Computer Science and Application 计算机科学与应用, 2021, 11(4), 975-982
Published Online April 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.114100

Hans汉斯

基于Asmuth-Bloom门限共享秘密图像信息隐藏算法研究

陈维启，李祯祯，张珍珍，丁海洋，李子臣

北京印刷学院信息工程学院，北京
Email: 550898639@qq.com

收稿日期：2021年3月22日；录用日期：2021年4月16日；发布日期：2021年4月23日

摘　要

为安全传输保密的图像，本文基于Asmuth-Bloom共享方案，设计了一个(*t*, *n*)门限秘密图像信息隐藏算法。首先将秘密图像共享成*n*份表面看似无意义的秘密共享图像，使用DCT算法将*n*份秘密共享图像分别嵌入到*n*个用户提供的彩色载体图像中，再将*n*份含秘密共享的载体图像分发给*n*个用户。在秘密恢复时，大于等于门限值*t*的用户从含秘密共享的彩色载体图像盲提取出秘密共享图像，再使用中国剩余定理还原秘密图像。实验结果表明，本文提出的算法能正确恢复秘密图像。通过峰值信噪比(PSNR)，平均结构相似性(MSSIM)，比特出错概率(BER)对本方案进行评估，优于其他方案。

关键词

Asmuth-Bloom秘密共享，中国剩余定理，门限，盲提取，信息隐藏

Research on Secret Image Threshold Sharing Information Hiding Algorithm Based on Asmuth-Bloom

Weiqi Chen, Zhenzhen Li, Zhenzhen Zhang, Haiyang Ding, Zichen Li

School of Information Engineering, Beijing Institute of Graphic Communication, Beijing
Email: 550898639@qq.com

Received: Mar. 22nd, 2021; accepted: Apr. 16th, 2021; published: Apr. 23rd, 2021

文章引用: 陈维启, 李祯祯, 张珍珍, 丁海洋, 李子臣. 基于 Asmuth-Bloom 门限共享秘密图像信息隐藏算法研究[J]. 计算机科学与应用, 2021, 11(4): 975-982. DOI: 10.12677/csa.2021.114100

Abstract

In order to transmit secret images more securely, this paper proposes a (*t*, *n*) threshold image data hiding algorithm based on Asmuth-Bloom secret sharing. First share the secret image into *n* meaningless secret shared images, use the DCT algorithm to embed the *n* meaningless images into *n* user-provided color cover images, and then distribute the *n* cover images with secret sharing to *n* users. Secondly, when the secret is recovered, users who are greater than or equal to the threshold *t* blindly extract meaningless secret sharing images from the cover image containing secret sharing, and then use the Chinese remainder theorem to recover the secret images. Finally, the experimental results proved that the algorithm proposed in this paper can recover the secret image correctly. This scheme is evaluated by peak signal-to-noise ratio (PSNR), mean structural similarity (MSSIM), and bit error ratio (BER), it is proved that this scheme is superior to other schemes.

Keywords

Asmuth-Bloom Secret Sharing, Chinese Remainder Theorem, Threshold, Blind extraction, Data Hiding

1. 引言

秘密共享将一个秘密信息分割成 n 共享份，分发给 n 位不同的用户，只有不少于 t 个用户才能重构秘密，t 为秘密共享方案的门限值。利用秘密共享方案将秘密形成分享份，分散保存，降低了密码集中存放在一处的风险。同时，(t, n)门限秘密共享方案还能够抵御$(t-1)$个用户合谋攻击。1979 年，基于拉格朗日插值多项式，Shamir 提出了首个秘密共享方案[1]。1983 年，基于中国剩余定理，Asmuth C.和 Bloom J. A.提出了著名的 Asmuth-Bloom 秘密共享门限方案[2]。Asmuth-Bloom 具有更好理论基础，且计算效率更高。信息隐藏[3]是将秘密信息隐藏在载体中，从而安全传送秘密信息的技术。选用数字图像作为载体进行信息隐藏已成为信息安全学界的热点[4]。

