A Patching Algorithm for Extended Visual Cryptography

Kai-Hui Lee[1], Pei-Ling Chiu[2], Chien-Chu Tsang[3], Pei-Shan Yeh[4]
[1, 3, 4]*Dept. Computer Science and Information Engineering, Ming Chuan University, Taipei*
[2]*Dept. Risk Management and Insurance, Ming Chuan University, Taipei*
Email: khlee@mail.mcu.edu.tw; plchiu@mail.mcu.edu.tw; joseph9436@gmail.com; beybey.ya@gmail.com

Abstract: Generally, shares of Visual Secret Sharing scheme (VSS scheme) consist of a lot of random pixels so that they looked meaningless. Hence, it is difficult for the participants to manage and identify these shares. For addressing the problem, Extended Visual Cryptography Scheme (EVCS) adds meaningful camouflage patterns to the shares. In previous conventional VSS schemes, the encryption manners cannot be applied to EVCS directly. Namely, the researchers have to reconstruct EVCS for each scheme. Additionally, the manners should introduce more pixel expansions, which is unpractical to store and deliver the share images. Moreover, the finding of the minimum expansion on EVCS is a NP-hard problem. Therefore, the paper proposes a novel EVCS algorithm for binary secret images; for a giving access structure, our algorithm can construct an EVCS without pixel expansion. On the first stage, the algorithm obtains a set of shares without pixel expansion by the existing constructions for traditional VSS scheme. On the second stage, the proposed algorithm adds meaningful camouflage patterns to the shares without pixel expansion. The experimental result shows that not only the EVCS construction manner doesn't introduce pixel expansion but also the quality of recovered image is very close to the quality of VSS without camouflage patterns.

Keywords: visual secret sharing; pixel expansion; extended visual cryptography scheme

使用补丁技术的扩充型视觉密码学

李开晖[1]，邱佩玲[2]，臧建柱[3]，叶培珊[4]
[1, 3, 4]铭传大学 资讯工程系，台北
[2]铭传大学 风险管理与保险系，台北
Email: khlee@mail.mcu.edu.tw; plchiu@mail.mcu.edu.tw; joseph9436@gmail.com; beybey.ya@gmail.com

摘　要：由于一般的视觉机密分享机制(Visual Secret Sharing scheme，简称 VSS scheme)所产生的分享影像，外观上杂乱无章，导致持有者难以辨认与管理的缺点。有鉴于此，扩充型视觉密码(Extended Visual Cryptography Scheme, EVCS)在分享影像上加入有意义的伪装影像，使得分享影像具有易于辨认和管理的好处。然而，原先适用于传统视觉密码学的编码方式，无法直接应用于扩充型视觉密码，需另行建构密码本。另一方面，使用传统视觉密码学编码的方式建构扩充型视觉密码，分享图会产生一定倍数的像素扩张，不利于分享图的储存与传递；尤有甚者，欲求取最小化像素扩张，更是一个 NP-hard 的问题。因此，本文提出一个适用于黑白二元影像的扩充型视觉密码学加密算法，能针对一个给定的存取结构，建构出无像素扩张的扩充型视觉密码。算法第一阶段直接使用现存的机密分享机制，建构一组无像素扩张分享图。第二阶段算法则是在所建构的分享图上加入伪装影像。实验结果显示，本文所提的算法确实不会造成还原影像的像素扩张，且影像的还原质量也非常接近一般无伪装影像视觉机密分享机制。

关键词：视觉机密分享机制;像素扩展;扩充型视觉密码

1 引言

1994 年，Naor 和 Shamir 两位学者提出应用在影像数据上的新的密码学方法，称为视觉密码(Visual Cryptography, VC)[1]。运用机密分享概念到影像讯息，将一张机密影像(secret image)分成 n 张不同的分享影像(share images)，印制在投影片(transparency)上，交予 n 位

资助信息：本研究部分接受科会编号：NSC98-2401-H-130-003 研究计划经费补助

978-1-935068-15-0 © 2010 SciRes.

