基于 Shamir 门限秘密分享的图像可视加密算法

谭亦夫，李子臣
（北京印刷学院信息工程学院 北京 102600）

摘　要：采用 Shamir 门限秘密分享方案，提出一种带有认证功能的图像可视加密算法。该算法主要思想是，先将二值秘密图像分块得到数据，然后使用 Shamir 的门限秘密共享方案得到子秘密数据，同时用 SM2 签名算法对秘密图像进行签名，并将分享数据和签名信息嵌入载体图像。还原时需要指定张数的子秘密图像进行信息的提取、还原与认证。仿真实验结果表明，该秘密图像分享方案提高了秘密图像存储与传输的安全性。

关键词：秘密共享；SM2 签名；数字水印；二值图
中图分类号：TP309.3
文献标识码：A
doi: 10.11959/j.issn.2096-109x.2018063

Image visualization encryption algorithm based on Shamir threshold secret key sharing

TAN Yifu, LI Zichen
School of Information Engineering, Beijing Institute of Graphic Communication, Beijing 102600, China

Abstract: An image visualization encryption algorithm with authentication function by using Shamir scheme was proposed. The main idea of this algorithm is to obtain the data by segmenting the binary secret image into blocks. Then, Shamir scheme was used to obtain the sub-secret data and simultaneously sign the secret image with the SM2 signature algorithm. And it would embed the shared data and signature information into carrier images. When the restoration is required, a specified number of sub-secret images are required for information extraction, restoration and authentication. The simulation experiment of the scheme shows that the secret image sharing scheme improves the security of secret image storage and transmission.

Key words: secret sharing, SM2 signature, digital watermarking, binary image

1　引言

计算机与互联网的发展把人们的信息交流方式提升到了一个新的层次，数字媒体时代的到来给人们的生活带来巨大的改变。但与此同时，数字媒体技术的发展也存在一定的风险，数字数据

收稿日期：2018-05-16；**修回日期：**2018-06-25
基金项目：国家自然科学基金资助项目（No.61370188）；北京市教委科研计划基金资助项目（No.KM201610015002, No.KM201510015009，No.KZ201510015015, No.KZ201710015010）；北京市高校改进方案基金资助项目（No.PXM2017_014223_000063）；北京印刷学院校级基金资助项目（No.Ec201803 Ed201802 Ea201806）
Foundation Items: The National Natural Science Foundation of China (No.61370188), The Scientific Research Common Program of Beijing Municipal Commission of Education (No.KM201610015002, No.KM201510015009, No.KZ201510015015, No.KZ201710015010), Beijing Municipal College Improvement Plan (No.PXM2017_014223_000063), BIGC Project (No.Ec201803 Ed201802 Ea201806)

很容易被别人篡改，被不法分子用来谋取利益。例如，数字图像、机密图像被盗取，不法分子进行篡改并宣传，造成或大或小的社会恐慌；对新闻图像有意无意的修改，会一定程度地扭曲事实，给人们带来错误的信息引导；医学上用来诊断的数字图像若遭到篡改，会造成对患者的误诊等。因此，在数字化时代，如何安全地存储与传输多媒体数据，保证数据的机密性与真实性，成为一个重要的问题。Shamir[1]提出的门限秘密共享方案可以将一个秘密生成 n 份子秘密，并能够使用 k 份子秘密还原秘密图像。此后，出现了多种不同改进的秘密共享方案，包括多秘密分享方案[2-4]，提升秘密分享的抗攻击性[5]。本文提出了秘密图像分享方案，使用该方案生成 n 份无意义图像，将分享后的无意义图像与秘密图像的签名数据嵌入载体图像中。还原图像后验证签名，这样既保证了图像存储与传输的安全，又保证了图像的真实性。

2 基础理论知识

2.1 Shamir 秘密共享

秘密共享方案是将秘密信息 S 分成 n 份子秘密信息 $\{S_1,S_2,\cdots,S_n\}$，将子秘密信息存储，S_i 分发给参与者 P_i，只有授权集合中的参与者子集可以利用其所拥有的子秘密恢复 S。

