基于恢复函数和误差扩散的灰度图像分存方案

欧锻灏[1] 吴小天[1] 孙 伟[2] 刘 娟[3]
(中山大学信息科学与技术学院 广州 510006)[1] (中山大学软件学院 广州 510006)[2]
(暨南大学信息科学与技术学院 广州 510632)[3]

摘 要 基于(n,n)-阈值的灰度图像分存方案利用恢复函数和误差扩散技术将一张秘密灰度图像分存到n张有意义的灰度分存图像中。所提方案选择n张有意义的灰度图像作为分存图像,以增强秘密图像的隐蔽性,达到保护图像信息安全的目的;采用误差扩散技术,可以产生具有良好视觉质量的分存图像。所生成的分存图像没有像素膨胀,其大小与秘密图像相等。此外,方案的重构过程简单快速,而且是无损的。实验结果和理论分析表明,所提方案能为秘密图像分存提供一个高安全和有效的机制。

关键词 秘密灰度图像分存,无损重构,有意义分存图像,误差扩散,恢复函数
中图法分类号 TP391 **文献标识码** A

Secret Gray-level Image Sharing Scheme Based on Recovery Function and Error Diffusion

OU Duan-hao[1] WU Xiao-tian[1] SUN Wei[2] LIU Juan[3]
(School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China)[1]
(School of Software, Sun Yat-sen University, Guangzhou 510006, China)[2]
(School of Information Science and Technology, Jinan University, Guangzhou 510632, China)[3]

Abstract A secret gray-level image sharing scheme based on a(n,n)-threshold, divides a secret gray-level image into n meaningful gray-level shadow images using recover function and error diffusion algorithm. In order to increase the steganographic effect for the security protection purpose, the proposed scheme selects n gray-level images containing meaningful contents as shadows. The proposed scheme can generate the shadow image with good visual quality by using error diffusion algorithm. The generated shadow image has no pixel expansion, and its size is equal to the secret image's. Furthermore, the reconstructing process is fast and lossless. Experimental results and theoretical analysis demonstrate that the proposed scheme offers a high secure and effective mechanism for secret image sharing.

Keywords Secret gray-level image sharing, Lossless reconstructing, Meaningful shadows, Error diffusion, Recovery function

1 引言

随着互联网技术和多媒体技术的快速发展,图像信息可以在网络上方便地传输和存储。在许多应用中,特别是商业应用和军事应用,重要和敏感的图像信息在存储和传播中需要受到保护。解决图像安全的问题,传统的方法有加密技术和隐藏技术。图像加密后变得不可读和无意义,虽然掩盖了秘密图像的内容,但容易引起攻击者的注意。隐藏技术则将秘密信息隐藏到载体图像中,形成伪装图像,使攻击者无法察觉秘密图像的存在。这两种方法的共同缺点是容错性差,密图或伪装图像一旦遭到破坏,将无法重构秘密信息。

为了解决以上问题,Blakely[1]和Shamir[2]在1979年分别独立地提出秘密分存概念。Shamir提出的(k,n)-阈值分存方案,将秘密信息分割成n份,然后分发给n位参与者。只有收集至少k份以上的分存份额,才可以无损地重构出秘密信息;否则,将得不到秘密的任何信息。秘密分存概念被提出以后,在图像领域上主要对黑白图像的分存算法进行研究。1995年,Noar和Shamir[3]提出秘密的可视分存方案。可视分存方案的重构简单,只需要将分存图像叠加在一起,通过人眼即可获取秘密信息,不需要任何复杂的计算。由于其重构的方便性和简单性,该方案得到了大多数人的青睐。然而,其在可视分存方案中存在像素膨胀问题,且重构过程是有损的。可视分存的缺点,在一定程度上限制了方案的应用。

为了扩展分存的应用,Thien和Lin[4]在2002年将Shamir的秘密分存概念应用于灰度图像领域,提出基于拉格朗日插值的图像分存方案。灰度图像分存方案[4]提出后,有

到稿日期:2012-04-10 返修日期:2012-07-08 本文受中山大学广东省计算科学重点实验室(201106006),澳门特别行政区科学技术发展基金(006/2011/A1),国家自然科学基金数学天元基金(11126064)资助。
欧锻灏(1986-),男,博士生,主要研究方向为信息隐藏、秘密分存,E-mail:ouduanh@mail2.sysu.edu.cn;吴小天(1985-),男,博士生,主要研究方向为秘密图像的可视分存;孙 伟(1972-),男,博士,教授,博士生导师,主要研究方向为多媒体信息安全和数字媒体;刘 娟(1983-),女,博士,讲师,主要研究方向为微分方程数值解、数学物理反问题。