参与者。将所有参与者所持投影片迭合，以人类视觉系统，无需任何数学运算或加密知识，便能重现机密影像。但是，无法由任何一张或部分的分享影像还原机密影像。因为解密只需直接迭合投影片即可还原机密，在无法使用计算机解密的情况下，是一个很好的解决方案。

Naor 和 Shamir 两位学者提出的视觉机密分享机制是研究如何从 n 张分享图中，任意拿取 k $(2 \le k \le n)$ 张或更多的分享讯息，就得以还原机密影像的加密方法。这个架构又称为 n 中取 k 视觉机密分享机制（k -out-of- n VSS scheme，记为 (k,n) -VSS scheme），又称为门坎型视觉机密分享机制(threshold VSS scheme)[1]。过去十余年来，已有学者提出许多不同的解决方案[2-3]。

传统视觉机密分享机制，每张分享影像都是一些随机的像素。虽然隐藏了机密影像，但是拥有者也无法藉由视觉来辨识并了解每一张分享影像的用途，因此产生了管理上的不便。扩充型视觉密码机制(Extended Visual Cryptography Scheme，EVCS)除了在分享图上加密机密影像外，并为每一张分享图加上不同伪装影像(cover image)以利于辨识，可以解决分享影像的管理问题[5-7]。

然而，建构扩充型视觉密码遭遇两个问题：第一，原先适用于传统视觉密码学的编码方式，无法直接应用于扩充型视觉密码，亦即扩充型视觉密码，需另行建构密码本。第二，使用传统视觉密码学编码的方式建构扩充型视觉密码，分享图会产生一定倍数的像素扩张，不利于分享图的储存与传递。像素扩张不但影响分享影像的携带便利与否，也是储存容量与传递频宽的重要考虑。因此成为机密分享机制效能评估的重要指标之一。以 Ateniese 等人提出对 EVCS 的解决方案为例，在参与人数不超过 4 人的情况下，即便不考虑维持还原机密图长宽比，以传统的视觉密码学的编码方式建构，仍会产生 2~8 倍的像素扩张。Ateniese 也已证明他们所提的方法有最小的像素扩张，以及欲求取最小化像素扩张，是一个 NP-hard 的问题等特质[4,5,8,9]。

有鉴于此，本文提出一个适用于黑白二元影像的扩充型视觉密码学加密算法，能针对一个给定的存取结构，建构出无像素扩张的扩充型视觉密码。为避免产生像素扩张，我们并不直接使用传统视觉密码学的编码方式，而是改用补丁(patching)技术来建构扩充型视觉密码。算法第一阶段直接使用现存的机密分享机制，建构一组无像素扩张分享图。第二阶段算法则是在所建构的分享图上加入伪装影像。

我们将透过实作与展示的方式，来证明算法的有效性。同时，使用还原影像的对比为效能指针，来衡量二元机密影像的还原质量。

2 加密算法

本文所提算法的加密程序如Figure 1所示。算法的第一阶段直接借用现存的机密分享机制，建构无伪装的分享图 P_1，…，P_n。第二阶段则是将伪装图加在这些分享图上，完成扩充型视觉密码的加密程序。

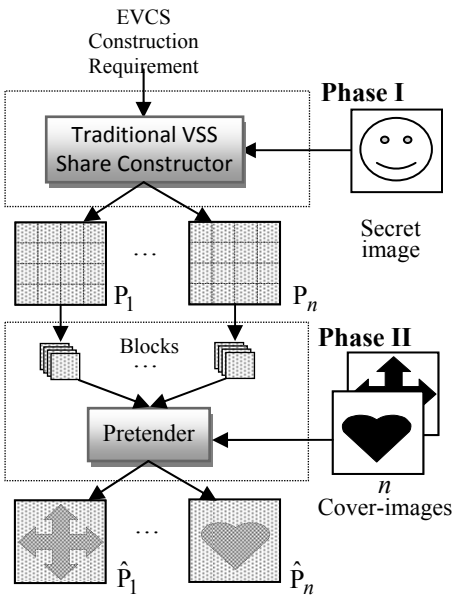


Figure 1: The encryption procedure for EVCS.

