基于改进 FEMD 算法的可逆秘密图像共享方案

马利民[1]，王佳慧[2]
（1. 北京信息科技大学计算机学院，北京 100101；2. 国家信息中心信息与网络安全部，北京 100045）

摘 要：基于改进的 FEMD 算法提出了一种可逆秘密图像共享方案。首先改进秘密数据的嵌入过程，使原始像素对和嵌入后含密像素对成为一对一的映射；然后通过设置溢出标识位来记录溢出像素对的原始值并进行相应处理。实验数据和分析表明，所提算法可以在保证生成高质量的含密图像的同时，解决不能恢复原始载体图像的问题。

关键词：秘密图像共享；隐写术；FEMD；含密图像
中图分类号：TN918.1
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019130

Invertible secret image sharing scheme based on improved FEMD

MA Limin[1], WANG Jiahui[2]
1. School of Computer Science, Beijing Information Science &Technology University, Beijing 100101, China
2. Department of Information and Security, the State Information Center, Beijing 100045, China

Abstract: Based on the improved FEMD algorithm an invertible secret image sharing scheme was proposed. Firstly, the embedding process of secret data was improved to make the original pixel pair and the stego pixel-pair to become a one-to-one mapping. Then a unique status flag was set to be calculated to record and process the original status of the over flow pixel-pair. Experimental data and analysis show that the proposed algorithm can guarantee the generation of high quality cryptographic images and solve the problem that the original carrier image can not be restored.

Key words: secret image sharing, steganography, FEMD, stego image

1 引言

网络技术的高速发展对于数据传输具有重要意义，然而如何保证秘密数据在网络上的传输安全已成为一个亟待解决的问题。秘密图像共享技术可以将需要安全存放及传输的秘密图像按照一定方法进行划分并分别交给不同管理人。假设目标秘密图像被划分为 n 个图像，只有同时拥有其中的 $t(2\leqslant t\leqslant n)$个划分图像时，才能恢复出秘密图像，防止秘密过于集中，达到一定的安全性；另一方面，如果有划分图像丢失或者损坏，只要剩余的划分图像个数大于或等于 t，仍然可以恢复秘密图像，因此该技术对安全风险具有一定的容忍性。隐写术是信息隐藏技术的一种，用于实现数字内容在网络中的安全存放及传输[1-2]。基于隐写术的秘密图像共享将 n 个共享图像嵌入 n 个载体图像当中，生成 n 个含密图像，通过传输含密图像达

收稿日期：2019−02−22；**修回日期**：2019−05−05
通信作者：王佳慧，wangjiahui@sic,gov.cn
基金项目：中央引导地方科技发展专项基金资助项目（No.Z171100004717002）；北京市教育委员会科技计划基金资助项目（No.KM201811232017）
Foundation Items: Central Guide to Local Science and Technology Development (No.Z171100004717002), The Science and Technology Project of Municipal Education Commission of Beijing (No.KM201811232017)

到安全传输秘密图像的目的。

Shamir[3]首次提出了基于拉格朗日多项式内插原理实现的秘密共享技术，又称为(t, n)−门限秘密共享技术。Thien 等[4]基于(t, n)−门限秘密共享技术提出了秘密图像共享的概念，其中，秘密图像中的每一个像素作为一个秘密信息，与文献[3]不同，他们将$(t-1)$次多项式的每一个系数均用于携带秘密信息，因此生成的每一个划分图像的大小是原始秘密图像大小的$\frac{1}{t}$。此后的一些秘密图像共享方案大都是为了减小生成的划分图像而设计的，如文献[5-6]。Wang 等[5]提出将哈夫曼编码应用于秘密图像的差分图像编码以减少划分图像。Lin 等[6]提出了一种基于隐写术的秘密图像共享方案，将产生的噪声隐藏在多幅载体图像中。基于文献[6]提出的算法框架，后续研究人员提出了许多基于隐写技术的秘密图像共享方案[7-13]。其中，Amir 等[7]利用 OAEP（optimal asymmetric encryption padding）和 IDA（information dispersal algorithm）进一步提高了共享秘密图像的密钥的安全性，并采用 FEMD（fully exploiting modification direction）隐写算法提高了隐写图像质量。Jamal 等[8]通过在共享图像时利用细胞自动机技术来替代上述基于拉格朗日多项式内插原理实现的秘密共享技术，取得了更好的隐写图像质量。上述算法性能较好，但存在的共同问题是载体图像不可恢复，假如载体图像是一些敏感图像（例如军事图像、医学图像），考虑到载体图像的实用价值，应尽量避免这种情况发生。因此，可逆的秘密图像共享技术更具有实用性。

可逆秘密图像共享方法设计过程中，需要考虑载体图像的恢复，因此在秘密共享阶段，需要将载体图像的一些特征信息连同秘密图像一起生成含密图像。这样就可以在秘密图像恢复阶段，利用载体图像特征信息恢复载体图像。对于此类算法，一方面，特征信息提取越少生成的划分图像越小，嵌入载体图像后生成的含密图像质量越高；另一方面，隐写术算法性能的优劣也将决定含密图像的质量。因此，基于隐写术的秘密共享算法需要同时注重这两方面的因素。Lin 等[14]提出一种基于模运算的可逆秘密图像共享机制，该机制利用（$t-1$）次多项式的 t 系数中的$\lceil \log_m 255 \rceil$个系数来携带载体图像中像素的值，剩余的系数则用来携带秘密数据。随后，Lin 等[15]又提出一种能提高嵌入秘密数据量的改进方案，但是这 2 种方案都需要解决溢出问题[16]。Feng 等[17]基于(t, n)−门限秘密共享技术提出一种可逆的主动式秘密图像共享方案，可以实现对生命周期较长的秘密图像进行安全保护，但是生成的含密图像质量有待提高。Liu 等[18]提出一种针对 H.264 的可逆数据共享方案，通过在空间域嵌入秘密信息，但是嵌入数据量较小。

