

结合随机映射和改进缝合线的纹理合成隐藏

李国利,邵利平,任平安

(陕西师范大学 计算机科学学院,陕西 西安 710119)

摘要:传统修改式信息隐藏无法抵抗密写分析的检测,纹理构造式信息隐藏只能生成简单质地的纹理,不能对秘密信息进行有效掩盖,纹理拼接式信息隐藏,秘密信息与样本小块之间存在着固定的映射关系以及码块间的区别特征,会导致信息泄露,降低其安全性。针对以上问题,提出了一种结合随机映射和改进缝合线的纹理合成隐藏方法。首先将样本图像划分为样本小块并依据样本小块均值划分为不同类别,然后通过建立起秘密信息分段和样本小块类别间的随机映射关系来编码秘密信息并将其放置在空白图像的特定位置上,最后按改进缝合线纹理合成方法将放置小块与相邻小块进行纹理合成并生成含密纹理。实验结果表明,该方法可通过合成纹理来对秘密信息进行掩盖,秘密信息分段和编码样本小块不一一对应,该方法完全依赖于用户密钥且具备一定的抗攻击能力。

关键词:纹理合成;信息隐藏;图像缝合;生成式隐藏;样例纹理合成

中图分类号:TP309.7

文献标识码:A

文章编号:1673-629X(2020)01-0106-06

doi:10.3969/j.issn.1673-629X.2020.01.019

Texture Synthesis Information Hiding Method Combining Random Mapping and Improved Image Quilting

LI Guo-li, SHAO Li-ping, REN Ping-an

(School of Computer Science, Shaanxi Normal University, Xi'an 710119, China)

Abstract: Traditional modified information hiding cannot resist detections from steganographic analysis. Texture constructive information hiding can only generate simple texture and it cannot cover secret information effectively. In texture splicing information hiding, it leads to information leakage and poor security due to the fixed mapping relationship between secret information segments and sample blocks or the distinguishing features of coding blocks. To address these problems, texture synthesis information hiding method combining random mapping and improved image quilting is proposed. Firstly, the sample image is divided into sample blocks and then classified into different categories by sample block means. Secondly, secret information sections are encoded then placed in blank image at particular positions by setting a random mapping relationship between secret information segments and the sample categories. Finally, an improved image quilting method is used to stitch each encoding block with its adjacent blocks in order to generate a stego texture. Experiment shows the proposed method can cover secret information by texture synthesis. Secret information segmentations and encoding sample blocks do not correspond to each other. The proposed method relies entirely on user key 0uuopp090j01;-s and has some anti-attack capability.

Key words: texture synthesis; information hiding; image quilting; generative hiding; sample texture synthesis

1 概述

随着互联网的发展,越来越多的信息通过网络传输,在给人们带来极大便利的同时,也存在一定安全隐患。为保护传输中的秘密信息安全,人们提出用图像

来隐藏秘密信息的方法,并把它应用在分存^[1-4]、密写^[5-6]和水印上。但这些方法的本质都是传统修改式嵌入的信息隐藏方法,需修改载体图像,会对嵌密载体视觉质量造成较大影响,容易引起攻击者的怀疑。

收稿日期:2019-01-28

修回日期:2019-05-30

网络出版时间:2019-09-24

基金项目:国家自然科学基金(61100239);陕西省自然科学基金(2011JQ8009, 2016JM6065);中央高校基本科研业务费支持项目(GK201402036, GK201703057)

作者简介:李国利(1991-),女,硕士研究生,研究方向为纹理合成信息隐藏;邵利平,博士,副教授,研究生导师,通信作者,CCF会员(11901M),研究方向为数字图像音频置乱、加密、密写、水印、隐匿、分存、伪装和欺骗等;任平安,副教授,研究生导师,研究方向为计算机网络安全。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20190924.1537.042.html>

为避免这类问题,人们提出了纹理生成式无载体信息隐藏,它主要包括纹理构造式信息隐藏和纹理拼接式信息隐藏。其中纹理构造式信息隐藏是通过模拟纹理生成的方式来产生一些类自然纹理,例如文献[7-9]生成类水影画纹理来隐藏秘密信息,但这类方法所生成的纹理都是非自然纹理,从而不能对秘密信息进行有效掩盖。

