基于灰度概率矩阵的视觉密码方案

付正欣,黄航璎,郁 滨
(信息工程大学密码工程学院,河南郑州 450001)

摘 要: 针对概率型视觉密码所恢复的灰度图像存在灰度表现力不强的问题,本文提出了一种基于灰度概率矩阵的设计方案,生成了能够呈现多种灰度的共享份,以提高恢复效果. 首先,以提高分享策略集合的整体差异性和灰度识别率为目标,依据视觉密码的对比性条件和安全性条件建立约束方程组,建立了目标优化模型. 在此基础上,利用序列二次规划算法求解该目标优化模型得到优化后的灰度概率矩阵,并设计了秘密分享算法. 实验结果表明,本文方案适用于(k,n)门限存取结构,恢复图像具有灰度失真程度低、表现力强的特点,在传统和新型图像质量评价指标上的表现,较同类方案均有所提升.

关键词: 概率型视觉密码方案;灰度概率矩阵;灰度失真;恢复图像质量;分享策略集合
基金项目: 国家自然科学基金(No.61602513)
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112(2023)08-2188-14
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20211256

Visual Cryptography Scheme Based on Grayscale Probabilistic Matrix

FU Zheng-xin, HUANG Hang-ying, YU Bin
(*Department of Cryptography Engineering*, *Information Engineering University*, *Zhengzhou*, *Henan* 450001, *China*)

Abstract: To enhance the grayscale expressiveness of probabilistic visual cryptography when recovering gray images, a scheme based on grayscale probabilistic matrix was designed by using shares with multiple gray values. Firstly, we constructed a new objective function to improve the diversity of sharing strategies and the recognition rate of target zone, and established an optimization model with the contrast and security conditions of visual cryptography as constraints. On this basis, the optimized grayscale probabilistic matrix was obtained by solving the target optimization model with sequential quadratic programming and then the sharing algorithm was presented. Experimental results show that our scheme can be applied to (k, n) threshold access structure and the recovered image of this scheme has low grayscale distortion and strong grayscale expressiveness, which is verified through both traditional and recently proposed image quality assessment metrics when compared with relative schemes.

Key words: probabilistic visual cryptography scheme; grayscale probabilistic matrix; grayscale distortion; quality of recovered image; set of sharing strategies
Foundation Item(s): National Natural Science Foundation of China (No.61602513)

1 引言

视觉密码[1,2](Visual Cryptography,VC)是一类可通过直接物理叠加实现秘密恢复的图像分存方案. 其设计的关键是构造基础矩阵. 学者们先后提出了基于累积矩阵[3]、MDS码[4]、BIBD码[5]、概率矩阵[6]、线性方程组[7]的基础矩阵构造方案. 针对这些方案的评价指标主要有像素扩展度$m(m\geq 1)$和相对差$\alpha(0<\alpha\leq 1)$. 对于同一类方案,像素扩展度越小意味着秘密份额传输代价越低;相对差越大意味着恢复图像对比度越高,方案性能越佳[8]. 概率型视觉密码方案[9](Probabilistic Visual Cryptography Scheme,PVCS)是一类重要的像素不扩展的视觉密码方案,其像素扩展度m=1,处理的图像通常为二值图像.

为扩大概率型视觉密码所适用的图像范围,Wang等人[10]结合概率型视觉密码思想,利用两级布尔矩阵构造多级布尔矩阵,实现了一个面向灰度图像的PVCS. 但该方案恢复图像存在较多噪声且对比度较低、视觉效果不佳等问题. 为提升恢复图像对比度,

收稿日期:2021-09-13;修回日期:2022-03-01;责任编辑:王天慧

Chen等人[11]结合直方图均衡算法,将原始图像灰度变化范围划分为若干子区间,为每个子区间设计一个布尔矩阵,分享时以像素块为单位进行分享. 该方案能够有效提升恢复图像对比度,但是对比度的提升以局部细节失真为代价.

区别于上述思路,Lin等人[12]指出直接利用阈值判断法将灰度图像转化为二值图像,未能充分保留原始图像的邻域信息,此类信息损失将直接导致恢复图像质量的下降. 因此,文献[12]依据空间填充曲线确定扫描路径,结合抖动技术获得了信息损失程度更低的二值图像,以该二值图像作为秘密分享对象,有效提高了恢复图像的灰度表现力. Sharma等人[13]通过优化半色调处理过程,将半色调算法引入的噪声尽可能地转化为蓝噪声,使得秘密分享算法输入图像内少数像素分布更加均匀,进一步降低了恢复图像的低频噪声含量,但仍旧没有从根本上解决灰度图像在转化为二值图像过程中所带来的信息损失问题.

为进一步平滑恢复图像内的视觉噪声,Hou等人[14]提出了多点分享算法. 该方案通过改变分享算法流程,同时分享多个像素,降低了恢复图像的块内方差,其纹理过渡更加自然,但细节表现力不足. Lee等人[15]采用半色调算法对灰度图像进行预处理,并利用多级布尔矩阵,结合直方图均衡技术设计秘密像素块与恢复像素块之间的映射关系,对预处理得到的二值图像进行分享. 该方案恢复图像视觉效果改善明显,但与原图相比,保真度不足. Yan等人[16]综合考虑人类视觉系统模型特点,进一步整合了半色调处理过程和多点分享过程,通过引入误差扩散机制,有效均衡了恢复图像的噪声分布. Sun等人[17]结合直接二值搜索算法,进一步优化了Yan等人的方案. 但该类方案仍旧存在灰度表现力不强和存取结构受限的问题.

以上方案均基于布尔基础矩阵实现,叠加恢复图像内只含两种灰度值,恢复图像质量提升空间受到二值基础矩阵的限制. Dutta等人[7,18]尝试扩充共享份内的颜色数量,通过建立并求解环上线性方程组,求解相应的多值基础矩阵. Aswad等人[19]借助蝙蝠算法对多值图像的分享参数进行了优化. 然而,上述方案的颜色叠加模型为同色叠加模型[20],即同色叠加灰度值不变,异色叠加呈现黑色,与灰度叠加实际并不相符. Cimato等人[21]指出,考虑到光通过灰度胶片的损失规律,两个相同的灰度图像叠加后会变暗[22],实际灰度叠加可近似使用实数乘法模拟. 基于这一结论,Chen等人[23]使用3个灰度级为(2,2)的门限结构设计6个灰度矩阵,依据直方图均衡算法将原始图像灰度变化范围划分为6个子区间,每个子区间内的像素使用同一个灰度矩阵进行分享,获得了灰度表现力更强的恢复图像. 然而,文献[23]并未给出上述灰度矩阵的通用构造算法.

综上所述,大多数面向灰度图像的概率型视觉密码方案恢复图像仅含黑白两种灰度值,未能保留原始秘密图像的多级灰度值;而部分基于多级灰度的方案仍存在灰度级数较少以及存取结构受限的不足. 因此,如何为基于多级灰度的概率型视觉密码方案建立一个通用的数学模型,是设计此类方案的一个关键问题.

针对上述问题,本文提出了基于灰度概率矩阵的视觉密码方案的定义,以分享策略集合的整体差异性和灰度识别率最大化为优化目标,依据视觉密码的对比度条件和安全性条件构造约束方程组,建立以灰度概率矩阵为核心的目标优化模型. 运用序列二次规划算法[24](Sequential Quadratic Programming,SQP)迭代求解该模型,取得了优化后的灰度概率矩阵,并利用该矩阵分享秘密图像,能够有效提升恢复图像质量.

2　方案定义

本文首先对灰度图像$G=(g_{ij})_{H\times W}$归一化处理[16],其像素取值范围为[0,1]. 对于输入为256级的灰度图像,若$g_{ij}=128$,其归一化后对应的像素值为128/256=0.5. 所设计的概率型视觉密码方案,其分享规则取值于一个多元灰度集合GrayPalette. 该集合与参与者数目n共同决定了分享规则集合.

定义1　分享规则集合R. 设参与者数目为n,L为GrayPalette规模,分享规则v为元素取值于GrayPalette的n维向量,v_i表示该分享规则下,第i个参与者分配到的秘密份额. v的所有可能取值构成的集合被称为分享规则集合,记为R.

以n=2,L=3为例,有

$$R=\left\{\begin{bmatrix}g_1\\g_1\end{bmatrix},\begin{bmatrix}g_1\\g_2\end{bmatrix},\begin{bmatrix}g_1\\g_3\end{bmatrix},\begin{bmatrix}g_2\\g_1\end{bmatrix},\begin{bmatrix}g_2\\g_2\end{bmatrix},\begin{bmatrix}g_2\\g_3\end{bmatrix},\begin{bmatrix}g_3\\g_1\end{bmatrix},\begin{bmatrix}g_3\\g_2\end{bmatrix},\begin{bmatrix}g_3\\g_3\end{bmatrix}\right\} \tag{1}$$

取GrayPalette={0, 0. 5, 1},则有

$$R=\left\{\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}0\\0.5\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}0.5\\0\end{bmatrix},\begin{bmatrix}0.5\\0.5\end{bmatrix},\begin{bmatrix}0.5\\1\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}1\\0.5\end{bmatrix},\begin{bmatrix}1\\1\end{bmatrix}\right\} \tag{2}$$

分享规则集合R给出了分享单个秘密像素时,可能采用的分享策略. 但为了保证视觉密码方案的安全性,对于像素取值不同的秘密像素需要匹配不同的分享策略.

