JIG
JOURNAL OF IMAGE AND GRAPHICS
主办：中国科学院遥感与数字地球研究所
中国图象图形学学会
北京应用物理与计算数学研究所

中国图象图形学报

2020
01
VOL.25
ISSN1006-8961
CN11-3758/TB

古代壁画分类 P92

中国图象图形学报

刊名题字：宋健 | 月刊（1996年创刊）

主管单位 中国科学院
主办单位 中国科学院遥感与数字地球研究所
中国图象图形学学会
北京应用物理与计算数学研究所

主　　编 顾行发
编辑出版 《中国图象图形学报》编辑出版委员会
通信地址 北京市海淀区北四环西路19号
邮　　编 100190
电子信箱 jig@radi.ac.cn
电　　话 010-58887035
网　　址 www.cjig.cn

广告发布登记号 京朝工商广登字20170218号
总 发 行 北京报刊发行局
订　　购 全国各地邮局
海外发行 中国国际图书贸易集团有限公司
（邮政信箱：北京399信箱　邮编：100048）
印刷装订 北京科信印刷有限公司

第25卷第1期（总第285期）
2020年1月16日

中国精品科技期刊
中国国际影响力优秀学术期刊
中国科技核心期刊
中文核心期刊

Journal of Image and Graphics

Title inscription: Song Jian | Monthly, Started in 1996

Superintended by Chinese Academy of Sciences
Sponsored by Institute of Remote Sensing and Digital Earth, CAS
China Society of Image and Graphics
Institute of Applied Physics and Computational Mathematics

Editor-in-Chief Gu Xingfa
Editor, Publisher Editorial and Publishing Board of Journal of Image and Graphics
Address No. 19, North 4th Ring Road West, Haidian District, Beijing, P. R. China
Zip code 100190
E-mail jig@radi.ac.cn
Telephone 010-58887035
Website www.cjig.cn

Distributed by Beijing Bureau for Distribution of Newspapers and Journals
Domestic All Local Post Offices in China
Overseas China International Book Trading Corporation (P.O.Box 399, Beijing 100048,P.R.China))
Printed by Beijing Kexin Printing Co., Ltd.

CN 11-3758/TB
ISSN 1006-8961
CODEN ZTTXFZ

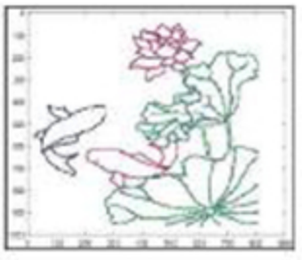
国外发行代号 M1406
国内邮发代号 82-831
国内定价 60.00元

2020年1月 第25卷 第1期（总第285期）
中国图象图形学报 Zhongguo Tuxiang Tuxing Xuebao

目次

采用卷积核金字塔和空洞卷积的单阶段目标检测(第0102页)

顾及目标关联的自然场景文本检测(第0126页)

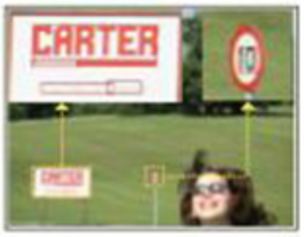


关键点选取的最小二乘渐进迭代逼近(第0148页)

Volume 25, Number 1
Published January 16, 2020

CONTENTS
JOURNAL OF IMAGE AND GRAPHICS

Single-stage object detection using filter pyramid and atrous convolution(P0102)



Association of text and other objects for text detection with natural scene images(P0126)

Least squares progressive-iterative approximation based on key points(P0148)

中图法分类号:TP309.7　　**文献标识码**:A　　**文章编号**:1006-8961(2020)01-0043-17

论文引用格式:Wang Y, Shao L P and Lu H. 2020. Generative camouflage method combined with block rotation and photo mosaic . Journal of Image and Graphics,25(01):0043-0059(王洋,邵利平,陆海. 2020. 结合块旋转和马赛克拼图的生成式伪装方法. 中国图象图形学报,25(01):0043-0059)[DOI:10.11834/jig.190069]

结合块旋转和马赛克拼图的生成式伪装方法

王洋,邵利平,陆海

陕西师范大学计算机科学学院,西安　710119

摘　要:**目的**　搜索式无载体信息隐藏容量低,涉及大量载体密集传输;纹理合成无载体隐藏只能生成简单质地的纹理图像;马赛克拼图信息隐藏尽管能产生有意义图像,但需修改嵌入参数。针对以上问题,提出一种结合块旋转和马赛克拼图的生成式伪装方法。**方法**　将灰度图像进行圆形化并添加随机转角构建马赛克,通过随机坐标决定秘密信息的隐藏位置;在隐藏位置,根据密钥和放置位置来放置代表秘密比特串的圆形图像和施加认证转角,对于非隐藏位置则放置最接近圆形图像来掩盖秘密信息;将放置过程产生的偏差通过误差扩散分散给周围未处理像素。在提取时,结合质心旋转匹配提取秘密比特并进行转角认证。**结果**　采用圆形图像表达秘密信息而不涉及修改式嵌入,通过马赛克拼图产生有意义含密掩体,可通过质心旋转匹配提取秘密比特并进行转角认证。对密钥严格依赖,在遭受质量因子为50～80的JPEG压缩和随机转角攻击时,秘密信息可完整恢复,在遭受强度为8%～20%的椒盐噪声攻击时,提取信息的误码率低于5%,且对秘密信息的认证成功率均在80%以上。**结论**　所提方法具有较好的抗攻击能力,可抵御信道攻击且具备较高的安全性。