目前，基于隐写术的可逆秘密图像生成的含密图像质量不高，本文针对此问题提出了一种高质量的基于隐写术的可逆秘密图像共享算法，并通过实验进行分析比较。实验结果表明，本文提出的算法可以生成高质量的含密图像，同时可以无损恢复载体图像，在保证秘密图像安全存放的同时增强了其在网络传输的安全性。

2　相关工作

2.1　秘密共享技术

1979 年，Shamir[3]首先提出(t, n)−门限秘密共享技术，该技术基于拉格朗日多项式内插原理实现[19-20]。如果要保护的秘密为 s，则采用(t, n)−门限秘密共享方法进行秘密共享，具体实现步骤如下。

1) 根据式(1)生成一个$(t-1)$次多项式。

$$F(x)=(a_0+a_1x^1+\cdots+a_{t-1}x^{t-1}) \bmod \mathrm{GF}(p) \quad (1)$$

其中，$t\geqslant 2$，GF (p)是一个有限域，p 是一个素数或者 $p=2^m$，$a_0=s$，$a_1, a_2, \cdots, a_{t-1}$ 是随机选择且分布在$[0, p-1]$范围内的整数。

2) 根据 n 个参与者选定的密钥 $X=\{x_1, x_2, \cdots, x_i, \cdots, x_n\}$生成 n 个划分 $y_1, y_2, \cdots, y_i, \cdots, y_n$。

$$y_i=F(x_i),\ 1\leqslant i\leqslant n$$

其中，$n\geqslant t$。将 y_i 交由对应的参与者进行保管。

恢复秘密信息 s 时，需随机选择 t 个划分，即 $y_1, y_2, \cdots, y_t$，基于拉格朗日多项式内插方法重建多项式 $F(x)$，如式(2)所示，其常数项系数即是秘密信息 s 的值。

$$F(x)=\left[\sum_{i=1}^{t} y_i \prod_{\substack{j=1 \\ j\neq i}}^{t} (x_i-x_j)^{-1}(x-x_j)\right]_{\bmod \mathrm{GF}(p)} \quad (2)$$

2.2　FEMD 算法

在基于隐写术实现可逆秘密图像共享方案中，特征提取方法和隐写算法是决定含密图像质量好坏的关键因素。Kieu 等[21]给出了一种很好的隐写算法——FEMD 算法，但是由于嵌入过程中存在多对一的映射关系及溢出像素问题，该算法无法实现

载体图像的恢复。

FEMD 算法的基本思想是将一个 s^2 进制数嵌入一个像素对(a_i, a_{i+1})中，嵌入过程中对 a_i 或者 a_{i+1} 的最大改变量为 $r=\lfloor \frac{s}{2} \rfloor$，其中 $0 \leqslant a_i, a_{i+1} \leqslant 255$。当 s 值固定时，算法的最大嵌入量为 $\frac{\lceil \mathrm{lb}s^2 \rceil}{2}$ bit/pixel，因此 s 值越大，最大嵌入量越大，但嵌入失真也就越大。基于 FEMD 算法将 s^2 进制系统中的一个数 d 嵌入像素对(a_i, a_{i+1})中得到含密像素对(b_i, b_{i+1})，具体步骤如下。

步骤 1 定义提取函数 $F(x_i, x_{i+1})$如式(3)所示。

$$F(x_i, x_{i+1}) = ((s-1)x_i + sx_{i+1}) \bmod s^2 \tag{3}$$

步骤 2 建立一个 256×256 的映射矩阵 $\boldsymbol{M}$，如式(4)所示。

$$\boldsymbol{M}[x_i][x_{i+1}] = F(x_i, x_{i+1}),\ x_i, x_{i+1} = 0,1,2,\cdots,255 \tag{4}$$

步骤 3 根据式(3)计算(a_i, a_{i+1})的提取函数值 $F(a_i, a_{i+1})$。

步骤 4 若 $F(a_i, a_{i+1}) = d$，$(b_i, b_{i+1}) = (a_i, a_{i+1})$，嵌入结束；否则执行步骤 5。

步骤 5 在映射矩阵 $\boldsymbol{M}$ 中定义一个以(a_i, a_{i+1})为中心的方形搜索框 W，如式(5)所示。

$$W(s,(a_i, a_{i+1}), r) = \{\boldsymbol{M}[a_i - r + u][a_{i+1} - r + v] | 0 \leqslant u \leqslant 2r, 0 \leqslant v \leqslant 2r\} \tag{5}$$

步骤 6 扫描搜索框中的每一个元素，使 $\boldsymbol{M}[p][q]=d$。若满足条件的像素对(p,q)不止一个，则选择具有最小嵌入失真 D 的像素对赋值给(b_i, b_{i+1})，其中，D 根据式(6)进行计算。

$$D = |p - a_i| + |q - a_{i+1}| \tag{6}$$

在提取端，根据参数 s 来定义提取函数 $F(x_i, x_{i+1})$，s 需要通过一种安全保密的方式传递给提取端。假设提取端接收到的像素对为 (b_i', b_{i+1}')，则嵌入的秘密数据 $d' = F(b_i', b_{i+1}')$。