例如,对于式(2)所示分享规则集合R,p=[0.1,0.3,0,0,0.1,0,0.09,0.41,0]即一条分享策略,表示分

享规则$\begin{bmatrix}0\\0\end{bmatrix}$,$\begin{bmatrix}0\\0.5\end{bmatrix}$,$\begin{bmatrix}0.5\\0.5\end{bmatrix}$,$\begin{bmatrix}1\\0\end{bmatrix}$,$\begin{bmatrix}1\\0.5\end{bmatrix}$的选用概率分别为0.1、0.3、0.1、0.09、0.41,其余分享规则的选用概率均为0.在分享灰度图像时,首先需要对其内像素种类做一个划分,以便为不同类别的秘密像素匹配不同的分享策略.一条分享策略一般使用一个概率向量表示.该向量各元素即分享该子区间内灰度像素时各分享规则的选用概率,如图1所示.

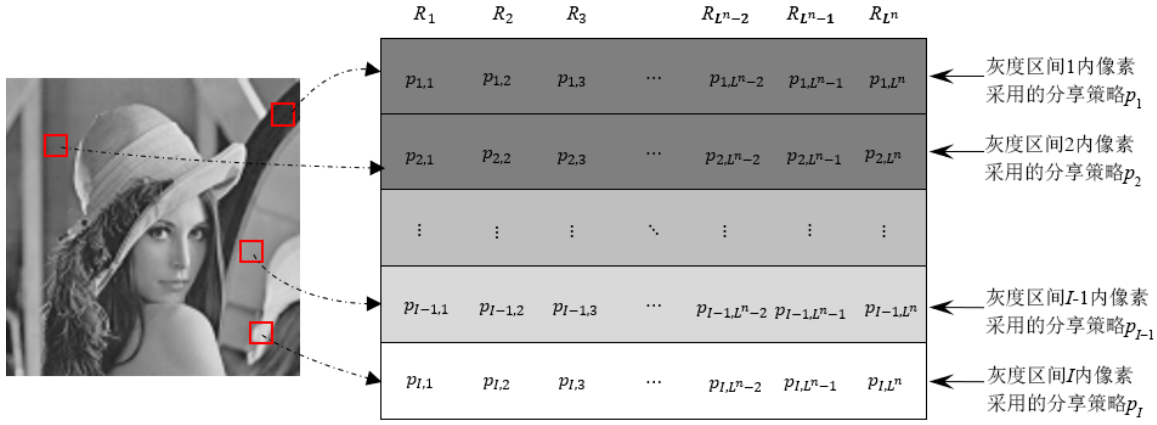


图1 分享策略集合示意图

定义2 灰度概率矩阵$\boldsymbol{C}$.设$\boldsymbol{p}_i$为元素取值于[0,1]的$1\times L^n$向量,其中,$\sum_{j=1}^{L^n}p_{i,j}=1,(i=1,2,\cdots,I)$.$p_{i,j}$表示分享属于第$i$个子区间内灰度像素时,选择第$j$条分享规则的概率$\left(j=1,2,\cdots,L^n\right)$,称由$I$个概率向量所构成的矩阵$\boldsymbol{C}$为一个灰度概率矩阵.

对于单个秘密像素,依据像素值和$\boldsymbol{C}$,从R中选择一条分享规则用于分享.可见,$\boldsymbol{C}$的设计为秘密分享算法的关键.

视觉密码的秘密恢复算法相对简单,只需将经秘密分享算法生成的共享份打印至透明胶片,再将透明胶片叠加即可实现秘密恢复.Cimato在文献[21]中对该类灰度叠加操作进行抽象,论证了其与实数乘法等价性,本文基于上述结论给出定义3.

定义3 灰度叠加运算Stack(·).任给一个元素取值于[0,1]的n维灰度向量$\boldsymbol{v}=\begin{bmatrix}g_1 & g_2 & \cdots & g_n\end{bmatrix}^{\mathrm{T}}$,$\mathrm{Stack}(v)=g_1\times g_2\cdots\times g_n=\prod_{i=1}^{n}g_i$,即这$n$个灰度像素的叠加结果.其中,"×"为实数乘法运算.

以$\boldsymbol{v}_1=\begin{bmatrix}0 & 0.5 & 1\end{bmatrix}^{\mathrm{T}}$和$\boldsymbol{v}_2=\begin{bmatrix}0.25 & 0.5 & 1\end{bmatrix}^{\mathrm{T}}$为例,其中,0表示黑色像素,0.25和0.5分别表示不同灰度值的灰度像素,1表示白色像素,有$\mathrm{Stack}(\boldsymbol{v}_1)=0$,$\mathrm{Stack}(\boldsymbol{v}_2)=0.125$.

结合上述要素,给出如下方案定义.

定义4 设参与者集合$P=\{1,2,\cdots,n\}$,2^P表示P的全部子集构成的幂集,k为门限值,L为GrayPalette的规模大小,I为分享策略数,每条分享策略对应于秘密图像的一个灰度区间.称矩阵$\boldsymbol{C}$构成一个基于灰度概率矩阵的视觉密码方案,即(k,n,L,I)-PVCS,当且仅当对于$\forall X\in 2^P$,如下两个条件成立:

(1)当$|X|<k$时,记$R'=\{\boldsymbol{v}|\boldsymbol{v}\in R[X]\}$,对于$\forall i_1,i_2\in\{1,2,\cdots,I\},d\in\left\{1,2,\cdots,L^{|X|}\right\}$,有

$$\sum_{j=1}^{L^n}p_{i_1,j}\times H(R_j[X],R'_d)=\sum_{j=1}^{L^n}p_{i_2,j}\times H(R_j[X],R'_d)\quad(3)$$

其中,$R[X]$表示取集合R中X对应行元素所构成的子集合,$H(x,y)$是从(x,y)到$\{0,1\}$的映射$H(x,y)=\begin{cases}1,x=y\\0,x\neq y\end{cases}$.

(2)当$|X|\geqslant k$时,$\forall i_1,i_2\in\{1,2,\cdots,I\}(i_1<i_2)$,有

$$\alpha_{i_2,i_1}=\sum_{j=1}^{L^n}\mathrm{Stack}\left(R_j[X]\right)\times p_{i_2,j}-\sum_{j=1}^{L^n}\mathrm{Stack}\left(R_j[X]\right)\times p_{i_1,j}>0\quad(4)$$

在上述定义中,条件1为安全性条件,表示当参与者数目$|X|$少于门限值k时,依据参与者手持共享份集合,推测原始秘密像素各可能取值的概率相等;条件2为对比性条件,表示当参与者数目$|X|$大于等于门限值k时,采用各分享策略分享后,叠加恢复像素的平均灰度值呈现有序差别,可以被人眼识别.

定理5 根据定义4的安全性条件,当参与者数目少于门限值k时,依据参与者手持共享份集合,推测原始秘密像素各可能取值的概率相等.

证明 设s为秘密像素,其可能取值为$s_1,s_2,\cdots,s_I$,当$|X|<k$时,设t为这$|X|$个参与者手持秘密份额组合,其可能取值为$t_1,t_2,\cdots,t_{L^{|X|}}$.由定义4,对于任意灰度级对应的分享策略,有秘密份额组合的各可能取值出现的概率相同,即$P\left(t\middle|s=s_1\right)=\cdots=P\left(t\middle|s=s_I\right)$.

敌手依据手持秘密份额组合推测秘密像素取值为

s_i的概率记为$P(s=s_i|t)$,由贝叶斯公式有,$P(s=s_i|t)=\dfrac{P(t|s=s_i)P(s=s_i)}{\sum_{j=1}^{I}P(t|s=s_j)P(s=s_j)}$,$i=1,2,\cdots,I$.

不失一般性,可假设秘密图像内像素均匀分布,即$P(s=s_1)=\cdots=P(s=s_I)$,故有$P(s=s_1|t)=\cdots=P(s=s_I|t)$,即当参与者数目少于门限值$k$时,依据参与者手持共享份集合,推测原始秘密像素各可能取值的概率相等,证毕.

以(2,2,3,5)-PVCS为例,其中,L=3,I=5,其分享规则如式(2)所示,对应的灰度概率矩阵为

$$\boldsymbol{C}=\begin{bmatrix}0&0&0.25&0&0.5&0&0.25&0&0\\0&0.25&0&0&0.25&0.25&0.25&0&0\\0&0.25&0&0.25&0&0.25&0&0.25&0\\0.25&0&0&0&0.25&0.25&0&0.25&0\\0.25&0&0&0&0.5&0&0&0&0.25\end{bmatrix}$$

显然,$\mu_1<\mu_2<\mu_3<\mu_4<\mu_5$,表明叠加恢复像素的平均灰度值呈现有序差别,满足定义4的对比性条件.