关键词:图像马赛克;无载体;生成式隐藏;质心旋转匹配;误差扩散;随机转角认证

Generative camouflage method combined with block rotation and photo mosaic

Wang Yang, Shao Liping, Lu Hai

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

Abstract: **Objective** Traditional search-based coverless information hiding usually searches natural and unmodified carriers that contain appropriate secret vectors to transmit secret information. However, for natural images and texts, the ability to express irrelevant secret information is low. Thus, the hidden capacity is low. Search-based coverless information hiding cannot avoid the dense transmission of massive carriers that attract attacks easily and results in distorted secret information. Texture-based coverless information hiding usually divides sample texture image into several blocks, creating the mapping relationship between texture blocks and secret segments. Although such methods generated stego texture images by sample texture synthesis, they can only generate simple unnatural texture images. Mosaic-based information hiding can generate meaningful stego images, but in essence, such methods are modification-based information hiding, and they inevitably leave modification traces in carriers and have no authentication strategy. Therefore, verifying the authenticity of recovered secret information is impossible. Moreover, mosaic-based information hiding typically uses the LSB (least significant bit)-based

收稿日期:2019-03-14;**修回日期**:2019-07-07;**预印本日期**:2019-07-14

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

Supported by: National Natural Science Foundation of China (61100239)

modification embedding strategy for a large embedding capacity to embed the transformation parameters. The LSB-based embedding strategy is sensitive to attacks, and the embedded information is easily lost when suffering attacks. To address these problems, this study proposed a generative camouflage method combined with block rotation and photo mosaic. **Method** In the embedding, the proposed method transformed grayscale images into circle images with pseudo-random angles by user keys to construct photo mosaics and then generated random integer coordinate sequence to determine the hidden positions of secret bit strings. For each hidden position, a circle image related to user key and position was placed to express secret bits, and then the random angle related to user key and position was added for authentication. For each non-hidden position, a circle image similar to cover image pixel was set to conceal the secret image, and the added random perturbation angle precluded distinguishing hidden and non-hidden positions. The deviation caused by the placement of the circle image was scattered around unprocessed pixels by the error diffusion method to form the stego photo mosaic image. In the extraction, coordinates for all secret bits in the stego photo mosaic image were obtained by user key, and circle images expressing secret bits were fetched. The centroid of each circle image that expresses secret bits was normalized into the right half-axis and then identified by the strategy of centroid rotation matching. Each circle image index was found to extract the hidden secret bits by the minimum quadratic difference distance. To authenticate the correctness of each circle image fetched secret bits, the factual and theory angles were compared, where the minimum quadratic difference distance of the factual angle, and the theory angle was computed by the user key, and the fetched secret bits. If the factual angle equals the theory angle, then the extracted secret bits are correctly recovered. **Result** The proposed method regards each circle image as a hidden unit and only involves the rotation of circle images without any modification. The added random rotation angles also provide the security assurance for the specific user to extract secret information and conduct angle authentication. Only the user with the correct user key can eliminate the influence of random rotation angles and extract the correct secret information with its corresponding authentication information. Moreover, the proposed method uses photo mosaic to hide secret information. The method is robust in anti-attacks and has good authentication accuracy. At the same time, the proposed strategy relies entirely on the user's key and has high security. The experiments show that secret information can be completely recovered only by the correct key. Whether one or more user key parameters are changed, the changed user key parameters lead to the inaccurate extraction of secret information. In addition, in case of JPEG compression attacks with a quality factor of 50～80 and random rotation angle attacks, the embedded secret information can be completely recovered. Even with salt-and-pepper noise attacks of 8%～20%, the error rate (ER) of extracted information remains approximately 5%. The authentication success rates of the restored information are all above 80%. **Conclusion** The proposed method uses randomly placed circle images to express secret information without any modification. The method can use photo mosaic to generate meaningful hidden carrier images and avoid the high cost of database creation and searching of the search-based coverless information hiding. The proposed method combines the parameter mapping and error diffusion mosaic image generation strategy to place stego circle images in their corresponding positions and then generate the stego mosaic image, avoiding the dense transmission of massive carriers in search-based coverless information hiding. Compared with the texture-based coverless information hiding, the proposed method can generate meaningful stego photo mosaic images, avoiding the generation of meaningless texture images in texture-based coverless information hiding. Even during attacks, each circle image expressed secret bits and its placement angle are not easily lost. The proposed method can extract secret information by centroid rotation matching and random rotation angle strategy based on user keys and improve the accuracy of secret information recognition.

Key words: photo mosaic; coverless; generative hiding; centroid rotation matching; error diffusion; random angular authentication

0 引 言

随着深度学习的不断深入、人工智能的继续发展以及量子计算机的初现端倪,传统修改式信息隐藏的研究形势变得十分严峻。一方面,压缩技术的持续发展使得可供利用的冗余空间越来越小;另一方面,基于机器学习的隐写分类器维数不断提高(Adeli 和 Broumandnia,2018;Holub 和 Fridrich,2015;Song 等,2017)导致修改隐匿信息不被发现的可能

性越来越小。针对此问题,2014 年全国信息隐藏与多媒体安全专家研讨会首次提出了无载体信息隐藏;2015 年第 12 届全国信息隐藏大会将无载体信息隐藏技术列入未来信息隐藏的前沿阵地;2016 年第 13 届全国信息隐藏大会将无载体信息隐藏正式定位为第 2 代信息隐藏技术;2018 年第 14 届全国信息隐藏大会为无载体信息隐藏组织了专场讨论。

目前关于无载体信息隐藏,比较典型的方法是基于搜索的无载体信息隐藏,主要通过检索数据库中包含指定秘密矢量的自然无修改载体来传递秘密信息。例如,Yuan 等人(2017)和 Zhou 等人(2015)通过检索数据库中哈希值与秘密比特小段相等的图像作为含密载体。Zhang 等人(2018)和 Zhou 等人(2017)则进一步利用标识来确定秘密信息所在的载体小块位置以提升安全性。Zheng 等人(2017)将图像划分为 9 个小块作为叶子节点,通过选取 9 个叶子节点的 256 种排列使得单幅载体图像最多可表示 256 种 18 bit 秘密信息。Zhou 等人(2018)将密图小块映射为哈希值,通过选取载体图像同哈希值小块来对密图进行近似马赛克图像重构。