近年来，互联网技术快速发展，改善了人类信息交互方式，给社会带来了便利。同时，我们也要看到数字媒体技术的脆弱，传输的秘密图像信息容易被盗取、篡改，从而为不法分子所用，对信息安全产生重大影响。所以在当今强调国家信息安全的数字化时代，如何安全、快速、可信、无损的传输图像信息，成为一个重要的命题。对此，学界提出了将秘密共享技术与图像处理技术相结合的方案来解决此问题[5]。秘密共享已经成为秘密信息安全传输的重要手段。

本文利用 Asmuth-Bloom 秘密共享门限技术，将需要安全传输的秘密图像分解成若干个看似毫无意义的秘密共享图像，并利用 DCT 信息隐藏算法将秘密共享图像嵌入到用户提供的彩色载体图像，分发给用户，保证了秘密图像传输过程的绝对安全。在秘密图像恢复时，被选定的用户进行秘密共享图像提取，获得共享秘密图像，选取不少于 t 份图像分享，进行原始秘密图像还原。若 n 个用于中出现泄露信息行为，可将该用户所拥有的子秘密删除，其余的不少于 t 个用户仍可计算出原始秘密图像。实验结果表明

本文设计的算法能正确恢复秘密图像，通过峰值信噪比(PSNR)，平均结构相似性(MSSIM)，比特出错概率(BER)对本方案进行评估，优于其他方案。

2. 预备知识

2.1. 秘密共享技术

在保密通信系统中，一般是由一个主秘钥决定整个系统的安全性。这样会出现以下一个问题，一旦主密钥丢失或者泄露，系统将被受到攻击，安全性无法得到保障。

在密码学中，秘密共享是将秘密信息分成众多子秘密，形成共享份，使用达到阈值的子秘密共享份就可以还原该秘密信息。秘密共享技术具体形式如下：

假设 s 为密码信息，将秘密 s 分成 n 份 $s_1, s_2, \cdots, s_n$，需要满足下面两个条件。

(1) 有任意 t 个或大于 t 个 s_i 可以算出 s。

(2) 若未拥有任意 t 个，只有任意 t - 1 个或更少份 s_i，不能算出 s。

其中 t 是一个小于 n 的整数，构成的秘密共享方案，称之为(t, n)门限方案。

2.2. Asmuth-Bloom 门限方案

Asmuth 和 Bloom 基于中国剩余定理(CRT)提出了一个(t, n)门限方案，其中，成员们手中的共享份是由秘密 s 计算得到的 y 与设置的模数 $m_1, m_2, \cdots, m_n$ 进行取模运算得到的 (m_i, y_i)。

2.2.1. 参数选取

选取一个大素数 q 与 n 个严格递增的模数 $m_1, m_2, \cdots, m_n$，且需要满足下面的条件。

(1) $q > s$。

(2) $\gcd(m_1, m_j) = 1, \forall i, j, i \neq j$。

(3) $\gcd(q, m_i) = 1, i = 1, 2, \cdots, n$。

(4) $N = \prod_{i=1}^{t} m_i > q \prod_{j=1}^{t-1} m_{n-j+1}$。

2.2.2. 秘密共享

首先，随机选取一个整数 A，且满足 $0 \le A \le \lfloor N/q \rfloor - 1$。

其次，由 A 与 q 根据公式 $y = s + Aq$，求得 y。则有 $y < q + Aq = (A+1)q \le \lfloor N/q \rfloor \cdot q \le N$。

最后，计算 $y_i \equiv y \bmod m_i \ (i = 1, 2, \cdots, n)$。

则 (m_i, y_i) 即一个子共享份，将它分发给系统中的 n 个用户。

当 t 个用户 $i_1, i_2, \cdots, i_t$ 拿出自己的子份额时，由 $\left\{ \left(m_{i_j}, y_{i_j} \right) \mid i = 1, 2, \cdots, t \right\}$ 建立方程组

$$\begin{cases} y \equiv y_{i_1} \bmod m_{i_1} \\ y \equiv y_{i_2} \bmod m_{i_2} \\ \quad \vdots \\ y \equiv y_{i_t} \bmod m_{i_t} \end{cases}$$