不少研究人员致力于对灰度图像分存方案的研究[5-7]。但是，文献[5-7]中的分存方案产生的分存图像是无意义的，需要利用隐藏技术[8]对无意义分存图像进行后处理，以得到有意义的分存图像。文献[9]研究了一种新的基于矢量化的分存方案，该方案可以实现有意义分存图像的分存，但是计算复杂度很大，而且其重构过程是有损的。吴小天等[10]提出的图像分存方案虽然在不需要隐藏技术下也可获得有意义的分存图像，但只适应于二值图像。

为了解决以上问题，本文提出了一种基于恢复函数和误差扩散技术的(n,n)-阈值的灰度图像分存方案。其秘密图像和分存图像均为灰度图像。在本文方案中，恢复函数设计的基本思想是，人眼能够识别的颜色空间有限，在一定小范围内调整灰度像素值并不会引起人眼视觉系统的注意。在分存过程中，调整预选的、有意义的载体图的像素值，使其通过恢复函数映射后得到的函数值与秘密图像的值相等。然后，利用误差扩散技术将调整过程产生的误差扩散到未处理的邻域像素，保证分存图像局部像素的平均值，以提高分存图像的视觉质量。方案中引入置乱技术，在执行分存过程前对秘密图像进行预处理，以进一步增强方案的隐蔽性和安全性。此外，本文方案对秘密图像的重构是无损的。

2 恢复函数的设计

恢复函数设计的基本思想是，由于人眼能够识别的颜色空间比较有限，在一定小范围内调整像素的值并不会引起人眼视觉系统的注意。由于灰度图像的像素用8bit表示，因此总共有2^8的颜色空间，人眼不可能识别所有颜色空间。鉴于此，在一定范围内调整预选的、有意义的载体图像的像素值，使其通过恢复函数映射后得到的函数值与秘密图像值相等，调整过程不影响载体图的视觉效果。以下探讨如何设计恢复函数。

在(n,n)-阈值的二值图像的分存方案中[10]，秘密图像和预选的载体图像的像素级别均为1bit。设n份预选的有意义的二值载体图为$\mathbf{I}_1,\mathbf{I}_2,\mathbf{I}_3,\cdots,\mathbf{I}_n$，二值的秘密图像为$\mathbf{S}$。将文献[10]中基于异或运算的操作用基于模运算的恢复函数等价表示如下：

$$\begin{aligned}\mathbf{S}(i,j)&=R(\mathbf{I}_1'(i,j),\mathbf{I}_2'(i,j),\cdots,\mathbf{I}_n'(i,j))\\&=bitxor(\mathbf{I}_1'(i,j),\mathbf{I}_2'(i,j),\cdots,\mathbf{I}_n'(i,j))\\&=(\mathbf{I}_1'(i,j)+\mathbf{I}_2'(i,j)+\cdots+\mathbf{I}_n'(i,j))\bmod 2\end{aligned}\quad(1)$$

式中，$\mathbf{I}_1'(i,j),\mathbf{I}_2'(i,j),\cdots,\mathbf{I}_n'(i,j)$为调整后的分存图像中$(i,j)$位置的像素值。秘密像素$\mathbf{S}(i,j)$无论为'0'或者'1'，只需要更改$\mathbf{I}_1(i,j),\mathbf{I}_2(i,j),\cdots,\mathbf{I}_n(i,j)$中某一个像素值，即可使得通过恢复函数$R$映射得到的值与秘密像素$\mathbf{S}(i,j)$相等。此时，像素的调整值范围为$\{-1,0,1\}$。例如，由'1'调整为'0'，其调整值为$-1$；由'0'调整为'1'，其调整值为1；而当调整值为0时，说明像素不变。

