一种完全恢复的(2,*n*)彩色视觉密码方案

张先环[1]，付正欣[1]，欧阳旦[2]，郁滨[1]
(1. 信息工程大学，河南 郑州 450000；2. 空军电子技术研究所，北京 100089)

摘要：基于异或运算，结合计算机显示技术的特点，*提出了一种完全恢复的(2,n)彩色视觉密码方案。该方案以构造行向量*$V_1,V_2,\cdots,V_n$*为基础，设计了彩色秘密图像的分享算法，*通过共享份异或并对得到的图像进行处理，完成秘密图像的恢复。实验结果表明，在保留视觉密码秘密恢复简单特点的基础上，方案以较低的像素扩展度为代价，能够实现秘密图像的完全恢复，每个参与者只需携带一个共享份，降低了共享份的管理难度。

关键词：视觉密码；彩色视觉密码；(2, *n*)；异或运算；完全恢复
中图分类号：TP309.7 文献标识码：A 文章编号：1004-731X (2016) 06-1439-06

Perfect Recovery (2,*n*) Color Visual Cryptography Scheme

Zhang Xianhuan[1], *Fu Zhengxin*[1], *Ouyang Dan*[2], *Yu Bin*[1]
(1. Information Engineering University, Zhengzhou 450000, China; 2. Institute of Electronic Technology, Beijing 100089, China)

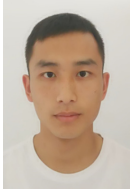
Abstract: Based on XOR operation and combining the characteristic of computer display technology, a perfect recovery (2,*n*) color visual cryptography scheme was proposed. Sharing algorithm of color secret image was designed on the basis of constructing row vectors $V_1,V_2,\cdots,V_n$. Through computing shares by XOR operation and dealing with recovery image, the secret image was recovered. The experimental results show that the scheme on the basis of keeping the simplicity in the reconstruction phase of visual cryptography can realize the secret image perfect recovery with low pixel expansion for price. Each participant only needs to carry a share which reduces the difficulty of share management.

Keywords: visual cryptography; color visual cryptography; (2,*n*); XOR operation; perfect recovery

引言

视觉密码[1](visual cryptography)由 Naor 和 Shamir 在 1994 年欧洲密码学年会上首次提出，将秘密共享和数字图像相结合，具有秘密恢复简单、安全性好、信息容量大的特点，特定场景中具有重要的应用价值。Naor 和 Shamir 的方案只能对二值图片进行分享，称为二值视觉密码方案。彩色图像所呈现的色彩接近于真实的自然界，相比二值图片更加美观且具有更加丰富的图像信息，对彩色图像进行加密的视觉密码方案称为彩色视觉密码方案(Color Visual Cryptography Scheme，CVCS)。

Verheul 等[2]首次提出彩色视觉密码方案，像素扩展度 $m=c^{n-1}$，其需要一个特殊的假设：不同颜色的像素进行叠加的结果是黑色像素。实际上，不同颜色的像素进行叠加，会得到另外一种颜色的像素。为了解决假设不切合实际的问题，Verheul 等基于有限域，对该方案进行了拓展，像素扩展度 $m=c^n$，但依然存在像素扩展度巨大的问题。Stelvio 等[3]和 Cimato 等[4]对 Verheul 等的方案进行了改进，改善了对比度和像素扩展度，分别得到了



收稿日期：2015-05-27 修回日期：2015-07-28；
基金项目：信息保障技术重点实验室开放基金(KJ-13-107)；
作者简介：张先环(1989-)，男，四川绵阳，硕士生，研究方向为视觉密码；付正欣(1986-)，男，山东曹县，讲师，研究方向为视觉密码。

对比度 $\alpha=\begin{cases}1/(c\bullet 2^{n-1}-1), \text{if } n\ odd\\ 1/(c\bullet 2^{n-1}-c+1), \text{if } n\ even\end{cases}$ 和像素扩展度 $m=c\binom{n}{k}2^{k-2}$ 的结果。为了降低方案的像素扩展度，Hiroki 等[5]基于增色模型，通过加法叠加算子 *add* 来恢复秘密图像，得到的方案像素扩展度较小，但该方案秘密图像中的颜色必须为特定组合，不能分享颜色较丰富的彩色图像。