通过研究 FEMD 算法发现，对于大部分像素对，可以通过将原始像素对的提取函数值作为秘密信息嵌入含密像素对中恢复原始像素对的值。但是对于有些像素对则不可恢复，本文称之为问题像素对。问题像素对可以分为 2 类，第一类是由嵌入秘密信息时可以对应不同含密像素对的问题像素对组成；第二类是由溢出像素对构成，所谓溢出像素对是指像素对中至少有一个像素的值落在区间 $[0, r) \cup (255-r, 255]$。

对于第一类问题像素对，其嵌入过程是一个一对多的映射，例如当 s=4 时，所建立的映射矩阵 $\boldsymbol{M}$ 如图 1 所示。选择的像素对$(a_i, a_{i+1}) = (4, 5)$，浅灰色矩形框为根据式(5)构建的方形搜索框 W，深灰色标注位置为所要嵌入的秘密数据 d=11，按照 FEMD 算法嵌入数据后得到的含密像素对的值为$(b_i, b_{i+1})=(5, 3)$或者$(b_i, b_{i+1})=(5, 7)$，此时无法通过 FEMD 算法将 $F(a_i, a_{i+1})$ 的值嵌入(b_i, b_{i+1})中来恢复(a_i, a_{i+1})的值。对于第二类问题像素对，即溢出像素对，采用 FEMD 算法在一个像素对(a_i, a_{i+1})中嵌入秘密数据时，可能无法从搜索框 $W(s,(a_i,a_{i+1}),r)$中找到一个元素等于所要嵌入的秘密数据。因此，FEMD 算法在一个载体图像中嵌入秘密数据之前，将位于区间$[0, r)$ 和 $(255-r, 255]$的所有数据作为溢出像素，分别用 r 和 $255-r$ 来替换，然后在修改后的像素中嵌入秘密信息。这样对溢出像素对的修改过程是一个多对一的映射，因此根据修改后数值无法知晓原始溢出像素的值。

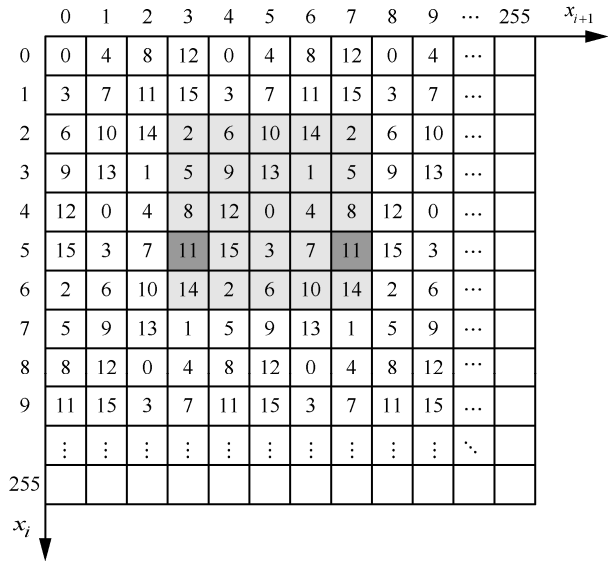


图 1 当 s=4 时 FEMD 算法中构建的映射矩阵 $\boldsymbol{M}$

FEMD 算法作为一种隐写术算法，实现了较高的嵌入量和较好的含密图像质量，此后 Kuo 等[22]对其进行了改进，提出一种新的隐写术算法，在秘密数据嵌入载体像素时，利用数学式计算含密像素。Kuo 等[23]提出一种基于 FFEMD（formula FEMD）算法和像素值差分办法来克服溢出问题。这些算法大多只是改进隐写术的性能而没有在秘密共享方面进行设计。

3　可逆秘密图像共享算法的设计

3.1　改进 FEMD 算法

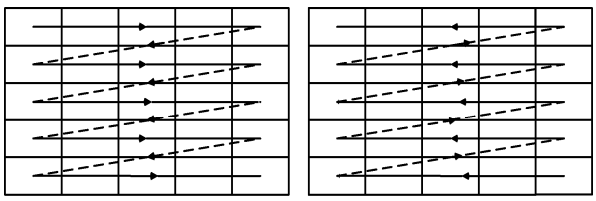
针对 FEMD 算法处理过程中遇到的问题像素对，本文从嵌入过程和溢出像素对处理两方面解决像素对的可逆性恢复问题。

3.1.1　改进的 FEMD 算法嵌入过程

在采用 FEMD 算法嵌入秘密数据时，需按照一定方向遍历搜索框，使原始像素对和嵌入后含密像素对成为一对一的映射。对 FEMD 算法嵌入过程的步骤 6 改进如下。

步骤 6 按照图 2 (a)中所示方向遍历搜索框，嵌入过程为自左至右，扫描到最右边后从下一行最左侧开始继续遍历，直到找到满足条件 $\boldsymbol{M}[p][q]=d$ 且具有最小嵌入失真 D 的像素对(p, q)，如果这样的像素对不止一对，则将最先扫描到的像素对赋值给(b_i, b_{i+1})。

在使用改进 FEMD 算法进行秘密信息嵌入后，利用提取函数 $F(a_i, a_{i+1})$和 s 就可以从含密像素对(b_i, b_{i+1})中恢复原始像素对(a_i, a_{i+1})。但恢复时需按图 2(b)中所示方向进行遍历，与嵌入时扫描方向相反。



