2012309)。

参考文献 (References)

[1] Horstmann, C.S. and Cornell, C. (2012) Java 核心技术. 机械工业出版社, 北京.

[2] 刘剑鸣 (2008) 图像数字水印的 JAVA 实现. 哈尔滨地图出版社, 哈尔滨.

[3] 韩妍妍 (2009) 可视密码技术的研究. 西安电子科技大学, 西安.

[4] 董昊聪 (2012) 可视密码及其应用研究. 西安电子科技大学, 西安.

[5] 王勇 (2012) 数字版权保护技术的难题与对策研究. *理论研究*, **01**, 1-4.

[6] 陈晓苏 (2006) 网络环境下数字图像版权保护安全协议的设计与分析. *计算机学报*, **09**, 7.

[7] 刘皓 (2008) 数字水印技术的现状及发展. *黑龙江科技信息*, **31**, 51.

[8] 王秀丽 (2010) 基于 DCT 域的图像数字水印技术研究. 河南科技大学, 洛阳.

[9] 王丽侠 (2010) 数字水印技术的研究. *计算机安全*, **05**, 71-77.

[10] 胡春强 (2013) 秘密共享理论及相关应用研究. 重庆大学计算机学院, 重庆.