Hou 等[6]采用半色调技术，以降低对比度为代价，构造能够分享彩色图像的 CVCS，但恢复图像的效果较差。为了解决 CVCS 中像素扩展度较大的问题，Chen 等[7]基于随机栅格设计的(n,n)彩色视觉密码方案，像素扩展度 $m=1$，对比度 $a=1/2^{n-1}$，恢复图像视觉效果不佳。文献[2-7]中的方案以透明胶片作为共享份载体，透明胶片的携带、保存十分不便。随着信息技术的进步，基于透明胶片构造的视觉密码方案在像素扩展度、对比度等参数优化上，特别对于彩色图像，受到明显的限制，阻碍了彩色视觉密码的深入研究及应用。

Lukac 等[8-10]以计算机作为共享份载体，将每个彩色像素用 24 位二进制进行表示，对每位采用二值视觉密码进行分享，构造出能够完全恢复的彩色视觉密码方案，然而该类方案像素扩展度较大，需要占用系统较大的存储空间。Wang 等[11]基于异或运算，构造了 $(n,n)-CVCS$，像素扩展度 $m=1$，能够完全恢复秘密图像。Dong 等[12]利用文献[11]中$(2,n)$二值视觉密码方案的构造方法，构造了 $(2,n)-CVCS$。该方案每个参与者需要携带 $r(r=1,2,\cdots)$ 个共享份，对比度 $\alpha=(1-(1/2)^r)^{24}$，参与者携带的共享份越多，恢复图像效果越好，但不方便管理且不能实现秘密图像的完全恢复。Chao 等[13]构造了一种 $(k,n)-CVCS$，通过设计共享份分配矩阵，方案像素扩展度 $m=(2\times(n-k+1))/n$。在秘密恢复过程中，需要额外的共享份分配矩阵参与计算，而且需要进行多次异或运算，秘密恢复过程较复杂。Sachin 等[14]通过概率型视觉密码的设计思想进行秘密分享，得到的方案没有像素扩展，但对比度很低，为 $\alpha=1/(n-1)^2$。

综上所述，本文在每个参与者携带一个共享份的前提下，利用计算机显示技术，通过构造行向量 $V_1,V_2,\cdots,V_n$，设计一个完全恢复的$(2,\ n)$彩色视觉密码方案，并对其有效性进行证明，为彩色图像的秘密共享问题提供了新的解决思路。

1 方案设计

为方便描述，本文中所用到的符号及其含义如表 1 所示。

表 1 本文中所用符号含义表

符号	含义
$P=\{1,2,\cdots,n\}$	n 个参与者的集合
$\oplus$	异或运算
S	彩色秘密图像
m	像素扩展度
$s(i,j)$	S 中位置 (i,j) 像素的颜色值
$S_1,S_2,\cdots,S_n$	n 个共享份
$s_t(i,j)$	共享份 S_t 中位置 (i,j) 像素的颜色值
$prob(A)$	事件 A 发生的概率
V	元素为像素颜色值的行向量
$G(V,c)$	V 中颜色值为 c 的元素个数

在计算机中，有多种颜色模型。为方便描述，本文只考虑计算机最常用的 RGB 模型，即用一个 24 位二进制数表示一个彩色像素的颜色值。本文中用 0 表示 24 位全为 0 的二进制数。

定义 1 两个彩色像素进行异或运算指各像素的颜色值按位进行异或运算。

定义 2 两个共享份进行异或运算指共享份中位置相同的像素其颜色值进行异或运算。

1.1 秘密分享算法

秘密分享流程图如图 1 所示，具体步骤如下。

输入：大小为 $a\times b$ 的秘密图像 S

输出：大小为 $a\times mb$ 的共享份 $S_1,S_2,\cdots,S_n$

步骤 1. 令 $i=1$，i 表示行计数器；

步骤 2. 令 $j=1$，j 表示列计数器；

步骤 3. 随机生成 m 个 24 位二进制数 $c_1,c_2,\cdots,c_m$；

步骤 4. 计算 $c_1'=s(i,j)\oplus c_1$，$c_2'=s(i,j)\oplus c_2,\ldots,$

$c_m' = s(i,j) \oplus c_m$；

步骤 5. 构造 n 个行向量 $V_1, V_2, \cdots, V_n$，行向量 $V_1, V_2, \cdots, V_n$ 的具体构造方式在下节给出；