纹理拼接式隐藏最早来源于文献[10-11],通过样例纹理填充的方式对表达秘密信息的局部二值模式像素点进行掩盖,但由于不能很好地对局部二值模式进行掩盖,从而易引起密写分析者的怀疑和秘密信息泄露。为避免此问题,文献[12-14]都是通过纹理小块拼接的方式来产生与给定样本相似的含密纹理。但文献[12]引入镜像操作使得编码和非编码样本小块存在明显的区别特征,导致编码小块直接泄露。文献[13-14]中秘密信息分段和样本小块类别之间存在着固定的一一对应关系,易引起攻击者的怀疑,导致安全性较低。另外文献[12-14]都是采用缝合线算法^[15]来对重叠区域的纹理进行缝合。缝合线算法的原理是由特定位置出发,在重叠区域寻找差异最小的缝合线将重叠区域的纹理进行缝合,但由特定位置起始的差异最小的缝合线并不意味着是经历重叠区域所有像素差异最小的缝合线,易产生缝合痕迹,从而不能对秘密信息进行掩盖。

针对文献[12-14]存在的问题,文中提出了一种结合随机映射和改进缝合线的纹理合成信息隐藏方法。首先根据样本小块的均值大小将其分为若干类别,通过结合编码小块的随机放置位置建立起秘密信息分段和样本小块类别之间的随机映射关系,然后结合编码小块的随机坐标位置,从对应样本小块类别中随机选择一个作为编码样本小块来对秘密信息进行表达并将其放置在空白图像中的特定坐标位置上。最后将相邻编码样本小块按改进缝合线纹理合成方法来生成含密纹理。

同文献[12-14]相比,该方法可生成较高质量的纹理图像来对秘密信息进行掩盖;同文献[13-14]相比,秘密信息分段和编码样本小块之间不存在固定的一对一关系,从而具有较高的安全性。

2 隐藏方法

首先将样本图像 S 经光栅扫描得到的样本小块 P_0, P_1, \dots, P_c 按样本小块的核心区域均值排序策略划分为 n_0 个类别;其次由密钥 R 生成的随机坐标来确定二值秘密信息 B 划分的十进制数 B_k 所对应的样本块类别编号 \hat{k} ;再次从第 \hat{k} 个类别中随机选取 \hat{P} , 并将其

放置在空白图像 Q 上起始坐标为 (p'_k, q'_k) 的位置上,最后按改进缝合线策略得到含密纹理图像 Q 。以下对该策略进行详细说明。

记 $S = (s_{i,j})_{m \times n}, s_{i,j} \in \{0, 1, \dots, 255\}$ 是分辨率为 $m \times n$ 的灰度样本图像,将 S 按光栅扫描顺序逐像素滑动分块,划分为 $c = (m - f_h + 1)(n - f_v + 1)$ 个分辨率为 $f_h \times f_v$ 的样本小块 P_0, P_1, \dots, P_{c-1} , 选取 P_0, P_1, \dots, P_{c-1} 中心分辨率为 $a_h \times a_v$ 的区域作为核心区域 $P_0^{\text{Core}}, P_1^{\text{Core}}, \dots, P_{c-1}^{\text{Core}}$, 将核心区域以外的样本小块其他区域作为边界区域。其中核心区域主要用于编码和提取秘密信息,边界区域主要用于相邻样本小块的拼接。记 e_h, e_v 分别对应样本小块水平边界和垂直边界相对于核心区域水平边界和垂直边界的距离,由式1确定。

$$\begin{cases} e_h = \lfloor (f_h - a_h)/2 \rfloor \\ e_v = \lfloor (f_v - a_v)/2 \rfloor \end{cases} \quad (1)$$

其中,符号“ $\lfloor \cdot \rfloor$ ”表示向下取整。

记 $P_{c-1}^{\text{Core}} = (P_{i,j}^{\text{Core}, c-1})_{f_h \times f_v}$, 则 $P_0^{\text{Core}}, P_1^{\text{Core}}, \dots, P_{c-1}^{\text{Core}}$ 的均值 $\text{avg}_0, \text{avg}_1, \dots, \text{avg}_{c-1}$ 可按式2进行计算,然后将 P_0, P_1, \dots, P_{c-1} 按 $P_0^{\text{Core}}, P_1^{\text{Core}}, \dots, P_{c-1}^{\text{Core}}$ 均值大小划分为 n_0 个类别,记第 $k, k \in \{1, 2, \dots, n_0\}$ 个类别中的均值为 $\text{avg}_0^k, \text{avg}_1^k, \dots, \text{avg}_{s_i}^k$, 则 $\text{avg}_0^k, \text{avg}_1^k, \dots, \text{avg}_{s_i}^k$ 满足式3且满足 $\alpha = (\max_{\text{avg}} - \min_{\text{avg}})/n_0$ 。

$$\text{avg}_{c-1} = \frac{1}{a_h a_v} \sum_{i=0}^{a_h-1} \sum_{j=0}^{a_v-1} P_{i,j}^{\text{Core}, c-1} \quad (2)$$

$$\begin{aligned} \min_{\text{avg}} + (k-1)\alpha &< \text{avg}_0^k, \text{avg}_1^k, \dots, \text{avg}_{s_i}^k < \min_{\text{avg}} + k\alpha \\ \max_{\text{avg}} &= \max(\text{avg}_0, \text{avg}_1, \dots, \text{avg}_{c-1}) \\ \min_{\text{avg}} &= \min(\text{avg}_0, \text{avg}_1, \dots, \text{avg}_{c-1}) \end{aligned} \quad (3)$$