以下类比二值图像的分存方法，设计灰度图像的恢复函数。设预选的两幅载体图像分别为$\mathbf{GI}_1,\mathbf{GI}_2$，秘密图像为$\mathbf{GS}$，由于灰度图像的像素级别为8bit，现设计(2,2)-阈值灰度图像分存方案的恢复函数R如下：

$$\begin{aligned}\mathbf{GS}(i,j)&=R(\mathbf{GI}_1'(i,j),\mathbf{GI}_2'(i,j))\\&=(16\times\mathbf{GI}_1'(i,j)+\mathbf{GI}_2'(i,j))\bmod 256\end{aligned}\quad(2)$$

式中，$\mathbf{GI}_1'(i,j),\mathbf{GI}_2'(i,j)$分别为$\mathbf{GI}_1(i,j),\mathbf{GI}_2(i,j)$在范围$\{-15,-14,\cdots,-1,0,1,\cdots,14,15\}$调整后的值。在调整$\mathbf{GI}(i,j)$像素时，如果调整后的值$\mathbf{GI}'(i,j)$大于255或者小于0，可以对像素$\mathbf{GI}'(i,j)$做如下处理：$\mathbf{GI}'(i,j)=(\mathbf{GI}'(i,j)+256)\bmod 256$，使得调整后的值$\mathbf{GI}'(i,j)$仍然处在$\{0,1,2,\cdots,255\}$的范围。

可以证明，无论$\mathbf{GS}(i,j)$为$\{0,1,2,\cdots,255\}$中的何值，当前像素$\mathbf{GI}_1(i,j),\mathbf{GI}_2(i,j)$在$\{-15,-14,\cdots,-1,0,1,\cdots,14,15\}$范围的调整下，均能通过恢复函数$R$(式(2))的映射，使得函数值与秘密像素$\mathbf{GS}(i,j)$相等。证明过程如下：

证明：设当前像素$\mathbf{GI}_1(i,j)$和$\mathbf{GI}_2(i,j)$的调整值分别为Δ_1和Δ_2，其中Δ_1和Δ_2属于$\{-15,-14,\cdots,0,\cdots,14,15\}$。

又：

$$\begin{aligned}&16\times\mathbf{GI}_1'(i,j)+\mathbf{GI}_2'(i,j)-\mathbf{GS}(i,j)\\&=16\times(\mathbf{GI}_1(i,j)+\Delta_1)+\mathbf{GI}_2(i,j)+\Delta_2-\mathbf{GS}(i,j)\\&=(16\times\mathbf{GI}_1(i,j)+\mathbf{GI}_2(i,j)-\mathbf{GS}(i,j))+(16\times\Delta_1+\Delta_2)\end{aligned}$$

因为上式中$(16\times\Delta_1+\Delta_2)$在调整值范围下，可以遍历$-255\sim255$的所有值，所以无论$\mathbf{GS}(i,j)$为$\{0,1,2,\cdots,255\}$中的何值，均可以找到合适的$\Delta_1$和$\Delta_2$使得：

$16\times\mathbf{GI}_1'(i,j)+\mathbf{GI}_2'(i,j)-\mathbf{GS}(i,j)$整除256

即$\mathbf{GS}(i,j)=(16\times\mathbf{GI}_1'(i,j)+\mathbf{GI}_2'(i,j))\bmod 256$成立，得证！

在以上所述的(2,2)-阈值灰度图像分存方案中，假设参与者仅拥有分存图像$\mathbf{GI}_2$，现在想通过猜测$\mathbf{GI}_1$获得秘密图像的信息。设x为未知像素$\mathbf{GI}_1(i,j)$的值，由恢复函数(式(2))可知，$\mathbf{GI}_1(i,j)$的乘法因子为16。那么因为$16\mid256$，所以$(16\times x)\bmod256$在$x\in\{0,1,2,\cdots,255\}$的遍历下，仅有16个剩余系。所以攻击者仅需要尝试16次即可获得对应位置秘密像素$\mathbf{GS}(i,j)$的值，因此方案的安全性相对较弱。在讨论解决方法前，先介绍一个命题，描述如下。

命题1 假设x为未知图像的像素值，如果α与256互素，则当x遍历$\{0,1,2,\cdots,255\}$时，$\alpha x \bmod 256$的剩余系也遍历$\{0,1,2,\cdots,255\}$。

证明：设x_i和x_j为$\{0,1,2,\cdots,255\}$中的任意两个不同的剩余系，即$x_i\neq x_j \bmod 256$。以下用反证法证明。

