基于三角剖分的数字图像分存算法

袁茜茜 蔡占川

(澳门科技大学资讯科技学院 澳门 999078)

摘 要 网络的不安全性导致图像信息在传输过程中容易丢失、损坏,或被不法分子窃取并用于非法传输,因此,研究数字图像的加密技术可以有效加强图像信息的安全性。数字图像分存算法是一种重要的图像信息加密技术,但是以往的图像分存技术没有考虑像素灰度分布特征,对图像进行逐像素加密,既降低了安全性,也产生了不必要的时空开销。为此,文中采用了基于数字图像像素灰度特征的非均匀三角剖分算法,结合门限方案,提出了一种新的数字图像分存算法。首先,使用非均匀三角网格剖分算法,得到随图像灰度值变化的剖分网格;其次,使用门限方案对剖分网格中每一个子三角形的顶点像素进行加密和共享;最后,使用拉格朗日插值多项式和剖分网格编码信息重构出原始图像。实验结果表明,该方法降低了像素的冗余加密,提高了安全性且图像重构效果较好,是一种有效的图像分存算法。

关键词 图像分存,三角剖分,门限方案

中图法分类号 TP391.41 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.04.020

Digital Image Sharing Algorithm Based on Triangular Partition

YUAN Xi-xi CAI Zhan-chuan

(Faculty of Information Technology, Macau University of Science and Technology, Macao 999078, China)

Abstract The digital image is easily lost, damaged, and stolen by cheaters and used for illegal transmission because of the insecure network. Therefore, the digital image encryption technology can effectively enhance the security of image. The digital image sharing algorithm is an important encryption technology. However, the conventional image sharing technologies repeat encryption pixel by pixel without considering the gray distribution characteristic, resulting in both reduced security and unnecessary space-time overhead. To handle the above problems, a new digital image sharing algorithm was proposed by adopting the gray distribution characteristic based non-uniform triangular partition algorithm and the threshold scheme. First, the non-uniform triangular partition algorithm is used to obtain the mesh of the image according to the gray distribution characteristic. Second, the threshold scheme is used to encrypt and share the vertex pixels of each sub-triangle in the mesh. Finally, the original image is reconstructed by using the Lagrange interpolation polynomial and the mesh coding information. The experimental results show that the proposed method reduces the redundant encryption of pixels, improves the security and has good image reconstruction effect, so it is an effective image sharing algorithm.

Keywords Image sharing, Triangular partition, Threshold scheme

1 引言

信息安全是互联网技术发展的重要研究课题。数字图像作为信息传输的重要载体之一,其安全性研究具有重要意义。图像分存技术是图像信息安全领域中的主要内容之一,此外还有图像信息隐藏、数字水印等[1-4]。图像分存技术可以有效防止意外事故引起的秘密信息遗失,及进一步导致的秘密信息被窃取或无法解密,适用于解决需要多个参与者同时合作才可以达到某种目的的问题,如档案管理、财产分割和导弹的控制与发射等[5-6]。

图像分存是指将秘密图像拆分为多幅无意义或杂乱无章的影子图像,或伪装到多幅有意义的图像中进行存储或传输。其利用满足门限数量的影子图像来完成对秘密图像的完整重构,当拥有任何低于门限数量的子图像时,无法得到秘密图像的任何信息。因此,上述策略具有的优点在于少数分存图像的丢失不会引起秘密信息的泄漏,个别分存图像的破坏也不

到稿日期:2018-06-21 返修日期:2018-08-13 本文受国家基础研究计划"973"项目(2011CB302400),澳门科技发展基金项目(048/2016/A2,0012/2018/A1,0069/2018/A2),国家自然科学基金面上项目(61272364),浙江大学CAD&CG国家重点实验室开放课题(A1910),北京理工大学珠海学院科研发展基金项目(XK-2018-04)资助。

袁茜茜(1992-),女,博士生,主要研究方向为计算机图形图像处理,信息安全;蔡占川(1973-),男,博士,教授,博士生导师,CCF会员,主要研究方向为计算机图形图像处理、数值分析,E-mail:zccai@must.edu.mo(通信作者)。