记二值秘密信息序列 B 的长度为 l , 由于编码样本小块 P_0, P_1, \dots, P_{c-1} 总共有 n_0 个类别,因此每个编码样本小块可表达 $\log_2 n_0$ 个秘密比特,从而将 B 划分为 L 组,即: b^0, b^1, \dots, b^{L-1} 。其中 L 和 l 之间满足式4的约束,将 b^0, b^1, \dots, b^{L-1} 转换为10进制数,可得10进制数 B_0, B_1, \dots, B_{L-1} 。

$$L = \lceil l / \log_2 n_0 \rceil \quad (4)$$

由密钥 R 可伪随机生成满足式5约束的坐标序列 $(p'_k, q'_k), k=0, 1, \dots, L-1$ 且满足任意两个生成的随机坐标为起点在放置编码样本块时不会产生重叠。

$$\begin{aligned} p'_k \bmod (e_h + a_h) &= 0 \\ q'_k \bmod (e_v + a_v) &= 0 \end{aligned} \quad (5)$$

为避免秘密信息分段和样本小块类别之间存在固定的映射关系,文中按式6来确定 B 划分的10进制数 B_k 对应的样本块类别编号 \hat{k} 。

$$\hat{k} = (p'_k \cdot q'_k + B_k + p'_k + q'_k) \bmod n_0 \quad (6)$$

记编号 \hat{k} 所在类别的样本小块为 $P_0^{\hat{k}}, P_1^{\hat{k}}, \dots, P_{s_k}^{\hat{k}}$, 从中可随机选择一个编码样本小块 \hat{P} 来代表 B_k , 然后将 \hat{P} 放置在分辨率为 $g_h \times g_v$ 的空白图像 Q 上, 位于起始坐标为 $(p_k^{\hat{k}}, q_k^{\hat{k}})$ 且大小为 $f_h \times f_v$ 的小块上。

在放置完秘密信息 \hat{P} 之后时, 用 P_0, P_1, \dots, P_{c-1} 来填充 Q 上的空白区域, 若和已放置后的样本小块存在重叠区域, 则需要重叠区域的缝合。文献[12-14]都是采用缝合线算法^[15]来对重叠区域的纹理进行缝合, 其基本原理是在重叠区域由特定位置出发寻找差异最小的缝合线来将重叠区域的纹理进行缝合, 但由特定位置起始的差异最小的缝合线并不意味着是经历重叠区域所有像素差异最小的缝合线, 易产生拼接痕迹, 从而不能对秘密信息进行掩盖。为避免此问题, 文中采用改进缝合线纹理合成方法来生成含密纹理图像。

记当前要放置的样本块为 P_{cur} , 其对应的边界区域如图1(a)所示, 分别为0边界区、1边界区、2边界区和3边界区, 其中0边界区和2边界区的大小为 $e_h \times (2e_v + a_v)$, 1边界区和3边界区的大小为 $e_v \times (2e_h + a_h)$ 。假设 P_{cur} 放置区域存在4个相邻的样本块记为 P^0, P^1, P^2, P^3 , 如图1(b)所示, 其中 P^i 与 P_{cur} 的 \tilde{i} 边界区相邻。将 P_{cur} 放置在 P^0, P^1, P^2, P^3 的重叠区域, 意味着需要将 P_{cur} 的 i 边界区域和 P^i 的 \tilde{i} 边界区域进行纹理合成, i 与 \tilde{i} 的对应关系如式7所示。

$$\tilde{i} = (i + 2) \bmod 4, i = 0, 1, 2, 3 \quad (7)$$

注: 若 $P^i = \Phi$, 则意味着 P_{cur} 的 i 边界区不存在相邻的样本块, 因此仅需直接将 P_{cur} 的 i 边界区直接放置在对应该区域即可, 而不需要进行缝合。

