基于三维立体分享图像的(2, 2)视觉密码方案 *

郭 璠，刘丽珏†，刘熙尧，陈白帆

(中南大学 信息科学与工程学院，长沙 410083)

摘 要：传统(2, 2)视觉密码方案由于其共享图像为毫无意义的二值图像而易引起攻击者的怀疑。为此，提出了一种基于三维立体分享图像的(2, 2)视觉密码方案。该方案将分享图像伪装成有意义的三维立体图，由此可较好地避免恶意攻击。而当两幅分享图像进行叠加等处理，人类视觉系统就能直接辨认出秘密信息。与其他图像加密方法的性能对比与定量评估说明，本方案在较好隐藏秘密信息的同时，具有相对较快的运算速度。正是由于该方案秘密恢复的简单性和有效性，具有广泛的应用前景。

关键词：视觉密码；三维立体图；分享图像；(2, 2)方案

中图分类号：TP309.7

(2, 2) visual cryptography scheme based on autostereogram sharing images

Guo Fan, Liu Lijue†, Liu Xiyao, Chen Baifan

(*School of Information Science and Engineering*, *Central South University*, *Changsha* 410083)

Abstract: Traditional (2, 2) visual cryptography scheme can easily cause the suspicion of attackers since the sharing images are meaningless binary images. For this reason, this paper proposes a (2, 2) visual cryptography scheme based on the autostereogram sharing images. The scheme disguises the sharing images as a meaningful autostereogram, so we can avoid the malicious attack. Once the two sharing images stack together, human visual system can directly recognize the secret information. The performance comparison and qualitatively evaluation with other image decryption methods demonstrate that the proposed scheme can conceal the secret information well, and keep a relatively fast speed at the same time. Because of the simplicity and effectiveness of the secret recovery, many areas can apply the scheme.

Key Words: visual cryptography; autostereogram; sharing images; (2, 2) scheme

0 引言

视觉密码由 Naor 和 Shamir 在 1994 年欧洲密码学年会上提出[1]，它以门限秘密共享思想为基础，将秘密共享和数字图像结合起来，形成了一个新的研究热点。其秘密分享算法是将秘密图像按像素点编码到若干个共享图像中，此单个共享图像中的黑、白像素点随机分布，因而从中无法得到任何关于秘密图像的信息。视觉密码的秘密恢复算法非常简单，只需将一定数目的共享图像打印至透明胶片并进行叠加，人的视觉系统就可以直接辨认出秘密信息[2]。正是由于视觉密码的理论安全性和秘密恢复的简单性，因此具有较好的应用前景和研究价值。从应用领域来说，视觉密码可广泛应用于身份认证、电子投票、消费电子、信息隐藏等领域。从秘密共享的角度来看，视觉密码可应用于群体参与或控制领域，如口令分存、密钥管理、安全多方计算、数字水印、数据保密、签名认证等。此外，由于其使用简单，视觉密码还可以在缺乏计算设备的特殊情况下提供应急方案。

对于数字图像或其他多媒体内容而言，由于其所具有的数据容量和临近像素的强相关性等内在特征，因此有必要设计专门的加密算法。图像加密机制主要是将原秘密图像转变为近似于随机的图像，其一般可分为两类：空域方法[3-8]和频域方法[9,10]。空域方法直接作用于原秘密图像，其主要分为两个阶段：乱序和掩码。通过上述处理原秘密图像的像素亮度值将会以伪随机序列的方式进行置换，同时还有可能与其他像素相混合以生成类似于随机图的共享图像。而频域方法是采用诸如快速傅里叶变换（FFT）、离散余弦变换（DCT）、离散小波变换（DWT）等算法将原秘密图像映射为一系列的频域系数，在此基础上通过逆变换将这些系数打乱以生成类似于随机图的共享图像。上

基金项目：国家自然科学基金青年基金资助项目（61502537，61602527；61403423）；湖南省科技计划重点项目（2015WK3006）；湖南省自然科学基金青年科学基金资助项目（2017JJ3416）；中国博士后科学基金资助项目（2017M612585）

作者简介：郭璠（1982-），女，讲师，博士，主要研究方向为图像处理、模式识别；刘丽珏（1973-），女（通信作者），副教授，博士，主要研究方向为模式识别、机器学习、智能计算（ljliu@csu.edu.cn）；刘熙尧（1987-），男，讲师，博士，主要研究方向为医学图像安全保护、数字内容安全保护、多媒体及医学图像基于内容的检索等；陈白帆（1979-），女，副教授，博士，主要研究方向为计算机视觉、机器学习、SLAM.