假设x_i和x_j乘以因子α后，有$\alpha x_i\equiv\alpha x_j \bmod 256$。

由假设，可得$\alpha(x_i-x_j)\mid256$。又由$(\alpha,256)=1$可得$(x_i-x_j)\mid256$，即$x_i\equiv x_j \bmod 256$，与前提矛盾！

所以，x_i和x_j分别乘以因子α后，得到的αx_i和αx_j仍然属于不同的剩余系。

可以得出结论，当x遍历$\{0,1,2,\cdots,255\}$时，$\alpha x \bmod 256$的剩余系也遍历$\{0,1,2,\cdots,255\}$。至此，命题1得证！

由命题1所述，只要恢复函数中$\mathbf{GI}(i,j)$的系数与模数256互素，攻击者想要通过猜测$\mathbf{GI}(i,j)$获得秘密信息，需要尝试256次，这样有利于增强方案的安全性。然而，为了保证分存图像的视觉，像素的调整值范围不能太大，所以选择的系数必须接近恢复函数(式(2))中的系数。譬如在(2,2)-阈值方案的恢复函数R中，可以选择接近16的17。此外，在恢复函数设计中，为了降低分存图像和秘密图像之间的相关性，在恢复函数中对每幅分存载体图像乘以一个与256互素的因子，实验中选择因子95可以得到更好的效果。此时恢复函数为：

$\mathbf{GS}(i,j)=R(\mathbf{GI}_1'(i,j),\mathbf{GI}_2'(i,j))$

$$=95\times(17\times \mathbf{GI}_1'(i,j)+\mathbf{GI}_2'(i,j)) \bmod 256 \tag{3}$$

式中，$\mathbf{GI}_1'(i,j)$和$\mathbf{GI}_2'(i,j)$分别是$\mathbf{GI}_1(i,j)$和$\mathbf{GI}_2(i,j)$像素在范围{−16,−15,…,−1,0,1,…,15,16}内调整后的值。

当$n>2$时，同样可以通过类比设计相应的恢复函数。例如当$n=3$时，其恢复函数设计如下：

$$\begin{aligned}\mathbf{GS}(i,j)&=R(\mathbf{GI}_1'(i,j),\mathbf{GI}_2'(i,j),\mathbf{GI}_3'(i,j))\\&=(49\times \mathbf{GI}_1'(i,j)+7\times \mathbf{GI}_2'(i,j)+\mathbf{GI}_3'(i,j))\\&\quad \bmod 256\end{aligned} \tag{4}$$

式中，调整值的范围为{−6,−5,…,−2,−1,0,1,2,…,6}。

3 误差扩散技术的概述

在对预选的、有意义载体图像的像素进行调整时，产生的误差会对图像视觉效果产生影响。调整后的图像看起来不光滑，有人为伪造的迹象，容易引起细心攻击者的注意。

误差扩散的基本概念是由 Floyd 和 Steinberg[11] 提出来的，它主要将连续色调图像转换成二值图像，并且保留原图像大部分轮廓和细节的技术。本文在方案中主要利用误差扩散技术将产生的调整误差扩散到未处理的邻域像素，以保持局部平均像素值不变，从而产生视觉质量良好的分存图像，提高分存方案的隐蔽性。误差扩散的方式如图 1 所示，在误差扩散过程中采用的误差扩散核为 Floyd 核。

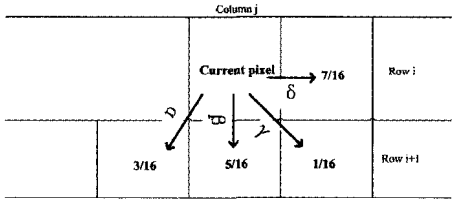


图 1 使用 Floyd 误差扩散核向右和向下扩散误差(权重因子的和：$\alpha+\beta+\gamma+\delta=1$)

4 基于恢复函数和误差扩散的(n,n)-阈值分存方案

本节主要介绍如何设计基于(n,n)-阈值的灰度图像分存方案。该方案分两个小节来介绍，分别是分存阶段和重构阶段。在执行分存过程前，采用 Arnold 置乱技术对秘密图像进行预处理，以增强方案的隐蔽性和安全性。分存阶段，主要介绍如何将秘密灰度图像分存到n张有意义的灰度图像中。同时，在调整载体图像像素的过程中，利用误差扩散技术将调整产生的误差扩散到未处理的领域像素，以增强伪装隐蔽的效果。重构阶段则相对比较简单，主要利用恢复函数和 Arnold 逆变换，从n份分存图像中无损地重构出秘密图像。