记 P_{cur} 的 i 边界区为 P_{cur}^i , P^i 的 \tilde{i} 边界区为 \tilde{P}^i , 图1(c)以0边界区和2边界区为例给出了将 P_{cur}^i 和 \tilde{P}^i 融合在一起的传统缝合线方法, 即首先按式8对 P_{cur}^i 和 \tilde{P}^i 做差构造差异矩阵 $D = (d_{i,j})_{m \times cn}$ 。

$$D = |P_{cur}^i - \tilde{P}^i| \quad (8)$$

按式9寻找 D 第 $j = 0$ 列的最小差值点坐标 (\hat{i}, j) , 其中记 D_j 表示 D 的第 j 列, 并按式10计算 $d_{i-1,j+1}, d_{i,j+1}, d_{i+1,j+1}$ 中有效点的最小差值点 $(\hat{x}, j+1)$ 。

$$\hat{i} = \underset{i \in \{0, 1, \dots, m-1\}}{\operatorname{argmin}} (D_j^C) \quad (9)$$

$$\hat{x} = \underset{\substack{x \in \{i-1, i, i+1\} \\ \wedge x \in \{0, 1, \dots, m-1\}}}{\operatorname{argmin}} (d_{x,j+1}) \quad (10)$$

然后更新 $j = j + 1$, 将 \hat{x} 赋值给 \hat{i} , 执行式10直至计算出第 $cn - 1$ 列上的差值点 $(\hat{x}, cn - 1)$, 并连接所有差值点构成缝合线, 将缝合线两侧位于 P_{cur}^i 和 \tilde{P}^i 的像素连接在一起生成重叠区域的合成纹理。这里将以列为单位, 由传统的缝合线算法生成的缝合线记为

式11。

$$L_0^C = \text{Quilt}(D, 0, "C") \quad (11)$$

其中, "C" 表示以列为单位, 对于1边界区和3边界区, 应以行为单位进行缝合。从式11可看出, L_0^C 只能保证经过第0列的差值点最小, 如式9所示; 但并不意味着在非0列的差值点最小, 如式10所示, 从而不能保证合成纹理的视觉质量。为克服这个缺陷, 文中给出了改进的缝合线算法, 即按式12计算 $L_j^C, j = 0, 1, \dots, cn - 1$, 然后从中找到差异最小的缝合线来对重叠区域进行纹理合成, 如式13所示。图1(d)给出了改进后的缝合线算法示意。

$$L_j^C = \text{Quilt}(D, j, "C"), j = 0, 1, \dots, cn - 1 \quad (12)$$

$$L_j^C = \arg \min_{j=0, 1, \dots, cn-1} (L_j^C) \quad (13)$$

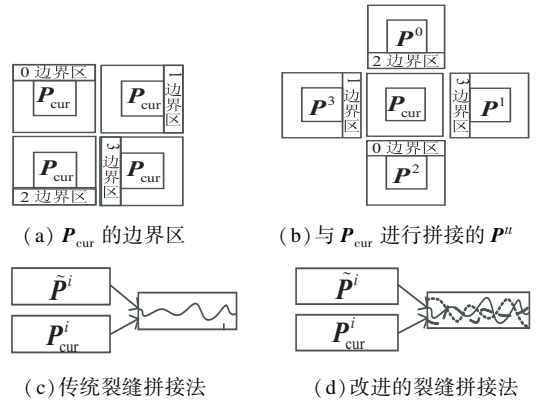


图1 拼接过程示意

3 提取方法

首先将样本图像 S 经光栅扫描得到的样本小块 P_0, P_1, \dots, P_c 按小块核心区域的均值排序策略划分为 n_0 个类别, 然后由含密纹理图像 Q 和密钥 R 生成的随机坐标通过编码样本小块截取策略得到编码样本小块 U_0, U_1, \dots, U_{L-1} , 通过小块之间的相似度比较得到与 U_k 最相似的样本小块 \hat{P} , 进而得到 U_k 对应的类别编号 \hat{k} , 最后通过二值秘密信息恢复策略得到二值秘密信息 B 。以下对该策略进行说明。

输入分辨率为 $g_h \times g_v$ 的含密样本图像 Q , 由密钥 R 生成满足式5约束的坐标序列 $(p_k^{\hat{k}}, q_k^{\hat{k}}), k = 0, 1, \dots, L - 1$ 且满足任意两个坐标不同, 以 $(p_k^{\hat{k}}, q_k^{\hat{k}})$ 为坐标起点从 Q 上提取分辨率为 $f_h \times f_v$ 的纹理小块 U_0, U_1, \dots, U_{L-1} 。