1979 年，Shamir 和 Blakley 分别用代数学和几何学的方法给出了最早的门限秘密共享算法。其方案如下：给定正整数 k 和 n，其中，$k \leqslant n$，(k,n) 门限秘密共享方案指的是将秘密信息 S 分成 n 份子秘密，其中的任意 k 份或更多的子秘密可以重构秘密信息 S，而任意 $k-1$ 份或更少的子秘密则无法得到 S 的任何信息。Shamir 提出的秘密分享方案被广泛使用，实现过程如下所示。

选择有限域 F_q，其中，$q \geqslant n$，设参与者集合为 $P=\{P_1,P_2,\cdots,P_n\}$，k 为门限值，秘密信息 $S \in F_q$。选择 F_q 上 n 个互不相同的非零元素 $x_1,x_2,\cdots,x_n$，将这些元素公开。

随机选择 F_q 上的 $k-1$ 次多项式 $g(x)=a_0+a_1x+\cdots+a_{(k-1)}x^{(k-1)}$，其中，$a_0=S$，其余的 a_i 随机地选自 F_q。分别计算 $S_i=g(x_i),i=1,2,\cdots,n$，$n$ 将 (x_i,S_i) 作为子秘密分发给成员 P_i。

任意 k 位成员可以将其持有的子秘密共享，从而通过拉格朗日插值公式恢复出秘密 S。设 k 位成员的子秘密为 $\left\{\left(x_{i_1},s_{i_1}\right),\cdots,\left(x_{k_t},s_{k_t}\right)\right\}$，拉格朗日插值公式如下。

$$g(x)=\sum_{r=1}^{k}S_{i_r}\prod_{\substack{t=1\\t\neq r}}^{k}\frac{x-x_{i_t}}{x_{i_r}-x_{i_t}} \tag{1}$$

由多项式理论可知，若 2 个 k–1 次多项式在变量的 k 个不同取值处得到的函数值相等，则这 2 个多项式必定相等，于是式(1)成立，由此计算出 $S=a_0=g(0)$。

2.2 国密 SM2 签名算法

SM2 是国家密码管理局于 2010 年 12 月 17 日发布的椭圆曲线公钥密码算法。因为基于椭圆曲线上离散对数问题的困难性要高于一般乘法群上离散对数问题的困难性，且椭圆曲线所基于域的运算位数远小于传统离散对数的运算位数，椭圆曲线密码体制比原有的密码体制（如 RSA 和 DSA）更具有优越性[6]。SM2 算法的可证安全性达到了公钥密码算法的最高安全级别，其实现效率相当于或略优于一些国际标准的同类椭圆曲线密码算法[7]。数字签名算法由一个签名者对数据产生数字签名，并由一个验证者验证签名的可靠性。签名者持有一个私钥和一个公钥，签名者用私钥产生签名，验证者用公钥验证签名。

ECC 的参数是有限域上的椭圆曲线，包括：有限域 F_q 的规模 q，定义椭圆曲线 $E(F_q)$ 方程的 2 个元素 $a,b \in F_q$，$E(F_q)$ 上的基点 $G=(x_G,y_G)$ $(G \neq 0)$，其中，x_G,y_G 是 F_q 中的 2 个元素。

在 SM2 签名算法中，签名者 A 的秘密对包括签名者的公钥 P_A 和私钥 d_A。其中，$P_A=[d_A]G=(x_A,y_A)$，用户 A 具有位长为 $entlen_A$ 的可辨别表示 ID_A，记 $ENTL_A$，它是由 $entlen_A$ 转换而成的 2 byte 数据，签名者和验证者都需要使用密码杂凑算法求得用户 A 的杂凑值 $Z_A=H_{256}(ENTL_A \| ID_A \| a \| b \| x_G \| y_G \| x_A \| y_A)$。SM2 数字签名算法所使用到的 H_{256} 算法规定为 SM3 密码杂凑算法。