(1)当$|X|=1$时

对于单个秘密像素,其可能取值为$s_1,s_2,\cdots,s_5$.参与者仅拥有1个秘密份额,该秘密份额的所有可能取值构成一个新的分享规则集合$R'=\{\boldsymbol{v}|\boldsymbol{v}\in R[X]\}=\{0,0.5,1\}$.对于该参与者而言,它仅能通过$R'$内元素在共享份内的分布规律推测秘密信息.

记$\mathrm{P}(R_j[X]=y|s_i)=\sum_{j=1}^{3^n}p_{i,j}\times H(R_j[X],y),y\in R'$,$i\in\{1,2,\cdots,5\}$,则有

$$\mathrm{P}(R_j[X]=0|s_1)=\cdots=\mathrm{P}(R_j[X]=0|s_5)=0.25$$

$$\mathrm{P}(R_j[X]=0.5|s_1)=\cdots=\mathrm{P}(R_j[X]=0.5|s_5)=0.5$$

$$\mathrm{P}(R_j[X]=1|s_1)=\cdots=\mathrm{P}(R_j[X]=1|s_5)=0.25$$

由定理5,有$\mathrm{P}(s=s_1|R_j[X])=\dfrac{1}{3}$,同理可得$\mathrm{P}(s=s_2|R_j[X])=\cdots=\mathrm{P}(s=s_5|R_j[X])=\dfrac{1}{3}$.

这表明从$\boldsymbol{C}$中任选一条分享策略,R'内各元素在单个共享份内出现的概率保持不变,即依据单个共享份推测秘密像素各可能取值的概率相等,满足定义4的安全性条件.

(2)当$|X|=2$时

对于单个秘密像素,参与者拥有2个秘密份额,依据定义3给出的灰度叠加运算计算各分享策略对应恢复像素的平均灰度有:

$$\mu_1=\sum_{j=1}^{3^n}\mathrm{Stack}(R_j[X])\times p_{1,j}=0.125$$

$$\mu_2=\sum_{j=1}^{3^n}\mathrm{Stack}(R_j[X])\times p_{2,j}=0.1875$$

$$\mu_3=\sum_{j=1}^{3^n}\mathrm{Stack}(R_j[X])\times p_{3,j}=0.25$$

$$\mu_4=\sum_{j=1}^{3^n}\mathrm{Stack}(R_j[X])\times p_{4,j}=0.3125$$

$$\mu_5=\sum_{j=1}^{3^n}\mathrm{Stack}(R_j[X])\times p_{5,j}=0.375$$

3　方案流程

本文方案整体流程如图2所示,由目标优化模型、秘密分享算法和秘密恢复算法3个部分组成.其中,秘密恢复算法仅包括共享份的打印和叠加,无须计算设备的参与,在后续内容中不再单独说明.

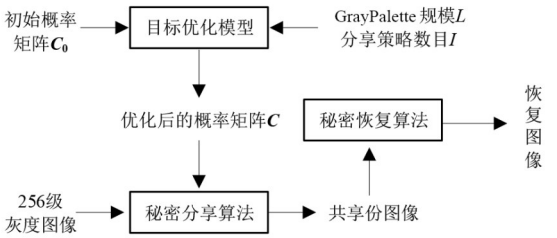


图2　本文方案整体流程图

3.1　目标优化模型

传统的视觉密码方案仅含两种灰度值(即GrayPalette={0,255}),采用黑白像素整体相对差作为恢复质量优化的目标函数.对应式(4)中i_1和i_2只能取1或2,分别代表一个灰度级,不失一般性.令$i_1=1$,$i_2=2$,则目标函数为$\max(\alpha_{2,1})$.

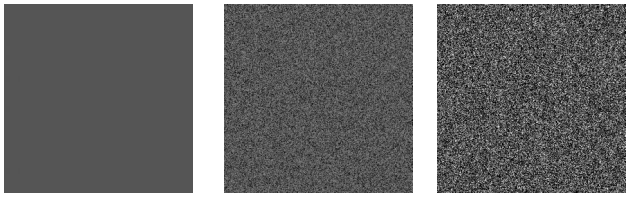
当GrayPalette规模增大时,容易出现灰度等价现象.以(2,2,3,3)-PVCS为例,记灰度概率矩阵$\boldsymbol{C}=[\boldsymbol{p}_1\ \ \boldsymbol{p}_2\ \ \boldsymbol{p}_3]^{\mathrm{T}}$,$\boldsymbol{p}_2'=[1/3,0,0,0,0,1/3,0,1/3,0]$和$\boldsymbol{p}_2''=[0,1/3,0,1/3,0,0,0,0,1/3]$.分别运用$\boldsymbol{p}_2'$和$\boldsymbol{p}_2''$分享第2灰度级对应像素,有

$$\sum_{i=1}^{3^2}\mathrm{Stack}(R_i[\{1,2\}])\times p'_{2,i}=1/3$$

$$\sum_{i=1}^{3^2}\mathrm{Stack}(R_i[\{1,2\}])\times p''_{2,i}=1/3$$

若仅以相对差作为多级灰度视觉密码方案的优化目标,则选定$\boldsymbol{p}_1$和$\boldsymbol{p}_3$,有$\alpha_{2',1}=\alpha_{2'',1}$,$\alpha_{3,2'}=\alpha_{3,2''}$,则称灰度概率矩阵$\boldsymbol{C}'=[\boldsymbol{p}_1\ \ \boldsymbol{p}_2'\ \ \boldsymbol{p}_3]^{\mathrm{T}}$与$\boldsymbol{C}''=[\boldsymbol{p}_1\ \ \boldsymbol{p}_2''\ \ \boldsymbol{p}_3]^{\mathrm{T}}$等

价. 然而,$\boldsymbol{p}_2'$和$\boldsymbol{p}_2''$对应恢复图像区域的视觉效果却不尽相同,如图3所示.



(*a*) 原始纯色灰度图 (*b*) $\boldsymbol{p}_2'$对应的恢复效果 (*c*) $\boldsymbol{p}_2''$对应的恢复效果

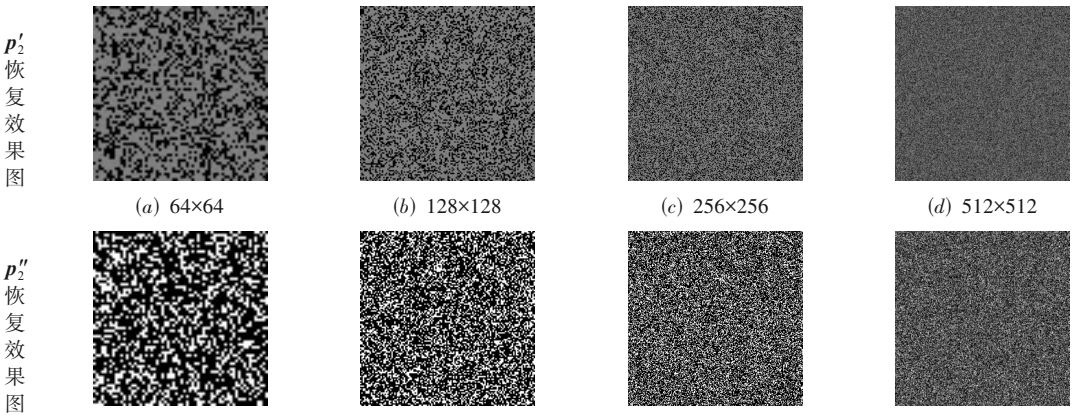
图3 平均灰度等价效果

分析$\boldsymbol{p}_2'$和$\boldsymbol{p}_2''$对应恢复图像区域的方差,有$\sigma_2'=\sum_{i=1}^{3^2}\left(\mathrm{Stack}(R_i[\{1,2\}])-\frac{1}{3}\right)^2\times p_{2,i}'=0.0556$,

$\sigma_2''=\sum_{i=1}^{3^2}\left(\mathrm{Stack}(R_i[\{1,2\}])-\frac{1}{3}\right)^2\times p_{2,i}''=0.2222$.

由概率型视觉密码的识别区域理论的3σ识别法则[8],同色区域恢复方差越小,识别同一灰度所需要的像素数量越少,识别率越高,具体如图4所示.

人眼观察时,一般依据中心像素及其邻域像素所构成的像素块判断该像素点的灰度等级. 由图4可知,当恢复区域平均灰度相同时,由于分享策略$\boldsymbol{p}_2'$的恢复方差要小于$\boldsymbol{p}_2''$,所以在恢复图像中,$\boldsymbol{p}_2'$还原中间灰度所需要的图像尺寸要比$\boldsymbol{p}_2''$小. 一般地,在灰度自然图像内不存在如图3(*a*)所示512×512大小的纯色块,分享策略$\boldsymbol{p}_2$所负责的纯色块的大小可能小于64×64. 在这些小区域上,图4(*a*)较图4(*e*)的灰度表现力更强.