(a) 嵌入过程　　(b) 恢复过程

图 2　扫描方向

3.1.2　溢出像素对处理

为每一个溢出像素对分配一个溢出标志位 sf 来记录其原始状态，然后分别用 r 和 $255-r$ 替换溢出像素对的值。为了唯一地恢复原始像素对的值，本文在对溢出像素对(a_i, a_{i+1})设计溢出标志位 sf 时，分为 2 种情况进行处理。

1) a_i和 a_{i+1}的值都属于区间$[0,r]\cup[255-r,\ 255]$

$$\mathrm{sf}=(a_i \bmod (255-r))(r+1)+(a_{i+1} \bmod (255-r)) \tag{7}$$

2) 像素对中只有一个数位于区间 $[0,r]\cup[255-r,\ 255]$

$$\mathrm{sf}=\min(a_i \bmod (255-r), a_{i+1} \bmod (255-r)) \tag{8}$$

如果一个溢出像素对(R_j, R_{j+1})经上述方法处理后，像素对为(R'_j, R'_{j+1})，溢出标志位为 sf，那么根据(R'_j, R'_{j+1})和 sf 可以通过下面的方法恢复(R_j, R_{j+1})。

1) 若 $R'_j, R'_{j+1}\in\{r, 255-r\}$，$(R_j, R_{j+1})$可以根据式(9)计算得到。

$$\begin{aligned} R_j &= \left\lfloor \frac{R'_j}{255-r} \right\rfloor (255-r)+\left\lfloor \frac{\mathrm{sf}}{r+1} \right\rfloor \\ R_{j+1} &= \left\lfloor \frac{R'_{j+1}}{255-r} \right\rfloor (255-r)+(\mathrm{sf} \bmod (r+1)) \end{aligned} \tag{9}$$

2) 若 R'_j 和 R'_{j+1} 中只有一个数等于 r 或者 $255-r$，为解释方便，本文将等于 r 或者 $255-r$ 的数据表示为 X'，另一个数据表示为 Y'，其相应的原始像素的值分别表示为 X 和 Y，那么 $Y=Y'$，X 可以根据式(10)计算得到。

$$X=\left\lfloor \frac{X'}{255-r} \right\rfloor (255-r)+\mathrm{sf} \tag{10}$$

通过上述对溢出像素对的处理方法可以实现基于改进的 FEMD 算法来恢复原始溢出像素对的值，实现载体图像的无损恢复。

3.2　秘密图像共享及嵌入

在本文提出的方法中，用一幅灰度图像作为载体图像，利用(t, n)−门限秘密共享技术来生成共享划分，最后基于改进 FEMD 算法将生成的共享划分单独地嵌入一幅载体图像中形成 n 个含密图像。为了恢复原始载体图像的值，提取端需要知道载体图像的所有像素对的特征值。对于载体图像的每个像素对，根据式(1)构建$(t-1)$次多项式时，需要根据 3.1 节提出的算法，利用一个或 2 个系数存储该像素对的特征值，用剩余的系数来携带来自于秘密图像的秘密信息。在实现方案中，采用基于 2^m 的有限域 GF (2^α)来构建$(t-1)$次多项式，为此需要将秘密图像中的每个像素采用 2^α 进制数来表示。对于参数为 s 的改进 FEMD 算法，其可嵌入的秘密数据的数值落在$[0, s^2)$，为了兼容，采取的有限域 GF (2^α)算法中要求 $2^\alpha=s^2$，因此本文中 $\alpha=s=2$ 或者 $\alpha=s=4$。

假设秘密图像 I 大小为 $h_s\times w_s$，宿主载体图像 C 大小为 $h_c\times w_c$，n 个参与者所对应的 n 个互不相同的密钥表示为 $X=\{x_1, x_2, \cdots, x_n\}$，则基于改进的 FEMD 可逆秘密图像共享方案的共享及嵌入流程如图 3 所示，算法过程如下。