但这类方法存在的问题是:1)图像或文本等自然未修改载体对与之不相关的秘密信息表达能力十分有限,若需足够表现能力,则需收集足够多的样本。2)随着数据库文本和图像信息表达能力的增强,需要搜索的数据量也呈几何级数增加,即使借助倒排索引,对于大数据量的搜索、存储和维护也将是沉重负担。3)由于这类方法单载体嵌密容量极低,涉及大量载体在信道中密集传输,从而容易诱发攻击,导致传输的秘密信息遭受破坏。

基于纹理合成的生成式无载体信息隐藏方法也是一类典型的无载体信息隐藏方法,其主要思想是将给定的样例纹理划分为纹理小块,并建立纹理小块与秘密信息之间的映射关系,通过样例纹理合成来生成与之相似的含密纹理。例如,Xu 等人(2015)在空白图像上书写秘密信息,然后添加掩盖图案,最后通过类水影画形变来产生含密纹理。Wu 和 Wang(2015)将秘密信息与图像纹理小块的 MSE(mean sqacre ernor)等级相对应,从中选择合适的纹理小块来形成嵌密掩体。Qin 等人(2017)根据纹理小块核心区域的复杂度将纹理小块分类用于代表秘密信息并将所选小块随机放置在掩体图像中,然后利用其他小块对其进行拼接来对秘密信息进行掩盖。Qian 等人(2016)用不同类别的纹理小块代表不同的秘密信息来形成含密掩体。但这类方法只能生成简单质地的纹理图像,不能生成复杂的有意义图像。

传统基于马赛克拼图的信息隐藏方法可产生有意义图像。例如,Lai 和 Tsai(2011)通过选取与密图特征相似的公开图像,以密图小块为字典来替换与之相似的公开图像小块,从而将密图伪装成公开图像。Zhai 等人(2015)和张梦等人(2016)采用相似块替换,将秘密图像分成 n 个分支分别嵌入 n 幅掩体图像中。

为避免 Lai 和 Tsai(2011)选取与密图特征相似的公开图像,Lee 和 Tsai(2014)根据密图小块和掩体图像小块的均值和标准差分别排序,建立一一映射关系来嵌入秘密信息。为减少参数嵌入,Hou 等人(2016)在 Lee 和 Tsai(2014)基础上引入均值聚类对密图小块和掩体小块进行分类和匹配。刘小凯等人(2018)引入了分类阈值优化算法来改进 Hou 等人(2016)的方法,使匹配密图小块与掩体小块的均方误差更小。

除了基于图像划分小块拼接的马赛克拼图以外,还存在一种将有意义图像直接作为马赛克图像的图像马赛克拼图方法。这种拼图方法可将不同的图像作为马赛克,用以产生具有任意表现力的其他图像。结合图像马赛克拼图,Lin 和 Tsai(2004)将多个等大矩形图像拼接为掩体图像,通过加噪调整每个矩形图像左右上下 4 条边的方差来表达 2 bit 秘密信息并依据大于设定阈值的最小边方差来提取秘密信息。

相对于纹理合成的生成式无载体信息隐藏方法,Hou 等人(2016),Lai 和 Tsai(2011),Lee 和 Tsai(2014),Lin 和 Tsai(2004),刘小凯等人(2018),Zhai 等人(2015)和张梦等人(2016)的方法尽管可生成有意义图像,但都需要借助修改载体的方式嵌入秘密信息。例如,Hou 等人(2016),Lai 和 Tsai(2011),Lee 和 Tsai(2014)和刘小凯等人(2018)通过基于 LSB(least significant bit)的可逆嵌入方法(Coltuc 和 Jean-Marc,2007)嵌入和提取秘密信息。Zhai 等人(2015)通过简单 LSB 方法将相关参数嵌入在掩体图像中。张梦等人(2016)通过差值扩展嵌入相关参数并提取秘密信息。Lin 和 Tsai(2004)

通过修改马赛克图像边界信息的方式嵌入秘密信息。因此这些方法的本质都是传统基于修改式的信息隐藏方法,无法抵抗密写分析算法的检测。同时这些方法均涉及 LSB 嵌入,鲁棒性差,在遭受攻击时,容易导致嵌入的参数丢失。除此之外,这些方法都不具备对提取信息的认证能力,从而无法对提取信息的真实性进行检验。

传统搜索式无载体信息隐藏(Yuan 等,2017;Zhang 等,2018;Zheng 等,2017;Zhou 等,2015,2017,2018)隐藏容量低且涉及大量载体密集传输;基于纹理合成的无载体信息隐藏(Qian 等,2016;Qin 等,2017;Wu 和 Wang,2015;Xu 等,2015)无法生成有意义图像;基于马赛克拼图的信息隐藏(Hou 等,2016;Lai 和 Tsai,2011;Lee 和 Tsai,2014;Lin 和 Tsai,2004;刘小凯 等,2018;Zhai 等,2015;张梦 等,2016)尽管能产生有意义图像,但需采用修改式嵌密的方法嵌入变换参数。