将样本图像 S 划分为分辨率为 $f_h \times f_v$ 的样本小块 P_0, P_1, \dots, P_{c-1} , 按 P_0, P_1, \dots, P_{c-1} 的核心区域 $P_0^{\text{Core}}, P_1^{\text{Core}}, \dots, P_{c-1}^{\text{Core}}$ 均值大小划分为 n_0 个类别。按式14从 $P_0^{\text{Core}}, P_1^{\text{Core}}, \dots, P_{c-1}^{\text{Core}}$ 中选取和 U_k 核心区域 U_k^{Core} 最接近的样本核心区域 \hat{P}^{Core} , 记录 \hat{P}^{Core} 对应的样本块编号 \hat{k} , 作为 U_k 的类别编号 \hat{k} 。

$$\hat{P}_i^{\text{Core}} = \arg \min_{i \in \{0,1,\dots,c-1\}} \|U_k^{\text{Core}} - P_i^{\text{Core}}\|_2^2 \quad (14)$$

按式15提取出对应10进制秘密信息 $B_k, k=0,1,\dots,L-1$,将 B_0, B_1, \dots, B_{L-1} 转换为长度为 $\log_2 c$ 比特的二值比特位串,从而可得到二进制数 b^0, b^1, \dots, b^{L-1} ,然后按式16截取前 l 个比特作为最终提取出的秘密信息 B 。

$$B_k = (\hat{k} + (n_0 - 1)(p_k' \cdot q_k' + p_k' + q_k')) \bmod n_0 \quad (15)$$

$$B = \text{trunc}(b^0 \| b^1 \| \dots \| b^{L-1}, l) \quad (16)$$

其中, $\text{trunc}()$ 函数是二值比特位串截取函数。

4 完整的结合随机映射和改进缝合线的纹理合成信息隐藏与提取算法

以下给出完整的结合随机映射和改进缝合线的纹理合成信息隐藏与恢复算法,记为算法1和算法2。

算法1:结合随机映射和改进缝合线的纹理合成隐藏算法。

(1)输入样本图像 S ,将 S 按光栅扫描顺序逐像素滑动得到样本小块 P_0, P_1, \dots, P_c ,将 P_0, P_1, \dots, P_c 的中心区域作为核心区域 $P_0^{\text{Core}}, P_1^{\text{Core}}, \dots, P_c^{\text{Core}}$;

(2)计算样本小块核心区域 $P_0^{\text{Core}}, P_1^{\text{Core}}, \dots, P_c^{\text{Core}}$ 的均值 $\text{avg}_0, \text{avg}_1, \dots, \text{avg}_c$,然后将样本小块 P_0, P_1, \dots, P_c 按照其核心区域 $P_0^{\text{Core}}, P_1^{\text{Core}}, \dots, P_c^{\text{Core}}$ 均值大小分成 n_0 个类别;

(3)将二值秘密信息比特位串 B 转换为 L 个10进制数 B_0, B_1, \dots, B_{L-1} ,由密钥 R 伪随机生成 L 个坐标 (p_k', q_k') ,初始化 $g_h \times g_v$ 的空白图像 Q ;

(4)确定编码单元 B_k 对应的编码样本块编号 \hat{k} ,从编号 \hat{k} 所在类别 $P_0^k, P_1^k, \dots, P_{s_k}^k$ 中随机选择一个编码样本小块 \hat{P} 来代表秘密信息10进制数 B_k ;

(5)将编码样本块 \hat{P} 放置在 Q 上坐标起始位置为 (p_k', q_k') 且大小为 $f_h \times f_v$ 的矩形小块上;

(6)用 P_0, P_1, \dots, P_c 来填充 Q 上的空白区域,将存在重叠区域的小块按照改进缝合线算法对相邻小块拼接,最终将 Q 作为含密纹理图像输出。

算法2:结合随机映射和改进缝合线的纹理合成信息提取算法。

(1)输入样本图像 S ,将 S 按光栅扫描顺序逐像素得到样本小块 P_0, P_1, \dots, P_c ,将 P_0, P_1, \dots, P_c 的中心区域作为核心区域 $P_0^{\text{Core}}, P_1^{\text{Core}}, \dots, P_c^{\text{Core}}$;

(2)计算样本小块核心区域 $P_0^{\text{Core}}, P_1^{\text{Core}}, \dots, P_c^{\text{Core}}$ 的均值 $\text{avg}_0, \text{avg}_1, \dots, \text{avg}_c$,然后将样本小块 P_0, P_1, \dots, P_c 按照其核心区域 $P_0^{\text{Core}}, P_1^{\text{Core}}, \dots, P_c^{\text{Core}}$ 均值大小分成 n_0 个类别;

(3)输入含密纹理图像 Q ,由密钥 R 伪随机生成 L 个坐标 (p_k', q_k') ,然后以 (p_k', q_k') 为坐标起点从 Q 上提取出 L 个分辨率为 $f_h \times f_v$ 的纹理小块 U_0, U_1, \dots, U_{L-1} ;