1) 将 I 中的数据重新排列为一维矢量 $\boldsymbol{S}=\{s_1, s_2, \cdots, s_{(h_s\times w_s)}\}$。

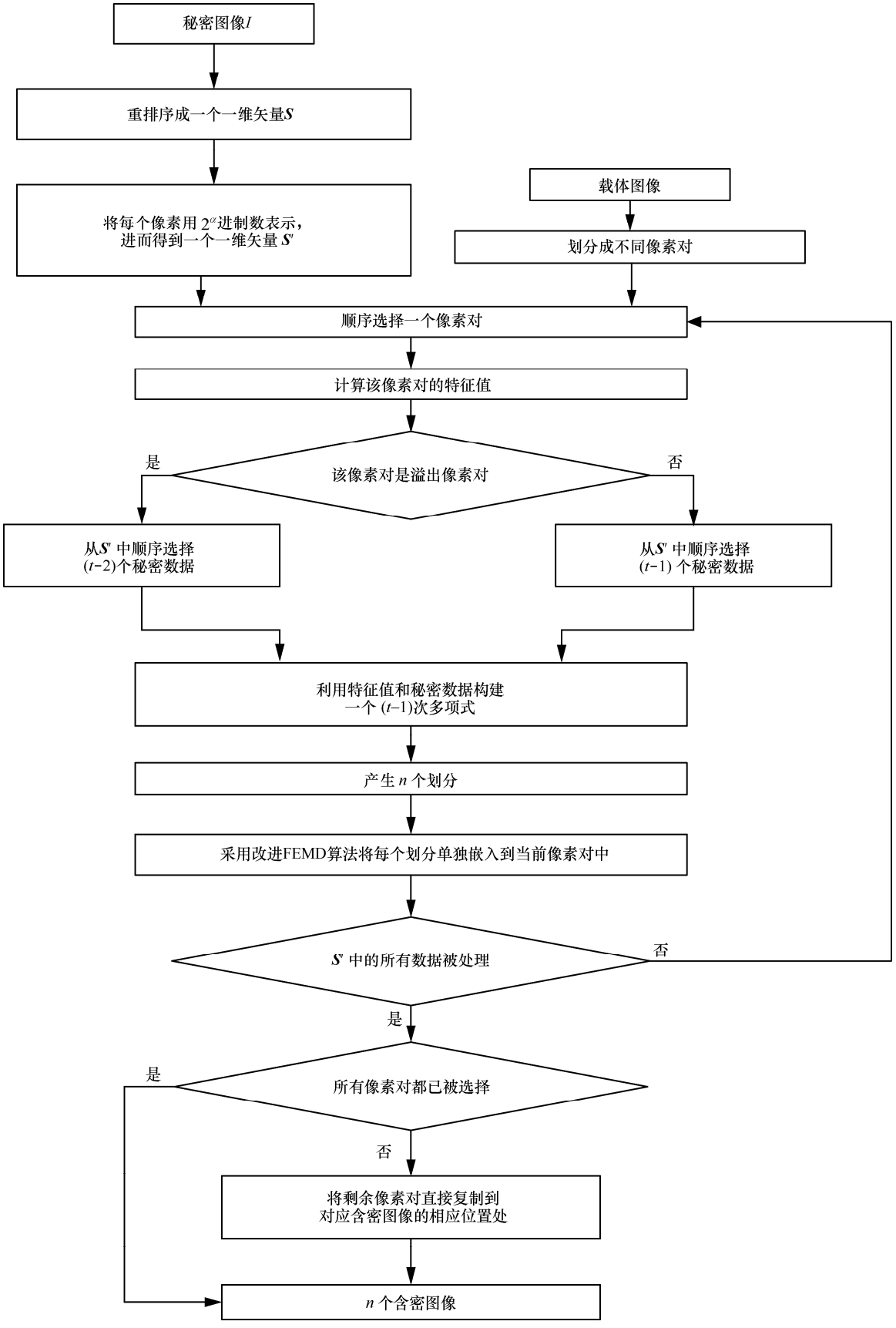


图 3　可逆秘密图像共享及嵌入流程

2) 将 $\boldsymbol{S}$ 中的每一个像素用 $\left\lceil \frac{8}{\alpha} \right\rceil$ 个 2^{α} 进制数表示，进而形成一个矢量 $\boldsymbol{S}'=\{d_1,d_2,\cdots,d_l,\cdots,d_{(h_s\times w_s\times\left\lceil\frac{8}{\alpha}\right\rceil)}\}$，其中，$0\leqslant d_l<2^{\alpha}$, $l=1, 2, \cdots, h_s\times w_s\times\left\lceil\frac{8}{\alpha}\right\rceil$。

3) 顺序化遍历 C 中的每一个像素，将相邻 2 个像素作为一个像素对(c_i, c_{i+1})。

4) 若(c_i, c_{i+1})是溢出像素对，按照式(7)或式(8)计算溢出标志位 sf，然后利用式(3)计算经溢出过程处理后的修改像素对的提取函数值 f；否则，直接计算(c_i, c_{i+1})的提取函数值f。

5) 若(c_i, c_{i+1})是溢出像素对，从 $\boldsymbol{S}'$中顺序选择$(t-2)$个连续的 2^{α} 进制数，形成划分片段$(\mathrm{ds}_1^j,\mathrm{ds}_2^j,\cdots,\mathrm{ds}_{t-2}^j)$；否则，从 $\boldsymbol{S}'$中顺序选择$(t-1)$个数据，形成划分片段$(\mathrm{ds}_1^j,\mathrm{ds}_2^j,\cdots,\mathrm{ds}_{t-1}^j)$。

6) 若(c_i, c_{i+1})是溢出像素对，利用 f、sf 和$(\mathrm{ds}_1^j,\mathrm{ds}_2^j,\cdots,\mathrm{ds}_{t-2}^j)$构建式(11)。

$$F_j(x)=(f+\mathrm{sf}x^1+\mathrm{ds}_1^j x^2+\cdots+\mathrm{ds}_{t-2}^j x^{t-1})\mathrm{GF}(2^{\alpha}) \tag{11}$$

否则，构建式(12)。

$$F_j(x)=(f+\mathrm{ds}_1^j x^1+\cdots+\mathrm{ds}_{t-1}^j x^{t-1})\mathrm{GF}(2^{\alpha}) \tag{12}$$

7) 将 n 个密钥 x_k 分别代入 $F_j(x)$中得到 $F_j(x_k)$，其中，$k\in[1, n]$。

8) 对于每个 $F_j(x_k)$，$k\in[1, n]$，基于改进 FEMD 算法单独嵌入(c_i, c_{i+1})中得到含密图像 SI_k 中对应的含密像素对。

9) 重复执行步骤 3)～步骤 8)，直到 $\boldsymbol{S}'$中的所有数据处理完毕。

10) 至此，若载体图像中尚有剩余像素对没有嵌入数据，则直接将剩余的像素对复制到含密图像 SI_k 的对应位置。

经过上面的处理，可以得到 n 个大小为 $h_c\times w_c$ 的含密图像 SI_k，$k=1, 2, \cdots, n$，这 n 个含密图像将由相应的参与者保管。另外，由于提取端需要知道秘密图像大小 $h_s\times w_s$ 和参数 s 才能恢复出秘密图像和载体图像，这 2 个信息将作为算法的私钥通过一种安全的方式发送给提取端。