图 1. 所提 EVCS 的两阶段加密流程。

2.1 第一阶段加密

本小节将以 n 中取 n 的机密分享机制((n,n) -VSS scheme)为例，说明第一阶段的加密方法。

本文使用 Yang 所发展的 (n,n) -门坎型视觉机密分享机制，来产生未经伪装的分享图 P_1，…，P_n。密码本的建置规则如下[3]：

令 C_0 与 C_1 为 $n \times 1$ 矩阵的集合，分别表示产生 n 张分享图的白区与黑区的编码。其中 $C_0 = \{\mu_{i,0}, i \in Even, 0 \le i \le n\}$，$C_1 = \{\mu_{i,1}, \quad i \in Odd, 0 \le i \le n\}$。$\mu_{i,0}$ 与 $\mu_{i,1}$ 被选取的机率均为 $\binom{n}{i} \Big/ 2^{n-1}$。

例如，若欲建构 $(3,3)$ -EVCS，依上述规则可得

(3,3) -VSS 机制的密码本：

$$C_0 = \{\mu_{0,0}, \mu_{2,0}\} = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \right\},$$

$$C_1 = \{\mu_{1,1}, \mu_{3,1}\} = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\},$$

C_0 与 C_1 中每一个 3×1 矩阵被选取的机率均为 1/4 。使用 C_0 与 C_1 建构分享图的过程中，以 8×8 的小区块为处理单位。若小区块内，机密图白/黑区分别有 γ_0 与 γ_1 个像素，则我们透过妥善的安排，使区块内白/黑区的各种编码出现的机率尽量呈均匀分布，亦即白/黑区的各种编码均分别被选取(接近) $\gamma_0/4$ 与 $\gamma_1/4$ 次。此举是为了让产生的基本分享图中的黑点分布较为均匀，对还原的机密视觉质量有一定的帮助。

2.2 第二阶段加密算法

Table 1定义了与算法相关的符号。第二阶段加密主要是将伪装图像中的黑色区域，依给定的黑点散布密度差值，将黑点散布到分享图中。由于此步骤采随机的方式选取黑点，为避免黑点的散布不够均匀，先将分享图切割成大小相等的区块，再进行伪装。为了让所产生分享图的伪装影像有较好的质量，我们所提出的算法也允许依不同伪装影像的内容，给定不同的伪装黑点密度，来调整伪装影像质量。第二阶段加密算法的伪码如4 结论

本文提出了一个两阶段加密算法来建构扩充型视觉密

Algorithm 1所列。

4 结论

本文提出了一个两阶段加密算法来建构扩充型视觉密

Algorithm 1的步骤 1 是初始化分享图。步骤 2 将每一张分享图分割成 m 个小区块。步骤 3 计算每一张分享图的黑点分布密度。步骤 4 求取每一区块所需的伪装黑点数量。步骤 5 计算 F 矩阵。步骤 6 散布黑点到分享图中，使每一区块的黑点密度与给定的伪装密度相同。最后，步骤 7 输出分享图。

显而易见地，步骤 6 主宰了算法 1 的时间复杂度。步骤 6 需根据伪装图黑点重迭的次数依次决定是否增加伪装的黑点到每一张分享图中，因此4 结论

本文提出了一个两阶段加密算法来建构扩充型视觉密

Algorithm 1的时间复杂度是 $O(n^2wh)$ 。

3 实验结果

在本节中，我们将展示所提算法的实作结果。我们以 512x384 像素黑白二元影像为实验对象，来建构 (3,3) -EVCS，Figure 2(a)~(c)是伪装图(cover images)，Figure 2(d)则是机密图。为节省篇幅，本节所有的图均缩小为原图的 25%。