$\boldsymbol{p}_2'$恢复效果图

(*a*) 64×64 (*b*) 128×128 (*c*) 256×256 (*d*) 512×512

$\boldsymbol{p}_2''$恢复效果图

(*e*) 64×64 (*f*) 128×128 (*g*) 256×256 (*h*) 512×512

图4 识别区域大小与分享策略方差的关系

为对上述等价概率矩阵做出区分,并从中选出恢复方差更小的分享策略,本文以各级灰度对应的平均恢复灰度与理想平均灰度之差最小化、恢复方差最小化为优化目标,对比性条件和安全性条件作为约束,为(k,n,L,I)-PVCS建立如下目标优化模型.

设GrayPalette规模为L,灰度子区间数目为I,$\boldsymbol{R}=\left(r_{i,j}\right)_{n\times L^n}$,灰度概率矩阵$\boldsymbol{C}=\left[\boldsymbol{p}_1\quad\boldsymbol{p}_2\quad\cdots\quad\boldsymbol{p}_I\right]^{\mathrm{T}}$.

基于定义4方案模型,以平均恢复灰度与理想平均灰度差的平方与恢复灰度方差之和为目标函数,对于(k,n,L,I)-PVCS,可建立如下目标优化模型.

目标函数:

$$\min\sum_{Y\in\{X||X|\geqslant k\}}f(C,Y)=\sum_{Y\in\{X||X|\geqslant k\}}\sum_{i=1}^{I}\left\{\left(\mu_i-\beta\times\frac{i-1}{I-1}\right)^2+\alpha\times\sum_{j=1}^{L^n}\left[\mathrm{Stack}\left(R_j[Y]\right)-\beta\times\frac{i-1}{I-1}\right]^2\times p_{i,j}\right\}\tag{5}$$

约束条件:

$$\forall|X|<k,\ \forall d\in\{1,2,\cdots,L^{|X|}\},\ \sum_{j=1}^{L^n}p_{i+1,j}\times H(R_j[X],R_d')-\sum_{j=1}^{L^n}p_{i,j}\times H(R_j[X],R_d')=0\tag{6}$$

$$\forall|X|\geqslant k,\ \sum_{j=1}^{L^n}\mathrm{Stack}\,(R_j[X])\times p_{i+1,j}-\sum_{j=1}^{L^n}\mathrm{Stack}\,(R_j[X])\times p_{i,j}>0\tag{7}$$

$$\sum_{j=1}^{L^n}p_{1,j}=\cdots=\sum_{j=1}^{L^n}p_{I,j}=1\tag{8}$$

$$\forall 1\leqslant i\leqslant I,\ \forall 1\leqslant j\leqslant L^n,\ 0\leqslant p_{i,j}\leqslant 1\tag{9}$$

其中,$\mu_i=\sum_{j=1}^{L^n}\mathrm{Stack}\,(R_j[Y])\times p_{i,j},\ i\in\{1,2,\cdots,I\}$. $\Delta_1(i)=\left(\mu_i-\beta\times\frac{i-1}{I-1}\right)^2$为第$i$级灰度对应的平均恢复灰度与理想平均灰度之差,$\beta$为缩放系数;$\Delta_2(i)=\sum_{j=1}^{L^n}\left[\mathrm{Stack}\left(R_j[Y]\right)-\beta\times\frac{i-1}{I-1}\right]^2\times p_{i,j}$为第$i$级灰度对应的

恢复方差;α为平衡Δ_1和Δ_2重要性的权重系数.

3.1.1 目标函数

目标函数主要由$\Delta_1(i)$和$\Delta_2(i)$两部分组成. $\Delta_1(1),\cdots,\Delta_1(I)$是对$I$条分享策略对应恢复灰度的差异性要求,将灰度动态变化区间[0,1]均匀划分为I-1段,取I个端点值乘以缩放系数β作为理想点,要求μ_i尽可能地逼近理想点. $\Delta_2(1),\cdots,\Delta_2(I)$是对$I$条分享策略对应恢复灰度的识别率要求,要求分享策略所选中分享规则对应的叠加结果尽可能地逼近μ_i.

对于只存在一个授权参与者集合的存取结构,如(n,n)门限结构,将$\Delta_1(1),\cdots,\Delta_1(I)$和$\Delta_2(1),\cdots,\Delta_2(I)$按照$f(C,Y)$进行综合即可. 对于存在多个授权参与者集合的存取结构,则需要对多个单目标优化函数$f(C,Y)$进行综合.

3.1.2 约束条件

约束条件主要由4部分构成,式(6)为安全性约束,对应于定义4中视觉密码的安全性条件;式(7)为对比性约束,对应于视觉密码的对比性条件;式(8)为归一化约束,源于定义2中灰度概率矩阵的归一化条件;式(9)为决策变量的取值范围.

3.1.3 模型求解

由3.1.1节和3.1.2节可知,基于式(5)所定义的目标函数为二次函数,而基于式(6)~(9)所定义的决策空间为一凸集. 因此,该目标优化问题为凸优化问题中的二次规划问题. 本文选择序列二次规划方法作为求解该优化问题的基本方法,依据图5所示流程图,对该目标优化模型进行求解,即可获得对应参数下的最优灰度概率矩阵. 其中,$\boldsymbol{C}_0$使用随机初始化方法生成.

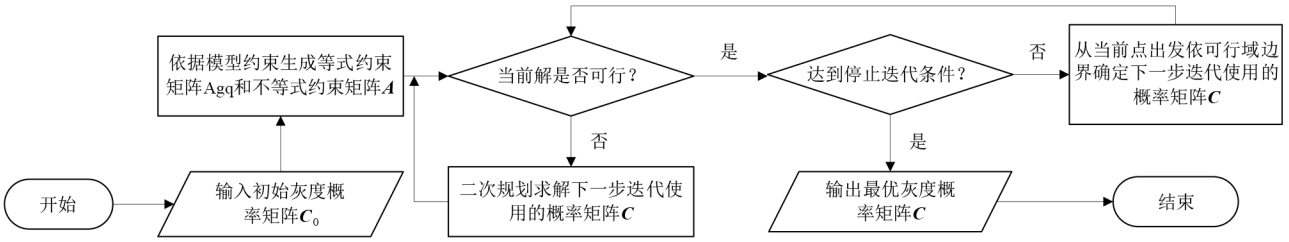


图5　目标优化模型求解流程图

3.2 秘密分享算法

对于任给256级灰度图像,首先将灰度取值区间映射至[0,1],再依据秘密图像直方图以及分享策略数I,将输入图像的灰度变化区间划分为I个子区间,保证每个子区间内像素数量相同. 然后,逐点遍历整幅图像,依据各个像素灰度值确定所属灰度子区间以及对应概率向量,再根据该概率向量随机选择一条分享规则用于分享,伪代码如算法1所示.

算法1　秘密分享算法

输入:灰度图像G,参与者数目n,恢复门限k,灰度概率矩阵$\boldsymbol{C}$

输出:共享份$T_1\sim T_n$

步骤1. 计算G的行数H,列数W,直方图分布$Hist$;依据$\boldsymbol{C}$计算分享策略数目I, GrayPalette的规模L;依据n和L生成分享规则矩阵$\boldsymbol{R}$;初始化共享份$T_1\sim T_n$为$H\times W$的零矩阵

步骤2. 依据$Hist$对G进行直方图均衡化

步骤3. 令$\text{GrayInterval}(l)=255*(l-1)/(I-1), 1\leqslant l\leqslant I$

步骤4. 遍历G内灰度像素$G(i,j)$, $1\leqslant i\leqslant H, 1\leqslant j\leqslant W$

步骤5. IF $\text{GrayInterval}(l-1)\leqslant G(i,j)\leqslant\text{GrayInterval}(l)$