2.3 基于 LSB 信息隐藏算法

信息隐藏的目的是降低引起攻击者注意的可

能性，从而降低被攻击的可能。数字水印是多媒体数据版权保护的方案之一[8-9]。基于 LSB 的数字水印算法是空域信息隐藏算法中的典型算法，然而针对空域的各种处理，会对不显著分量进行一定压缩，LSB 对这些操作很敏感[10]，所以 LSB 大多用在脆弱水印。该算法的主要特点是，信息容量大，但是嵌入位置固定，隐藏的信息易被破坏。

LSB 方法通过调整载体图像像素值的最低若干有效位实现数据的嵌入，使所隐藏的信息在视觉上很难被发觉，而且只有知道秘密信息嵌入的位置才能正确提取出秘密信息。显然，LSB 隐藏算法改动最低位的概率是 50%，它在原始图像中引入了极小的噪声，在视觉上是不可见的。事实上，对于灰度图像来说，改变其最低 2 位也能取得较好效果。

3　秘密图像分享方案设计与实现

3.1　子秘密图像生成

子秘密图像生成过程如图 1 所示。为了将一幅秘密图像分享为 n 份无意义的子秘密图像，需要使用 Shamir 秘密分享方案对秘密图像的像素值进行生成子秘密的运算。

本文使用 256×256 二值图作为秘密图像，生成子秘密之前，先对秘密图像进行分组，秘密图像每 2×2 矩阵位分为一组，组成的数据 $S_i\in[0,15]$，遍历整幅图片，得到 S。使用 SM2 对 S 进行签名，并将签名数据嵌入载体图像中。同时，为每个 S_i 随机生成 $k-1$ 阶多项式 $y=S_i+a_1x+\cdots+a_{(k-1)}x^{(k-1)}$，并且随机选取 x_i 值，得到 y_i。为了使数据范围变小，对 y_i 进行模运算。$y_i'=y_i \bmod p$，其中，p 是素数且 $p>15$（本文取 $p=17$），当 $y_i'>15$ 时，舍弃相应的 x_i 和 y_i，重新取点计算。每个 S_i 都能够计算得到 n 个点 $(x_1,y_1'),(x_2,y_2'),\cdots,(x_n,y_n')$，分别将每个点存入 n 个矩阵当中。数据存储方式如图 2 所示。

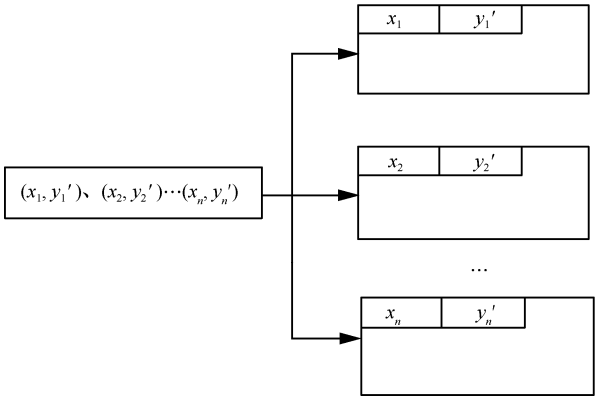


图 2　数据存储方式

图 2 表示的是由 S_1 分享而得出的 n 个点，依次嵌入 n 幅图像的前 8 位。对所有的 S_i 进行上述处理，至此得到 n 份完整无意义的子秘密图像分享，使用水印算法将 n 份子秘密图像嵌入 n 份载体图像中，得到 n 份带有秘密图像与签名信息与子秘密信息的载密图像。由 S_i 生成的每个点都用 x 和 y 这 2 个坐标值表示，导致子秘密图像的大小从秘密图像的 256×256 扩展到了 512×256。