4.1 分存阶段

设秘密灰度图像为 **GS**，选择n张灰度载体图 $\mathbf{GI}_1,\mathbf{GI}_2,\mathbf{GI}_3,\cdots,\mathbf{GI}_n$，图像大小均为$M\times M$。现在，我们想将秘密图像 **GS** 分存到这$n$张有意义的分存图像中，分存的过程具体描述如下：

步骤 1 首先采用 Arnold 置乱算法，对秘密图像 **GS** 进行置乱，减少像素之间的关联性，得到一个均匀的噪声图 **GS**′。方案中采用的 Arnold 置乱算法用式(5)实现[12]。

$$\begin{bmatrix}i'\\j'\end{bmatrix}=\begin{bmatrix}1&1\\1&2\end{bmatrix}\begin{bmatrix}i\\j\end{bmatrix}(\bmod M) \tag{5}$$

式中，(i',j')表示置乱之后位置，(i,j)表示置乱前位置。

步骤 2 根据第 2 节所述的方法和n，设计相应的恢复函数R。

步骤 3 按光栅扫描的顺序，从左到右、从上到下逐个地处理图像 **GS**′中下一个未处理过的像素 $\mathbf{GS}'(i,j)$。通过遍历调整值范围，分别调整 $\mathbf{GI}_1(i,j),\mathbf{GI}_2(i,j),\mathbf{GI}_3(i,j),\cdots,\mathbf{GI}_n(i,j)$的当前像素值(其中，$\mathbf{GI}_1(i,j),\mathbf{GI}_2(i,j),\mathbf{GI}_3(i,j),\cdots,\mathbf{GI}_n(i,j)$的当前像素为原始像素值与邻域扩散误差值的总和)，使调整后的像素 $\mathbf{GI}_1'(i,j),\mathbf{GI}_2'(i,j),\mathbf{GI}_3'(i,j),\cdots,\mathbf{GI}_n'(i,j)$通过恢复函数$R$映射得到的函数值与 $\mathbf{GS}'(i,j)$的值相等。

由第 2 节可知，根据恢复函数的设计，必然存在着这样的调整方案；且在满足条件的调整方案中，选择各像素因调整产生的误差和最小的那个方案。

同样，如果调整后的值 $\mathbf{GI}'(i,j)$大于 255 或者小于 0，可以对 $\mathbf{GI}'(i,j)$值做如下处理：$\mathbf{GI}'(i,j)=(\mathbf{GI}'(i,j)+256)\bmod 256$，使得 $\mathbf{GI}'(i,j)$值仍然处在{0,1,2,…,255}的范围内。容易证明，经处理后的 $\mathbf{GI}'(i,j)$依然满足恢复函数。

步骤 4 确定调整方案后，各像素因调整产生的误差如下：

$$e_1=\mathbf{GI}_1'(i,j)-\mathbf{GI}_1(i,j)$$
$$e_2=\mathbf{GI}_2'(i,j)-\mathbf{GI}_2(i,j)$$
$$\cdots$$
$$e_n=\mathbf{GI}_n'(i,j)-\mathbf{GI}_n(i,j)$$

利用第 3 节的误差扩散技术，将误差$e_1,e_2,\cdots,e_n$分别扩散到 $\mathbf{GI}_1(i,j),\mathbf{GI}_2(i,j),\mathbf{GI}_3(i,j),\cdots,\mathbf{GI}_n(i,j)$邻域内未被处理的像素中。

步骤 5 如果图像 **GS**′中还有未处理的像素，则转到步骤 3 继续处理。当 **GS**′中所有的像素被处理完毕后，则可以获得n份被调整过的、满足恢复函数的灰度分存图像 $\mathbf{GI}_1',\mathbf{GI}_2',\mathbf{GI}_3',\cdots,\mathbf{GI}_n'$。

4.2 重构阶段

重构过程是分存过程的简单逆过程。在重构过程中，首先收集n份分存图像 $\mathbf{GI}_1',\mathbf{GI}_2',\mathbf{GI}_3',\cdots,\mathbf{GI}_n'$。然后利用恢复函数进行计算，再将计算结果进行逆 Arnold 变换，便可以无损地重构出秘密图像。重构过程具体描述如下：