会影响秘密信息的恢复[7-9]。

图像信息分存技术主要源于密码学中的秘密共享概念，秘密共享技术最早由 Shamir 和 Blakley 分别结合拉格朗日插值法和矢量空间点性质提出[10-12]。1994 年，Naor 等[13]首次提出图像秘密共享的思想，并构造出加密黑白图像的(k,n)-可视分存方案(Visual Cryptography Scheme，VCS)，之后其被多次改进[14-16]，但普遍存在像素膨胀和失真的问题[17-18]。2002 年，Thien 等[19]提出了一种基于 Lagrange 插值多项式的秘密图像分存和重构策略，可有效解决文献[13]中存在的问题，但仍无法解决分发者和参与者的欺诈问题，而且最大素数的选择也受到限制，导致重构图像质量不佳。其后又有一些研究学者从不同角度相继提出了其他分存方案，如彩色图像分存方案[20]，渐进秘密图像分存方案[21]，基于混沌系统、矩阵分解、中国剩余定理、二次剩余定理等的图像分存技术，基于(k,n)门限方案的图像分存技术等[22-24]，研究人员致力于寻找分存效果好、实现简单且数据膨胀率低的分存方法。

为了探索更有效的图像分存算法，提高加密算法的效率和安全性，本文提出一种新的基于三角剖分的图像分存算法。非均匀网格剖分算法是文献[25]提出的一种更合理地划分图像区域定义域的方法，便于将基于像素的图像信息转化为数学表达形式。根据图像像素的灰度变化特征，使用拟合算法和自相似剖分方法得到的非均匀剖分网格，将灰度相似的相邻图像区域划分到一个子域中，这种剖分网格可以映射为图像灰度信息，并且已经被成功应用于多个图像处理领域[26-27]。非均匀剖分算法主要包括矩形剖分和三角剖分，三角形作为平面域的单纯形，具有比其他类型的多边形更多的特性和优点[28]，因此本文使用非均匀三角剖分算法对秘密图像进行预处理。结合门限秘密共享策略和非均匀三角网格剖分算法，本文提出了一种安全性更高的图像分存算法。

2 基于非均匀三角剖分的图像分存算法

图像分存技术属于信息加密技术的一种，本文设计的加密系统结构如图 1 所示。

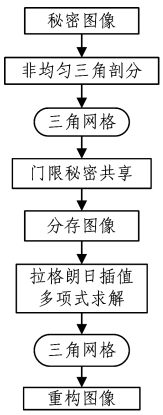


图 1 基于三角剖分的图像分存算法的结构图

Fig. 1 Structure of image sharing algorithm based on triangular partition

由秘密图像到分存图像的实现过程属于加密阶段，主要使用了非均匀三角剖分策略、秘密共享策略，涉及最小二乘拟合算法和门限方案。由分存图像到重构图像的实现过程属于解密阶段，主要涉及的算法有拉格朗日插值求解和二元多项式插值。

2.1 非均匀三角剖分算法

在图像加密阶段需要首先使用非均匀三角剖分算法提取秘密图像的特征像素，然后使用门限共享策略对这些像素信息进行分存。在图像解密阶段，通过多个分存可以恢复出特征像素的灰度值，然后由特征像素和剖分网格重构出秘密图像。非均匀三角剖分的编码和实现过程如下。

把图像看作矩形区域 G 上的二元函数 $z=f(x,y)$，$(x,y)\in G$。x,y 分别为图像像素点所处的行和列，z 为该点像素的灰度值。视 G 为初始区域，首先将其剖分成两个或多个子三角形区域，以其作为初始剖分，然后对每个子三角形区域作进一步的自相似三角剖分。按自相似规则，假设由 G 初始剖分得到的一个子三角形区域为 G_0，先将 G_0 剖分为 4 个自相似的子区域，分别记为 G_1,G_2,G_3,G_4。对每个子区域，可以进一步自相似地分割为 4 个更小的子区域，这个过程可以一直进行下去[23]。