　　THEN $p=\boldsymbol{C}(l,:)$为当前像素的分享策略

步骤6. 依据p将区间[0,1]划分为$s(s=L^n)$个子区间,记为$x_1\sim x_s$

步骤7. 生成随机数$r, r\in[0,1]$

步骤8. IF r属于区间$x_{\text{index}}, 1\leqslant\text{index}\leqslant s$

　　THEN 选用R中第index条规则$\text{rule}=\boldsymbol{R}(:,\text{index})$进行秘密分享

步骤9. 对于t=1~n,令$T_t(i,j)=\text{rule}(t)$

步骤10. 完成对全部像素的分享,算法结束

4 实验与结果分析

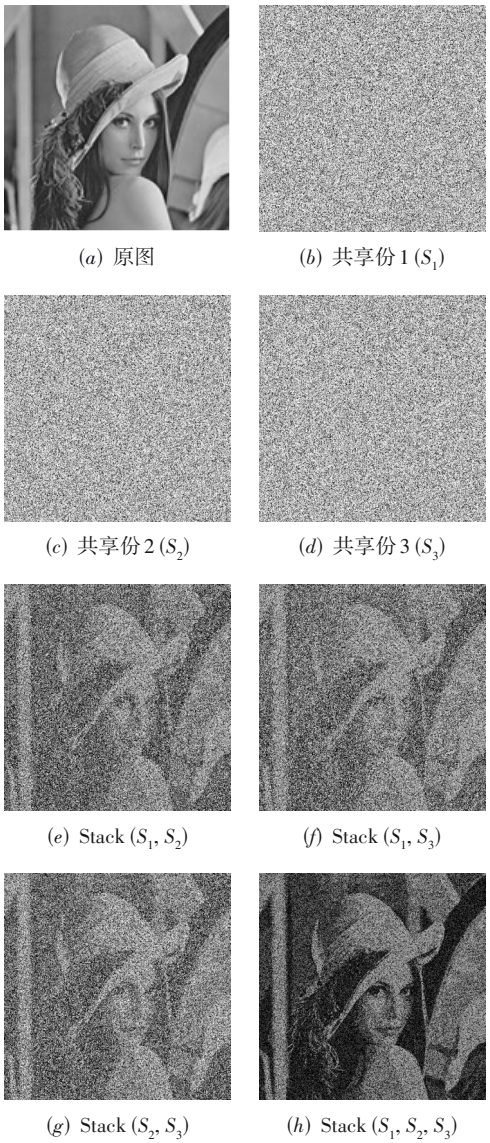
本节采用标准Lena图像和Kodak图像集(附录3-图1)作为测试图集,均为512×512的灰度图像. 首先以(2,3,3,4)-PVCS为例说明方案在(k,n)门限结构上的适用性,以验证方案的有效性;再结合$(2,3,L,I)$-PVCS分析参数I和L对恢复效果的影响;最后,由于现存同类方案适用的存取结构受限,结合本文(2,2,6,6)-PVCS与同类方案进行参数指标对比,得出结论.

4.1 有效性验证

以(2,3,3,4)-PVCS为例,参与者集合$P=\{1,2,3\}$,参与者子集$\{1\},\{2\},\{3\}$无法获得任何秘密图像相关信息,被称为禁止参与者集合. 参与者子集$\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}$可以将手持共享份叠加,通过人类视觉系统识别秘密图像信息,被称为授权参与者集合.

对于任意I和L,均可通过求解目标优化模型,得到一个最优概率矩阵解. 其中,当I=4, L=3, $\alpha=0.6$, $\beta=$

0.4, GrayPalette = {0, 0.7, 1} 时，解得一个规模大小为 4 × 27 的灰度概率矩阵 $\boldsymbol{C}$（见附录 1）. 结合灰度概率矩阵 $\boldsymbol{C}$，运用算法 1 对标准 Lena 图像进行分享，所得共享份及恢复图像如图 6 所示.



(a) 原图 (b) 共享份 1 (S_1)

(c) 共享份 2 (S_2) (d) 共享份 3 (S_3)

(e) Stack (S_1, S_2) (f) Stack (S_1, S_3)

(g) Stack (S_2, S_3) (h) Stack (S_1, S_2, S_3)

图 6 本文(2,3,4,3)-PVCS 实验结果

由图 6(b)~图 6(d)可知，运用灰度概率矩阵 $\boldsymbol{C}$ 分享所得共享份图像在视觉上均为杂乱无章的噪声图像. 由第 3 节目标优化模型的安全性约束可知，运用满足安全性约束的灰度概率矩阵进行秘密分享，任意禁止参与者集合均无法从手持共享份获得与秘密图像相关信息. 直观起见，运用该灰度概率矩阵对 Kodak 图像集进行分享，分别统计各秘密图像对应 S_1, S_2, S_3 内各颜色像素的出现频次，其平均值如表 1 所示. 由表可知，对于任意秘密图像，单个参与者所获得的共享份内各灰度像素出现频率基本相同，符合定理 5 的结论，单个参与者无法依据共享份统计规律推知秘密图像信息，验证了本文方案的安全性.

表 1 (2,3,4,3)-PVCS 统计量

像素灰度值	S_1 内对应像素数目	S_2 内对应像素数目	S_3 内对应像素数目
0	58 704	58 706	58 706
0.7	86 017	85 908	86 046
1	117 423	117 530	117 392

此外，由图 6(e)~图 6(h)可见，对于授权参与者集合，叠加恢复所得图像能够有效呈现原始秘密图像信息，从而验证了本文目标优化模型以及分享算法的有效性.

4.2 参数分析

本文目标优化模型涉及 5 个可变参数：L, I, α, β 以及 GrayPalette. 一般地，GrayPalette 依据 L 直接将灰度值变化区间 $[0,1]$ 均匀划分为 L 等份，取这 L 段的起点即构成 GrayPalette. 参数 α 为目标权重系数，可以依据需要设置. α 越大，意味着 Δ_2 的重要程度越高. 此时，目标优化模型可能牺牲 Δ_1 以优化 Δ_2. 理想灰度值缩放系数 β 为经验参数，目标函数中的理想点取决于对比度和方差的理论上限. 而多值情况下的这一理论上限尚未可知，对于不同存取结构、L 和 I, β 需取不同值，以逼近理想点.

设计灰度概率矩阵并运用多值共享份分享灰度图像的目的在于降低恢复图像的失真程度、提升灰度表现力. 为了定量、客观地评价恢复图像在上述两方面的提升，引入了多尺度结构相似度[25]（Multi-Scale Structural SIMilarity, MS-SSIM）和感知相似度[26]（Learned Perceptual Image Patch Similarity, LPIPS）作为恢复图像的全参考质量评价指标[27].

MS-SSIM 属于传统图像质量评价指标. 该类指标设计的基本假设是：人类视觉系统对于图像结构相似度的感知极其敏感，且其感知规律可以通过设计一个简单的公式对其输出结果进行模拟. 该指标在计算过程中通过采样模拟多种尺度，在各尺度上分别依据式(10)计算结构相似度，最后依据给定的权重综合各尺度上的评分结果，给出最终得分. 得分越高，恢复图像在各个尺度上与原始图像在亮度、对比度和结构 3 方面的相似度最高. 因此，可以认为 MS-SSIM 值越大，图像的灰度表现力越强.

$$\mathrm{SSIM}(G,G')=\frac{1}{N}\sum_{b=1}^{N}\frac{(2\mu_{G_b}\mu_{G'_b}+C_1)(2\sigma_{G_bG'_b}+C_2)}{(\mu_{G_b}^2+\mu_{G'_b}^2+C_1)(\sigma_{G_b}^2+\sigma_{G'_b}^2+C_2)} \tag{10}$$

其中，$C_1=(0.01\times\gamma)^2$ 和 $C_2=(0.03\times\gamma)^2$ 是用于确保计算结果稳定的常数（γ 为像素值的取值范围，即 255）. μ_{G_b}

和$\mu_{G_b'}$分别为$\boldsymbol{G}$和$\boldsymbol{G}'$第b个子像素块的均值,$\sigma_{G_b}^2$和$\sigma_{G_b'}^2$分别为$\boldsymbol{G}$和$\boldsymbol{G}'$第b个子像素块的方差,$\sigma_{G_bG_b'}$是$\boldsymbol{G}$和$\boldsymbol{G}'$第b个子像素块的协方差,设置5级观测尺度,1~5级尺度对应的权重分别为0.044 8、0.285 6、0.300 1、0.236 3和0.133 3.

LPIPS由Zhang等人[26]在CVPR 2018上提出,其设计的基本假设是:人类视觉系统机理相当复杂,对于单幅图像的评价可能存在多个侧面,无法使用统一的公式拟合人类主观打分结果. 该指标利用深度神经网络的高维语义特征计算恢复图像相较于原始图像的感知相似度损失,在各类图像处理标准数据集上的表现均优于传统基于公式计算的图像质量评价指标. LPIPS越小,意味着恢复图像与原始图像之间的感知相似度距离越小,恢复图像失真程度越低.

取α和β为0.5,以(2,2,L,I)-PVCS为例,研究灰度子区间数I和GrayPalette规模L对算法1的影响. 设置I和L的变化区间为2~10,在各I和L下,分别求解目标优化模型,获得最优灰度概率矩阵(对应目标函数最优值见附录2),运用上述概率矩阵分享Kodak图像集,采用MS-SSIM和基于AlexNet的LPIPS评价恢复图像,测试结果如图7和图8所示.

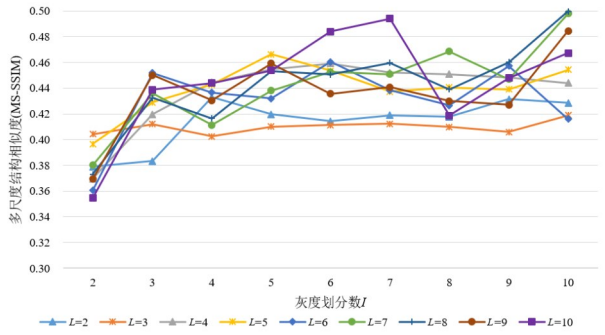


图7　不同I和L下,MS-SSIM变化趋势($\alpha=0.5,\beta=0.5$)

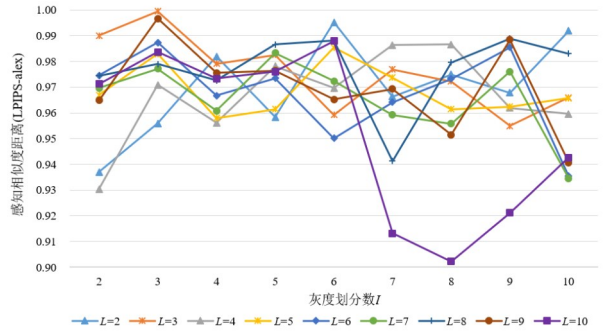


图8　不同I和L下,LPIPS变化趋势($\alpha=0.5,\beta=0.5$)

由图7、8可知,随着L的增加,感知相似度损失并非是线性变化关系,对于给定图像或图像集,存在一个最合适的I和L. 以上述Kodak图像集为例,使用本文算法1,取L=10,I=7,恢复图像的综合质量最高.