3.3　秘密图像提取和载体图像恢复

根据(t, n)−门限秘密共享技术原理，恢复出共享的秘密图像至少需要 t 个不同的含密图像，假设所提供的含密图像是 $\mathrm{SI}_1, \mathrm{SI}_2, \cdots, \mathrm{SI}_t$，对应的参与者所拥有的密钥分别是 $x_1, x_2, \cdots, x_t$，则提取端进行秘密图像提取和原始载体图像恢复的过程如下。

1) 对于每个含密图像 SI_i，$i=1, 2, \cdots, t$，顺序选择 2 个相邻的像素作为一个像素对$(\mathrm{SI}_j^i,\mathrm{SI}_{j+1}^i)$，根据式(3)计算其提取函数值$f_i$。

2) 根据步骤 1)得到的 t 组数据(x_i, f_i)，$i=1, 2, \cdots, t$，来重建多项式 $F(x)$，如式(13)所示，其中 $\alpha=s$。

$$F(x)=\left[\sum_{i=1}^{t} f_i\prod_{\substack{j=1\\ j\neq i}}^{t}(x_i-x_j)^{-1}(x-x_j)\right]_{\mathrm{mod\,GF}(2^{\alpha})}=$$
$$(a_0+a_1x^1+\cdots+a_{t-1}x^{t-1})_{\mathrm{mod\,GF}(2^{\alpha})} \tag{13}$$

3) 根据共享过程可知，a_0所承载的信息就是原始载体图像对应像素对（或修改后溢出像素对）的提取函数值，因此根据 $(\mathrm{SI}_j^i,\mathrm{SI}_{j+1}^i)$ 的值，利用 3.1 节中给出的原始像素对恢复方法即可得到之前像素对的值，这里用 (R'_j, R'_{j+1}) 来表示。根据 a_0 和 $(\mathrm{SI}_j^1,\mathrm{SI}_{j+1}^1)$ 的值以及恢复算法计算得到 (R'_j, R'_{j+1})。

4) 通过以下步骤提取秘密图像和恢复载体图像中像素对(R_j, R_{j+1})的值。

① 如果 R'_j 和 R'_{j+1} 都不等于 r 或者 $255-r$，则说明宿主载体中的原始像素对不是溢出像素对，此时(R_j, R_{j+1})的值等于 (R'_j, R'_{j+1}) 的值。因此，重建多项式 $F(x)$中系数$(a_1, a_2, \cdots, a_{t-1})$均承载的是秘密数据。

② 如果 R'_j 和 R'_{j+1} 之间至少有一个等于 r 或者 $255-r$，则说明宿主载体中的原始像素对是溢出像素对。根据嵌入过程可知，系数 a_1 所承载的是溢出标志位的信息，其他系数$(a_2, a_3, \cdots, a_{t-1})$承载的是秘密信息。这时可以根据溢出标志位 a_1 和 (R'_j, R'_{j+1}) 的值来恢复原始像素对(R_j, R_{j+1})的值。

5) 重复执行步骤 1)～步骤 4)，直至所提取出的秘密数据个数为 $h_s\times w_s\times\left\lceil\frac{8}{\alpha}\right\rceil$，然后将含密图像 SI_1 中的剩余像素直接赋值给载体图像中的相应位置处，即可恢复宿主载体图像。

6) 顺序化排列得到的秘密数据。将每 $\left\lceil\frac{8}{\alpha}\right\rceil$ 个相邻的秘密数据转化成一个十进制数可以得到一个一维矢量，然后将其重新排列为 $h_s\times w_s$ 的二维矩阵即可获取秘密图像内容。

4　实验结果及分析

首先，为了分析所提算法对不同载体图像进行处理后得到的含密图像的质量，在模拟实验中本文使用 10 幅 512 像素×512 像素的灰度图像作为作载体图像来测试算法性能，根据有限域 GF (2^{α})算法中要求 $2^{\alpha}=s^2$，改进 FEMD 算法中的参数 $s=\alpha=4$。对于本文算法来说，可供嵌入的秘密图像的最大尺寸为 $h_s \times w_s = \dfrac{h_c \times w_c \times (t-1)}{2 \times \left\lceil \dfrac{8}{\alpha} \right\rceil}$，实验中选取的秘密图像是 300 像素×300 像素的图像，如图 4 所示，因此需设置实验参数为 $t=3$，$n=3$。对于基于隐写术实现秘密图像共享的算法，生成的含密图像失真越小，在网络中传输时越不易被攻击者察觉，安全性越好。本文用 PSNR（peak signal to noise ratio）指标来衡量得到的含密图像质量。