步骤 6. 令 $s_t(i,(m\times j-m+1)\sim(m\times j)) = V_t(t=1,2,\cdots,n)$，表示将行向量 V_t 中的 m 个元素值赋给第 t 个共享份第 i 行第 $m\times j-m+1$ 到第 $m\times j$ 个像素；

步骤 7. 令 $j=j+1$，若 $j \leqslant b$，则转至步骤 3；否则转至步骤 8；

步骤 8. 令 $i=i+1$，若 $i \leqslant a$，则转至步骤 2；否则分享流程结束。

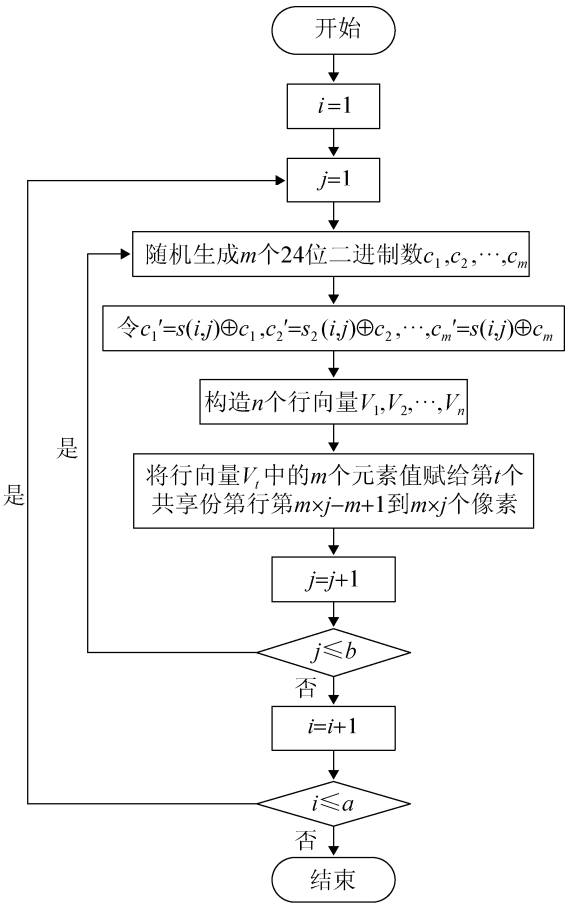


图 1 秘密图像分享流程图

1.2 秘密恢复算法

秘密恢复算法如下：

输入：任意 2 个共享份、像素扩展度 m

输出：恢复图像 R'

步骤 1. 任意 2 个共享份直接进行异或运算得到图像 R''；

步骤 2. 从 R'' 的第 1 行开始到第 a 行结束，将每 m 个像素分成一组。每组像素中，只包含两种颜色 $s(i,j)$ 和 0。

步骤 3. 选择每组像素中不为 0 的颜色作为一个新像素的颜色，若该组像素中的颜色全为 0，则选择 0 作为新像素的颜色，最后得到完全恢复的秘密图像 R'。

2 行向量 $V_1, V_2, \ldots, V_n$ 的构造

(2,n)方案中，由于 $c \oplus c' = s(i,j)$ (c, c' 表示 $c_1, c_2, \cdots, c_m, c_1', c_2', \cdots, c_m'$ 中序号相同的颜色值，$c \in \{c_1, c_2, \cdots, c_m\}$，$c' \in \{c_1', c_2', \cdots, c_m'\}$)，为了不泄露 $s(i,j)$ 的任何信息，任意单个行向量中不能同时包含 c, c'；为了能够恢复 $s(i,j)$，任意两个行向量相同位置的元素组合至少有一个为 $\begin{pmatrix} c \\ c' \end{pmatrix}$ 或 $\begin{pmatrix} c' \\ c \end{pmatrix}$。其中，像素扩展度满足 $2^m \geqslant n$，可推出方案的最小像素扩展度 $m = \lceil \ \rceil$。