针对这些问题,所提方法结合马赛克拼图,首先将多个灰度图像转换为具有伪随机转角的圆形图像来构建马赛克,通过生成随机整数坐标序列来决定二值秘密信息比特位串在掩体上的隐藏位置。其次对于隐藏位置,放置与密钥和位置关联的圆形图像来表达二值秘密比特串,并对含密圆形图像施加与密钥和位置关联的随机转角以进行认证,对于非隐藏位置则放置与对应像素最接近的圆形图像以掩盖隐藏的秘密信息。最后将放置过程产生的偏差利用误差扩散传递给掩体周围未处理像素从而产生马赛克图像,在提取阶段根据密钥结合质心旋转匹配从马赛克图像中提取秘密比特串并对其进行认证。与基于纹理合成的无载体信息隐藏相比,所提方法采用马赛克拼图的方法来生成有意义含密掩体;与基于搜索的无载体信息隐藏相比,所提方法避免了搜索无载体信息隐藏容量低和大量载体在信道中密集传输;与传统基于马赛克拼图的信息隐藏相比,所提方法采用质心旋转匹配来对隐藏的二值秘密信息比特进行识别和提取,并可通过随机转角认证来验证提取信息的准确性,具有良好的认证精度,避免了对比方法不具备相应认证能力的问题,且所提方法的提取过程完全依赖于密钥,原始掩体不在信道中传输且无法获取,生成的含密掩体为非自然图像载体,可抵抗传统基于自然图像统计的密写分析方法的检测;与修改式嵌入方法相比,所提方法利用圆形马赛克图像来表达秘密信息,具有较强的抗攻击鲁棒性,可容忍高强度噪声攻击和低质量 JPEG 压缩,且对随机剪切擦除攻击具有一定的抗攻击容忍能力。

1 本文方法

本文提出的结合块旋转和马赛克拼图的生成式伪装方法处理流程如图 1 所示,其中虚线框代表输入或输出处理集合,实线框为处理环节,三角箭头表示信息流动的方向,圆形箭头表示处理环节满足的约束条件。具体步骤为:1)通过圆形及随机转角初始化策略将分辨率为 $(2r-1)\times(2r-1)$ 像素的正方形图像 $\boldsymbol{H}_0,\boldsymbol{H}_1,\cdots,\boldsymbol{H}_{l-1}$ 转换为添加随机初始转角且半径为 r 的圆形图像 $\boldsymbol{H}'_0,\boldsymbol{H}'_1,\cdots,\boldsymbol{H}'_{l-1}$;2)从 $\boldsymbol{H}'_0,\boldsymbol{H}'_1,\cdots,\boldsymbol{H}'_{l-1}$ 中选取 $\boldsymbol{H}'_k$,用于对二值秘密信息序列 $\boldsymbol{B}$ 截取的 $\log_2 l$ 比特秘密信息 X_{cu} 进行表达,并通过 $\boldsymbol{H}'_k$ 的二次随机转角来构造 X_{cu} 的认证信息;3)结合误差扩散来生成与给定掩体图像 $\boldsymbol{T}$ 外观相似的马赛克图像 $\boldsymbol{M}$,用以对 $\boldsymbol{B}$ 进行掩盖;4)通过质心旋转匹配和随机转角认证的秘密信息恢复策略,从信道接收的马赛克图像 $\boldsymbol{M}'$ 中提取出秘密信息序列 $\boldsymbol{B}'$ 和秘密信息认证图 $\boldsymbol{A}$,并对 $\boldsymbol{B}'$ 的正确性进行认证。图 1 给出的策略主要包括 3 个关键处理环节:1)圆形及随机转角初始化策略,主要对样本图像进行圆形和随机转角初始化,用以构造秘密信息的表达样本;2)结合参数映射和误差扩散的马赛克图像生成策略,主要用于秘密信息的嵌入并进一步生成秘密信息的掩盖;3)结合质心旋转匹配和随机转角认证的秘密信息恢复策略,用于秘密信息的重构并对恢复出的秘密信息正确性进行认证。

1.1 圆形及随机转角初始化策略

记 $\boldsymbol{H}_k=(h^k_{i,j})_{(2r-1)\times(2r-1)}$,$k=0,1,\cdots,l-1$ 是 l 个分辨率为 $(2r-1)\times(2r-1)$ 像素的灰度样本图像,将其转换为具有初始转角 α_{in} 且半径为 r 的圆形图像 $\boldsymbol{H}'_k=(h'^k_{i,j})_{(2r-1)\times(2r-1)}$,得

$$\boldsymbol{H}'_k=Rot(\boldsymbol{H}_k,r,\alpha^k_{\mathrm{in}}) \tag{1}$$

式中,$Rot(\cdot)$ 是逆时针旋转函数,r 为圆形图像半径,$\alpha^k_{\mathrm{in}}\in[0,2\pi)$ 是逆时针旋转角度。

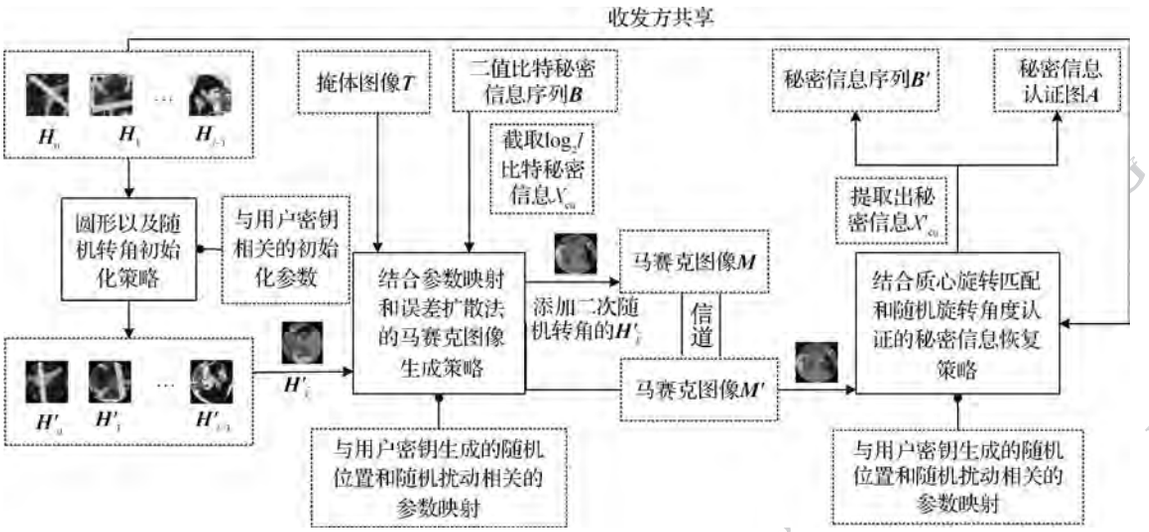


图 1　结合块旋转和马赛克拼图的生成式伪装方法框图

Fig. 1　The diagram of generative camouflage method combined with block rotation and mosaic