可以求得

$$y \equiv y' \bmod N'$$

其中 $N' = \prod_{j=1}^{t} m_{i_j} \ge N$，由 $y' \bmod q$ 解得秘密 s。

2.2.3. 秘密恢复

当 t 个用户 $i_1,i_2,\cdots,i_t$ 拿出自己的子份额时，由 $\left\{\left(m_{i_j},y_{i_j}\right)\mid i=1,2,\cdots,t\right\}$ 建立方程组

$$\begin{cases} y\equiv y_{i_1} \bmod m_{i_1} \\ y\equiv y_{i_2} \bmod m_{i_2} \\ \quad\vdots \\ y\equiv y_{i_t} \bmod m_{i_t} \end{cases}$$

可以求得

$$y\equiv y' \bmod N'$$

其中 $N'=\prod_{j=1}^{t}m_{i_j}\geq N$，由 $y'-Aq$ 解得秘密 s。

2.3. DCT 信息隐藏算法嵌入参数选择

本文方案中待嵌入的数据是一个共享灰度图。首先遍历将该图像，进行 4 × 4 分块，再通过二维 DCT 变换，按照 Zigzag 顺序进行扫描[6]，将这些 DCT 矩阵中的 DCT 系数，按照从低频到高频进行排列，控制其中某个或多个 DCT 系数之间存在的相关性对秘密信息进行隐藏。而本文方案要求完全无损的还原出原秘密信息图像，因此选择在中高频范围内的系数进行秘密信息嵌入(图 1)。

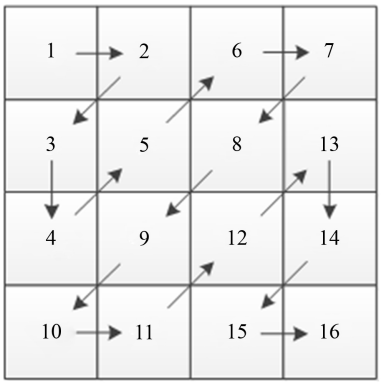


Figure 1. Zigzag scanning sequence diagram
图 1. Zigzag 扫描顺序图

3. 基于 Asmuth-Bloom 门限秘密共享方案信息隐藏算法

本文设计的(*t*, *n*)门限秘密图像信息隐藏算法的流程图如下图 2。

3.1. 子秘密共享图像生成

选取 n 个互素且递增的模数 $m_1,m_2,m_3,\cdots,m_n$。选取素数 q，满足与以上模数互素的要求。本文选取的秘密图像是像素值大小为 64 × 64 的二值图像(BIGC 图)，秘密即为 BIGC 图中的每个像素。二值图像中的每个像素为 0 或 1，所以选取 $q=7$ 满足 q 大于秘密 s。在范围 $\left[0,\left\lfloor\frac{N}{q}\right\rfloor-1\right]$ 内随机取参数 A。再使用公式 $y=s+Aq$ 求得参数 y。最后将参数 y 带入公式 $y_i\equiv y \bmod m_i$。$\left(m_i,y_i\right)$ 即是一个共享份，由于 m_i 已经公开，只要保存 y_i 至 5 个 64 × 64 的矩阵中便可生成 5 份可视的子秘密共享。在本文的实验结果部分将给出参数论证例子及效果展示。

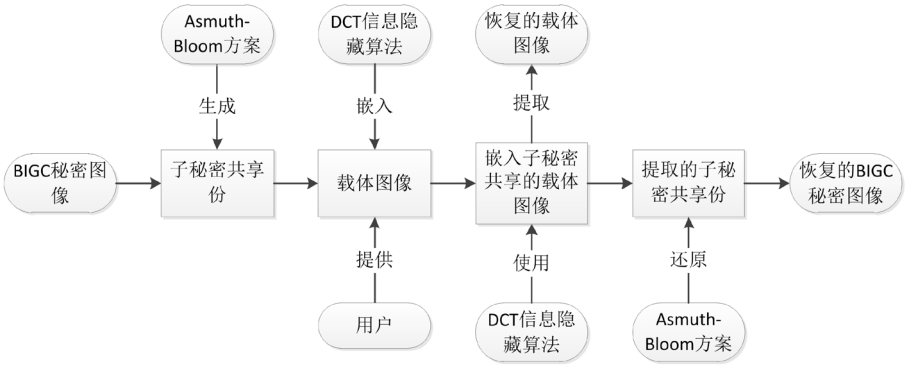


Figure 2. Flow chart of the scheme
图 2. (t, n)门限秘密图像信息隐藏算法的流程图

3.2. DCT 信息隐藏算法

本文选取上文所述第 i 个 DCT 分块中的第 12 个系数(缩写为 $K12_i$)进行秘密信息的嵌入，将水印英文(Watermark)简略为W_i 表示第 i 个水印值，嵌水印规则如下：