输入： $n, m, c_1, c_2, \cdots, c_m, c_1', c_2', \cdots, c_m'$

输出：行向量 $V_1, V_2, \cdots, V_n$

步骤 1. 构造初始化矩阵 $C_{2\times 1} = \begin{pmatrix} c_1 \\ c_1' \end{pmatrix}$；

步骤 2. 若 $n=2$，跳至步骤 5；否则令 $j=2$；

步骤 3. 构造矩阵

$$C_{2^j\times j} = \begin{pmatrix} & c_j \\ & c_j \\ C_{2^{j-1}\times(j-1)} & \vdots \\ & c_j \\ & c_j' \\ & c_j' \\ C_{2^{j-1}\times(j-1)} & \vdots \\ & c_j' \end{pmatrix} \begin{matrix} \\ \\ \} 2^{j-1}\text{个} \\ \\ \\ \\ \} 2^{j-1}\text{个} \\ \end{matrix};$$

步骤 4. 令 $j=j+1$，若 $j \leqslant m$，跳至步骤 3；否则得到矩阵 $C_{2^m\times m}$；

步骤 5. 任取 $C_{2^m\times m}$ 的 n 行得到行向量 $V_1, V_2, \cdots, V_n$。

3 有效性分析

定理 1. 任意 2 个行向量可以恢复出 $s(i,j)$。

证明：

$$\text{任取矩阵 } \boldsymbol{C}_{2^m\times m}=\begin{pmatrix} & c_m \\ & c_m \\ C_{2^{m-1}\times(m-1)} & \vdots \\ & c_m \\ & c_m' \\ & c_m' \\ C_{2^{m-1}\times(m-1)} & \vdots \\ & c_m' \end{pmatrix}\begin{matrix} \\ \\ \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} 2^{m-1}\text{个} \\ \\ \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} 2^{m-1}\text{个} \end{matrix}$$

两行构成的矩阵中，至少有一列为 $\begin{pmatrix}c\\c'\end{pmatrix}$ 或 $\begin{pmatrix}c'\\c\end{pmatrix}$。任取 $C_{2^m\times m}$ 的 n 行得到行向量 $V_1,V_2,\cdots,V_n$，由于 $c\oplus c'=s(i,j)$，$c\oplus c=0$，$c'\oplus c'=0$，从 $V_1,V_2,\cdots,V_n$ 任取 2 个行向量 $V_w,V_t(w,t\in[1,2,\cdots,n],w\neq t)$ 进行异或运算，得到行向量 $V=V_w\oplus V_t$，则可推出 $G(V,s(i,j))+G(V,0)=m$ 且 $G(V,s(i,j))\geqslant 1$，通过秘密恢复算法，可恢复出 $s(i,j)$。

证毕。

定理 2. 单个行向量得不到 $s(i,j)$ 的任何信息。

证明：当分享秘密图像中任意一个像素的颜色值 $s(i,j)$ 时，先得到 $c_1,c_2,\cdots,c_m,c_1',c_2',\cdots,c_m'$。由于 $c\oplus c'=s(i,j)$，$s(i,j)$ 由 c 和 c' 共同决定，c 随机与秘密图像没有任何关系，在仅知 c' 的情况下，得不到 $s(i,j)$ 的任何信息。在 $V_1,V_2,\cdots,V_n$ 中，任意一个行向量中不同时包含序号相同的像素颜色 c,c'，无法恢复出 $s(i,j)$。因此，单个行向量得不到秘密图像的任何信息。

证毕。

4 仿真实验与结果分析

为了验证方案的有效性，本节分别通过(2, 2)和(2, 3)方案对 2 幅秘密图像进行仿真实验，并分析了实验结果。

4.1 仿真实验

图 2 是(2, 2)方案实验效果图。其中，S 表示秘密图像 baboon，S_1,S_2 表示共享份。从图中可以看出，单个共享份呈杂乱无章的噪声图像，从中得不到秘密图像的任何信息；由于(2, 2)方案是(n,n)方案的一种特殊情况，共享份无像素扩展，在用秘密恢复算法恢复秘密图像过程中，第一步得到的图像 R'' 和第 3 步得到的图像 R' 都是完全恢复的。