生成过程中所涉及的部分数据的数据范围如下。

1) 因为采用 2×2 数据分组，所得结果有 4 位的数据量，所以 $S_i\in[0,15]$。

2) P 是素数且 P>15，取 P=17。

3) $x_i\in[1,15]$，不取 0 是因为当 $x_i=0$，$y_i=S_i$，代表信息没有被隐藏。

4) $y_i\in[0,15]$。

5) k 小于用户数目，所以 $k<n$。

3.2　分享图像的隐藏

信息隐藏的主要方法包括在时间域、空间域、变换域的隐藏[11]，实验采用容量更大的空间域隐

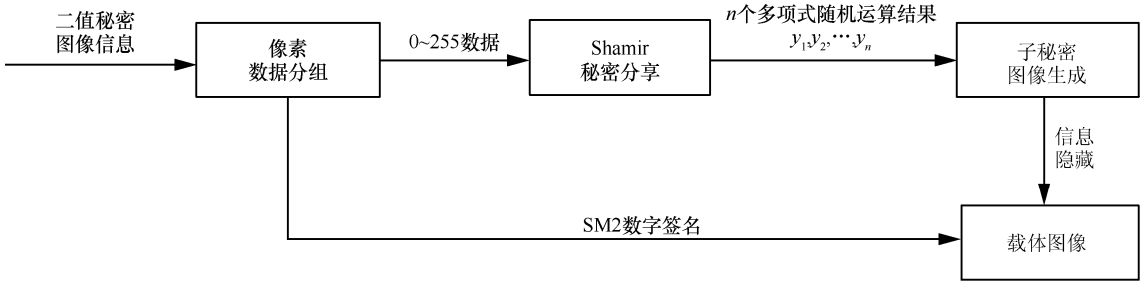


图 1　子秘密图像生成

藏方法。生成分享图像后，需要将分享图像隐藏在载体图像中，使分享图像变得不可感知，避免攻击者的恶意破坏。由于图像信息量较大，并且验证的过程需要水印信息能够 100%正确提取，所以信息嵌入方法采用基于 LSB 的信息隐藏算法，在载体图像的最低位进行信息嵌入，实现方便，同时可以保证隐藏信息的不可感知性。由于可以在每一个像素点的最低位嵌入数字信息，因此有较大的信息嵌入量。一般可以在载体图像的最低一位或者两位进行信息嵌入，嵌入位数太多会被人眼察觉，破坏隐藏信息的不可感知性。秘密图像大小为 256×256，但在进行分享处理后会产生像素扩展，使分享图像大小扩大为 512×256，如果使用 256×256 的图像作为载体，那么需要向载体图像的每个像素的低两位都嵌入信息，再加上需要嵌入的签名信息，完整的嵌入步骤会占用载体图像所有像素的低两位与部分像素的第三位，这样会造成不可感知性的损失。所以，尽量选取尺寸较大的载体图像来保证水印的不可感知性。

根据以上结论，选取大小为 512×512 的图像作为载体图像，将分享图像逐行嵌入载体图像的最低有效位。完成分享图像的嵌入后，只占用了整幅载体图像一半的最低有效位，有效保证了水印的不可感知性。

3.3 秘密图像恢复与验证

从 k 份载秘图像提取出嵌入的水印信息，包括秘密图像的签名信息和 k 份坐标数组 $\{(x_1,y_1),(x_2,y_2),\cdots,(x_i,y_i)\}$（其中，$i$ 是秘密图像以 2×2 方式分块形成的份数）。

秘密图像的恢复与验证流程如图 3 所示。

使用拉格朗日插值法对 k 份数据进行处理，将得出的数据转换成二进制，再按照生成时的数据分组方法进行填充，还原出秘密图像。使用提取出的签名信息计算得出 R，对比 R 与签名信息 r 是否一致，一致则认证通过，否则认证不通过。

4 实验结果

4.1 实验 1 秘密图像的签名

设签名者 A 的身份是：ALICE123@YAHOO.COM。用 ASCII 编码记为 ID_A:414C 49434531 3233405941484F4F 2E434F4D，$ENTLA_A$=0090。