4.3　方案对比

考虑到文献[16]和文献[23]适用的存取结构有限,本小节以(2,2,6,6)-PVCS为例(对应灰度概率矩阵见附录1),取Kodak图像集作为测试图集,以文献[10]、文献[16]和文献[23]作为对比文献,首先结合MS-SSIM和LPIPS两个指标,对各方案恢复图像质量进行对比分析,再从计算复杂度和算法适用性两方面总结本文方案优势. 测试环境为MATLAB2018a和PyCharm2020.3.3,测试主机CPU为Intel i7-10750H,主频为2.59 GHz.

4.3.1　恢复质量对比

选用大小为512×512的Kodak图像集作为测试图像,将各方案生成的共享份叠加后获得相应恢复图像集,运用MS-SSIM(设置五级尺度,综合权重同4.2节)和LPIPS(基于AlexNet实现)对恢复图像进行评价.

由图9可知,由于引入多值灰度像素,本文算法以及文献[23],较文献[10,16]在灰度表现力方面有所提升. 对比方案从劣至优的排序依次为:文献[10]、文献[16]、文献[23]、本文方案. 其中,本文方案恢复图像参见附录3-图2. 以Kodak-22为例对该评价过程予以说明,如表2所示.

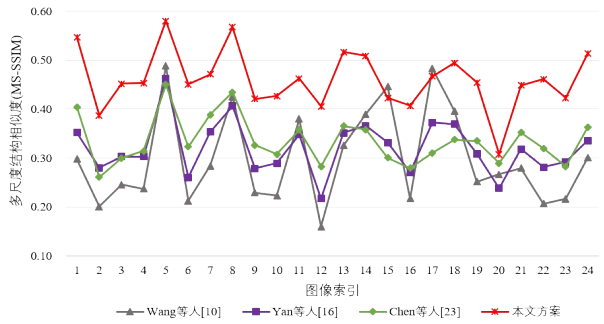


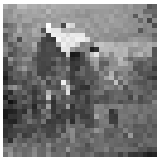
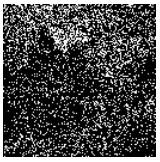
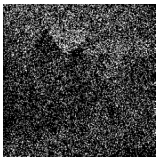
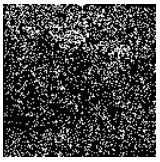
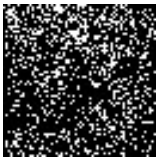
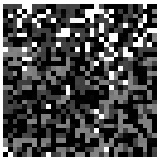
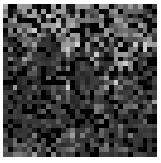
图9　各对比方案的多尺度平均结构相似度

由表2可见,随着尺度等级升高,基于多值共享份的方案较基于二值共享份的方案,质量下降速度更加缓慢. 在尺度1,由于引入基于误差扩散的反馈调节机制,文献[16]得到了较为平滑的恢复图像,但是本文方案灰度表现力更强. 在尺度2,基于二值共享份的方案所恢复图像内木屋基本不可被识别,但基于多值共享份的方案仍旧可以识别木屋的大体轮廓. 在尺度3,本文方案较文献[23]以及基于反馈的方案优势更加明显.

另一方面,LPIPS利用深度神经网络模拟人类视觉系统(Human Visual System,HVS)处理恢复图像的过程,是定量分析恢复图像内信息失真程度的一个客观评价指标,评价结果如图10所示.

由图10可知,文献[10]和[16]恢复图像为二值图

表2 各对比方案在各尺度下的恢复图像

尺度	1 (512×512)	2 (256×256)	3 (128×128)	4 (64×64)	5 (32×32)
原图					
文献[10]					
文献[16]					
文献[23]					
本文方案					

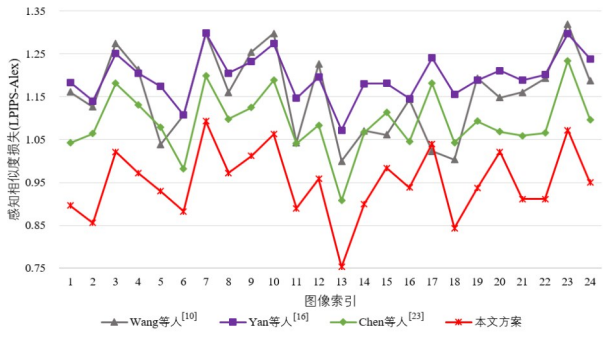


图10 各对比方案的感知相似度损失

像,仅能通过二值像素排布密度差异模拟多级灰度,经HVS处理提取得到的有效信息与原始灰度图像的感知差异较大;文献[23]和本文恢复图像为多值图像. 相较于二值图像,局部像素块特征模式更加显著,感知相似度损失更小,失真程度更低. 各方案在LPIPS指标上表现由优至劣依次为:本文方案、文献[23]、文献[10]和文献[16].

综合来看,基于多值共享份的方案在两类指标上的平均表现要优于基于二值共享份的方案. 本文方案由于使用了优化后的灰度概率矩阵,在测试集上的MS-SSIM均值以及LPIPS均值表现较同类方案更加优秀,其恢复图像较现有方案具备更强的灰度表现力和更高的感知相似度.

4.3.2 计算复杂度分析

由于各对比方案的秘密恢复过程均通过叠加实现,具有相同的计算开销. 因此,在效率分析方面,重点对分享算法计算复杂度进行分析和测试.

计算复杂度可以由算法在执行时所需要的基本运算次数度量,由于采用逐像素分享方式,本方案与对比方案的计算复杂度都是秘密图像尺寸的线性函数,即$O(HW)$,H和W分别代表灰度秘密图像的行宽和列宽. 假设各方案分享单个像素所需随机实数获取时间相同,记T_{compare}为单次比较所需要的时间,T_{add}为单次加法所需要的时间,T_{mul}为单次乘法所需要的时间. 并通过测试各方案分享Kodak图像集的平均耗时,比较各方案分享算法效率. 在最坏的情况下,各方案分享单个像素所需要的基本运算次数以及分享单幅图像平均耗时如表3所示. 其中,m为(k,n)二值视觉密码方案对应的像素扩展度,对于(n,n)门限结构,$m=2^{n-1}$.

各分享算法的耗时主要由灰度区间匹配、分享规则选取和误差反馈这3类操作耗时组成. 文献[10]

表3　各方案分享算法计算复杂度对比

比较项 / 方案	灰度区间匹配	分享规则选取	误差扩散	分享单幅图像平均耗时/s
文献[10]	$(I-1)T_{\text{compare}}$	$\left[(I-1)m-1\right]T_{\text{compare}}$	0	0.23
文献[16]	T_{compare}	$\left[(I-1)m-1\right]T_{\text{compare}}$	$5T_{\text{add}}+4T_{\text{mul}}$	0.12
文献[23]	$5T_{\text{compare}}$	$\left(L^{\text{n}}-1\right)T_{\text{compare}}$	0	0.34
本文方案	$(I-1)T_{\text{compare}}$	$\left(L^{\text{n}}-1\right)T_{\text{compare}}$	0	0.34

中,I=6,L=2,不需要误差反馈;文献[16]中,I=2,L=2,需要误差反馈;文献[23]中,I=6,L=3,不需要误差反馈;本文算法中,I=6,L=6,不需要误差反馈.

测试结果表明,分享算法运行耗时:文献[23]≈本文方案>文献[10]>文献[16],本文算法运行耗时不占优. 关键原因在于灰度区间匹配以及分享规则选取操作耗时过长. 而测试过程中的灰度区间匹配以及分享规则选取操作均基于MATLAB内置查找算法实现,实际应用过程中,可针对上述两类操作的实现效率进行优化.

4.4　小结

综上所述,本节从算法适用性、恢复图像质量以及计算复杂度3个方面分析了本文方案的优势与不足,相关指标对比各项指标汇总如表4所示.

由表4可知,本文方案适用于任意(k,n)门限结构,对于任意多元灰度集合GrayPalette、秘密图像灰度划分数,依据本文目标优化模型均可求解得到相应的最优灰度概率矩阵,实现灰度图像秘密分享. 而文献[10]和文献[16]仅适用于二元灰度集合,文献[23]仅适用于三元灰度集合,文献[16]和文献[23]适用的存取结构受限. 在计算复杂度方面,本文方案分享单个像素耗时为一常数,分享算法的计算复杂度取决于输入图像规模,与对比方案属于同一量级.