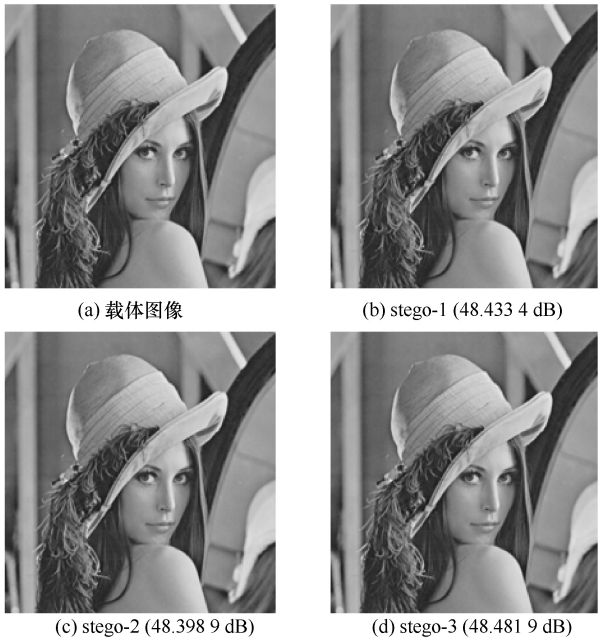
图 4　秘密图像（300 像素×300 像素）

表 1 为 10 幅图像作为载体图像使用改进的 FEMD 算法得到含密图像的 PSNR 结果。此外，图 5 展示了 Lena 图像作为载体图像时得到的 3 幅含密图像。从表 1 及图 5 可以看出，在以上实验条件下，嵌入的秘密图像大小为 300 像素×300 像素，本文提出的改进 FEMD 算法可以取得高达 48 dB 的含密图像质量，同时肉眼无法看出含密图像与原始载体图像的差别，因此所提算法具有良好的不可见性。

其次，为了进一步比较分析算法性能，将本文算法与文献[15-17]算法进行比较。其中，为使对比算法可以取得最好的结果，并保持相同的实验条件，即嵌入的秘密图像为 300 像素×300 像素的图像，在实现文献[15]算法时将其参数 m 设置为 3，将文献[16]算法中参数 α 设置为 2，将文献[17]算法中参数设置为 $t=7$，$m=3$。表 2 是实验数据对比，就含密图像质量来说，本文算法相比文献[15]、文献[16]和文献[17]中算法可以分别实现 6.4 dB、2.8 dB 和 0.57 dB 的性能提高。

表 1　　**含密图像质量**

载体图像	PSNR of stego-1/dB	PSNR of stego-2/dB	PSNR of stego-3/dB	平均 PSNR/dB
Lena	48.433 4	48.398 9	48.481 9	48.438 1
baboon	48.439 2	48.390 5	48.502 2	48.443 9
pepper	48.429 3	48.389 7	48.448 2	48.422 4
boat	48.454 7	48.391 8	48.490 3	48.445 6
bridge	48.408 0	48.343 7	48.433 4	48.395 0
man	48.015 7	47.989 7	48.013 2	48.006 2
tiffany	48.412 8	48.338 5	48.419 9	48.390 4
zelda	48.427 0	48.358 3	48.375 3	48.386 9
alaine	48.438 7	48.389 4	48.491 1	48.439 7
barbara	48.452 0	48.397 1	48.491 7	48.446 9
平均	48.391 0	48.338 7	48.414 7	48.381 5



(a) 载体图像　(b) stego-1 (48.433 4 dB)　(c) stego-2 (48.398 9 dB)　(d) stego-3 (48.481 9 dB)

图 5　含密图像质量评估

对于本文算法，当 $t=3$，$s=4$ 时，采用本文算法共享和嵌入一个 8 bit 数据在一个像素上所引入的误差可以通过式(14)计算得到，为 1.375。采用文献[15]算法和文献[16]算法，实现一个 8 bit 数据的共享和嵌入时，在载体图像的一个像素上引入的误差可以分别通过式(15)和式(16)来计算，当 $t=3$，$m=3$，$\alpha=2$

时，引入的误差分别为 5 和 2.5。因此本文算法得到的含密图像质量比较好。本文算法可以为秘密图像的安全存放和传输提供一种很好的一体化解决方案。

表 2　　算法性能比较

载体图像	含密图像的平均 PSNR/dB			
	文献[15]算法	文献[16]算法	文献[17]算法	本文算法
Lena	42.038 7	45.625 6	47.803 5	48.438 1
baboon	42.048 7	45.620 8	47.801 2	48.443 9
pepper	42.055 1	45.632 1	47.810 1	48.422 4
boat	42.037 8	45.602 9	47.791 5	48.445 6
bridge	42.100 2	46.714 6	47.843 6	48.395 0
man	41.993 9	45.698 1	47.785 9	48.006 2
tiffany	42.035 3	45.620 4	47.825 2	48.390 4
zelda	42.037 7	45.623 6	47.795 4	48.386 9
alaine	42.045 2	45.604 3	47.806 8	48.439 7
barbara	42.049 8	45.617 3	47.834 2	48.446 9
平均	42.044 2	45.735 9	47.809 7	48.381 5

$$E=\frac{\lceil \log_{16}255\rceil}{3-1}\times\left(4\times\frac{1}{16}+4\times\frac{2}{16}+3\times\frac{4}{16}+4\times\frac{5}{16}\right)\times\frac{1}{2}=\frac{44}{32}=1.375 \tag{14}$$

$$E_{15}=\frac{\lceil \log_{m}255\rceil}{t-1}\times\left(\frac{1}{m}\times1+\frac{1}{m}\times2^2+\cdots+\frac{1}{m}\times(m-1)^2\right) \tag{15}$$

$$E_{16}=\frac{\left\lceil\frac{8}{\alpha}\right\rceil}{t-1}\times\left(\frac{1}{2^{\alpha}}\times1+\frac{1}{2^{\alpha}}\times2^2+\cdots+\frac{1}{2^{\alpha}}\times(2^{\alpha}-1)^2\right) \tag{16}$$