步骤 1 读取n份在分存阶段生成的、有意义的分存图像 $\mathbf{GI}_1',\mathbf{GI}_2',\mathbf{GI}_3',\cdots,\mathbf{GI}_n'$。

步骤 2 利用恢复函数R对这n份分存图像的每个像素进行如下计算：

$$\mathbf{GS}'(i,j)=R(\mathbf{GI}_1'(i,j),\mathbf{GI}_2'(i,j),\cdots,\mathbf{GI}_n'(i,j))$$

所有像素计算完毕后，可以得到一个无意义的噪声图 **GS**′。

步骤 3 将步骤 2 中产生的结果 **GS**′进行逆 Arnold 变换，便可以无损地重构出原来的秘密图像 **GS**。

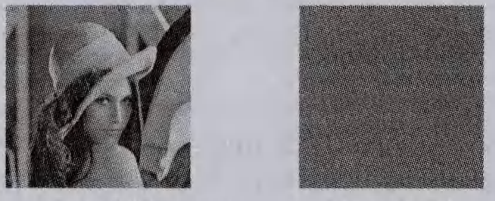
5 实验结果及分析

这一节主要展示实验结果和分析，以验证本文方案的有效性和高安全性。在实验中，选用灰度图像 Lena 作为秘密图像，选用灰度图像 Peppers，Baboon，Lake 作为分存载体图像，所有测试图像的大小均为 512×512。本文为了客观评价方案所产生的分存图像，利用图像的峰值信噪比 PSNR 来客观地衡量图像的视觉质量。PSNR 的计算如下：

$$PSNR=10\log_{10}\frac{W\times H\times 255^2}{\sum_{i=1}^{W}\sum_{j=1}^{H}[(I_{i,j}-O_{i,j})^2]} \tag{6}$$

式中，I 为测试图像，O 为原始图像，$W\times H$ 表示图像的大小。

在执行分存过程前，首先利用 Arnold 置乱算法对秘密图像 Lena 进行置乱变换，由于图像大小为 512×512，因此其 Arnold 周期为 384[12]。由实验可知，图像在置乱 218 次后，具有很好的置乱效果，所以本次实验选择置乱次数为 218，其相应的逆 Arnold 置乱次数为 166。Lena 的置乱结果如图 2 所示。从图 2 可看出，置乱后得到的是一个无意义的、均匀的噪声图，有利于增强方案的隐蔽性和安全性。



(a) Lena 原图　　(b) Lena 置乱图

图 2　图像置乱的实验结果

5.1　分存结果

在分存过程中分别做了两个实验。第一个实验，使用本文的分存方案对秘密图像 Lena 执行(2,2)-阈值分存。选择 Peppers 和 Baboon 作为分存载体图像。利用第 4.1 节的分存算法，将 Lena 图像分存到 Peppers 和 Baboon 中。实验结果如图 3 所示(分存图像 Peppers 和 Baboon 的 PSNR 值分别为 34.12dB 和 33.06dB)。

(a) 原始载体图像 Peppers　(b) 原始载体图像 Baboon　(c)生成的分存图像Peppers (PSNR=34.12dB)　(d)生成的分存图像 Baboon (PSNR=33.06dB)

图 3　图像 Lena 的(2,2)-阈值分存方案

第二个实验，使用本文分存方案对秘密图像 Lena 执行(3,3)-阈值分存。分别选择 Peppers、Baboon 和 Lake 作为分存载体图像。同样，利用第 4.1 节的分存算法生成秘密图像的分存图像，实验结果如图 4 所示(分存图像 Lake、Peppers 和 Baboon 的 PSNR 值分别为 41.53dB、41.12dB 和42.23dB)。

(a) 原始载体图像Lake　(b) 原始载体图像 Peppers　(c)原始载体图像 Baboon

(d) 生成的分存图像Lake (PSNR=41.53dB)　(e)生成的分存图像 Peppers (PSNR=41.12dB)　(f)生成的分存图像 Baboon (PSNR=42.23dB)

图 4　图像 Lena 的(3,3)-阈值分存方案

图 3 和图 4 的实验结果表明，所生成的分存图像具有较高的 PSNR 值，且具有较好的视觉效果，通过肉眼无法分辨出原始载体图像和分存图像的区别，具有很好的隐蔽性；随着 n 的增大，所生成的分存图像的 PSNR 值也变得越来越高，表明分存图像的视觉质量越来越好。