假设所标记的子三角形区域为 G_m，则正整数 m 的 4 进制表示如式(1)所示：

$$m=m_p4^p+m_{p-1}4^{p-1}+m_{p-2}4^{p-2}+\cdots+m_14^1+m_04^0 \quad (1)$$

简记为：

$$m=(m_pm_{p-1}m_{p-2}\cdots m_1m_0)_4 \quad (2)$$

其中，$m_i\in\{0,1,2,3\}$，$i=0,1,2,\cdots,k$。

剖分的详细过程及子三角形的编号示意图可参见文献[25-26]。

对于给定的图像，非均匀剖分过程的描述如下：考虑在剖分的某一步，取定一个子区域 G_m(从初始剖分出发)，将 G_m 上所包含的像素记为$\{Q_i\}$，其对应的灰度值$\{z_i\}$为已知数据，n 为 G_m 上的像素个数，用 k 次二元多项式 $f_m(P)$对$\{Q_i\}$作最小二乘拟合，其中 $i\in[0,n-1]$，当满足式(3)时，即得到了拟合多项式 $f_m(P)$($P\in G_m$)并停止下一次剖分，其中 ε 是剖分精度阈值，对不满足 $e<\varepsilon$ 条件的子三角形区域 G_m，逐个考察 G_{mn}($n=1,2,3,4$)，记录满足 $e<\varepsilon$ 的 mn 及 $f_{mn}(P)$，依次类推，完成对整幅图像的剖分。

$$e=\sum_{i=0}^{n-1}(f_m(Q_i)-z_i)^2<\varepsilon \quad (3)$$

$$f_m(x,y)=ax+by+c \quad (4)$$

在实际应用中，G_m 上的 $f_m(P)$通常取 1 次或 2 次多项式，次数过高将会使计算复杂度增加，因此不予采用。图像区域的非均匀剖分过程就是数字图像矢量化的过程，得到的结果是对数字图像具有一定精度的分片多项式逼近，这种矢量化方法可以应用于多项图像处理技术，如图像信息隐藏和伪装等方面[29-30]。本文将其应用于图像分存领域并验证了算法的有效性。

2.2 门限秘密共享策略

完成秘密图像的剖分之后，需要使用门限策略对特征像素点进行加密。门限秘密共享的主要内容如下。

Shamir 提出的(k,n)门限方案的特点是：可以将秘密信

息分发为 n 个份额，当且仅当 k 个参与者同时贡献出他们的影子份额时，才可以恢复出秘密。能够重构出秘密的人数 k 为充分必要条件，参与者的总人数为 n。每一个参与者都知道 n 值、k 值，以及秘密的可能范围集合。规范性的描述如下[31]。

条件：1）确定非负整数 n，k，且 $k<n$；2）秘密 D 的可能范围集合为 $D\in\{0,1,\cdots,S-1\}$。

要求：将 D 分为多个分存（子密钥）$D_1,D_2,\cdots,D_n$，则任意 k 个子密钥合作可以重构并得到秘密 D，任意 $k-1$ 个子密钥合作不能得到关于 D 的任何信息。

这个策略的适用条件为：一个秘密必须分散放在 n 个不同的位置，以达到便利性和容错性的要求，同时，必须能抵抗 $k-1$ 个违规者，以防止敏感数据泄漏或者参与者不可信。

不同于以往的加密协议，Shamir 门限计算复杂度较低且容易证明。文献[31]对 Shamir 门限秘密共享方案进行了具体描述：

任选素数 p，满足

1）$p\geqslant\max(D,n+1)$（Z_p 为对 p 求余的值域）；

2）任意不相等的 $a_1,a_2,\cdots,a_{k-1}\in Z_p$；

3）选择多项式 $q(x)=D+a_1x+\cdots+a_{k-1}x^{k-1}$；

4）$D_i=q(i) \bmod p\in Z_{p'}(1\leqslant i\leqslant n)$；

5）$D=q(0)$。

从以上描述可以看出，门限秘密共享方案满足已知 k 个点是能够解出 $q(x)$ 的充分必要条件。条件 4）通过求余代替实际值可以增加计算的准确性，避免了计算机运算中对大数的处理。条件 1）中所选大素数 p 的值要大于秘密 D，否则所求多项式的值永远小于 D，即无法得到秘密 D 的值。此外，p 的值要大于参与者的个数 n，如果 $p=n$，则第 n 个参与者的分存即为秘密 D 的值；如果 $p<n$，则第 $n+1$ 个参与者的分存与第一个参与者的分存相同，对于计算无效。上述 5 项要求亦是求解 (k,n) 门限算法的必要条件。