之所以按式(1)将 $\boldsymbol{H}_k$ 转换为 $\boldsymbol{H}'_k$，是为了让 $\boldsymbol{H}'_k$ 不仅可通过灰度均值来表示掩体图像像素，还可任意角度的摆放来进行转角认证；若 α_{in}^k 由密钥生成，则可对 $\boldsymbol{H}'_k$ 的摆放角度添加随机扰动，从而仅有掌握密钥的用户才能滤除 α_{in}^k 的影响并提取认证信息。

在本文中，$\alpha_{\text{in}}^k \in [0,2\pi)$ 是由密钥 k_0 产生的随机整数 $in_k \in [0,n-1]$ 按式(2)映射得到，其中 $k = 0,1,\cdots,l-1$。

$$\alpha_{\text{in}}^k = in_k \cdot 2\pi/n \tag{2}$$

将 $\boldsymbol{H}_k$ 转换为半径为 r 的圆形图像 $\boldsymbol{H}'_k$，即

$$h'^k_{i,j} = \begin{cases} -1 & (i-r+1)^2 + (j-r+1)^2 \leqslant r^2 \\ 0 & \text{其他} \end{cases} \tag{3}$$

将 $\boldsymbol{H}'_k$ 进行初始化，用于保留 $\boldsymbol{H}_k$ 半径 r 范围内的像素 $h_{i,j}^k, (i,j) \in \{(i-r+1)^2 + (j-r+1)^2 \leqslant r^2\}$。为使 $\boldsymbol{H}'_k$ 具有随机初始转角 α_{in}^k，这里需将 $\boldsymbol{H}_k$ 上的像素由平面直角坐标转换为极坐标，记 $h_{i,j}^k, (i,j) \in \{(i-r+1)^2 + (j-r+1)^2 \leqslant r^2\}$ 对应的极坐标为 $h_{i,j}^{k,\rho,\theta}$，按

$$(\rho,\theta) = \begin{cases} \rho = \sqrt{(i-r+1)^2 + (j-r+1)^2} \\ \theta = (j-r+1)/(i-r+1) \end{cases} \tag{4}$$

进行转换，按

$$(i_1,j_1) = \begin{cases} i_1 = [\rho \cdot \cos(\theta + \alpha_{\text{ind}})] \\ j_1 = [\rho \cdot \sin(\theta + \alpha_{\text{ind}})] \end{cases} \tag{5}$$

添加随机转角 α_{in}^k（式(5)中“[ ]”为四舍五入操作符）。然后将 $h_{i,j}^k$ 赋值给 $\boldsymbol{H}'_k$ 中元素 $h'^k_{i_1,j_1}$，其中当 $i = r, j = r$ 时，则直接将 $h_{i,j}^k$ 作为 $h'^k_{i_1,j_1}$。

由于极坐标和平面直角坐标在转换过程中不完全匹配，因此 $\boldsymbol{H}'_k$ 会存在缺失像素点 $h'^k_{i,j} = -1, (i,j) \in \{(i-r+1)^2 + (j-r+1)^2 \leqslant r^2\}$，这里可通过插值拟合来对缺失像素进行补全，具体为

$$h'^k_{i_1,j_1} = \sum_{k=0}^{co-1} \frac{P_k}{d_k} \Big/ \sum_{k=0}^{co-1} \frac{1}{d_k} \tag{6}$$

式中，$P_0, P_1, \cdots, P_{co-1}$ 是位于圆形图像内且以 $h'^k_{i,j} = -1$ 为中心的 5×5 邻域内的非缺失像素，$d_0, d_1, \cdots, d_{co-1}$ 是与之对应的二次距离。

式(2)—式(6)构成了本文的圆形及随机转角初始化策略，即式(1)。通过式(1)，可将方形图像转换为圆形图像并添加初始随机转角。与传统基于马赛克的信息隐藏方法修改式嵌入变换参数的方法不同，本文将圆形图像直接作为秘密信息的编码表示单元，只涉及圆形图像的放置角度而不涉及对圆形图像的任意修改嵌入，因此可避免传统基于马赛克拼图的信息隐藏由于修改引发的密写异常问题，同时添加的随机转角也为特定用户提取秘密信息和进行角度认证提供安全保证，使得掌握特定密钥的用户才能滤除随机转角的影响并提取对应的认证信息。

图 2 是对选取的 8 位灰度样本图像进行圆形及随机转角初始化策略后得到的圆形图像。

图 2　样本图像圆形及随机转角初始化验证图

Fig. 2　The sample images and their corresponding initialized circle images ((a) sample images; (b) circle images)

1.2　结合参数映射和误差扩散的马赛克图像生成策略

记 $\boldsymbol{T}=(t_{i,j})_{m_0\times n_0}$ 为灰度掩体图像，初始化全 0 的灰度半色调图像 $\boldsymbol{M}=(m_{i,j}=0)_{m_2\times n_2}$，且 $m_2\times n_2$ 满足的约束为

$$m_2=m_0(2r-1),n_2=n_0(2r-1) \tag{7}$$

即 $\boldsymbol{M}$ 最多可划分为 m_0n_0 个 $(2r-1)\times(2r-1)$ 像素的正方形网格用于放置 m_0n_0 个半径为 r 的圆形图像。