述两类算法的主要目的是生成不体现原秘密图像任何有用信息的共享图像。由于大多数的已有加密机制均是生成毫无意义的由黑白像素随机组成的二值图像，在公共渠道上传播此类图像容易引起怀疑而受到攻击，密码分析者会觉得这些看似随机的图像来自于重要信息的变换。例如，Usman 等人[11]提出的轻量级加密算法即是生成一幅无规则、无意义的加密图像。因此，密码分析者就很有可能会对诸如此类的随机图进行拦截，使其遭受到攻击。近年来，出现了许多密码分析攻击方法，一些上述提及的加密机制已被破解或被发现安全漏洞[12, 13]。为了降低密码分析攻击的机会，许多国内外学者开始研究让所生成的共享图像看起来不再随机，并具有一定意义的加密机制。例如，Naor 等人[1]提出了使用与原图无关的图像掩饰分享图像的（2, 2）门限密码视觉方案，使分享图像看起来具有一定的意义；文献[14]提出了一种利用掩饰图像隐藏秘密信息的算法，但是像素扩展比较严重；文献[15]给出了一种对原有(k, n)VSSS (visual secret sharing scheme)方案的扩充方案，即利用 n 幅掩盖图像形成 n 个子秘密；文献[16]结合半色调技术提出了一个具有掩盖图像的（2, 2）可视密码方案。Rozouvan[17]采用分形图像作为强密钥对图像进行加密处理，此图像加密方法不仅加密速度快，而且安全性高。郁滨团队还利用排列组合[18]、XOR 运算[19]、基本矩阵变换[20]等方法构造出了新的视觉密码方案。王洪君等人[21]提出了一种具有伪装图像像素不扩展的(2,2)视觉密码方案。该方案对秘密图像分享时等概率随机抽取基本矩阵的一列，然后将所得向量的每个元素分配给相应的分享图像。Yi 等人[22]将传统（2,2）视觉密码与类似壁纸效果的立体图相结合，所生成的灰度共享图可用于获取原秘密信息。2015 年，Bao 等人[23]提出了生成有意义共享图像的加密机制，该机制采用已有加密方法对原秘密图像进行加密，然后再将所生成的类似随机的共享图像嵌入到一个有意义的寄主图像中，由此再在公共渠道上传播就不会引起任何怀疑。在该方法的基础上，Kanso 等人[24]在 2017 年又提出一种无损视觉意义图像加密机制。等等这些方法都是采用具有一定意义的无关图像来掩饰分享图像，以使分享图像隐藏在有意义的伪装图像中，达到有效抵抗外来攻击的目的。

上述视觉密码与人类视觉系统关系密切，而对于人类视觉系统而言，三维立体图也因其独特的视觉体验而广受关注。对于三维立体图来说，其立体效果隐藏于一幅单独的二维图像中，观察者只有正确地将目光聚集之后才能观察到立体影像。早在 19 世纪，Wheatstone 等人[25, 26]就发现可以由两幅 2D 图像获取 3D 立体图像效果这一现象。Tyler 等人[27]设计了可直接用眼观看的单幅图像随机点立体图。Julesz 等人[28]发明了通过两幅稍有不同的图像实现随机点立体图的方法。在此之后，Thimbleby 等人[29]提出了一种生成立体图的对称算法。同时，Minh 等人[30]采用了新的方法来检测 3D 场景的隐藏面，并将该算法扩展至对运动对象的处理。2016 年，Yankelevsky 等人[31]研究了从三维立体图中感知深度信息的难易度与用于产生深度感的立体图基本模式选择之间的依赖关系。上述这些三维立体图生成方法，仅仅只能揭示某些三维图像信息，而未能与视觉密码相结合以同时隐藏秘密信息。

针对上述问题，本文所提方法受 Yi 等人方法[22]的启发，同时借鉴 Rozouvan[17]所提出的采用分形图像作为图像加密密钥的思路，通过一个（2, 2）视觉密码方案将视觉密码秘密恢复的简单性与立体图像的三维效果相结合，以生成两幅伪装成三维立体图像的共享图像，将此共享图像进行叠加等处理即可获得原秘密信息。实验结果表明：所提算法所获得的共享图像可被伪装成具有三维效果的立体图像，这就较好地解决了传统视觉密码中分享图为毫无意义的随机噪声图像，从而不易引起攻击者的怀疑，因而本文所提方案具有较好的安全性。

1　所提视觉密码方案

1.1　算法流程

所提（2,2）视觉密码方案的加解密流程如图 1 所示。从该图可以看出，包含秘密信息的秘密图像利用视觉密码加密后，首先会得到两幅原始共享图像。其中一幅共享图像可以看做秘密图像加密后得到的密文，而另一幅原始共享图像可看做为解密所需的密钥。为了避免由于共享图像无意义所引起的攻击者的怀疑，所提方案又利用相关深度图和纹理图分别生成了两幅三维立体图像，并将此立体图像分别与上述两幅原始共享图像相融合以获得最终的共享图像。由此，最终的两幅共享图像由于展示了三维立体信息而具有一定的意义，且密码破译者从任意一幅共享图中都无法得到秘密图像的任何信息，只有将两幅共享图像叠加在一起，才可以通过此组合共享图像获得解密后的图像，从而确保了方案的安全性。由此可见，所提方案的关键步骤主要为：原始共享图的生成、三维立体图像的生成、以及基于最终立体分享图像的（2,2）视觉密码加解密过程。

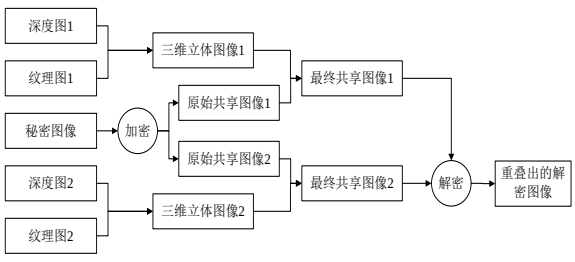


图 1　所提（2, 2）视觉密码方案的加解密流程示意图

1.2　原始共享图的生成

在（2,2）视觉密码方案中，由黑白两种像素所组成的原秘密图像中的每一个像素都被分享到两张共享图像中，在此原始共享图像中该像素被加密成两个子像素。上述黑、白像素加密规则如表 1 所示。