2.3　具体方案

在使用非均匀三角剖分算法和门限秘密共享策略的基础上，本节给出加密过程和解密过程的完整图像分存方案。

1）加密阶段。秘密图像共享方案的实现，首先要有一个可信中心负责将秘密图像的影子份额分发给参与者，并公开必要的验证和用于秘密重构的信息。基于非均匀三角剖分的秘密图像分存方案在分存图像分发阶段，首先要由可信中心对秘密图像 S 进行剖分处理，得到三角剖分网格，可选择式（4）作最小二乘拟合多项式；然后对子三角形的顶点进行加密，并共享给 n 个参与者。

$$y=S_i+a_1x_i+\cdots+a_{k-1}x_i^{k-1} \bmod p \tag{5}$$

其中，S_i 代表当前加密顶点的灰度值；$a_i(i=1,2,\cdots,k-1)$ 为多项式系数，可取随机值；p 取小于 255 的最大素数即 251。我们给出如下一种取值策略：门限值取 3，即 $k=3$；3 个顶点 $(1,1)$，$(3,1)$，$(3,3)$ 的灰度值 $S_i(i=1,2,3)$ 分别取为 11，13，15，如图 2 所示，它们对应的 a_i 的取值如式（6）所示。以第二个分存为例，分存图像子三角形顶点的灰度值计算如下：

$$\begin{aligned}
y_{1,1}&=(S_1+a_{1,1}x+a_{1,2}x^2) \bmod p\\
&=(11+4\times2+3\times2^2) \bmod 251=31\\
y_{1,2}&=(S_2+a_{2,1}x+a_{2,2}x^2) \bmod p\\
&=(13+8\times2+9\times2^2) \bmod 251=65\\
y_{1,3}&=(S_3+a_{3,1}x+a_{3,2}x^2) \bmod p\\
&=(15+12\times2+27\times2^2) \bmod 251=147
\end{aligned} \tag{6}$$

我们以图 2 和图 3 为例，给出一个子三角形区域的加密过程。其他分存的加密策略与此类似，图 3 列出了前 4 个分存图示。

对于未加密的像素区域，系统将产生随机灰度值，最终得到与原始图像大小相同的分存图像。由于 i 值不同，每个参与者得到的加密信息也不同，参与者可以公开其拥有的分存图像，但不能公开 i 值，否则有可能被欺骗者获取并得到秘密图像。在该例子中至少需要 3 个参与者提供密钥信息，才可以恢复该点的灰度值，因此是 $(3,n)$ 门限方案。如果要提高门限值，只需要增加相应的未知参数的个数即可。

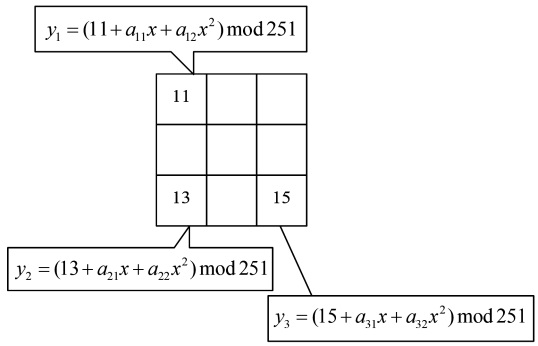
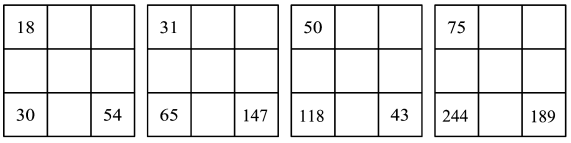


图 2　加密图像图示

Fig. 2　Encrypted image illustration



（a）分存网格 1　（b）分存网格 2　（c）分存网格 3　（d）分存网格 4

图 3　分存图像图示

Fig. 3　Sharing image illustrations

2）解密阶段（重构阶段）。由达到门限值数量的参与者把密钥信息 i 和分存图像（视觉看上去为黑白像素点随机分布的图像）提供给可信中心。可信中心根据剖分网格，从分存图像中提取出加密像素点，然后通过式（7）求出原始图像三角形顶点的灰度值，最后由 3 个顶点的灰度值恢复出整个三角形平面。这里采用的是多项式插值求解方法，比如 3 个顶点灰度值可以反解出式（4）的系数，进而插值得到该二维平面上的所有灰度值。如果将式（4）换成 $f_m(x,y)=ax^2+by^2+cx+dy+exy+f$，将会通过插值得到一个二维曲面，波动的曲面将存在大于 250 的灰度值。下面采用拉格朗日插值多项式的求解算法给出秘密重构的过程。