(4)从 P_0, P_1, \dots, P_{c-1} 的核心区域 $P_0^{\text{Core}}, P_1^{\text{Core}}, \dots, P_{c-1}^{\text{Core}}$ 中选取和 U_k 的核心区域 U_k^{Core} 最接近的 \hat{P} ,记录 \hat{P} 对应的编号 \hat{k} ;

(5)结合 U_k 对应的编号 \hat{k} ,提取出二值比特位串 B 。

同文献[12-14]相比,所提方法可生成较高质量的纹理图像来对秘密信息进行掩盖;同文献[13-14]相比,秘密信息分段和编码样本小块之间不存在固定的一对一关系,从而具有较高的安全性。

5 实验

实验测试环境为 Window 10 操作系统, CPU 为 Intel(R) Core(TM) i5-6600,主频为 3.31 GHz,内存为 8.00 GB,编码语言为 JAVA jdk1.8.0_65,采用的测试样例图像如图2(a)和2(b)所示,分别是分辨率为 128×128 的8位灰度图像 stone1 和 stone2。嵌入秘密信息为“陕西师大”,其对应的二值比特位串为64位,如图2(c)所示。

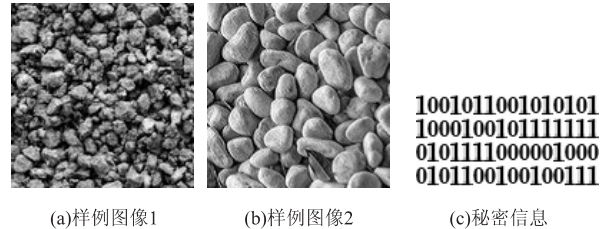


图2 测试样例图像和二值比特秘密信息

使用峰值信噪比(PSNR)对攻击以后的含密样本图像视觉质量进行衡量,通过误码率(EBR)对秘密信息恢复情况进行评价,所有计算均保留小数点后4位有效数字。PSNR和EBR的计算式为:

$$\text{PSNR} = 10 \log \frac{255^2}{\text{MSE}} \quad (17)$$

$$\text{MSE} = \frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (p_{i,j} - p'_{i,j})^2}{m \times n} \quad (18)$$

其中, $p_{i,j}$ 和 $p'_{i,j}$ 为待比较的图像的像素值; $m \times n$ 为图像的分辨率。

$$\text{EBR} = \frac{b_{\text{err}}}{b_{\text{all}}} \times 100\% \quad (19)$$

其中, b_{err} 为错误的秘密信息比特数; b_{all} 为秘密信息总比特数。

在实验中,由样例图像按光栅扫描顺序逐像素滑动得到的样本小块分辨率为 32×32 ,这些样本小块的核心区域被设定为样本小块中心大小为 16×16 的中

心区域并按均值大小划分为 16 个类别。

5.1 正确性验证实验

为验证正确性,选取样例图像(图 2(a)和图 2(b)),由 3 组不同的密钥分别按算法 1 隐藏秘密信息并按算法 2 提取秘密信息。图 3 和图 4 分别给出了生成的含密纹理图像和提取的秘密信息,与之对应的实验参数和秘密信息恢复情况如表 1 所示,其中生成的含密纹理图像的大小为 224 × 224。

从图 3 可以看出,算法 1 生成的含密纹理图不会产生明显的缝合痕迹,整体视觉质量较好。从表 1 和图 4 可以看出,对于不同的密钥,算法 2 均能完全提取秘密信息,提取的秘密信息相对于原秘密信息的 EBR 为 0,说明秘密信息可完整恢复,因此正确性得以验证。

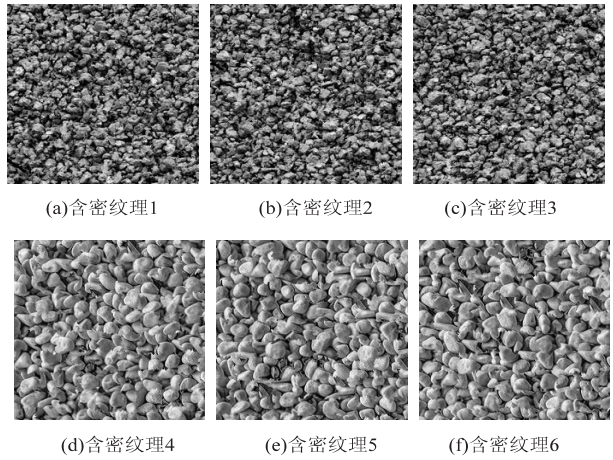


图 3 正确性验证实验含密纹理图样



图 4 正确性验证实验秘密信息恢复图样

表 1 正确性验证实验

编号	样例图像	密钥 <i>R</i>	生成的含密纹理图像	提取的秘密信息	EBR
1	图 2(a)	5	图 3(a)	图 4(a)	0
2		8	图 3(b)	图 4(b)	
3		10	图 3(c)	图 4(c)	
4	图 2(b)	5	图 3(d)	图 4(d)	
5		8	图 3(e)	图 4(e)	
6		10	图 3(f)	图 4(f)	