当原秘密图像中某像素为黑色像素时，在表 1 中随机选择对应于黑像素的两种像素组合的任意一种，在两张共享图像中都对应为一黑一白两子像素，共享图像重叠后得到的是两个黑色子像素；而当原秘密图像中的某像素为白色像素时，在表 1

中随机选择对应于白色像素的两种像素组合中的任意一种，在两张共享图像中都对应为一黑一白两子像素，共享图像重叠后仍为一黑一白两子像素。因此，当原秘密图像中的像素都用这种方法加密到共享图像中时，重叠后可通过视觉系统辨认出原秘密图像中的黑白像素。此外，由于原秘密图像中的一个像素被扩展成两个子像素，所以共享图像的面积是原图像的两倍。同时，由于随机性，原秘密图像中的黑或白像素在共享图像中都被加密成一黑一白两个子像素，因而从一张共享图像中得不到原秘密图像的任何信息，只有当两张共享图像对齐后重叠才能得出原始图像中的信息。具体而言，上述视觉密码的加解密过程可表示为：首先构造两个矩阵集合：

$$C_0=\left\{\begin{bmatrix}0&1\\0&1\end{bmatrix},\begin{bmatrix}1&0\\1&0\end{bmatrix}\right\},\ C_1=\left\{\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}0&1\\1&0\end{bmatrix}\right\} \tag{1}$$

其中的元素值 0、1 分别代表白色和黑色。C_0 的矩阵元素表示对应像素在第 i 张共享图像中的第 j 个子像素的颜色。将矩阵中第 j 列的所有元素作“或”运算，得到的结果是重叠后共享图像中第 j 个子像素的颜色。如果原图像中像素为白色，则从 C_0 中随机挑选出一个矩阵；如果是黑色，则从 C_1 中随机挑选出一个矩阵。矩阵的第 i 行代表原始像素在第 i 张共享图像中对应位置子像素的颜色。由此按序处理原秘密图像的每一个像素即可得到两幅共享图像。图 2 即为（2, 2）视觉密码方案的共享图像生成示例。

表 1　(2, 2)视觉密码方案的加密规则

像素	概率	共享图像 1	共享图像 2	共享图像 1、2 叠加
□	P=1/2			
	P=1/2			
■	P=1/2			
	P=1/2			

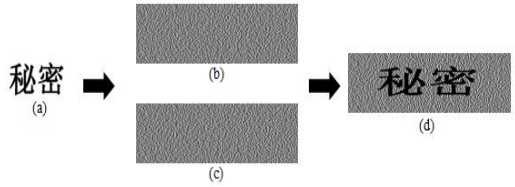


图 2　(2, 2）视觉密码方案的共享图像生成示例. (a)为原秘密图像. (b)和(c)为生成的两幅共享图像. (d)为叠加上述两幅共享图像所得到的解密图像。

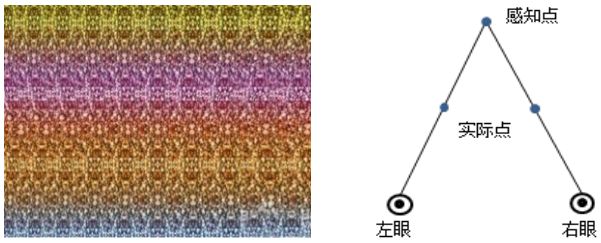
1.3　三维立体图像的生成

三维立体图像提供了一种通过双目视觉所揭示的深度感知原理来描述 3D 物体的方法。传统的立体图需要人们正确聚焦目光，大脑和双眼整合观察图像或物体时产生至少两条目光束。若某一条目光束未同时成像，则会产生视觉失调。之所以将分散人们注意力的二维图像元素引入立体图像中，主要是因为二维图像尽管有可能引起视觉失调，但其也会让简单的立体图像变得妙趣横生，同时所产生的立体效果还能让原本平面的二维图像凸显出来，这种互补的视觉感知会让所呈现的三维立体效果更加明显。观看立体图时，最好采用平行视线或分散视线观察。图 3 即为一幅三维立体图示例及观看立体图所惯常采用的平行视线示意图，采用此平行视线去如图 3(a)所示的三维立体图可观看到一组数字。

本文所涉及的三维立体图像主要由一系列在水平方向上重复的细窄图案构成，这些图案之间存在细微的差别。观察此类立体图的关键是视差。在立体图中，视差是指构成立体图的重复元素之间的距离。图 4 即给出了针对三维立体图像的相关几何描述及各主要参数之间的相互关系。由该图即可推知场景物体的景深 z 与三维立体图中某点相关的像素对距离 s 之间的关系，此关系可表示如下：

$$s=\frac{(1-uz)}{2-uz}\cdot E \tag{2}$$

其中：s 为某一点的立体分割距离，z 为从如图 4 所示的较远平面至较近平面的向量，其取值范围为[0, 1]。E 表示两眼之间的距离，u 为一固定常数，其值被设置为 1/3。由上式可知，较小的距离 s 值会产生较小的 z 值，并对应采用平行视线所观察到的离眼较近的虚拟点。实验中观看者对 z 值的感知取决于所输入的深度图，深度图的像素值越大（越趋近于 255），对应的 s 值和 z 值越大，其所生成的三维立体图的纵深感越强。



(a)　　(b)

图 3　三维立体图示例及平行视线示意图.
(a)为三维立体图示例. (b)为平行视线示意图.