根据 (k,n) 门限方案的设定条件，可以通过拉格朗日插值多项式重构出秘密，即 $q(0)$。

$$q(0)=\sum_{i=1}^{k}\Big(\prod_{j=1,j\neq i}^{k}\frac{j}{j-i}\times q(i)\Big) \bmod p \tag{7}$$

图 4 给出使用前 3 个分存图像重构出一个加密图像的子三角形顶点灰度值的过程。其中，4 个网格图从左至右依次为分存网格 1，分存网格 2，分存网格 3 和重构图像。

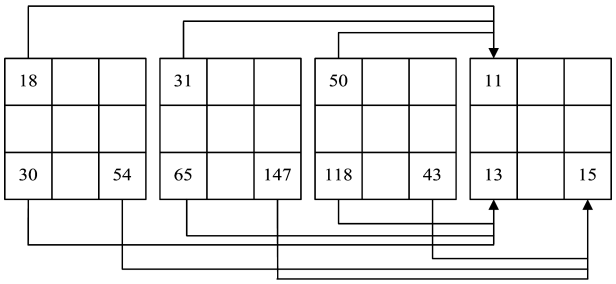


图 4 秘密重构过程图示

Fig. 4 Secret reconstruction process

其具体计算过程如下：

$$S_1=(18\times\frac{2\times3}{(2-1)(3-1)}+31\times\frac{1\times3}{(1-2)(3-2)}+50\times\frac{1\times2}{(1-3)(2-3)})\bmod 251=11$$

$$S_2=(30\times\frac{2\times3}{(2-1)(3-1)}+65\times\frac{1\times3}{(1-2)(3-2)}+118\times\frac{1\times2}{(1-3)(2-3)})\bmod 251=13$$

$$S_3=(54\times\frac{2\times3}{(2-1)(3-1)}+147\times\frac{1\times3}{(1-2)(3-2)}+244\times\frac{1\times2}{(1-3)(2-3)})\bmod 251=15 \quad (8)$$

3 算法描述

下面给出由一幅图像生成 n 个分存图像，以及由 k 个分存重构出秘密图像的算法描述。

Step 1 对秘密图像进行初始划分，得到两个或多个子三角形区域 G_m。

Step 2 使用式(4)拟合当前区域。

Step 3 对不满足式(3)的区域进行自相似剖分，得到 4 个更小的子三角形区域；满足式(3)的区域停止剖分。重复步骤 3 直至完成整幅图像的剖分，得到非均匀三角剖分网格。

Step 4 使用式(5)依次将三角形网格顶点的特征像素进行门限加密，非特征像素取随机灰度值，生成 n 份分存，加密过程参考式(6)。

Step 5 由 k 个参与者提供分存及秘密图像的三角网格编码信息。

Step 6 由网格编码信息找到特征像素的位置。

Step 7 使用式(7)和 k 个参与者提供的影子图像恢复出特征像素，重构过程参考式(8)。

Step 8 由特征像素依次解出式(3)中的未知系数，并由像素坐标值求出该点所在位置的像素灰度值。

Step 9 重构出三角网格中所有的子三角形区域，得到原始秘密图像。

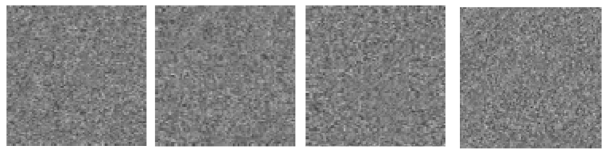
4 实验结果及分析

本文通过一系列实验验证了算法的可行性。图 5 为秘密图像 Lena，选取剖分精度阈值 $\varepsilon=20$ 对其进行剖分，并用$(3,n)$方案对其进行加密。图 6 列举了其中的 4 幅影子图像$(x_i=1,2,3,4)$。图 7－图 10 给出了原始图像上的非均匀剖分网格和重构图像，原图大小均为 256×256 像素，分别为 Lena、Peppers、Pelican 和澳门科技大学校徽(MUST)。每组实验的精度阈值分别取 $\varepsilon=30,20$。