5.2 密钥依赖性实验

为验证密钥依赖性,选取图 2(a)作为样例图,按表 2 对密钥 *R* 进行调整,然后按算法 2 提取秘密信息。

表 2 是密钥依赖性实验的参数,其中“-”表示被修改;图 5 是密钥依赖性实验提取的秘密信息,其中“1”和“0”代表提取的“1”和“0”是错误的。

从表 2 可看出,密钥参数的改变,将导致提取出的秘密信息 EBR 趋近于 0.5,从而半数左右的秘密信息比特在提取时发生错误,秘密信息无法提取,因此文中所述策略对密钥的改变具有完全的依赖性。

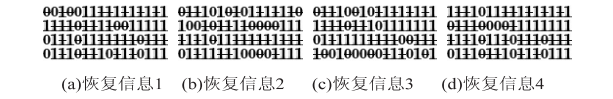


图 5 密钥依赖性实验秘密信息恢复图样

表 2 密钥依赖性验证实验参数

编号	含密图像	原始密钥 <i>R</i>	修改的密钥 <i>R</i>	秘密信息	EBR
1	图 2(a)	5	8	图 5(a)	0.531 3
2			10	图 5(b)	0.531 3
3			13	图 5(c)	0.468 8
4			20	图 5(d)	0.484 4

5.3 抗攻击实验

为验证所提策略的抗攻击能力,按不同强度的椒盐噪声和不同质量因子的 JPEG 压缩分别对图 3(a)加密载体进行攻击,然后按算法 2 提取秘密信息。椒盐噪声攻击强度分别为 5%、15% 和 20%, JPEG 压缩中选取的质量因子分别为 80 和 90。图 6 和图 7 是攻击后的含密纹理图像和与之对应的秘密信息恢复结果。

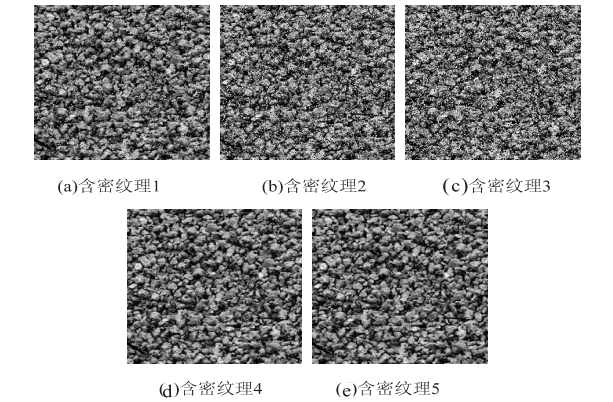


图 6 抗攻击实验含密纹理图样

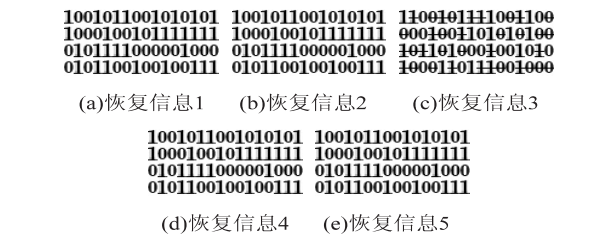


图 7 抗攻击实验秘密信息恢复图样

表 3 给出了对应的实验参数。从表 3 和图 6 可以看出,椒盐噪声和 JPEG 压缩都会导致含密纹理图的视觉质量下降。以给定的实验样例纹理为例,对于

5%、15%和20%的椒盐噪声攻击,含密纹理图对应的PSNR约为17~9 dB;对于JPEG压缩,当取质量因子为80~90时,其对应的含密纹理图像的PSNR为30.749 8~36.568 2 dB。含密纹理图像尽管遭受了不

同程度噪声以及JPEG压缩攻击,当椒盐噪声强度为5%和15%,JPEG压缩质量因子为80和90时,按算法2提取的恢复信息的误码率为0,表明所提方法具备一定的抗攻击能力,且能有效提取秘密信息。