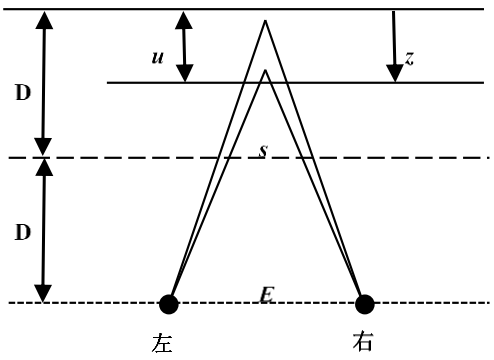
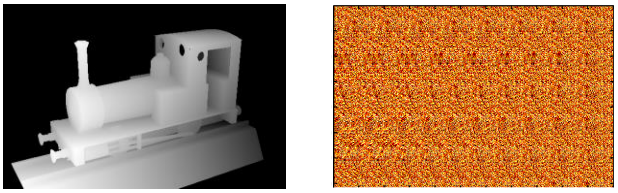


图 4　三维立体图像的几何关系描述.

1.4　基于立体分享图像的加解密方案

视觉密码是一种依靠视觉系统解密的秘密共享技术，所提基于立体分享图像的加解密方案主要将上述传统视觉密码方案与三维立体图像的生成算法相结合。为此，所提方法将立体图

像的 3D 信息与秘密共享机制的共享图像相融合，同时确保所复原图像的对比度以使解密图像中的秘密信息得以突显。由于上述方法得到的每一共享图均为一立体图，密码破译者从任意一张三维立体共享图像中都无法得到秘密图像的任何信息，因而具有较好的安全性。其中，所提（2, 2）视觉密码方案对于原始共享图的求取结果示例如图 2 所示，而对于三维立体图的生成采用的则是由国外学者 Geselowitz 提出的随机点立体图算法[32]。该立体图生成算法在输入深度图的情况下能自动快速、有效地生成相关立体图，这里的深度图是一幅能代表景深距离的灰度图，其像素值越大，表示距离越近。反之，像素值越小，表示距离越远。图 5 即给出了采用此随机点立体图算法所生成的立体图效果。其中图 5(a)为深度图，图 5(b)为采用随机点立体图算法所生成的三维立体图。



(a)　　(b)

图 5　三维立体图的生成示例.

在此基础上，所提（2，2）视觉密码方案依据图 1 所示的加解密流程，将所生成的两幅原始共享图像与两幅采用上述算法得到的三维立体图进行融合，得到用于解密的最终共享图像。上述融合过程所获得的两幅最终共享图像 S_f^k 可按下式求取得到：

$$S_f^k(x,y)=w_1\cdot S_o^k(x,y)+w_2\cdot A_g^k(x,y) \tag{3}$$

其中：$S_o^k(x,y)$ 和 $A_g^k(x,y)$ 分别表示原始共享图和三维立体图，k 为图像编号，$k\in\{1,2\}$。最终共享图像 S_f^k 由上述两类图像线性加权求得，w_1 和 w_2 分别为两权重值用于调控原始共享图与三维立体图在最终共享图像中的比例，且 $w_2=1-w_1$。由此，所获得的单幅最终共享图像即将信息伪装成立体图以展现 3D 立体场景，从而避免引起密码攻击者的怀疑，而通过对两幅最终共享图像进行相关处理即可获得解密后的秘密信息。此解密算法可实现如下：

算法输入：一幅原秘密图像、两幅纹理图像、两幅深度图像

算法输出：两幅最终分享图像、一幅秘密恢复图像

a）由两幅纹理图和两幅深度图分别求取其对应的两幅三维立体图，同时由一幅原始秘密图像求取其对应的两幅原始共享图像；

b）将上述两幅三维立体图和两幅原始共享图像分别进行融合处理以得到两幅最终共享图；

c）对以上求得的两幅最终共享图进行异或操作以得到原秘密信息恢复图像；

d）将原秘密信息恢复图像转换为灰度图像，并对其进行二值化处理；

e）求取此二值恢复图像的 Sobel 梯度图像，并通过不同的颜色显示将恢复得到的明文从背景中突显出来。上述处理过程可表示为：

$$S(x,y)=S_f^1(x,y)\oplus S_f^2(x,y) \tag{4}$$

上式中 $S_f^1(x,y)$ 和 $S_f^2(x,y)$ 分别表示两幅最终共享图像，$\oplus$ 为异或处理，S 为原秘密信息恢复图像。然后对此图像 S 进行灰度化和二值化处理，得到二值图像 S_{bw}。再求取此二值图像 S_{bw} 的 Sobel 梯度矩阵，目的是加强图像中所恢复秘密信息的边缘，从而使恢复的秘密信息得以突显。此操作所用的 Sobel 梯度算子分别为

$$S_x=\begin{bmatrix}1&0&-1\\2&0&-2\\1&0&-1\end{bmatrix}\quad S_y=\begin{bmatrix}1&2&1\\0&0&0\\-1&-2&-1\end{bmatrix} \tag{5}$$

将上述梯度算子与二值图像 S_{bw} 作卷积，即可分别得到横向及纵向的亮度差分近似值 G_x 和 G_y。由此，该 Sobel 梯度图像各像素的灰度值 G 可按照以下公式，通过其横向及纵向的灰度值求得：

$$G=\sqrt{G_x^2+G_y^2} \tag{6}$$

在此基础上，可将上述图像 G 的灰度数值按大小转换为不同颜色，以便在坐标轴对应位置处以这种颜色染色，从而通过不同的颜色显示来突显图像背景中所恢复的秘密信息。

2　实验结果与分析

所提算法的有效性和实时性，采用 MATLAB 在 Pentium(R) D，3.00 GHz，2 GB 内存的 PC 机上构建了大量的（2, 2）视觉密码。以下将分别从算法的实现效果、参数调节、以及运算时间三个方面对所提算法进行分析。