$$\begin{cases} K12_i \geq 0 & W_i = 1 \\ K12_i < 0 & W_i = 0 \end{cases}$$

嵌入过程分两种情况讨论，即分 W_i 取值不同时，即

当 $W_i = 0$ 时，保证 DCT 系数 $K12_i \leq -k$，参数 k 是水印嵌入强度，嵌入公式如下：

$$K12_i = \begin{cases} -K12_i & K12_i > k \\ -k & k \geq K12_i \geq -k \\ K12_i & K12_i < -k \end{cases}$$

当 $W_i = 1$ 时，保证 DCT 系数 $K12_i \geq k$，嵌入公式如下：

$$K12_i = \begin{cases} K12_i & K12_i > k \\ k & k \geq K12_i \geq -k \\ -K12_i & K12_i < -k \end{cases}$$

水印提取过程通过检测 DCT 系数$K12_i$的正负性，提取水印W_i，公式如下所示：

$$W_i = \begin{cases} 1 & K12_i \geq 0 \\ 0 & K12_i < 0 \end{cases}$$

本文的方案将每一份子秘密图像的像素值连在一起存成五个大字符串进行五次 DCT 嵌入，提取时不需要获得整个字符串，只需要知道字符串的长度，便可以实现水印的盲提取。进行五次提取，可完整提取出嵌入的字符串，再将它们还原存进五个像素矩阵中，即恢复五个 64 × 64 的子秘密图像。

3.3. 秘密图像恢复

在经过以上秘密信息提取过程后，获得 n 份子秘密图像，任意取其中的 t 份即可恢复原秘密图像。具体过程为先提取子份额，由 $\left\{\left(m_{i_j}, y_{i_j}\right) \mid j = 1, 2, \cdots, t\right\}$ 建立方程组 $\begin{cases} y \equiv y_{i_1} \bmod m_{i_1} \\ y \equiv y_{i_2} \bmod m_{i_2} \\ \vdots \\ y \equiv y_{i_t} \bmod m_{i_t} \end{cases}$，此处 t 为门限。y 为待

求解的数，根据中国剩余定理可求得 $y \equiv y' \bmod N'$，再有 $N' = \prod_{j=1}^{t} m_{i_j} \geq N$,最后计算 $y' \bmod q$ 得到秘密 s，即原秘密图像的每一个像素，生成 64 × 64 大小的矩阵，得出原秘密图像。

4. 实验结果

为了更好的展示基于 Asmuth-Bloom 门限秘密图像信息隐藏算法，本文对基于(3, 5)门限秘密图像信息隐藏算法的进行论证。最后，使用峰值信噪比(PSNR)、平均结构相似性(MSSIM)、比特出错概率(BER)与其他方案效果进行分析和比较。

4.1. 基于(3, 5)门限秘密图像共享信息隐藏算法

本方案选取互素模数 $m_1 = 73$， $m_2 = 79$， $m_3 = 83$， $m_4 = 89$， $m_5 = 97$。素数 $q = 7$，$N = \prod_1^3 m_i = 478661 > q \times m_4 \times m_5 = 7 \times 89 \times 97 = 60431$，参数 A 在 $\left[0, \left\lfloor \frac{N}{q} \right\rfloor - 1\right]$ 范围内随机选取，即[0, 68379]内，此处取 A=51638 进行论证。验证 BIGC 图的第 64 × 64 个像素，即最后一个像素。

选取最后一个像素 1 为秘密。通过公式 $y = s + Aq = 1 + 51638 \times 7 = 361467$。代入公式 $y_i \equiv y \bmod m_i$，得出 y_i。如下公式所示

$$\begin{cases} y_1 \equiv y \bmod m_1 \equiv 361467 \bmod 73 \equiv 44 \\ y_2 \equiv y \bmod m_2 \equiv 361467 \bmod 79 \equiv 42 \\ y_3 \equiv y \bmod m_3 \equiv 361467 \bmod 83 \equiv 2 \\ y_4 \equiv y \bmod m_4 \equiv 361467 \bmod 89 \equiv 38 \\ y_5 \equiv y \bmod m_5 \equiv 361467 \bmod 97 \equiv 45 \end{cases}$$