表3 抗攻击实验参数

编号	攻击		含密纹理 图像	攻击后的含密 图像	PSNR/dB	秘密信息	EBR
	类型	参数					
1	椒盐噪声	5%	图3(a)	图6(a)	17.920 9	图7(a)	0
2	椒盐噪声	15%		图6(b)	13.113 7	图7(b)	0
3	椒盐噪声	20%		图6(c)	9.766 0	图7(c)	0.546 8
4	JPEG压缩	80		图6(d)	30.749 8	图7(d)	0
5	JPEG压缩	90		图6(e)	36.568 2	图7(e)	0

6 结束语

传统修改式信息隐藏方法^[1-6]需修改原始载体图像,不仅会降低载体图像视觉质量,同时也易引起攻击者的怀疑。纹理构造式信息隐藏方法^[7-9]只能生成简单质地的非自然纹理,不能对秘密信息进行有效的掩盖。纹理拼接式信息隐藏方法^[12-14]秘密信息与样本小块之间存在着固定的映射关系或码块间的区别特征,导致安全性较低。针对以上问题,提出了一种结合随机映射和改进缝合线的纹理合成隐藏方法。首先根据样本小块核心区域均值将其分为若干个类别,每个类别中的小块代表相同的秘密信息,通过编码小块的随机位置建立起秘密信息分段和样本小块类别之间的随机映射关系,然后结合编码小块的随机位置,从对应样本小块类别中随机选择一个样本小块作为编码样本小块来对秘密信息进行编码并将其放置在空白图像中的特定位置上。最后将相邻编码样本小块按改进缝合线纹理合成方法来生成含密纹理图像。实验结果表明,该方法生成的含密纹理图像视觉质量较好,可通过高质量的合成纹理来对秘密信息进行掩盖,秘密信息分段和编码样本小块不一一对应,且完全依赖于用户密钥并具备一定的抗攻击能力。

参考文献:

[1] 邵利平,乐志芳. 基于DCT的多门限渐进秘密图像分存方案[J]. 信息网络安全,2018(3):54-62.

[2] 邵利平,乐志芳. 多版本备份和限制性双重认证主密钥(t,s,k,n)图像分存[J]. 电子学报,2019,47(2):390-403.

[3] 欧阳显斌,邵利平,乐志芳. 非等量备份和双认证自修复有限域图像分存[J]. 软件学报,2017,28(12):3306-3346.

[4] 欧阳显斌,邵利平,陈文鑫. 结合调整差值变换的(K,N)有意义图像分存方案[J]. 中国图象图形学报,2015,20(5):633-642.

[5] 张洋,邵利平,任平安. 免基向量EMD(n,m)模型及其在图像密写上的应用[J]. 计算机辅助设计与图形学学报,2018,30(8):1490-1504.

[6] 黄燕燕,邵利平. 结合EMD-cl嵌入的多载体密图分存方法[J]. 中国图象图形学报,2018,23(8):1108-1130.

[7] XU Jiayi, MAO Xiaoyang, JIN Xiaogang, et al. Hidden message in a deformation-based texture[J]. The Visual Computer,2015,31(12):1653-1669.

[8] PAN L, QIAN Z X, ZHANG X P. Digital steganography based on constructing marbling texture[J]. Journal of Applied Sciences,2016,34(5):625-632.

[9] QIAN Z X, PAN L, LI S, et al. Steganography by constructing marbling texture[C]//第14届全国信息隐藏暨多媒体信息安全学术会议. 广州:出版者不详,2018:17-35.

[10] OTORI H, KURIYAMA S. Data-embeddable texture synthesis[C]//International symposium on smart graphics. Kyoto, Japan:Springer,2007:146-157.

[11] OTORI H, KURIYAMA S. Texture synthesis for mobile data communications[J]. IEEE Computer Graphics and Applications,2009,29(6):74-81.

[12] WU K C, WANG C M. Steganography using reversible texture synthesis[J]. IEEE Transactions on Image Processing,2015,24(1):130-139.

[13] QIN Zhengcai, LI Meng, WU Bin. Robust steganography via patch-based texture synthesis[C]//International conference on internet multimedia computing and service. Qingdao, China:Springer,2017:429-439.

[14] QIAN Zhenxing, ZHOU Hang, ZHANG Weiming, et al. Robust steganography using texture synthesis[C]//Advances in intelligent information hiding and multimedia signal processing. Berlin:Springer,2017:25-33.

[15] EFROS A A, FREEMAN W T. Image quilting for texture synthesis and transfer[C]//Proceeding of the 28th annual conference on computer graphics and interactive techniques. [s. l.]:ACM,2001:341-346.