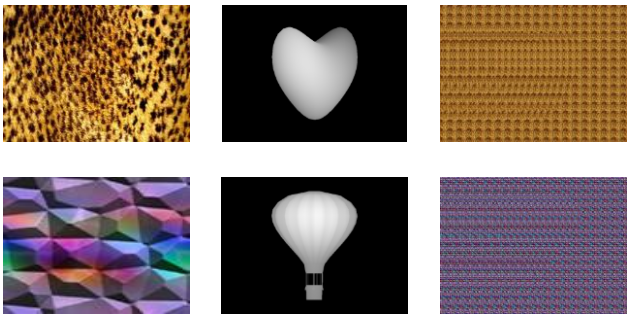
2.1　实现效果

实验选取了大量原秘密图像、纹理图和深度图，利用纹理图和深度图即可采用前述随机点立体图算法[31]生成三维立体图。然后，将此立体图像与由原秘密图像获得的原始共享图像相融合以获得最终共享图像。最后，对最终共享图像进行相关处理以获取恢复后的秘密信息。图 6 即为利用纹理图和深度图生成立体图像的结果示例，观看者可从图 6(c)中看到具有 3D 效果的心形图案和热气球图案。

图 7 为由一幅原秘密图像生成原始共享图像的结果示例。将图 6(c)所示的两幅立体图像分别与图 7(b)和图 7(c)所示的原始共享图像相融合即可获取最终的秘密信息。此秘密信息获取过程如图 8 所示，其中图 8(a)和图 8(b)分别为通过融合处理所获得的最终共享图，图 8(c)为对两幅最终共享图像进行前述相关处理后的秘密信息恢复结果。

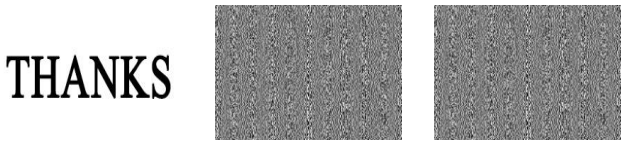
由图 7 和 8 可知，原秘密图像生成的原始共享图像是由黑、白两种像素所组成的二值图像，由于图像本身无任何意义，因此极易受到攻击。而由所提算法得到的最终共享图像由于其将

信息伪装承立体图，展现出的是 3D 立体场景，具有一定的意义，因而可有效避免引起密码攻击者的怀疑。同时，将最终共享图像进行相关处理后又可清晰地恢复原秘密信息，复原结果如图 8(c)所示。因此，相比于传统的视觉秘密方案，所提分享图像为有意义图像的方案具有更好的安全性。



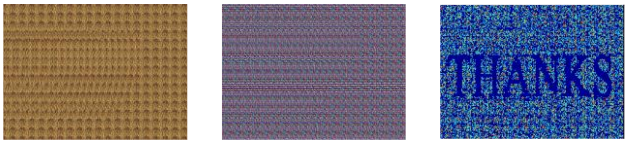
(a)纹理图　　(b) 深度图　　(c)三维立体图

图 6　利用纹理图和深度图生成立体图的结果示例.



(a) 原秘密图像　　(b) 原始共享图　　(c) 原始共享图

图 7　由原秘密图像生成原始共享图像的结果示例



(a)最终共享图　　(b) 最终共享图　　(c) 复原后的秘密信息

图 8　秘密信息恢复结果示例

2.2　参数调节

所提视觉密码方案所涉及的主要参数为权重值 w_1 和 w_2，为了确定最佳的权重值，采用不同权重值组合来检验最终的秘密信息复原效果。实验中权重参数 w_1 的取值范围为[0.1，0.9]，数值间隔为 0.1，图 9 即为针对图 7(a)所示的原秘密图像在不同权重值组合下的最终共享图生成结果与秘密信息复原效果示例。其中该图中的第一和第二行分别为不同权值下的最终共享图效果，第三行为不同情况下的秘密信息复原效果。由该图可知，当 w_1 = 0.2 时，尽管共享图的 3D 效果显著，但复原结果中的秘密信息却不明显。而当 w_1 = 0.5 时，尽管复原后的秘密信息较为清晰，但其共享图像的 3D 效果却难以体现。由此可推知：随着 w_1 值的增大，由于原始共享图的比重越来越大，因此最终秘密信息的复原效果也越好，但由此带来的问题是共享图的 3D 效果变得越来越不明显，因此对所提方案进行参数调节的关键在于在确保 3D 效果与突显秘密信息间寻找一个平衡点。通过大量实验证明：当 $w_1 = 0.3$（$w_2 = 0.7$）时，可在获得较好秘密信息复原结果的同时，使共享图像的三维立体效果得以较好保留。