若将第 1.1 节圆形图像 $\boldsymbol{H}'_k$，$k=0,1,\cdots,l-1$ 全部用于二值秘密比特表达，则每个 $\boldsymbol{H}'_k$ 所能表达的二值秘密比特数为 $\lfloor\log_2 l\rfloor$，若将二值秘密比特序列 $\boldsymbol{B}=(b_i)_{l_B}$，$b_i\in\{0,1\}$ 放置在 $\boldsymbol{M}$ 划分的 $(2r-1)\times(2r-1)$ 正方形网格上，则所需要的正方形网格数 l_0 需满足

$$l_0=\lceil l_B/\lfloor\log_2 l\rfloor\rceil,\ l_0<m_0n_0 \tag{8}$$

的约束。这里可通过密钥 k_1 随机产生 l_0 个两两不等的 $m_0\times n_0$ 范围内的坐标，来决定代表秘密信息的圆形图像在 $\boldsymbol{M}$ 中的网格放置位置，从而只有提供正确的 k_1 才能找到表示秘密信息的圆形图像。

记由 k_1 随机产生的用于隐藏秘密信息的坐标位置序列为 $\boldsymbol{T}_0=(p_i^0)_{l_0}$，$p_i^0=(x_i,y_i)$，按

$$\boldsymbol{B}_{cu}=trim(\boldsymbol{B},cu\cdot\lfloor\log_2 l\rfloor,\lfloor\log_2 l\rfloor) \tag{9}$$

可从 $\boldsymbol{B}$ 中截取长度为 $\lfloor\log_2 l\rfloor$ 的二值秘密比特 $\boldsymbol{B}_{cu}$，其中 $cu=0,1,\cdots,l_0-1$。式(9)中，$trim(\cdot)$ 是截断函数，其中第 1 个参数为输入的二值比特序列，第 2 个参数为截取的起始索引位置，第 3 个参数为截取长度，在截取过程中，若剩余二值比特不足，则截取剩余全部比特。

为避免 $\boldsymbol{B}_{cu}$ 和圆形图像 $\boldsymbol{H}'_k$，$k=0,1,\cdots,l-1$ 存在固定的一对一关系导致的安全隐患，按

$$\hat{k}=(X_{cu}+x_i+y_i+r_{x_i,y_i}+x_i\cdot y_i\cdot r_{x_i,y_i})\bmod l \tag{10}$$

将 $\boldsymbol{B}_{cu}$ 和网格坐标 $p_0=(x_i,y_i)$ 与用户密钥 k_2 绑定，来共同决定代表秘密信息的圆形图像 $\boldsymbol{H}'_{\hat{k}}$，$\hat{k}\in\{0,1,\cdots,l-1\}$。式(10)中，$X_{cu}$ 是 $\boldsymbol{B}_{cu}$ 对应的 10 进制数，r_{x_i,y_i} 是 k_2 生成的整数随机矩阵 $\boldsymbol{R}=(r_{i,j})_{m_0\times n_0}$，$r_{i,j}\in\{0,1,\cdots,l-1\}$ 在 (x_i,y_i) 位置的元素。

由式(10)可决定网格位置 $(x_i,y_i)\in\boldsymbol{T}_0$ 所放置的代表秘密信息的圆形图像。若 $(x_i,y_i)\notin\boldsymbol{T}_0$，这里依然需从 $\boldsymbol{H}'_k$，$k=0,1,\cdots,l-1$ 中选取最合适的圆形图像，用于对代表秘密信息的圆形图像进行掩盖，具体为

$$\hat{k}=\arg\min_{k\in\{0,1,\cdots,l-1\}}|\mathrm{mean}(\boldsymbol{H}'_k)-t_{x_i,y_i}| \tag{11}$$

式中，$\mathrm{mean}(\boldsymbol{H}'_k)$ 用于计算 $\boldsymbol{H}'_k$ 的均值，t_{x_i,y_i} 为灰度掩体图像 $\boldsymbol{T}$ 的 (x_i,y_i) 位置的像素。

式(10)和式(11)选取的圆形图像在放置过程中都会产生偏差，为保证最终输出的 $\boldsymbol{M}$ 与 $\boldsymbol{T}$ 外观相似，需将放置过程中的偏差 Δ_{x_i,y_i} 向 (x_i,y_i) 周围未处理的以 $(u,v)\in(x_i,y_i+1),(x_i+1,y_i-1),(x_i+1,y_i),(x_i+1,y_i+1)$ 为起点，分辨率为 $(2r-1)\times(2r-1)$ 的网格扩散。偏差 Δ_{x_i,y_i} 的计算式为

$$\Delta_{x_i,y_i}=\underset{(i-r+1)^2+(j-r+1)^2\leqslant r^2}{\mathrm{mean}}(\boldsymbol{H}'_k)-t_{x_i,y_i} \tag{12}$$

式中，mean 为块均值函数，$\underset{(i-r+1)^2+(j-r+1)^2\leqslant r^2}{\mathrm{mean}}$ 计算的是 $\boldsymbol{H}'_k$ 落入 $(i-r+1)^2+(j-r+1)^2\leqslant r^2$ 范围的全部像素均值。

扩散的方法为

$$\begin{cases}t_{x_i,y_i+1}=t_{x_i,y_i+1}-\dfrac{7}{16}\Delta_{x_i,y_i}\\ t_{x_i+1,y_i-1}=t_{x_i+1,y_i-1}-\dfrac{3}{16}\Delta_{x_i,y_i}\\ t_{x_i+1,y_i}=t_{x_i+1,y_i}-\dfrac{5}{16}\Delta_{x_i,y_i}\\ t_{x_i+1,y_i+1}=t_{x_i+1,y_i+1}-\dfrac{1}{16}\Delta_{x_i,y_i}\end{cases} \tag{13}$$

式(12)使得含密掩体 $\boldsymbol{M}$ 的视觉质量与掩体图像 $\boldsymbol{T}$ 相接近，而式(13)进一步将放置过程中产生的偏差向周围扩散以减少视觉损失。