整体而言,本文适用于任意门限存取结构,计算复杂度适中,通过优化灰度概率矩阵,使得恢复图像在MS-SSIM和LPIPS指标上的表现均优于对比文献,灰度表现力更强,失真程度更低.

表4　各方案参数指标对比

方案	灰度划分区间数I	GrayPalette规模L	适用存取结构	MS-SSIM均值(越大越好)	LPIPS均值(越小越好)	分享算法计算复杂度
文献[10]	任意	2	(k, n)	0.30	1.15	O(HW)
文献[16]	2或3	2	(n, n)	0.32	1.20	O(HW)
文献[23]	6	3	(2, 2)	0.33	1.09	O(HW)
本文方案	任意	任意	(k, n)	0.46	0.95	O(HW)

5　结论与展望

本文提出一种基于灰度概率矩阵的视觉密码方案,通过建立目标优化模型,求解灰度概率矩阵,可直接对灰度图像进行分享. 实验结果表明,运用本文方案可获得灰度表现力更强、感知相似度更高的恢复图像. 下一步,将深入探讨方案各参数关系,并尝试将多点分享机制引入基于灰度概率矩阵的视觉密码方案,以期进一步提升恢复图像的视觉效果. 此外,若需同时优化多个参与者的恢复效果,通过对相应的单目标优化函数赋予权重,构造渐进式灰度视觉密码方案,也是一个有趣的研究方向.

附录A

k=2,n=3,L=3,I=4时分享规则集合Rules和最优灰度概率矩阵$\boldsymbol{C}$.

$$\text{Rules}=\begin{bmatrix}0,0.7,1,0,0.7,1,0,0.7,1,0,0.7,1,0,0.7,1,0,0.7,1,0,0.7,1,0,0.7,1,0,0.7,1\\0,0,0,0.7,0.7,0.7,1,1,1,0,0,0,0.7,0.7,0.7,1,1,1,0,0,0,0.7,0.7,0.7,1,1,1\\0,0,0,0,0,0,0,0,0,0.7,0.7,0.7,0.7,0.7,0.7,0.7,0.7,0.7,1,1,1,1,1,1,1,1,1\end{bmatrix}$$

$$\boldsymbol{C}=\begin{bmatrix}0,0,0,0,0,0,0,0,0.2239,0,0,0,0.3275,0,0,0.0007,0,0,0,0.2239,0,0,0,0.2239,0,0\\0.0211,0.0002,0.0369,0,0,0.0005,0.0474,0.0006,0.1172,0,0.0007,0.0007,0,0.0075,0.1599,0.0006,0.1587,0,0.0304,0.0012,0.1326,0.0003,0.1592,0,0.1241,0,0\\0.0738,0,0.0677,0,0,0,0.058,0,0.0245,0,0,0,0,0,0.1612,0,0.1553,0.0117,0.0569,0,0.0255,0,0.009,0.1574,0.0352,0.1639,0\\0.2239,0,0,0,0,0,0,0,0,0,0,0,0,0.0566,0,0.0710,0.2006,0,0,0,0,0.0802,0.1907,0,0.177,0\end{bmatrix}$$

k=2，n=2，L=6，I=6时分享规则集合Rules和最优灰　　度概率矩阵$\boldsymbol{C}$.

$$\text{Rules}=\begin{bmatrix}0,0.2,0.4,0.6,0.8,1,0,0.2,0.4,0.6,0.8,1,0,0.2,0.4,0.6,0.8,1,0,0.2,0.4,0.6,0.8,1,0,0.2,0.4,0.6,0.8,1,0,0.2,0.4,0.6,0.8,1\\0,0,0,0,0,0,0,0.2,0.2,0.2,0.2,0.2,0.2,0.4,0.4,0.4,0.4,0.4,0.4,0.6,0.6,0.6,0.6,0.6,0.6,0.8,0.8,0.8,0.8,0.8,0.8,1,1,1,1,1,1\end{bmatrix}$$

$$\boldsymbol{C}=\begin{bmatrix}0,0,0,0,0,0,0.1295,0,0,0,0.0061,0.0494,0.1379,0,0,0,0.1157,0.0561,0.0013,0,0.01,0.1564,0.0155,0,0,0,0.1467,0.003,0,0,0,0.13,0.0412,0.0012,0,0,0\\0,0,0,0,0.0308,0.0987,0,0,0.0001,0.0154,0.0111,0.166,0,0,0.0056,0.0999,0.0635,0.004,0,0.0138,0.1459,0.022,0.0001,0,0.0035,0.1384,0.0077,0,0,0,0.1265,0.0456,0.0003,0,0,0\\0.0178,0,0,0,0.0286,0.0831,0,0,0,0.0016,0.0062,0.1856,0,0,0.0041,0.0983,0.0707,0,0.006,0.0046,0.1405,0.0308,0,0,0.0444,0.0827,0.016,0.0066,0,0,0.0618,0.1106,0,0,0,0\\0.1293,0.0002,0,0,0,0,0,0.005,0.0052,0.0278,0.0222,0.1333,0,0.0019,0.0003,0,0.0355,0.1354,0,0.0803,0,0.0537,0.0478,0,0,0,0.0938,0.0559,0,0,0.0007,0.1104,0.0613,0,0,0\\0.099,0.0305,0,0,0,0,0.031,0.1179,0,0,0,0.0446,0,0.0252,0,0,0.0813,0.0666,0,0.0002,0,0,0.0242,0.1574,0,0.0097,0.0026,0.1374,0,0,0,0.0144,0.158,0,0,0\\0.1005,0.0291,0,0,0,0,0.0295,0.0849,0.0731,0.0059,0,0,0,0.0813,0.0181,0.0267,0.007,0.04,0,0,0.0107,0.006,0.0017,0.1633,0,0,0.0152,0.0018,0.0673,0.0654,0,0.0026,0.0435,0.0969,0.0294,0\end{bmatrix}$$

附录B

表B-1　I=2~10,L=2~10时,(2, 2)方案目标函数最优值fval(保留至小数点后3位)

L	I	fval	L	I	fval	L	I	fval	L	I	fval	L	I	fval	L	I	fval	L	I	fval
2	3	0.203	2	4	0.271	2	5	0.340	2	6	0、410	2	7	0.480	2	8	0.551	2	9	0.620
3	2	0.087	4	2	0.092	5	2	0.087	6	2	0.088	7	2	0.087	8	2	0.088	9	2	0.089
3	3	0.114	4	3	0.115	5	3	0.114	6	3	0.116	7	3	0.117	8	3	0.116	9	3	0.116
3	4	0.132	4	4	0.132	5	4	0.131	6	4	0.134	7	4	0.137	8	4	0.139	9	4	0.138
3	5	0.155	4	5	0.153	5	5	0.155	6	5	0.158	7	5	0.162	8	5	0.160	9	5	0.163
3	6	0.180	4	6	0.179	5	6	0.181	6	6	0.188	7	6	0.187	8	6	0.185	9	6	0.194
3	7	0.204	4	7	0.203	5	7	0.204	6	7	0.217	7	7	0.218	8	7	0.212	9	7	0.220
3	8	0.230	4	8	0.230	5	8	0.238	6	8	0.255	7	8	0.253	8	8	0.255	9	8	0.260
3	9	0.259	4	9	0.262	5	9	0.280	6	9	0.264	7	9	0.280	8	9	0.281	9	9	0.290
3	10	0.280	4	10	0.292	5	10	0.296	6	10	0.316	7	10	0.306	8	10	0.309	9	10	0.314
10	3	0.118	10	4	0.144	10	5	0.165	10	6	0.188	10	7	0.221	10	8	0.221	10	9	0.258
2	2	0.125	2	10	0.689	10	2	0.089	10	10	0.327									

附录C

(*a*) Kodak-1

(*b*) Kodak-2

(*c*) Kodak-3

(*d*) Kodak-4

(*e*) Kodak-5

(*f*) Kodak-6

(*g*) Kodak-7

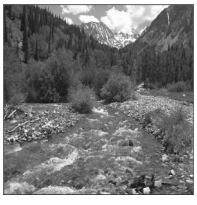
(*h*) Kodak-8

(*i*) Kodak-9

(*j*) Kodak-10

(*k*) Kodak-11

(*l*) Kodak-12



(*m*) Kodak-13

(*n*) Kodak-14

(*o*) Kodak-15

(*p*) Kodak-16

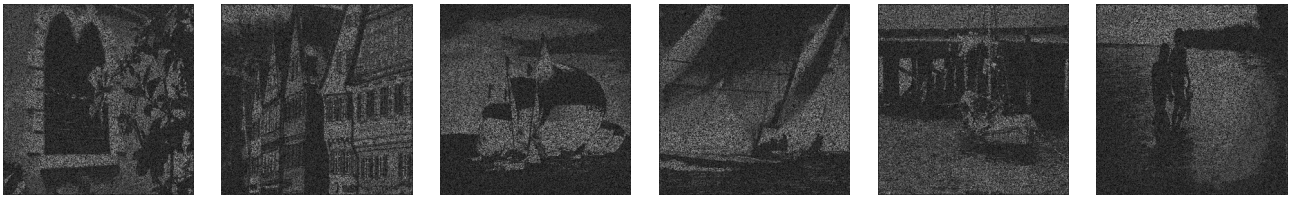
(*q*) Kodak-17

(*r*) Kodak-18

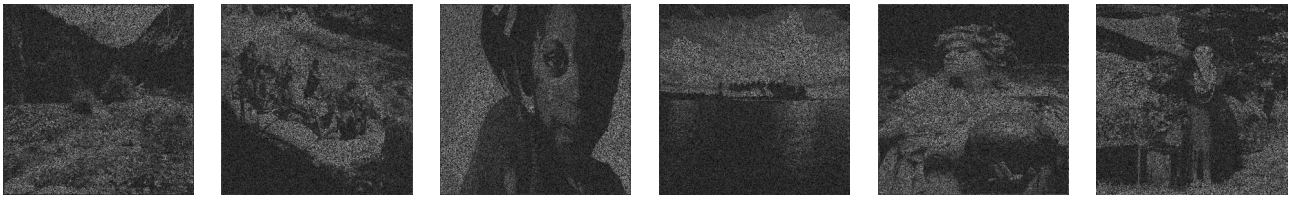
(*s*) Kodak-19　(*t*) Kodak-20　(*u*) Kodak-21　(*v*) Kodak-22　(*w*) Kodak-23　(*x*) Kodak-24