使用 SM2 签名算法对秘密图像进行签名，并得到签名数据(r, s)。SM2 签名算法所用到的参数如下。

1) 椭圆曲线方程为：$y^2=x^2+ax+b$。

2) 素数 p：8542D69E 4C044F18 E8B92435 BF6FF7DE 45728391 5C45517D 722EDB8B 08F1DFC3。

3) 系数 a：787968B4 FA32C3FD 2417842E 73BBFEFF 2F3C848B 6831D7E0 EC65228B 3937E498。

4) 系数 b：63E4C6D3 B23B0C84 9CF84241 484BFE48 F61D59A5 B16BA06E 6E12D1DA 27C5249A。

5) 基点坐标 x_G：421DEBD6 1B62EAB6 746434EB C3CC315E 32220B3B ADD50BDC 4C4E6C14 7FEDD43D。

6) 基点坐标 y_G：0680512B CBB42C07 D47349D2 153B70C4 E5D7FDFC BFA36EA1 A85841B9 E46E09A2。

7) 阶 n：8542D69E 4C044F18 E8B92435 BF6FF7DD 29772063 0485628D 5AE74EE7 C32E79B7。

8) 私钥 d_A：128B2FA8 BD433C6C 068C8D803DFF7979 2A519A55 171B1B65 0C23661D 15897263。

9) 公钥坐标 x_A：0AE4C779 8AA0F119 471BEE11 825BE462 02BB79E2 A5844495 E97C0

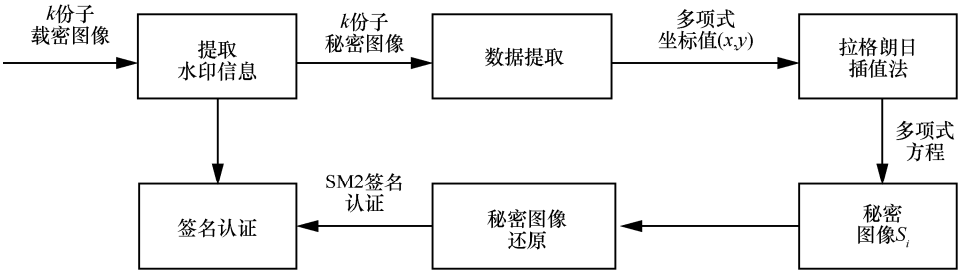


图 3 恢复与验证流程

4FF 4DF2548A。

10) 公钥坐标 y_A：7C0240F8 8F1CD4E1 6352A73C 17B7F16F 07353E53 A176D684 A9FE0C6B B798E857。

待签名数据 M 是由秘密图像转化成的文本文件，其中，逐行记录了秘密图像所有像素点的像素值。由于文件 M 内容较大，此处不予列出。根据签名者 A 的私钥，使用 SM2 签名算法对数据 M 进行签名得到数字签名（r, s）。

r: 3A4E289DAC1305B9E90BBCDC0623F90621A2F3D92AC984AA4E7A76BFBEF52DA2。

s: 06C9ABE66CC49DDCFB193DEFD1D81632AE72B960F7CAA9EB9CED97335CB0B398。

4.2 实验 2　图像分享与信息嵌入

实验要求秘密图像在经过分享后，能够使用 k 份子秘密图像恢复出秘密图像。秘密图像最终还需要进行签名认证，所以秘密图像的还原程度需要达到 100%，否则无法通过签名认证。