(a) w1=0.2　　(b) w1=0.3　　(c) w1=0.4　　(d) w1=0.5

图 9　不同权重值组合下的秘密信息复原效果

2.3　实现效果

为了有效衡量所提视觉密码方法的有效性，本文选取了轻量级图像加密算法[11]、基于分形图方式的图像加密算法[17]、Yi 方法[22]与本文方法进行定性评估与定量对比。选择上述算法作为对比算法的原因是：轻量级图像加密算法是生成随机性加密图像的代表方法之一，分形图加密算法采用“分形图”作为加密密钥的思想为本文方法提供了重要借鉴，Yi 方法与本文所提算法的大体思路相近。因此，选取上述几种与本文方法类似的方案进行对比，能更好地检验本方法相比于已有方法的性能优劣。

图 10 即给出了各方法的加、解密效果示例。从该图可以看出，轻量级图像加密算法[11]尽管具有较好的解密效果，但其仍具有大多数已有加密机制所存在的共性问题，即所生成的加密结果为由黑白像素随机组成的二值图像，由于此图像无任何意义，因此在公共渠道上传播该图像时容易引起怀疑而受到攻击。本文所提方法所获得的共享图像被伪装成具有三维效果的立体图像，相比于大多数已有方法所获得的随机噪声加密图像，本文方法所求取的共享图不易引起攻击者的怀疑，因而具有较好的安全性。

基于分形图方式的图像加密算法[17]将分形图作为加密密钥，利用分形图的随机性对原输入秘密图像进行加密处理，所获得的加密图像在较好地隐藏秘密信息的同时，具有一定的艺术美感。此外，解密结果忠实地还原了原秘密信息。

Yi 方法[22]将视觉密码与立体图相结合，所生成的灰度共享图可用于复原秘密信息。本文所提方法与 Yi 方法类似，所求得的共享图具有较为逼真的三维立体效果。但 Yi 方法所求得的共享图为灰度图，而本文方法由于采用不同的立体图生成方法可获得彩色的共享图。由于彩色图像在视觉效果上具有丰富的色彩，因而对秘密信息具有更好的伪装效果。这些彩色共享图即便被截获，也只是看似普通的三维立体图，不会让人引起这些图像是加密图像的怀疑，但原秘密信息已被较好地隐藏在此三维立体共享图中，因此秘密信息在传输过程中不易受到攻击，具有较好的安全性。同时，通过彩色共享图的叠加，原秘密信

息也可得到较好的恢复。各算法的相关加、解密效果如图 10 所示。

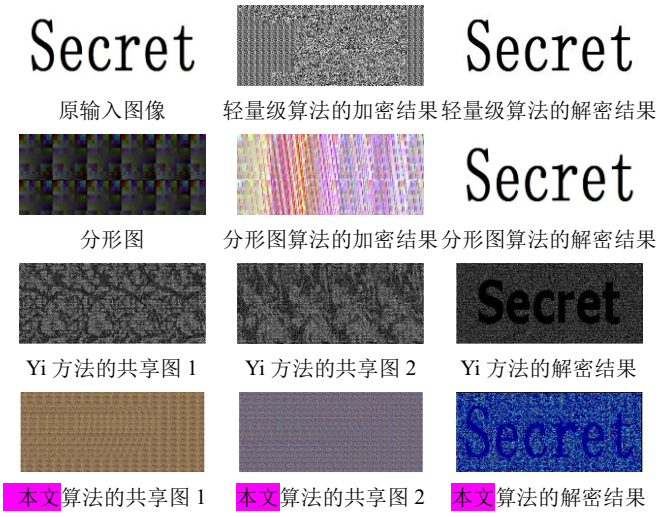


图 10　各方法的加解密效果对比

第一行:轻量级图像加密算法的实现效果示例；第二行:基于棋盘覆盖方式的图像加密算法的实现效果示例；第三行:Yi 方法的实现效果示例；第四行:本文算法的实现效果示例.

此外，为了客观、定量地评价上述各方法，首先将本文算法的解密图像转换为与其他方法解密结果一致的白底黑字显示效果。该步骤的具体做法为：先将本文方法结果和原秘密图像都转换为二值图，然后针对图像中每一个像素点判断其值在上述两幅图像中是否均为黑色，若均为黑色则保留此黑色像素点，否则将此像素的颜色变为白色。在此基础上，采用峰值信噪比（PSNR）和结构相似度（SSIM）[33]这两个量化指标对 158 幅秘密图像在各种算法下的解密效果进行衡量。对于一幅 M×N 的灰度图像 $f(i,j)$，其对应的峰值信噪比测度（PSNR）定义如下：

$$\mathrm{PSNR}=10\lg\left\{\frac{255^2}{\mathrm{MSE}}\right\} \tag{7}$$

$$\mathrm{MSE}=\frac{1}{\mathrm{MN}}\sum_{i=1}^{\mathrm{M}}\sum_{i=1}^{\mathrm{N}}\left[f(i,j)-D(i,j)\right]^2 \tag{8}$$

其中：$f(i,j)$和 $D(i,j)$分别为原秘密图像和解密图像。若令 x 表示原秘密图像，y 表示各方法的解密图像，则上述两图的结构相似度（SSIM）可定义为

$$\mathrm{SSIM}(x,y)=\frac{\left(2u_xu_y+c_1\right)\left(2\sigma_{xy}+c_2\right)}{\left(u_x^2+u_y^2+c_1\right)\left(\sigma_x^2+\sigma_y^2+c_2\right)} \tag{9}$$