遍历计算整张图片获得所有像素，计算得到以上 y_i。最后生成图片即可得到子秘密灰度图像。

还原时，首先随机选取(73, 44)、(83, 2)、(89, 38)三份共享份。参数 $M = m_1 \times m_3 \times m_4 = 539251$。计算 $M_i = \frac{M}{m_i}$，这是除了 m_i 以外其他两个模数的乘积。还需计算 t_i， t_i 是 M_i 模 m_i 意义下的逆元，公式表示为 $M_i t_i \equiv 1 \left(\bmod m_i\right)$。综合以上可以求出 $y \equiv \left(\sum_1^t y_i t_i M_i\right) \bmod M \equiv \left(44 \times 47 \times 7387 + 2 \times 65 \times 6497 + 38 \times 51 \times 6059\right) \bmod 539251 \equiv 361467$。最后一步得 $s \equiv y \bmod q \equiv 361467 \bmod 7 \equiv 1$。由此，证明完成，说明秘密共享生成与恢复过程正确，只需要遍历计算每一个像素值。

4.2. (3, 5)门限信息隐藏实验结果分析

第一步运行秘密共享程序，由秘密图像共享生成子秘密共享图像，如下图 3 所示。

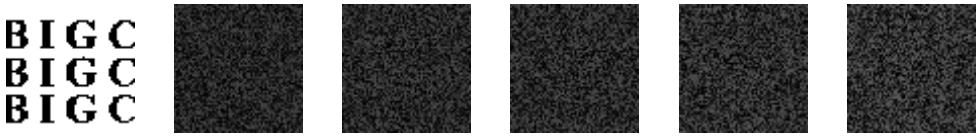
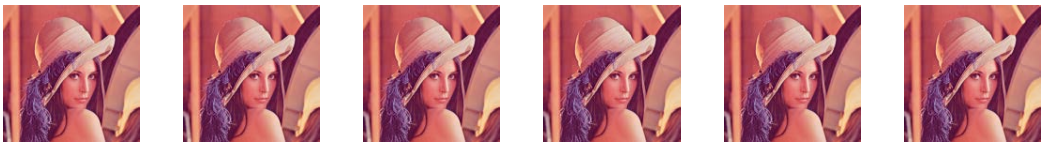


Figure 3. The original image and the generated secret sharing image
图 3. 原始图像与生成的秘密共享图像

由上图可以看出，子秘密共享看上去是无意义图像，也无法获得任何秘密信息。

第二步运用 DCT 信息隐藏算法，将子秘密共享图像嵌入到不同用户提供的带有个人特征的彩色图像，

可以是个人照片，本实验使用 512 × 512 的 Lena 图展示效果，Lena 图 4(b)~(f)表示用户 1~5 提供的图片。



(a) (b) (c) (d) (e) (f)

Figure 4. Comparison of carrier image between Lena original image and embedded secret sharing image
图 4. Lena 原图与嵌入子秘密共享图像的载体图像对比

从视觉角度看，嵌入子秘密共享的用户照片与原图没有区别。当 PSNR 值大于 33 时[7]，肉眼无法识别出嵌入前后的图像区别，嵌入的秘密信息亦不可感知。图片的不可见性随着 PSNR 值的增大而增强，子秘密共享隐藏性越好。在相同嵌入容量下，用 PSNR 值，即峰值信噪比反映嵌入共享的图像峰值信噪比，用 MSSIM 值，即平均结构相似性反应原载体图像与嵌入子秘密共享图像的图像相似度，越接近 1，图像信息隐藏效果越好。由下表体现本方案中信息隐藏的效果优于其他方案。见表 1。

Table 1. PSNR value and MSSIM value of this scheme are compared with other schemes
表 1. 本方案与其他方案 PSNR 值、MSSIM 值对比

图片	文献[8]		文献[9]		本方案	
	PSNR	MSSIM	PSNR	MSSIM	PSNR	MSSIM
Lena	55.46	0.9993	60.44	0.9999	61.34	0.9999