本文实验在以下运行环境中进行：Intel(R) Core(TM) i7-6700 CPU @3.40GHz 3.41GHz，16.0GB Ram，测试工具 Matlab (R2016)。

图 5 秘密图像 Lena

Fig. 5 Secret images Lena



(a)分存图像 1 (b)分存图像 2 (c)分存图像 3 (d)分存图像 4

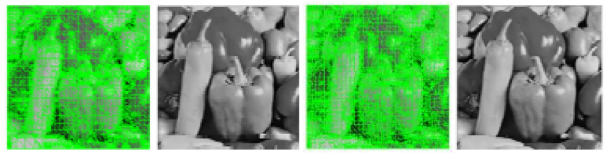
图 6 秘密图像 Lena 的 4 个分存图像($n=4,k=3$)

Fig. 6 Four sharing images of the secret image Lena ($n=4,k=3$)

(a)网格图像 1 ($\varepsilon=30$) (b)解密图像 1 ($\varepsilon=30$) (c)网格图像 2 ($\varepsilon=20$) (d)解密图像 2 ($\varepsilon=20$)

图 7 Lena 的剖分网格图像及重构图

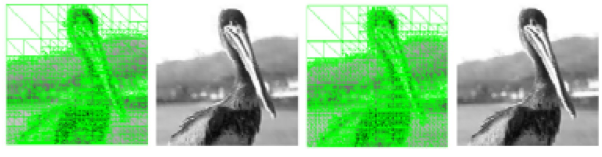
Fig. 7 Mesh and the reconstruction image of Lena



(a)网格图像 1 ($\varepsilon=30$) (b)解密图像 1 ($\varepsilon=30$) (c)网格图像 2 ($\varepsilon=20$) (d)解密图像 2 ($\varepsilon=20$)

图 8 Peppers 的剖分网格图像及重构图

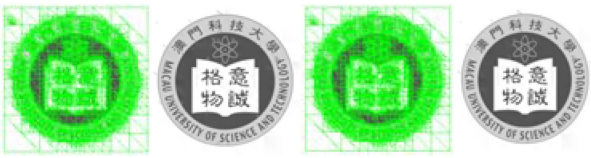
Fig. 8 Mesh and the reconstruction image of Peppers



(a)网格图像 1 ($\varepsilon=30$) (b)解密图像 1 ($\varepsilon=30$) (c)网格图像 2 ($\varepsilon=20$) (d)解密图像 2 ($\varepsilon=20$)

图 9 Pelican 的剖分网格图像及重构图

Fig. 9 Mesh and the reconstruction image of Pelican



(a)网格图像 1 (ε=30)　(b)解密图像 1 (ε=30)　(c)网格图像 2 (ε=20)　(d)解密图像 2 (ε=20)

图 10　MUST 的剖分网格图像及重构图

Fig. 10　Mesh and the reconstruction image of MUST

图 6 给出了图 5 中秘密图像的 4 个分存图像，分存图像大小与秘密图像和重构图像大小相同，无像素膨胀。可以发现，无法从分存图像中得到任何关于秘密图像的信息。

表 1 是图 7—图 10 的实验数据，列出了对 Lena、Pepper、Pelican 和澳门科技大学校徽(MUST) 4 幅图像进行剖分的剖分网格子三角形的个数和峰值信噪比(PSNR)。PSNR 是一种评价图像质量的客观标准，其定义如式(9)所示，其中 $I(i,j)$，$K(i,j)$分别代表原始图像和重构图像对应的像素值，m，n 表示图像的大小。

$$PSNR=10\log_{10}\frac{m\times n\times 255^2}{\sum_{i=0,j=0}^{m-1,n-1}\|I(i,j)-K(i,j)\|^2} \tag{9}$$

表 1　图 7—图 10 的实验数据

Table 1　Experiment results from Fig. 7 to Fig. 10

	剖分精度阈值	子三角形个数	PSNR
Lena	30	8003	35.6
	20	9452	39.3
Peppers	30	7700	35.3
	20	9272	38.7
Pelican	30	6422	37.3
	20	7403	40.1
MUST	30	7406	37.1
	20	7964	39.5