其中：u_x 是 x 的平均值，u_y 是 y 的平均值，σ_x^2 是 x 的方差，σ_y^2 是 y 的方差，σ_{xy} 是 x 和 y 的协方差。$c_1=\left(k_1L\right)^2$，$c_2=\left(k_2L\right)^2$ 是用来维持稳定的常数。L 是像素值的动态范围。$k_1=0.01$，$k_1=0.03$。结构相似性的范围为-1 到 1。对于峰值信噪比（PSNR）而言，其值越大，说明解密复原效果越好；对于结构相似度（SSIM），其值越接近于 1，说明解密效果越好。当解密图像与原秘密图像完全一样时，SSIM 的值等于 1。表 2 即为采用上述各算法对 158 幅秘密图像进行 PSNR、SSIM 指标评估的平均统计结果。

由该表可知，基于分形图方式的图像加密算法的 PSNR 值最大，且其 SSIM 值也最接近于 1，说明此算法的秘密信息恢复效果最好，轻量级图像加密算法次之。Yi 方法和本文方法在 PSNR 指标统计结果上与上述两种方法区别较大，究其原因主要是因为 Yi 方法和本文方法的解密结果主要是通过秘密信息与背景图像的对比度来展现，而其他方法则是尽量忠实还原输入的原秘密图像，因此 Yi 方法和本文方法与其他两种方法在秘密信息显示方式上存在本质不同。尽管如此，本文方法的 SSIM 指标统计结果与另外三种方法的 SSIM 指标结果相差不大，说明本文方法与其他三种方法一样都能较好地恢复原秘密图像的结构信息，该结论在图 10 的示例中也得到了验证。因此，本文方法作为一种新的（2, 2）视觉密码方案可有效隐藏和获取秘密信息，并将此秘密信息以人眼易于分辨的方式呈现出来。

表 2　各算法的相关评价指标的平均统计结果

方法	PSNR	SSIM
轻量级图像加密算法[11]	28.1226	0.9997
基于分形图方式的图像加密算法[17]	38.3118	0.9999
Yi 方法[22]	14.2683	0.9947
本文方法	13.7120	0.9939

2.4　运算时间

算法的运算时间也是定量衡量算法性能的一个重要指标。在 MATLAB 环境下，对于一幅大小为 260×127 的原秘密图像，原始共享图的生成需要 0.51 s，三维立体图的生成需要 0.19 s，最终共享图的求取及秘密信息的恢复共需 0.96 s，因此本文所提方案的整体处理时间约为 1.7 s。此外，本文还对各加密方案在不同图像大小下的运算时间进行了统计，统计结果如表 3 所示。从该表可以看出：随着原秘密图像的增大，各加密方案的整体运算时间均有所增加。对于同样大小的图像，各加密方案的运算时间按升序排列依次为：分形图算法、本文方法、Yi 方法、轻量级算法。轻量级算法为 64 位的分组密码，其需要 64 位的密钥来加密图像数据，因此运算时间相对较长。分形图算法采用“分形图”来随机生成强密钥，同时提供相关机制来控制密钥的强度，因此具有相对较快的运算速度。Yi 算法和本文方法在求取原始共享图的过程中，原秘密图像中的一个像素均会按照表 1 所示规则被扩展成两个像素，所以求取的原始共享图像的面积也会是原秘密图像的两倍，由此即造成了算法时间上的增多。但是相比于已有的大多数加密方案，本文方法仍具有较快的运算速度，如表 3 所示。

3　结束语

视觉密码将秘密共享和数字图像处理结合起来，形成了一个新的研究热点。尽管目前国内外学者对传统（2, 2）视觉密码方案进行了广泛研究，但是由于传统方案所求取的共享图像为

毫无意义的二值图像，这就很容易引起攻击者的怀疑，从而受到安全威胁。因此，本文主要针对（2, 2）视觉密码方案的安全性问题展开研究，其主要贡献与创新点为在构建三维立体图像的基础上，设计并实现了一个共享图像为有意义图像的（2,2）视觉密码方案，以将分享图像伪装成有意义的三维立体分享图像。与其他已有方法的对比实验结果表明：本文所提方案简单可行，因此可广泛应用于身份认证、电子投票、消费电子、信息隐藏等领域。但本文算法仍有待进一步完善，如所提方案仅适用于原秘密图像为黑白二值图像的情况，无法对灰度图或彩色图进行处理。另外，将本文提出的适用于（2,2）门限的方法扩展到（k, n）等一般门限结构也有待进一步研究。尽管如此，所提方案仍不失为解决视觉密码安全性问题的一种新的思路和处理途径。同时，相信本文所提出的解决共享图像安全性问题的信息伪装思想将会有助于解决密码学与图像处理领域的其他问题。

表 3　各加密方案对不同大小图像的整体运算时间

加密方法	不同图像大小下的运算时间(s)			
	300×200	600×400	1000×800	2048×1024
轻量级算法	68.29	68.43	72.10	73.05
分形图算法	2.76	2.80	3.15	3.92
Yi 方法	2.05	4.17	11.92	26.53
本文方法	1.61	3.65	10.07	24.98

参考文献：

[1] Naor M. , Shamir A. Visual cryptography [C]// Advances in Cryptography: EUROVRYPT. Berlin, Heidelberg: Springer, 1995: 1-12

[2] 郁滨, 付正欣, 沈刚等. 视觉密码 [M]. 合肥: 中国科学技术大学出版社. 2014: 18-25

[3] Zhang Y. Q. , Wang X. Y. A new image encryption algorithm based on non-adjacent coupled map lattices [J]. Applied Soft Computing, 2015, 26: 10-20