图 3 是(2, 3)方案实验效果图。其中，S 表示秘密图像 lena，S_1,S_2,S_3 表示共享份。从图中可以看出，单个共享份呈杂乱无章的噪声图像，从中得不到秘密图像的任何信息；在用秘密恢复算法恢复秘密图像过程中，第 1 步得到的图像 R''_1,R''_2,R''_3，其像素扩展度 $m=2$，第 3 步得到完全恢复的秘密图像 R'_1,R'_2,R'_3。

4.2 结果分析

在秘密恢复算法中，对恢复图像 R'' 进行处理会带来额外的计算开销，但不会增加恢复算法计算复杂度的阶数。大小为 $a\times b$ 的秘密图像 S，通过秘密分享算法得到 n 个像素扩展度为 m 的共享份。任意两个共享份进行异或运算得到恢复图像 R''，计算量为 $a\times b\times m$。在此基础上对 R'' 进行处理，从 m 个子像素中选择一个不为 0 的颜色值（若颜色值全为 0，则选择 0），总共需要进行 $a\times b$ 次选择，不会增加计算复杂度的阶数。因此，本文中秘密恢复过程中的计算复杂度为 $O(\lceil\log_2 n\rceil)$。在彩色视觉密码中，衡量恢复图像视觉效果的性能指标主要有对比度和峰值信噪比。本文选用对比度作为衡量恢复图像视觉效果的性能指标并与其它文献进行比较。文献[12,14]中，方案像素扩展度 $m=1$，对比度定义为 $\alpha=prob(r(i,j)=s(i,j))$（$r(i,j)$ 表示恢复图像中位置 (i,j) 像素的颜色值），表示秘密图像中每个像素的恢复概率，在无像素扩展的方案中，能够有效衡量恢复图像的视觉效果。文献[13]和本文的秘密图像都是完全恢复，对比度 $a=1$。

表 2 列出了本文 $(2,n)-CVCS$ 与其它文献

$(2,n)-CVCS$ 的比较结果，具体地说，主要表现在：1.与文献[12]相比，本文中每个参与者只需携带一个共享份，降低了共享份的管理难度；2.与文献[13]相比，本文在兼顾完全恢复的前提下，将计算复杂度降低到对数级；与文献[14]相比，能够实现秘密图像的完全恢复。