5　结束语

本文重点分析了基于隐写术的可逆秘密图像共享方案，提出了一种基于改进 FEMD 算法的可逆秘密图像共享算法。作为一种隐写算法，由于嵌入过程及在对溢出像素处理时的不唯一性，FEMD 算法无法实现可逆秘密图像共享方案设计。本文从嵌入过程和对溢出像素对处理两方面来改进 FEMD 算法，并利用改进的 FEMD 算法设计了一种基于隐写术的可逆秘密图像共享方案。实验结果表明，本文提出的算法可以生成高质量的含密图像，在保证秘密图像安全存放的同时增强了其在网络传输的安全性，具有较高的实用性。

参考文献：

[1] 梁建武,刘晓书,程资.基于图态和中国剩余定理的量子秘密共享方案[J]. 通信学报, 2018, 39(10): 72-78.
LIANG J W, LIU X S, CHEN Z. Quantum secret sharing with graph states based on Chinese remainder theorem[J]. Journal on Communications, 2018, 39(10): 72-78.

[2] 孙曦, 张卫明, 俞能海.基于空域图像变换参数扰动的隐写术[J].通信学报, 2017, 38(10): 167-174.
SUN X, ZHANG W M, YU N H. Steganography based on parameters' disturbance of spatial image transform [J]. Journal on Communications, 2017, 38(10): 167-174.

[3] SHAMIR A. How to share a secret[J].Communications of the ACM, 1979, 22(11): 612-613.

[4] THIEN C C,LIN J C.Secret image sharing[J].Computers and Graphics, 2002, 26(5): 765-770.

[5] WANG R Z, SU C H.Secret image sharing with smaller shadow images[J]. Pattern Recognition Letters, 2006, 27(6): 551-555.

[6] LIN C C, TSAI W H. Secret image sharing with steganography and authentication[J]. Journal of Systems and Software, 2004, 73(3): 405-414.

[7] AMIR M A, MARYAM A. A novel secret image sharing with steganography scheme utilizing optimal asymmetric encryption padding and information dispersal algorithms[J].Signal Processing: Image Communication, 2019, 74(5): 78-88.

[8] JAMAL Z A, MOHAMMADEBRAHIM S A, ALIMOHAMMAD L.An adaptive secret image sharing with a new bitwise steganographic property[J].Information Sciences, 2016, 369(C): 467-480.

[9] YANG C N, CHEN T S, YU K H, et al. Improvements of image sharing with steganography and authentication[J]. Journal of Systems and Software, 2007, 80(7): 1070-1076.

[10] WU C C, KAO S J, HWANG M S. A high quality image sharing with steganography and adaptive authentication scheme[J]. Journal of Systems and Software, 2011, 84(12): 2196-2207.

[11] ULUTAS M, ULUTAS G, NABIYEV V V. Secret image sharing with enhanced visual quality and authentication mechanism[J]. Journal of Photographic Science, 2011, 59(3): 154-165.

[12] ESLAMI Z, AHMADABADI J Z. Secret image sharing with authentication-chaining and dynamic embedding[J]. Journal of Systems and Software, 2011, 84(5):803-809 .

[13] CHANG C C, CHEN Y H, WANG H C, Meaningful secret sharing technique with authentication and remedy abilities[J]. Information Sciences, 2011, 181(14): 3073-3084.

[14] LIN P Y, LEE J S, CHANG C C. Distortion-free secret image sharing mechanism using modulus operator[J]. Pattern Recognition, 2009,

42(5): 886-895.

[15] LIN P, CHAN C. Invertible secret image sharing with steganography[J]. Pattern Recognition Letter. 2011, 31(13):1887-1893.

[16] LIN Y Y, WANG R Z. Improved Invertible Secret Image Sharing with Steganography[C]//International Conference of Intelligent Information Hiding and Multimedia Signal Processing. 2011: 93-96.

[17] FENG B, YUAN Q Q, GUO C, et al. Invertible proactive secret image sharing[J]. Journal of Chinese Computer Systems, 2015, 36(3): 514-518.

[18] LIU Y, CHEN L, HU M, et al. A reversible data hiding method for H.264 with Shami's (*t, n*)-threshold secret sharing[J]. Neurocomputing, 2016, 188(2):63-70.

[19] MENG Q Q, YANG X Y, ZHONG W D, et al. Implementation and optimization of S-box resisting DPA attacks based on secret sharing [J]. Netinfo Security, 2018, 18(2): 71-77.

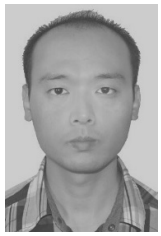
[20] CHENG Z, JIN L R, SHI J J. (*k*, *n*) Threshold quantum secret sharing scheme based on the generation of reed solomon code [J]. Netinfo Security, 2016, 16(4): 44-49.

[21] KIEU T D, CHANG C C. A steganographic scheme by fully exploiting modification directions[J]. Expert Systems with Applications. 2011, 38(8): 10648-10657.

[22] KUO W C, KAO M C. A steganographic scheme based on formula fully exploiting modification directions[J].IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,2013, E96-A(11): 2235-2243.

[23] KUO C W, LI J J, WANG C C, et al. An improved data hiding scheme based on formula fully exploiting modification directions and pixel value differencing method[C]// The 11th Asia Joint Conference on Information Security. 2016: 136-140.

[作者简介]



马利民（1983− ），男，山东泰安人，博士，北京信息科技大学讲师，主要研究方向为网络安全协议、信息隐藏技术、大数据安全。

王佳慧（1983− ），女，山西大同人，博士，国家信息中心研究员，主要研究方向为云计算安全、数据安全、大数据分析及安全、云取证安全。