载体图像如图 4 所示。

(a) Lena　(b) Barbara

(c) Baboon　(d) Peppers

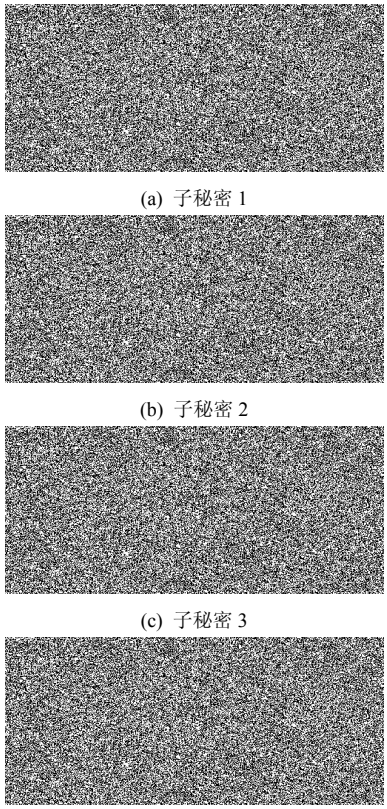
图 4　载体图像

秘密图像如图 5 所示。

秘密图像经过随机生成的 k 阶多项式处理得到子秘密图像，如图 6 所示。

签名信息的产生方法是将秘密图像的像素值转换成文本文件，使用 SM2 签名方案对文本文件进行签名，得到签名信息。

图 5　秘密图像



(a) 子秘密 1

(b) 子秘密 2

(c) 子秘密 3

(d) 子秘密 4

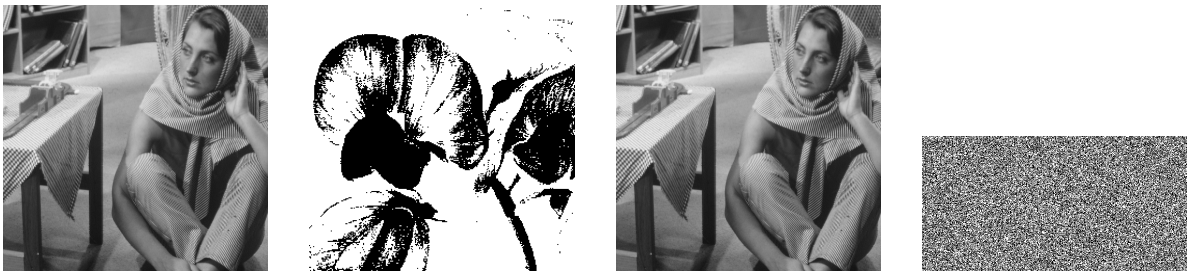
图 6　子秘密图像

嵌入水印信息的同时，将秘密图像的签名数据(r, s)转化为二进制数据，并嵌入载体图像中用于验证。嵌入方式是将数据 r 与 s 转换成二进制数据，各占一行，嵌入在子秘密图像嵌入位置的下方。图 7~图 10 为秘密图像（图 5）的嵌入与提取实验结果。图 7(a)、图 8(a)、图 9(a)、图 10(a)为载体图像，图 7(b)、图 8(b)、图 9(b)、图 10(b)为秘密图像，图 7(c)、图 8(c)、图 9(c)、图 10(c)为嵌入子秘密信息后的图像。图 7(d)、图 8(d)、图 9(d)、图 10(d)为提取出的子秘密图像。