对圆形图像添加随机转角，原则上不会对圆形图像均值产生影响，但由于平面直角坐标和极坐标不能完全对齐，从而存在缺失像素。本文通过

式(6)插值拟合，使得缺失像素与圆形图像均值趋于一致，从而使得随机添加的转角不会对圆形图像均值产生较大影响。由于转角对圆形图像均值影响较小，因此可在圆形图像初始随机转角的基础上进行二次转角，用于对提取秘密信息的正确性进行检验。采用的方法如下：

1)对索引为 $\hat{k}$ 的圆形样本图像计算 $[0,n-1]$ 范围内的整数 $in_{\hat{k}}$，具体计算为

$$in_{\hat{k}} = (X_{\mathrm{cu}} + x_i \cdot y_i + y_i \cdot r_{x_i,y_i} + x_i \cdot r_{x_i,y_i}) \bmod n \tag{14}$$

式中，若 $(x_i,y_i) \notin \boldsymbol{T}_0$，则取 $X_{\mathrm{cu}} = 0$。

2)按式(2)计算随机转角 $\alpha_{in_{\hat{k}}}$，将 $\boldsymbol{H}'_{\hat{k}}$ 按式(1)逆时针旋转 $\alpha_{in_{\hat{k}}}$ 作为 $\boldsymbol{H}''_{\hat{k}}$。

3)将 $\boldsymbol{H}''_{\hat{k}}$ 放置在 $\boldsymbol{M}$ 上以 $(x_i \cdot (2r-1), y_i \cdot (2r-1))$ 为起点，大小为 $(2r-1)\times(2r-1)$ 像素的矩阵小块上。

由式(14)可知，$in_{\hat{k}}$ 不仅与放置的秘密信息 X_{cu} 有关，还与放置的网格坐标位置 (x_i,y_i) 以及 k_2 生成的随机矩阵元素 r_{x_i,y_i} 密切相关，从而 X_{cu} 与 $in_{\hat{k}}$ 不存在简单固定的一对一映射关系而完全依赖于密钥。

通过式(14)和式(1)可对 $\boldsymbol{M}$ 上放置的每个圆形样本图像添加一个二次随机转角，而只有掌握密钥的合法用户才能获取二次随机转角并将其用于对秘密信息的正确性认证。

以上策略构成了本文结合参数映射和误差扩散的马赛克图像生成策略，该策略可生成有意义的马赛克拼图，并能通过放置在不同位置的圆形图像来表达秘密信息。避免了只能生成简单质地的纹理图像；同时，本策略可以将所有含密圆形图像隐藏在一张马赛克拼图中，避免了 Yuan 等人(2017)，Zhang 等人(2018)，Zheng 等人(2017)和 Zhou 等人(2015，2017，2018)的方法中涉及的大量嵌密载体密集传输问题；此外，对应的含密位置由密钥产生，含密圆形图像在放置过程中无需任何参数的修改式嵌入，避免了使用修改式嵌入导致的密写异常问题，同时所提策略是由圆形图像纹理直接表达秘密信息，因此相对 Hou 等人(2016)，Lai 和 Tsai(2011)，Lee 和 Tsai(2014)，刘小凯等人(2018)，Zhai 等人(2015)和张梦等人(2016)不耐攻击的 LSB 嵌入，具备较强的抗攻击鲁棒性。

1.3　结合质心旋转匹配和随机角度认证的秘密信息提取与认证策略

将信道接收到的可能遭受攻击的马赛克图像记为 $\boldsymbol{M}'$。在提取秘密信息时，需定位秘密信息在马赛克图像上的隐藏位置，从中找到代表秘密信息的圆形图像，并通过圆形图像的随机转角来对提取的秘密信息进行认证。因此为提取秘密信息和对秘密信息进行认证，需准确识别代表秘密信息的圆形图像索引和圆形图像的旋转放置角度索引，即二次转角索引。

对于代表秘密信息的圆形图像索引，由于代表秘密信息的圆形图像不仅添加了与用户密钥 k_0 相关的随机初始转角，而且添加了与放置位置、秘密信息和用户密钥 k_2 有关的二次认证转角，从而导致结合用户密钥 k_1 提取的圆形图像与接收方实际用于比对的圆形图像存在不同的随机转角。为快速准确地识别提取到的圆形图像对应的索引，可通过质心旋转匹配将待识别的圆形图像和与之比对的圆形图像的质心统一到圆形图像圆心右侧的正半轴上，然后通过二次差异距离最小匹配找到与之对应的圆形图像索引。具体的质心旋转匹配策略为：

接收方按发送方同样的方式由灰度图像 $\boldsymbol{H}_k$ 得到圆形图像 $\boldsymbol{H}'_k = (h'^{k}_{i,j})_{(2r-1)\times(2r-1)}$，其中，$k = 0, 1, \cdots, l-1$。对于每个圆形图像 $\boldsymbol{H}'_k$ 按

$$\begin{aligned} x^k_{\mathrm{ma}} &= \left(\sum_{(i-r+1)^2+(j-r+1)^2 \leqslant r^2} (j-r) \cdot h'^{k}_{i,j} \right) / m_{\mathrm{to}} \\ y^k_{\mathrm{ma}} &= \left(\sum_{(i-r+1)^2+(j-r+1)^2 \leqslant r^2} (r-i) \cdot h'^{k}_{i,j} \right) / m_{\mathrm{to}} \\ m_{\mathrm{to}} &= \left(\sum_{(i-r+1)^2+(j-r+1)^2 \leqslant r^2} h'^{k}_{i,j} \right) \end{aligned} \tag{15}$$

计算其质心 $(x^k_{\mathrm{ma}}, y^k_{\mathrm{ma}})$，并按

$$\alpha^k_{\mathrm{ma}} = \arctan(y^k_{\mathrm{ma}} / x^k_{\mathrm{ma}}) \tag{16}$$

计算其几何倾角 $\alpha^k_{\mathrm{ma}} \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$。其中，$\arctan(\cdot)$ 是反正切函数，用于计算 $y^k_{\mathrm{ma}}/x^k_{\mathrm{ma}}$ 的几何倾角。