从表 1 中可以看出，三角剖分之后的重构图像的 $PSNR$ 较高，表示重构图像与秘密图像几乎一样。虽然本文采用的是有损分存算法，但实验效果良好。

该方案基于(k,n)门限方案的加密算法，由门限秘密共享策略可知，该方案具有基于计算的安全性。此外，由于使用了非均匀剖分算法对秘密图像进行预处理，因此只需要对特征像素点进行加密处理即可，降低了对图像的冗余加密，增加了算法的安全性。在抗攻击性方面，该方案可以防止由于相邻像素灰度相近带来的欺诈问题[6]。就三角剖分网格而言，它也可以被视作一种密钥，当网格信息被分别分发给所有参与者时，每一个参与者的权限是相同的；当网格信息只分发给部分参与者时，这部分参与者相对于无网格信息的参与者具有更大的权限，但都满足只有大于或等于门限数量的分存个数才可以恢复出秘密图像。

结束语　本文提出了一种新的基于三角剖分的数字图像分存算法，实验结果表明，本文提出的算法具有可行性，可以得到较高质量的重构图像，且无像素膨胀。该算法具有一定的可靠性、安全性和防欺骗性，可用于解决现实中的信息加密问题。该算法的优点在于只需要对特征像素进行加密即可，减少了对冗余像素点的加密处理，具有基于门限方案的安全性；其缺点在于非均匀三角剖分的计算过程和剖分网格的存储带来的时空开销。

基于门限策略的图像分存方案经常需要考虑参与者之间的欺骗问题，以及分存图像的一次一秘、不可重复使用问题，未来可以进一步研究可验证和多秘密共享的图像分存方案。

参 考 文 献

[1] OUYANG X B，SHAO L P. A (K,N) Significant Nonexpansive Image Sharing Scheme Based on GF (2^3)[J]. Computer Science，2015，42(12)：251-256. (in Chinese)
欧阳显斌，邵利平. 一种基于 GF (2^3) 的(K,N)有意义无扩张图像分存方案[J]. 计算机科学，2015，42(12)：251-256.

[2] HU C Q，DENG S J，QIN M F，et al. Digital image encryption algorithm based on Logistic and standard mapping[J]. Computer Science，2010，37(12)：57-59. (in Chinese)
胡春强，邓绍江，秦明甫，等. 基于 Logistic 与标准映射的数字图像加密算法[J]. 计算机科学，2010，37(12)：57-59.

[3] SUN W，ZHOU J，ZHU S，et al. Robust Privacy-Preserving Image Sharing over Online Social Networks (OSNs)[J]. ACM Transactions on Multimedia Computing，Communications，and Applications (TOMM)，2018，14(1)：14.

[4] ROZANTSEV A，SALZMANN M，FUA P. Beyond sharing weights for deep domain adaptation[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence，2019，41(4)：801-814.

[5] SASAKI M，WATANABE Y. Visual Secret Sharing Schemes Encrypting Multiple Images[J]. IEEE Transactions on Information Forensics and Security，2018，13(2)：356-365.

[6] HU C Q. Research and Implementation of Image Secret Sharing Algorithm[D]. Chongqing：Chongqing University，2009. (in Chinese)
胡春强. 图像分存算法的研究与实现[D]. 重庆：重庆大学，2009.

[7] YI F，WANG D S，DAI Y Q. Multi-secure color image visual sharing scheme for general access structure[J]. Progress in Natural Science，2006，16(1)：95-100. (in Chinese)
易枫，王道顺，戴一奇. 一般存取结构的多密图彩色可视分存方案[J]. 自然科学进展，2006，16(1)：95-100.

[8] YI F，WANG D S，LUO P，et al. Two new color image (n，n) sharing schemes[J]. Journal of Communications，2007，28(5)：30-35. (in Chinese)
易枫，王道顺，罗平，等. 两种新的彩色图像 (n，n) 分存方案[J]. 通信学报，2007，28(5)：30-35.