从视觉上来说，嵌入水印信息后的图像与原图像没有区别，经过计算，嵌入信息后的图像峰值信噪比如表 1 所示。

(a) 载体图像　(b) 秘密图像　(c) 嵌入水印图像　(d) 提取子秘密图像

图 7　Lena 图嵌入与提取



(a) 载体图像　(b) 秘密图像　(c) 嵌入水印图像　(d) 提取子秘密图像

图 8　Barbara 图嵌入与提取

(a) 载体图像　(b) 秘密图像　(c) 嵌入水印图像　(d) 提取子秘密图像

图 9　Baboon 图嵌入与提取

(a) 载体图像　(b) 秘密图像　(c) 嵌入水印图像　(d) 提取子秘密图像

图 10　Peppers 图嵌入与提取

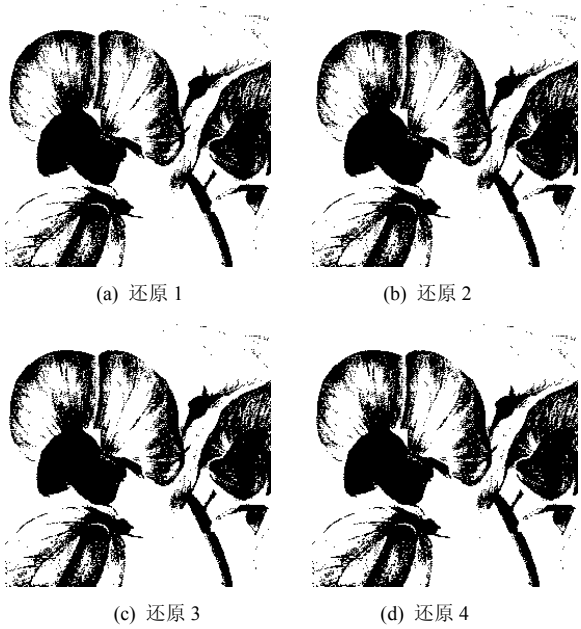
表 1　　**水印图像峰值信噪比**

载体图像	峰值信噪比/（dB）
Lena 图	57.26
Barbara 图	57.24
Baboon 图	57.21
Peppers 图	57.27

当 2 幅图像之间的峰值信噪比大于 33 时[12]，图像就具有了良好的不可感知性，肉眼无法识别嵌入前后的区别。

4.3　实验 3　秘密图像还原

根据实验 2 提取出的 4 幅子秘密图像，任意选取 3 幅进行图像还原，4 选 3 有 4 种组合，4 次还原结果如图 11 所示。



(a) 还原 1　(b) 还原 2

(c) 还原 3　(d) 还原 4

图 11　还原结果

还原结果表明，不同子秘密组合能够正确还原出秘密图像。

4.4　实验 4　签名认证

实验 3 结果表明，秘密图像的还原度达到 100%，能够满足数字签名认证需求。根据所还原的秘密图像再次生成 M 文本文件，作为签名认证过程的参数。结合签名者 A 公布的公钥与提取出的签名数据（r, s），计算得出 R，并与提取出的签名数据 r 进行比对。

提取的数字签名(r, s)如下。

r: 3A4E289DAC1305B9E90BBCDC0623F90621A2F3D92AC984AA4E7A76BFBEF52DA2。

s: 06C9ABE66CC49DDCFB193DEFD1D81632AE72B960F7CAA9EB9CED97335CB0B398。

验证得出的认证信息 R 如下。

R: 3A4E289DAC1305B9E90BBCDC0623F90621A2F3D92AC984AA4E7A76BFBEF52DA2。

其中，R=s，表明验证通过，秘密图像未被篡改。

5　安全性分析

本文提出的基于 Shamir 门限秘密分享的图像可视加密算法是有效的，满足以下条件。

1) 安全性：还原方法通过拉格朗日插值法，利用 k 个坐标值来确定 k−1 阶方程，方程的常数项就是秘密信息。如果少于 k 个坐标，那么无法正确还原方程，也无法获得秘密图像的任何信息。

2) 可恢复性：能够通过 k 份子秘密图像完美还原出秘密图像。

3) 可验证：由于 SM2 签名限制，攻击者篡改后的图像无法通过验证，并且由于签名算法私钥的限制，如果攻击者想要冒充签名者产生新的秘密图像与签名代替原始的秘密图像，那么攻击者需要解决一个基于椭圆曲线上的离散对数问题，这个问题是非常困难的，保证了签名的认证权威。

4) 不可感知性：使用基于 LSB 的信息隐藏算法，嵌入容量大，对载体图像的改动较小，使子秘密图像无法被攻击者察觉。即使被感知到，攻击者不知道嵌入位置，依旧无法获取子秘密图像。

6　结束语

秘密图像分享方案通过 Shamir(k, n)门限秘密分享方案，对秘密图像进行分享，使攻击者盗取 k 份以下的子秘密图像，无法获取秘密图像，提高了秘密图像传输与存储的安全性。通过 LSB 水印算法与 SM2 签名算法，使图像具有不可感知性与认证的能力，提高了秘密图像的安全性和真实性，能够很好地实现图像的安全传输与保存。但是也存在一定的不足，还需要对信息隐藏算法进一步改进。该方案采用的 LSB 算法非常脆弱，无法抵御攻击，选取顽健性强的水印算法并保证提取准确率达到 100%，可以提高分享图像的安全性且能够进行验证，这是下一步的改进方向。

参考文献：

[1] SHAMIR A. How to share a secret[J]. Communications of the ACM,1979,22(11): 612-613.