算法第 1 阶段加密采 2.1 节的密码本，第二阶段加密算法的验参数设定如下： w_b 定为 8， Δd_α 均为 30%。分享图与一部分迭合图的结果如Figure 3所示。Figure 3的结果印证了我们的方法确实可建构出像素不扩张的扩充型视觉密码。此外，Figure 3(d)的影像对比分别为 24.45%，几乎与 (3,3) -门坎型视觉机密分享机制的最佳对比值(25%)相同，显见我们的方法可以得到很好的还原机密影像质量。

Table 1: Notations.
表 1: Algorithm1 的符号定义。

n	：分享(伪装)影像的数量， $n\geq2, n\in Z$ 。
w	：影像的宽， $w\in Z$ 。
h	：影像的高， $h\in Z$ 。
w_b	：区块的边长， $w_b\in Z$ 。
m	：一个分享(伪装)影像的区块总数。
P_α	：表第一阶段算法所产生的第 α 张基本分享影像。
$\hat{\mathrm{P}}_\alpha$	：表示参与者 i_α 的分享影像。
$\hat{S}_\alpha$	：表示第 α 张伪装影像。
$\mathrm{A}^{\alpha,\beta}$ (resp. $\mathrm{B}^{\alpha,\beta}$)	：一个 $w_b\times w_b$ 的矩阵表示 $\hat{\mathrm{P}}_\alpha$ (resp. $\hat{S}_\alpha$) 第 β 个区块的位映样(bitmap)。 $a_{y,x}^{\alpha,\beta}$ (resp. $b_{y,x}^{\alpha,\beta}$) 为 $\mathrm{A}^{\alpha,\beta}$ (resp. $\mathrm{B}^{\alpha,\beta}$)在 (y,x) 的元素，表 $\hat{\mathrm{P}}_\alpha$ (resp. $\hat{S}_\alpha$)中对应坐标的像素，1 表示黑点，反之 0 表白点， $1\leq\alpha\leq n$， $1\leq\beta\leq m$， $\alpha,\beta\in Z$ 。
F^β	：一个 $w_b\times w_b$ 的矩阵表示所有的伪装影像的第 β 个区块的黑点重迭次数。 $f_{y,x}^\beta$ 为 F^β 在 (y,x) 的元素， $f_{y,x}^\beta=k$ 表有 k 个伪装影像的黑点出现在第 β 个区块坐标 (y,x) 处， $1\leq\beta\leq m, \beta\in Z$ 。
$\bar{d}_\alpha$	： $\hat{\mathrm{P}}_\alpha$ 的黑点平均密度， $1\leq\alpha\leq n$， $\alpha\in Z$ 。
Δd_α	： $\hat{\mathrm{P}}_\alpha$ 中伪装影像黑色区域的黑点密度增量， $1\leq\alpha\leq n$， $\alpha\in Z$ 。
$\hat{g}^{\alpha,\beta}$	： $\hat{S}_\alpha$ 中第 β 个区块的黑点数量， $1\leq\alpha\leq n$， $1\leq\beta\leq m$， $\alpha,\beta\in Z$ 。
$g^{\alpha,\beta}$	： $\hat{\mathrm{P}}_\alpha$ 中第 β 个区块在伪装影像黑色区域内已有的黑点数量， $1\leq\alpha\leq n$， $1\leq\beta\leq m$， $\alpha,\beta\in Z$ 。

978-1-935068-15-0 © 2010 SciRes.