[4] Kanso A. , Ghebleh M. An efficient and robust image encryption scheme for medical applications [J]. Communications in Nonlinear Science & Numerical Simulation, 2015, 24 (1–3): 98-116

[5] Wang X. , Liu L. , Zhang Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique [J]. Optics & Lasers in Engineering, 2015, 66 (66): 10-18

[6] Chen J. X. , Zhu Z. L. , Fu C. , et al. An efficient image encryption scheme using gray code based permutation approach [J]. Optics & Lasers in Engineering, 2015, 67: 191-204

[7] Hua Z. , Zhou Y. , Pun C. M. , et al. 2D sine logistic modulation map for image encryption [J]. Information Sciences, 2015, 297: 80-94

[8] Liu W. , Sun K. , Zhu C. A fast image encryption algorithm based on chaotic map [J]. Optics & Lasers in Engineering, 2016, 84: 26-36

[9] Luo Y. , Du M. , Liu J. A symmetrical image encryption scheme in wavelet and time domain [J]. Communications in Nonlinear Science & Numerical Simulation, 2015, 20 (2): 447–460

[10] Liu Z. , Xu L, Liu T. , et al. Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains [J]. Optics Communications, 2011, 284 (1): 123-128

[11] Usman M. , Ahmedy I. , Imran Aslamy M. , et al. SIT: A lightweight encryption algorithm for secure internet of things [J]. International Journal of Advanced Computer Science and Applications, 2017, 8 (1): 402-411

[12] Li C. , Li S. , Asim M, . et al. On the security defects of an image encryption scheme [J]. Image & Vision Computing, 2009, 27 (9): 1371-1381

[13] Zhang Y. Q. , Wang X. Y. Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation [J]. Nonlinear Dynamics, 2014, 77 (3): 687-698

[14] 夏光升, 袁中兰, 杨义先等. 一种新的图像单幅可视隐藏算法 [J]. 北京邮电大学学报, 2002, 25 (3): 12-16

[15] 甘明, 甘志, 陈克非. 具有掩盖图像的可视秘密共享方案 [J]. 计算机应用与软件, 2005, 22 (7): 1-2

[16] 牛冬梅. 具有掩盖图像的 (2, 2) 可视密码方案 [J]. 通信技术, 2009, 42 (7): 82-84

[17] Rozouvan V. Modulo image encryption with fractal keys [J]. Optics and Lasers in Engineering, 2009, 47: 1-6

[18] 陈勤, 彭文芳, 徐坤, 等. 基于排列组合的可防欺骗视觉密码方案 [J]. 计算机应用研究, 2011, 28 (1): 318-321

[19] 付正欣, 郁滨. 基于 XOR 运算的多秘密视觉密码 [J]. 计算机应用研究, 2011, 28 (2): 708-710

[20] Bonis A, Santis A. Randomness in secret sharing and visual cryptography schemes [J]. Theoretical Computer Science, 2004, 314 (3): 351-374

[21] 王洪君, 鲁晓颖, 牟晓丽, 等. 具有伪装图像像素不扩展的 (2, 2) 视觉密码方案 [J]. 吉林大学学报: 信息科学版, 2013, 31 (3): 297-301

[22] Yi F. , Wang D S. , Dai Y Q. Visual Secret Sharing Scheme with Autostereogram [J]. DBLP computer science bibliography, 2006, 12: 1-19

[23] Bao L. , Zhou Y. Image encryption: generating visually meaningful encrypted images [J]. Information Sciences, 2015, 324: 197–207

[24] Kanso A. , Ghebleh M. An algorithm for encryption of secret images into meaningful images [J]. Optics and Lasers in Engineering. 2017, 90: 196-208

[25] Wheastone C. Contributions to the physiology of vision, Part I: On some Remarkable and Hitherto Unobserved, Phenomena of Binocular Vision [J]. Journal of the Franklin Institute. 1838, 128: 371-394.

[26] Wheastone C. Contributions to the physiology of vision. Part II: On some remarkable, and hitherto unobserved, phenomena of binocular vision. A Bakerian lecture [J]. Journal of the Franklin Institute. 1852, 4 (3): 504-523.

[27] Tyler C. W, Clarke M. B. The autostereogram [J]. SPIE Stereoscopic Displays and Applications, 1990, 1256: 182-196

[28] Julesz B. Binocular Depth Perception of Computer Generated Patterns [J]. The Bell System Technical Journal, 1960, 39: 1125-1162

[29] Harold W, Thimbleby, Stuart Inglis, et al. Displaying 3D images: algorithms for single-image random-dot stereograms [J]. Computer. 1994, 27 (10): 38-

48.

[30] Minh S. T. , Fazekas K, Gschwindt A. The presentation of three-dimensional objects with single image stereogram [J]. Transactions on Instrumentation and Measurement, 2002, 51 (5): 955-961

[31] Yankelevsky Y. , Shvartz I. , Avraham T. , et al. Depth perception in autostereograms: 1//f noise is best [J]. Journal of the Optical Society of America A: Optics and Image Science, and Vision. 2016, 33 (2): 149-159

[32] Geselowitz L. The AbSIRD project: To create real-time SIRDs [EB//OL]. (2014-1-15) [2016-12-23]

[33] http://www. leweyg. com/download/SIRD/AbSIRD/essay. html

[34] Wang Z. , Bovik A. C. , Sheikh H. R. , et al. Image quality assessment: From error visibility to structural similarity [J]. IEEE Trans on Image Processing, 2004, 13 (4): 600-612.