图 C-1　Kodak 图像集

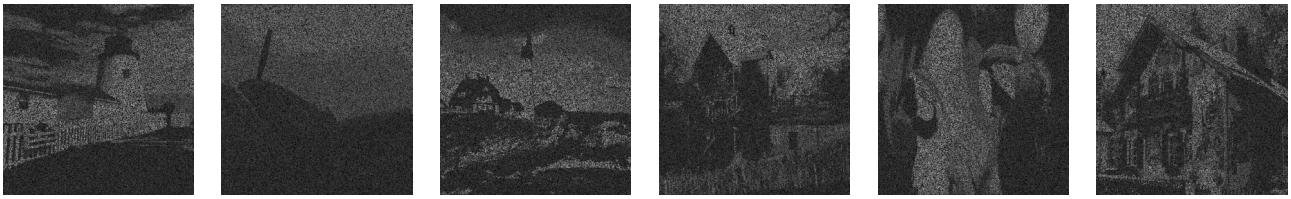
(*a*) Kodak-1　(*b*) Kodak-2　(*c*) Kodak-3　(*d*) Kodak-4　(*e*) Kodak-5　(*f*) Kodak-6



(*g*) Kodak-7　(*h*) Kodak-8　(*i*) Kodak-9　(*j*) Kodak-10　(*k*) Kodak-11　(*l*) Kodak-12



(*m*) Kodak-13　(*n*) Kodak-14　(*o*) Kodak-15　(*p*) Kodak-16　(*q*) Kodak-17　(*r*) Kodak-18



(*s*) Kodak-19　(*t*) Kodak-20　(*u*) Kodak-21　(*v*) Kodak-22　(*w*) Kodak-23　(*x*) Kodak-24

图 C-2　(2,2,6,6)-PVCS 在 Kodak 图像集上的恢复图像

参考文献

[1] NAOR M, SHAMIR A. Visual cryptography[C]// Proceedings of Workshop on the Theory and Application of Cryptography Techniques (EUROCRYPT). Berlin: Springer, 1994: 1-12.

[2] IBRAHIM D R, TEH J S, ABDULLAH R. An overview of visual cryptography techniques[J]. Multimedia Tools and Applications, 2021, 80(21): 31927-31952.

[3] ATENIESE G, BLUNDO C, DE SANTIS A, et al. Visual cryptography for general access structures[J]. Information and Computation, 1996, 129(2): 86-106.

[4] VERHEUL E R, VAN TILBORG H C A. Constructions and properties of *k* out of *n* visual secret sharing schemes [J]. Designs, Codes and Cryptography, 1997, 11(2): 179-196.

[5] OKADA K, KOGA H. A construction of the (4, *n*)-thresh-

old visual cryptography scheme using a 3-design[C]//2018 International Symposium on Information Theory and Its Applications (ISITA). Piscataway: IEEE, 2019: 223-227.

[6] HSU C S, TU S F, HOU Y C. An Optimization Model for Visual Cryptography Schemes with Unexpanded Shares [M]//Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006: 58-67.

[7] DUTTA S, SARDAR M K, ADHIKARI A, et al. Color visual cryptography schemes using linear algebraic techniques over rings[C]//KANHERE S, PATIL VT, SURAL S, et al. International Conference on Information Systems Security. Cham: Springer, 2020: 198-217.

[8] 付正欣, 郁滨, 房礼国. 一种新的多秘密分享视觉密码[J]. 电子学报, 2011, 39(3): 714-718.
FU Z X, YU B, FANG L G. A new multi-secret sharing visual cryptography[J]. Acta Electronica Sinica, 2011, 39(3): 714-718. (in Chinese)

[9] YANG C N. New visual secret sharing schemes using probabilistic method[J]. Pattern Recognition Letters, 2004, 25(4): 481-494.

[10] WANG D S, YI F, LI X B. Probabilistic visual secret sharing schemes for grey-scale images and color images [J]. Information Sciences, 2011, 181(11): 2189-2208.

[11] CHEN Y F, CHAN Y K, HUANG C C, et al. A multiple-level visual secret-sharing scheme without image size expansion[J]. Information Sciences, 2007, 177(21): 4696-4710.

[12] LIN C C, TSAI W H. Visual cryptography for gray-level images by dithering techniques[J]. Pattern Recognition Letters, 2003, 24(1/2/3): 349-358.

[13] SHARMA G R, SHIRISHA G, YADAV M N. Visual cryptography using space filling curve ordered dithering with adaptive clustering[J]. International Journal of Advanced Trends in Computer Science and Engineering, 2014, 3(1): 569-574.

[14] HOU Y C, TU S F. A visual cryptographic technique for chromatic images using multi-pixel encoding method[J]. Journal of Research and Practice in Information Technology, 2005, 37(2): 179-191.

[15] LEE C C, CHEN H H, LIU H T, et al. A new visual cryptography with multi-level encoding[J]. Journal of Visual Languages & Computing, 2014, 25(3): 243-250.

[16] YAN B, XIANG Y, HUA G. Improving the visual quality of size-invariant visual cryptography for grayscale images: An analysis-by-synthesis (AbS) approach[J]. IEEE Transactions on Image Processing, 2019, 28(2): 896-911.

[17] SUN R, FU Z X, YU B. Size-invariant visual cryptography with improved perceptual quality for grayscale image [J]. IEEE Access, 2020, 8: 163394-163404.

[18] DUTTA S, ADHIKARI A, RUJ S. Maximal contrast color visual secret sharing schemes[J]. Designs, Codes and Cryptography, 2019, 87(7): 1699-1711.

[19] ASWAD F M, SALMAN I, MOSTAFA S A. An optimization of color halftone visual cryptography scheme based on bat algorithm[J]. Journal of Intelligent Systems, 2021, 30(1): 816-835.

[20] CIMATO S, YANG C N. Visual cryptography and Secret Image Sharing[M]. Boca Raton: CRC Press, 2017: 545-547.

[21] CIMATO S, DE PRISCO R, DE SANTIS A. Colored visual cryptography without color darkening[J]. Theoretical Computer Science, 2007, 374(1/2/3): 261-276.

[22] JUMABAYEVA A, FRANK T, SHOSHAN Y B, et al. HVS-based model for superposition of two color halftones [C]// Proceedings of the 21st Color Imaging: Displaying, Processing, Hardcopy, and Application. San Francisco: Society for Imaging Science and Technology, 2016: 1-9.

[23] CHEN H H, LEE C C, LEE C C, et al. Multi-level visual secret sharing scheme with smooth-looking[C]//Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human. New York: ACM, 2009: 155-160.

[24] QIU S Q. Convergence of a stabilized SQP method for equality constrained optimization[J]. Computational Optimization and Applications, 2019, 73(3): 957-996.

[25] WANG Z, SIMONCELLI E P, BOVIK A C. Multiscale structural similarity for image quality assessment[C]//The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers. Piscataway: IEEE, 2004: 1398-1402.

[26] ZHANG R, ISOLA P, EFROS A A, et al. The unreasonable effectiveness of deep features as a perceptual metric [C]//2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE, 2018: 586-595.

[27] 高敏娟, 党宏社, 魏立力, 等. 全参考图像质量评价回顾与展望[J]. 电子学报, 2021, 49(11): 2261-2272.
GAO M J, DANG H S, WEI L L, et al. Review and

prospect of full reference image quality assessment[J]. Acta Electronica Sinica, 2021, 49(11): 2261-2272. (in Chinese)

作者简介

付正欣　男,1986年生,山东曹县人. 信息工程大学副教授. 主要研究方向为网络安全与视觉密码.
E-mail: fzx2515@163.com

黄航璎　女,1998年生,江西宜春人. 信息工程大学硕士研究生. 主要研究方向为视觉密码.

郁　滨　男,1964年生,河南郑州人. 信息工程大学教授. 主要研究方向为网络安全与视觉密码.