再从嵌入秘密信息的图像中提取出 5 份子秘密图像，并进行还原，完整得出原秘密图像 BIGC 图(图 5)。

Figure 5. The generated secret sharing image and the restored secret image
图 5. 生成的秘密共享图像与还原的秘密图像

通过 BER 函数，即误比特率函数。将图像像素连在一起排成一行大字符串，再转成 0、1 比特流，比较嵌入前与提取后的比特流，原秘密图像与提取图像的比特流，函数值为 0，说明比特流无误比特，即可以验证无误提取。表 2 展示本方案中秘密图像 BER 值。

Table 2. BER value of image before and after restoration
表 2. 恢复前后图像 BER 值

原图片	恢复或提取后的图片	BER 值
BIGC 图	恢复后的 BIGC 图	0
秘密共享图 1	提取后的秘密共享图 1	0
秘密共享图 2	提取后的秘密共享图 2	0
秘密共享图 3	提取后的秘密共享图 3	0
秘密共享图 4	提取后的秘密共享图 4	0
秘密共享图 5	提取后的秘密共享图 5	0

如表 2 所示，通过 BER 函数比较恢复前后秘密图像完全一致，本文方案正确的恢复了秘密图像。

5. 结语

本文利用 Asmuth-Bloom 门限秘密共享技术，设计了一个基于 Asmuth-Bloom 门限共享秘密图像信息隐藏算法。为了更好的理解本文设计的基于 Asmuth-Bloom 门限秘密图像信息隐藏算法，以(3, 5)门限秘密共享方案为例，设计了(3, 5)门限秘密图像共享信息隐藏算法。并对(3, 5)门限信息隐藏算法进行实验论证。实验结果表明本文设计的信息隐藏算法能正确恢复秘密图像，PSNR、MSSIM、BER 等指标优于其他方案。下一步将结合 Asmuth-Bloom 门限秘密共享技术，深入探究在灰度图、彩色图上信息隐藏算法，并选取灰度二维码、彩色二维码，进行秘密共享的应用研究。

基金项目

国家自然科学基金(61370188)；北京市教委科研计划一般项目(KM202010015009)；北京市教委科研计划资助(KM202110015004)；北京印刷学院博士启动金项目(27170120003/020)；BIGC Project (Ec202007)。

参考文献

[1] Shamir, A. (1979) How to Share a Secret. *Communications of the ACM*, **22**, 612-613. https://doi.org/10.1145/359168.359176

[2] Asmuth, C. and Bloom, J. (1983) A Modular Approach to Key Safeguarding. *IEEE Transactions on Information Theory*, **29**, 208-210. https://doi.org/10.1109/TIT.1983.1056651

[3] 王丽娜, 张焕国, 叶登攀, 等. 信息隐藏技术与应用[M]. 武汉: 武汉大学出版社, 2012: 17-18.

[4] Kutter, M., Jordna, F. and Bossen, F. (1997) Digital Signature of Color Images Using Amplitude Modulation. *Proceedings Volume* 3022, *Storage and Retrieval for Image and Video Databases V*, 200-205. https://doi.org/10.1117/12.263442

[5] 张亚泽. 图像秘密共享技术在信息保护中的应用研究[D]: [硕士学位论文]. 西安: 西安理工大学, 2020.

[6] Deng, Y., Kenney, C., Moore, M.S., *et al*. (1999) Peer Group Filtering and Perceptual Color Image Quantization. *IEEE International Symposium on Circuits and Systems*, Orlando, 30 May-2 June 1999, 21-24.

[7] 唐明伟. 图像信息隐藏与隐藏分析算法研究[D]: [博士学位论文]. 成都: 电子科技大学, 2012.

[8] Yuan, H.D. (2014) Secret Sharing with Multi-Cover Adaptive Steganography. *Information Sciences*, **254**, 197-212, https://doi.org/10.1016/j.ins.2013.08.012

[9] Singh, P. and Raman, B. (2018) Reversible Data Hiding Based on Shamir's Secret Sharing for Color Images over Cloud. *Information Sciences*, **422**, 77-97. https://doi.org/10.1016/j.ins.2017.08.077