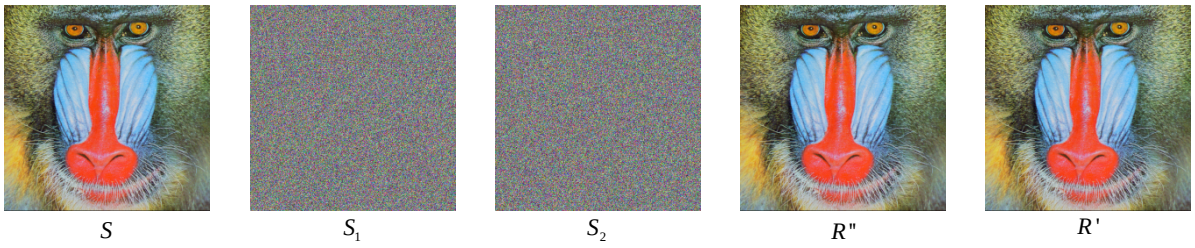


图 2　(2,2)方案实验效果图

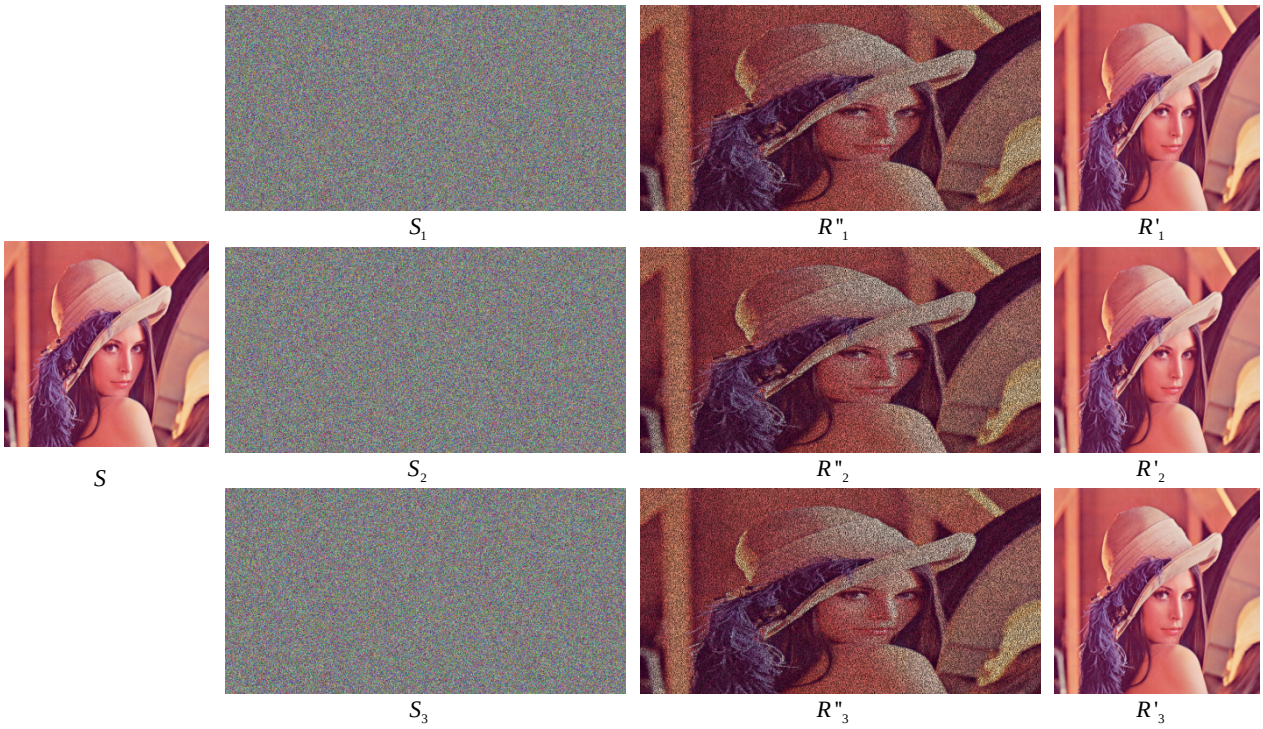


图 3　(2,3)方案实验效果图

表 2　$(2,n)-CVCS$

方案	像素扩展度	对比度	参与者携带共享份的数量	完全恢复	计算复杂度
文献[12]	$m=1$	$\alpha=(1-(1/2)^r)^{24}$	r	否	$O(r)$
文献[13]	$m=(2\times(n-1))/n$	$\alpha=1$	1	是	$O(n)$
文献[14]	$m=1$	$\alpha=1/(n-1)^2$	1	否	$O(1)$
本文	$m=\lceil\log_2 n\rceil$	$\alpha=1$	1	是	$O(\lceil\log_2 n\rceil)$

5　结论

本文对彩色视觉密码进行了研究，提出了一种完全恢复的(2, *n*)彩色视觉密码方案。给出了秘密分享和恢复算法，并从理论上对方案的安全性进行了分析。在每个参与者携带一个共享份的前提下，2 个共享份直接进行异或运算能够恢复秘密图像，具有较好的视觉效果，通过秘密恢复算法，能够实

现秘密图像的完全恢复，且计算复杂度由 $O(n)$ 降低到了 $O(\lceil \log_2 n \rceil)$。

参考文献:

[1] Naor M, Shamir A. Visual Cryptography [J]. Lecture Notes in Computer Science (S0302-9743), 1995, 950(1): 1-12.