[9] DENG S J，HU C Q，WANG F X，et al. Digital Image Sharing Algorithm Based on Quadratic Remainder Theorem[J]. Computer Engineering，2009，35(15)：124-125. (in Chinese)
邓绍江，胡春强，王方晓，等. 基于二次剩余定理的数字图像分存算法[J]. 计算机工程，2009，35(15)：124-125.

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

[11] BLAKLEY G R，KABATIANSKII G A. Linear algebra ap-

proach to secret sharing schemes[M]// Error Control, Cryptology, and Speech Compression. Springer, Berlin, Heidelberg, 1994:33-40.

[12] LIU S, WANG D S. (k,n) Visual Extension of True Color Extension[J]. Journal of Wuhan University(Natural Science Edition), 2008, 54(5):603-606. (in Chinese)
刘硕,王道顺. (k,n) 真彩色扩展可视分存技术[J]. 武汉大学学报(理学版), 2008, 54(5):603-606.

[13] NAOR M, SHAMIR A. Visual cryptography[C]// Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1994:1-12.

[14] WANG D S, ZHANG L, MA N, et al. Two secret sharing schemes based on Boolean operations[J]. Pattern Recognition, 2007, 40(10):2776-2785.

[15] LEE K H, CHIU P L. Sharing visual secrets in single image random dot stereograms[J]. IEEE Transactions on image processing, 2014, 23(10):4336-4347.

[16] DANG W, HE M, WANG D, et al. K out of K Extended Visual Cryptography Scheme Based on "XOR"[J]. International Journal of Computer and Communication Engineering, 2015, 4(6):439.

[17] KATZ J, MENEZES A J, VANOORSCHOT P C, et al. Handbook of applied cryptography[M]. CRC Press, 1996:64-69.

[18] DHAMIJA R, PERRIG A. Deja Vu-A User Study: Using Images for Authentication[C]// USENIX Security Symposium. 2000:4.

[19] THIEN C C, LIN J C. Secret image sharing[J]. Computers & Graphics, 2002, 26(5):765-770.

[20] SINGH P, RAMAN B. Reversible data hiding based on Shamir's secret sharing for color images over cloud[J]. Information Sciences, 2018, 422:77-97.

[21] YAN X, LIU X, YANG C N. An enhanced threshold visual secret sharing based on random grids[J]. Journal of Real-time Image Processing, 2018, 14(1):61-73.

[22] HUA W, LIAO X. A secret image sharing scheme based on piecewise linear chaotic map and Chinese remainder theorem [J]. Multimedia Tools and Applications, 2017, 76(5):7087-7103.

[23] BAO L, YI S, ZHOU Y. Combination of Sharing Matrix and Image Encryption for Lossless (k, n)-Secret Image Sharing[J]. IEEE Transactions on Image Processing, 2017, 26(12):5618-5631.

[24] MATSUMOTO R. Quantum stabilizer codes can realize access structures impossible by classical secret sharing[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, 100(12):2738-2739.

[25] 齐东旭,宋瑞霞,李坚. 非连续正交函数[M]. 北京:科学出版社, 2011:280-281.

[26] YU J D, SONG R X, QI D X. A scheme for steganography based on triangular partition of digital images [J]. Journal of Computer Research and Development, 2009, 46(9):1432-1437. (in Chinese)
余建德,宋瑞霞,齐东旭. 基于数字图像三角形剖分的信息伪装算法[J]. 计算机研究与发展, 2009, 46(9):1432-1437.

[27] U K T, JI N, QI D X, et al. A novel image denoising algorithm based on non-uniform triangular partition and interpolation[C]// 2010 International Conference on Future Power and Energy Engineering (ICFPEE). IEEE, 2010:67-70.

[28] CAI Z, LAN T. Method for coding data: U. S. Patent 9,755,661 [P]. 2017-09-05.

[29] SHARMA V K, SRIVASTAVA D K, MATHUR P. Efficient image steganography using graph signal processing[J]. IET Image Processing, 2018, 12(6):1065-1071.

[30] MUHAMMAD K, HAMZA R, AHMAD J, et al. Secure Surveillance Framework for IoT systems using Probabilistic Image Encryption[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8):3679-3689.

[31] TOMPA M, WOLL H. How to share a secret with cheaters[M]// Advances in Cryptology-CRYPTO' 86. Springer Berlin Heidelberg, 1987:261-265.