5.2　重构结果

在重构阶段，对生成的 n 份分存图像利用恢复函数和逆 Arnold 变换，重构出秘密图像。为了验证方案的有效性，实验在缺失分存图像的情况下对秘密图像进行重构，且重构过程假设可以获得置乱密钥(本次实验中置乱密钥为 166)。在基于(3,3)-阈值方案的重构阶段，分别利用图 4 中(d)(f)(e)，(d)(e)，(e)(f)，(d)(f)，(d)，(e)，(f)的分存图像和置乱密钥，尝试重构秘密图像，重构结果如图 5 所示。实验结果表示，只有当获得所有分存图像时，才可以无损地重构出秘密图像。在缺失分存图像的情况下，即使获得图像的置乱密钥，重构的结果仍是一个无意义的噪声图，保证了方案的有效性。同样，如果获得所有 n 份分存图像，但不知道图像置乱密钥，也是无法获得秘密信息的。实验结果再次验证了本方案的有效性和高安全性。

(a) (Lake, Peppers, Baboon)

(b) (only Lake)　(c) (only Peppers)　(d) (only Baboon)

(e) (Lake,peppers)　(f) (Lake,Baboon)　(g) (Peppers,Baboon)

图 5　图像 Lena 的(3,3)-阈值分存方案的重构结果：(a)分存图像 Lake，Peppers 和 Baboon 的重构结果；(b)－(g) 分存图像有缺失时的重构结果

5.3　鲁棒性测试

为了测试方案的鲁棒性，首先对分存图像施加各种攻击，如剪切、篡改、滤波和噪声等攻击。然后，利用受攻击的分存图像尝试重构秘密图像，通过比较重构图像和原始图像的差异来测试方案的鲁棒性。为了客观地描述重构图像与原始图像的差异，本文利用相关系数作为图像相似性的客观度量。相关系数的值越接近 1，表示重构图像与原始图像越相似、重构的效果越好。设 $\mathbf{f},\mathbf{g}$ 是大小为 $M\times N$ 的灰度图像，其相关系数计算如下：

$$CC(\mathbf{f},\mathbf{g})=\frac{\sum_{j=1}^{M}\sum_{k=1}^{N}(\mathbf{f}_{j,k}-\bar{\mathbf{f}})(\mathbf{g}_{j,k}-\bar{\mathbf{g}})}{\sqrt{\sum_{j=1}^{M}\sum_{k=1}^{N}(\mathbf{f}_{j,k}-\bar{\mathbf{f}})^2}\sqrt{\sum_{j=1}^{M}\sum_{k=1}^{N}(\mathbf{g}_{j,k}-\bar{\mathbf{g}})^2}}$$

式中，$\bar{\mathbf{f}}=\frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\mathbf{f}_{j,k}$，$\bar{\mathbf{g}}=\frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\mathbf{g}_{j,k}$。

实验利用(2,2)-阈值方案产生的分存图像 Peppers(见图 3(c))作为攻击对象，对其实施各种攻击，包括剪切、篡改、高斯噪声、椒盐噪声和高斯滤波等攻击。实验中，对分存图像 Peppers 分别施加 5 种攻击，具体描述如下：

1)对分存图像施加剪切攻击，从中间剪切 1/4 区域。

2)对分存图像施加篡改攻击，修改图像中的内容。

3)对分存图像施加均值为0、方差为0.01的高斯噪声。

4)对分存图像施加25%的椒盐噪声。

5)对分存图像施加窗口大小为3×3、方差为0.5的高斯滤波。

然后,对各种受攻击的图像分别尝试重构秘密图像,得到的实验结果如表1所列。

表1 分存图像Peppers在不同攻击下的重构结果

攻击手段	受攻击的Peppers	重构结果	相关系数CC
剪切			0.6469
篡改			0.7999
高斯噪声			0.0024
椒盐噪声			0.6465
高斯滤波			0.0041