[2] Verheul E R, Tilborg H C A V. Constructions and Properties of k out of n Visual Secret Sharing Schemes [J]. Designs Codes & Cryptography (S1573-7586), 1997, 11(2): 179-196.

[3] Stelvio Cimato, Roberto De Prisco, Santis A D. Optimal Colored Threshold Visual Cryptography Schemes [J]. Designs, Codes and Cryptography (S1573-7586), 2005, 35(3): 311-335.

[4] Cimato S, De Prisco R, De Santis A. Colored Visual Cryptography Without Color Darkening [J]. Security in Communication Networks (S0302-9743), 2005, 374: 261-276.

[5] Yamamoto H. Proposal of a Lattice-based Visual Secret Sharing Scheme for Color and Gray-scale Images [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences (S0916-8508), 1998, 81(6): 1262-1269.

[6] Hou Y C. Visual Cryptography for Color Images [J]. Pattern Recognition (S0031-3203), 2003, 36(7): 1619-1629.

[7] Chen T, Tsao K. Threshold Visual Secret Sharing by Random Grids [J]. Journal of System & Software (S0164-1212), 2011, 84(7): 1197-1208.

[8] Lukac R, Plataniotis K N. Colour Image Secret Sharing [J]. Electronics Letters (S0013-5194), 2004, 40(9): 529-531.

[9] Lukac R, Plataniotis K N. Bit-level based Secret Sharing for Image Encryption [J]. Pattern Recognition, 2005, 38(5): 767-772.

[10] Lukac R, Plataniotis K N. A Color Image Secret Sharing Scheme Satisfying the Perfect Reconstruction Property [C]//Multimedia Signal Processing, 2004 IEEE 6th Workshop on USA: IEEE, 2004: 351-354.

[11] Wang D, Zhang L, Ma N, et al. Two Secret Sharing Schemes based on Boolean Operations [J]. Pattern Recognition (S0031-3203), 2007, 40(10): 2776-2785.

[12] Dong L, Wang D, Li S, et al. (2, n) Secret Sharing Scheme for Gray and Color Images based on Boolean Operation [J]. Science in China (S1869-1919), 2012, 55(5): 1151-1161.

[13] Chao K, Lin J. Secret Image Sharing: a Boolean-Operations-Based Approach Combining Benefits of Polynomial-Based and Fast Approached [J]. International Journal of Pattern Recognition & Artificial Intelligence, 2011, 23(2): 263-285.

[14] Kumar S, Sharma R K. Threshold Visual Secret Sharing based on Boolean Operations [J]. Security & Communication Networks, 2014, 7(3): 653-664.

(上接第 1418 页)

[6] Keijo Haataja, Pekka Toivanen. Two practical man-in-the-middle attacks on Bluetooth secure simple pairing and countermeasures [J]. IEEE Transactions on Wireless Communications (S1536-1276), 2010, 9(1): 384-392.

[7] Andrew Y Lindell. Attacks on the pairing protocol of Bluetooth v2.1 [M]. Las Vegas, Nevada, USA: Black Hat, 2008.

[8] Jani Suomalainen, Jukka Valkonen, N Asokan. Security associations in personal networks: A comparative analysis [C]// 4th European Workshop, ESAS 2007, Cambridge, UK, Finland: NOKIA Research Center, 2007: 1-18.

[9] Bin Yu, Haiyan Li. Research and Design of one Key Agreement Scheme in Bluetooth [C]// Computer Science and Software Engineering, 2008 International Conference on. Wuhan: IEEE, 2008: 665-668.

[10] Diallo, Al-Khateeb, Wajdi Fawzi, et al. A Secure Authentication Scheme for Bluetooth Connection [C]// Computer and Communication Engineering (ICCCE). Kuala Lumpur: IEEE, 2014: 60-63.

[11] 施荣华, 翁丽萍, 王国才. 基于单向哈希链的网络密钥协商协议 [J]. 湖南大学学报(自然科学版), 2011, 38(3): 77-81.

[12] 张小彬, 韩继红, 王亚弟, 等. 基于分簇的Ad Hoc网络密钥协商协议[J]. 计算机工程, 2010, 36(1): 170-173.