$\Delta g^{\alpha,\beta}$	：$\hat{P}_\alpha$ 中第 β 个区块尚需增加的黑点数量，$1 \le \alpha \le n$，$\alpha \in Z$。

4 结论

本文提出了一个两阶段加密算法来建构扩充型视觉密码，此算法能在任何传统的视觉机密分享机制上，使用补丁技术，将原先不具意义的分享图，加上有意义的图像，使这些分享图更便于管理。实验结果证明，此算法不但不会引起还原影像的像素扩张，且还原影像能保有很好的对比。以像素扩张的观点而言，本算法突破了以传统视觉密码学加密方式的瓶颈。

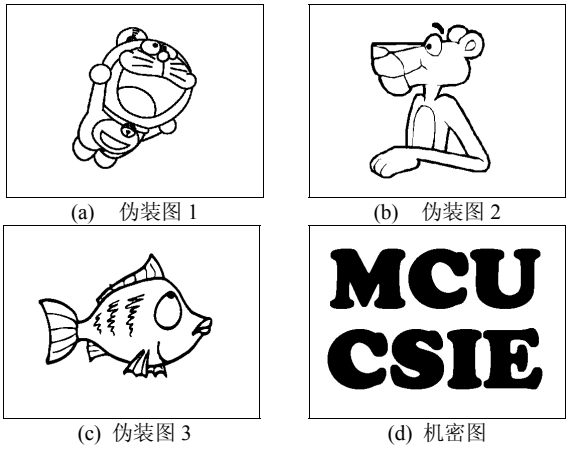
Algorithm 1: The second stage encryption procedure.
算法 1：第二阶段加密算法。

Input: $P_1, ..., P_n, \hat{S}_1, ..., \hat{S}_n, \Delta d_1, ..., \Delta d_n, w_b$.
Output: $\hat{P}_1, \ldots, \hat{P}_n$.

1. $\forall 1 \le \alpha \le n$, $\hat{P}_\alpha \leftarrow P_\alpha$.
2. $\forall 1 \le \alpha \le n$, divide $\hat{P}_\alpha$ and $\hat{S}_\alpha$ into m blocks. Each block contains $w_b \times w_b$ pixels.
3. $\forall 1 \le \alpha \le n, \bar{d}_\alpha \leftarrow \frac{1}{h \times w} \sum_{1 \le \beta \le m} \sum_{1 \le y \le w_b} \sum_{1 \le x \le w_b} a_{y,x}^{\alpha,\beta}$.
4. $\forall 1 \le \alpha \le n$, $\forall 1 \le \beta \le m$, calculate
   - 4.1 $\hat{g}^{\alpha,\beta} \leftarrow \sum_{1 \le y \le w_b} \sum_{1 \le x \le w_b} b_{y,x}^{\alpha,\beta}$.
   - 4.2 $g^{\alpha,\beta} \leftarrow \sum_{1 \le y \le w_b} \sum_{1 \le x \le w_b} (a_{y,x}^{\alpha,\beta} \times b_{y,x}^{\alpha,\beta})$.
   - 4.3 $\Delta g^{\alpha,\beta} \leftarrow \max\{0, (\bar{d}_\alpha + \Delta d_\alpha) \times \hat{g}^{\alpha,\beta} - g^{\alpha,\beta}\}$.
5. $\forall 1 \le \beta \le m$, $\forall 1 \le y \le w_b$, $\forall 1 \le x \le w_b$, $f_{y,x}^{\beta} \leftarrow \sum_{1 \le \alpha \le n} b_{y,x}^{\alpha,\beta}$.
6. **for** $\beta \leftarrow 1$ **to** m
   begin
   for $r \leftarrow n$ **downto** 1
   begin
   Empty queue Q
   $\forall 1 \le y \le w_b$, $\forall 1 \le x \le w_b$,
   if $f_{y,x}^{\beta} = r$ **then** enqueue $Q \leftarrow (y,x)$
   Shuffle Q
   while $Q \ne empty$ **do**
   begin
   Dequeue $(y,x) \leftarrow Q$
   $\forall 1 \le \alpha \le n$,
   If $\Delta g^{\alpha,\beta} \ne 0$ **and** $a_{y,x}^{\alpha,\beta} = 0$ **and** $b_{y,x}^{\alpha,\beta} = 1$ **then** $a_{y,x}^{\alpha,\beta} \leftarrow 1$, $\Delta g^{\alpha,\beta} \leftarrow \Delta g^{\alpha,\beta} - 1$.
   if $\forall 1 \le \alpha \le n$ **and** $\Delta g^{\alpha,\beta} = 0$ **then goto** 6
   end
   end
   end
7. $\forall 1 \le \alpha \le n$, output shares $\hat{P}_\alpha$.