[2] PANG L J, WANG Y M. A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing[J]. Applied Mathematics & Computation, 2005, 167(2):840-848.

[3] 荣辉桂, 莫进侠, 常炳国, 等. 基于 Shamir 秘密共享的密钥分发与恢复算法[J]. 通信学报, 2015(3):60-69.
RONG H G, MO J X, CHANG B G, et al. Key distribution and recovery algorithm based on Shamir's secret sharing[J]. Journal on Communications,2015(3): 60-69.

[4] 庞辽军, 王育民. 基于 RSA 密码体制(f, n)门限秘密共享方案[J]. 通信学报, 2005, 26(6):70-73.
PANG L J, WANG Y M. (t, n) threshold secret sharing scheme based on RSA cryptosystem[J]. Journal of China Institute of Communications, 2005, 26(6):70-73.

[5] 牛少彰,钮心忻,杨义先.基于 Shamir 秘密共享方案的数字水印算法[J]. 中国图象图形学报. 2003(10).
NIU S Z, NIU X X,YANG Y X. Digital watermarking algorithm

based on shamir secret sharing scheme[J]. Journal of Image and Graphics. 2003(10).

[6] 尚铭, 马原, 林璟锵, 等. SM2 椭圆曲线门限密码算法[J].密码学报, 2014, 1(2): 155-166.
SHANG M, MA Y, JING J W, et al. A threshold scheme for SM2 elliptic curve cryptographic algorithm[J]. Journal of Cryptologic Reseatch, 2014, 1(2): 155-166.

[7] 汪朝晖,张振峰.SM2 椭圆曲线公钥密码算法综述[J].信息安全研究,2016,2(11): 972-982.
WANG C H, ZHANG Z F. Overview on public key cryptographic algorithm SM2 based on elliptic curves[J]. Information security research, 2016, 2(11): 972-982.

[8] JAIN J, JOHARI P. Digital image watermarking based on LSB for gray scale image[J]. International Journal of Computer Science & Network Security, 2014.

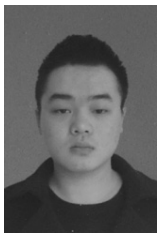
[9] 宋玉杰，谭铁牛. 基于脆弱性数字水印的图象完整性验证研究[J]. 中国图象图形学报, 2003, 8(1): 1-7.
SONG Y J, TAN T N. A brief review on fragile watermarking based image authentication[J]. Journal of Image and Graphics, 2003, 8(1): 1-7.

[10] 胡东, 刘晓云. 使用频域 LSB 水印算法的鲁棒性分析[J]. 电子科技大学学报, 2006, 35(5):770-773.
HU D, LIU X Y. Robust analysis for using LSB arithmetic to embed watermark in frequency domain[J]. Journal of University of Electronic Science and Technology of China, 2006, 35(5):770-773.

[11] 陈波, 谭运猛, 吴世忠. 信息隐藏技术综述[J]. 计算机与数字工程, 2005, 33(2):21-23.
CHEN B, TAN Y M, WU S Z. Research on information hiding techniques[J]. Computer & Digital Engineering, 2005, 33(2):21-23.

[12] DENG Y, KENNEY C, MOORE M S, et al. Peer group filtering and perceptual color image quantization[C]//IEEE International Symposium on Circuits and Systems. 1999.

[作者简介]



谭亦夫（1994-），男，湖南株洲人，北京印刷学院硕士生，主要研究方向为数字水印。

李子臣（1962-)，男，河南温县人，博士，北京印刷学院教授、博士生导师，主要研究方向为公钥密码、数字签名、后量子密码。