由表1可得,本文方案对剪切($CC=0.6469$)、篡改($CC=0.7999$)和椒盐噪声($CC=0.6465$)的攻击具有一定的鲁棒性。但方案对高斯噪声($CC=0.0024$)和高斯滤波($CC=0.0041$)的攻击则较敏感。本文方案由于是在空域上进行的,即对每个秘密像素独立地进行分存和重构,而剪切、篡改和椒盐噪声攻击只是修改部分像素的值,不影响对其他像素的重构。因此在损坏像素较少的情况下,仍然可以重构出大量的秘密信息,重构结果具有一定的鲁棒性。而对于高斯噪声和各种滤波攻击,其攻击是作用于图像中的所有像素,因此方案对这种攻击手段一般比较敏感。

另外,本文所提方案主要应用于秘密的分享,对秘密的重构往往要求是完全无损的,所以在这种应用场景下,对攻击的鲁棒性要求是无意义的。例如,假设秘密图像是一个码本,如果码本不能够被完全重构,即使能够恢复出码本的大量信息,对于基于码本的解码过程也起不到作用。

5.4 安全性分析

根据第2节中恢复函数的设计可知,当缺少一张分存图像时,攻击者想通过猜测获得秘密像素需要尝试256次。设秘密图像**GS**的大小为$M\times M$,所以攻击者想通过猜测来完全重构出秘密图像的概率为$(1/256)^{M\times M}$。又因为$(1/256)^{M\times M}$是个非常小的数,攻击者想要在这么低的概率下无损地重构出秘密图像几乎是不可能的。譬如当$M=10$时,$(1/256)^{10\times 10}$足以抵抗大量攻击。

此外,本方案至少还提供了两层的安全保护。第一层,本文方案在预处理阶段对秘密图像进行Arnold置乱,增强了方案的安全性和隐蔽性。在得不到置乱密钥的前提下,即使获得所有分存图像,同样无法重构出秘密图像的信息。第二层,分存方案所产生的分存图像是有意义的,增强了隐蔽伪装的效果,不易引起攻击者的注意。因此本文所提分存方案具有较高安全性的。

结束语 本文通过对恢复函数的研究,设计了一个分存方案,即将秘密灰度图像分存到n张有意义的灰度图像中。由理论证明可知,所设计的恢复函数具有高安全性。本文方案引入误差扩散技术来减少分存图像中因调整产生的误差,以提高分存图像的视觉质量,从而增强了方案的隐蔽性和安全性。

方案的重构过程简单快速,仅利用恢复函数和逆置乱算法,便可从n张分存图像中无损地重构出秘密图像。在缺失分存图像的情况下,即使获得预处理时的置乱密钥,仍无法重构秘密图像的任何信息,保证了方案的有效性。实验结果和理论分析再次验证了本文方案的有效性和高安全性。此外,由于对秘密图像的重构是无损的,还可以将本文方案应用到对密码本的分存上。

参 考 文 献

[1] Blakley G R. Safeguarding cryptographic keys[C]// Proceedings of the National Computer Conference. 1979:313

[2] Shamir A. How to share a secret [J]. Commun ACM, 1979, 22(11):612-613

[3] Naor M, Shamir A. Visual cryptography[M]. Springer Berlin / Heidelberg, 1995, 950:1-12

[4] Thien C C, Lin J C. Secret image sharing [J]. Computers & Graphics, 2002, 26(5):765-770

[5] Wang R Z, Su C H. Secret image sharing with smaller shadow images[J]. Pattern Recognition Letters, 2006, 27(6):551-555

[6] Alharthi S S, Atrey P K. An improved scheme for secret image sharing[C]// Multimedia and Expo (ICME), 2010 IEEE International Conference. 2010:1661-1666

[7] Alharthi S S, Atrey P K. Further improvements on secret image sharing scheme[C]// Proceedings of the 2nd ACM workshop on Multimedia in forensics, Security and Intelligence (MiFor '10). 2010:53-58

[8] Yang C H, Chen T S, Yu K H, et al. Improvements of image sharing with steganography and authentication[J]. Journal of Systems and Software, 2007, 80(7):1070-1076

[9] Chen T S, Chang C C. New method of secret image sharing based upon vector quantization[J]. Electron Imaging, 2001, 10:988

[10] 吴小天,孙伟. 基于误差扩散的图像分存方案[J]. 计算机应用, 2011(1):74-77

[11] Floyd R, Steinberg L. An adaptive algorithm for spatial gray-scale[J]. Proceedings of the Society for Information Display, 1976, 17(2):75-77

[12] Tang Z J, Zhang X Q. Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies[J]. Journal of Multimedia, 2011, 6(2):202-206