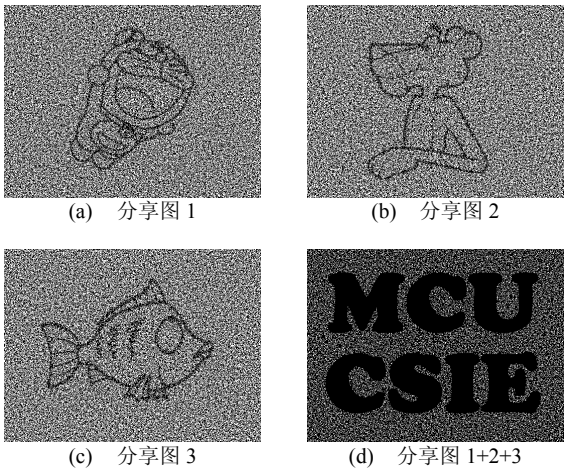
本算法具有下列特点：首先是模块化，加密流程的两个模块关联性小，因此可单独设计，也具备可替换性。第二，可让加密者调整分享图上伪装影像的黑像素密度，以提高伪装影像的质量。

本文的主要贡献有：第一，提出解决扩充型视觉密码像素扩充问题的解决方案。第二，发展出补丁技术，使得扩充型视觉密码的设计，可直接使用传统视觉密码学的结果，无需再设计新的密码本。



(a) 伪装图 1　(b) 伪装图 2　(c) 伪装图 3　(d) 机密图

Figure 2: Cover images and secret image for the experiment.
图 2. 实验用的伪装图与机密图。



(a) 分享图 1　(b) 分享图 2　(c) 分享图 3　(d) 分享图 1+2+3

Figure 3: The experimental results.
图 3. 实验结果。

References (参考文献)

[1] M. Naor and A. Shamir, "Visual Cryptography," in *Advances in Cryptology: Eurprocrypt'94,* 1995, pp. 1-12.
[2] E. R. Verheul and H. C. A. van Tilborg, "Constructions and Properties of k out of n Visual Secret Sharing Schemes," *Designs, Codes and Cryptography,* vol. 11, pp. 179-196, 1997.

[3] C. N. Yang, "New Visual Secret Sharing Schemes using Probabilistic Method," *Pattern Recognition Letters,* vol. 25, pp. 481-494, 2004.

[4] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Constructions and Bounds for Visual Cryptography," in *Proc. ICALP,* 1996, pp. 416-428.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual Cryptography for General Access Structures," *Information and Computation,* vol. 129, pp. 86-106, 1996.

[6] W. P. Fang, "Friendly Progressive Visual Secret Sharing," *Pattern Recognition,* vol. 41, pp. 1410-1414, 2008.

[7] T. H. Chen, K. H. Tsao, and Y. T. Yang, "Friendly color visual secret sharing by Random Grids," *Fundamenta Informaticae,* vol. 96, pp. 61-70, 2009.

[8] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended Capabilities for Visual Cryptography," *Theoretical Computer Science,* vol. 250, pp. 143-161, 2001.

[9] D. Wang, F. Yi, and X. Li, "On General Construction for Extended Visual Cryptography Schemes," *Pattern Recognition,* vol. 42, pp. 3071-3082, 2009.

978-1-935068-15-0 © 2010 SciRes.