式(15)采用 $j-r$ 和 $r-i$ 来计算 $(x^k_{\mathrm{ma}}, y^k_{\mathrm{ma}})$，而非 $j-r$ 和 $i-r$，原因是计算机图像采用的默认坐标系是以图像左上角为坐标原点，采用向左和向下的方向为对应坐标轴的正半轴，而质心计算默认的平面直角坐标系则以向左和向上为坐标轴正半轴。因此，为保持计算结果的一致性，采用 $j-r$ 和 $r-i$ 来计算 $(x^k_{\mathrm{ma}}, y^k_{\mathrm{ma}})$。

将 $\boldsymbol{H}'_k, r, 2\pi - \alpha^k_{\mathrm{ma}}$ 代入式(1)，可将 $\boldsymbol{H}'_k$ 的质心统

一到圆心右侧的正半轴上。记对应的圆形图像为 $\boldsymbol{H}_k'''$，可将式(15)、(16)和式(1)对应的质心旋转策略简记为

$$\boldsymbol{H}_k''' = Rot_{\mathrm{ma}}(\boldsymbol{H}_k') \tag{17}$$

记 $\boldsymbol{M}'$ 中截取的分辨率为 $(2r-1)\times(2r-1)$ 像素的含密圆形图像为 $\boldsymbol{M}_t$，将其代入式(17)，并将其质心统一到圆心右侧的正半轴上，记为 $\boldsymbol{M}_t'$。通过计算 $\boldsymbol{M}_t'$ 和 $\boldsymbol{H}_k'''$，$k=0,1,\cdots,l-1$ 的最小二次差异距离可找到 $\boldsymbol{M}_t$ 对应的索引 $\hat{k}$，具体为

$$\hat{k} = \arg\min_{k=0,1,\cdots,l-1} \|\boldsymbol{M}_t' - \boldsymbol{H}_k'''\|_2^2 \tag{18}$$

对于 $\boldsymbol{M}_t$，可通过下面方式获取，即

由密钥 k_1 生成代表秘密信息的圆形图像在掩体图像 $\boldsymbol{M}'$ 中的嵌入位置 $\boldsymbol{T}_0$，对于每个位置 $(x,y)\in\boldsymbol{T}_0$，按

$$\begin{aligned} u &= x\cdot(2r-1)\\ v &= y\cdot(2r-1) \end{aligned} \tag{19}$$

计算 (x,y) 在 $\boldsymbol{M}'$ 中的坐标位置 (u,v)，然后以 (u,v) 为起点，从 $\boldsymbol{M}'$ 中截取 $(2r-1)\times(2r-1)$ 像素的含密圆形图像作为 $\boldsymbol{M}_t$。

对于代表秘密信息的圆形图像的旋转放置角度索引，由于代表秘密信息的圆形图像在放置过程中，仅涉及 n 个转角 $\alpha_k = k\times 2\pi/n$，$k=0,1,\cdots,n-1$，这里可按与式(18)类似的方法，将 $\boldsymbol{M}_t$ 依次旋转 n 个转角，记为 $\boldsymbol{M}_t^k$，$k=0,1,\cdots,n-1$，然后从中找到与 $\boldsymbol{H}_{\hat{k}}'$ 二次差异距离最小的，从而得到其对应的旋转放置角度索引，即 $\boldsymbol{M}_t$ 的二次转角索引 in_{re}，具体为

$$in_{\mathrm{re}} = \arg\min_{k=0,1,\cdots,n-1} \|\boldsymbol{M}_t^k - \boldsymbol{H}_{\hat{k}}'\|_2^2 \tag{20}$$

式中，准确获取 in_{re} 的前提是获取准确的 $\boldsymbol{H}_{\hat{k}}'$，而 $\boldsymbol{H}_{\hat{k}}'$ 不仅涉及 $\boldsymbol{H}_{\hat{k}}$，还涉及 $\boldsymbol{H}_{\hat{k}}$ 的初始转角，这个初始转角与用户密钥 k_0 有关，从而只有掌握用户密钥 k_0 的合法用户才能滤除初始转角的影响。

得到了代表秘密信息的圆形图像 $\boldsymbol{M}_t$ 的索引 $\hat{k}$ 和 $\boldsymbol{M}_t$ 的二次转角索引 in_{re}，可按

$$X_{\mathrm{cu}} = (\hat{k} + (l-1)\cdot (x + y + r_{x,y} + x\cdot y\cdot r_{x,y}))\bmod l \tag{21}$$

提取出秘密信息 X_{cu}，然后利用式(14)生成的 $in_{\hat{k}}$ 和 in_{re} 是否一致来判断提取的 X_{cu} 是否准确。可分别通过0和1来表示认证是否准确，将其记为

$$a = \mathrm{Authen}(in_{\mathrm{re}}, X_{\mathrm{cu}}, (x_i,y_i), r_{x_i,y_i}),\ a\in\{0,1\} \tag{22}$$

式(21)和式(14)均涉及随机扰动 $r_{x,y}$，该随机扰动是由用户密钥 k_2 生成，而对应的坐标位置由用户密钥 k_1 生成，从而保证只有掌握合法密钥 k_1 和 k_2 的用户才能提取秘密信息和参与认证，而认证时只有掌握用户密钥 k_0 的合法用户才能滤除初始转角的影响。

将所有的 X_{cu} 转化为 $\log_2 l$ 位2进制序列 $\boldsymbol{B}_{\mathrm{cu}}$ 并进行连接，可获得对应的秘密信息序列 $\boldsymbol{B}'$，将所有的 a 构成序列，可得到秘密信息的认证序列 $\boldsymbol{A}$。

以上策略即构成了本文质心旋转匹配和随机角度认证的秘密信息提取与认证策略。其中，质心旋转匹配用于含密圆形图像与样本图像的快速匹配，以及确定样本图像索引，并通过用户密钥提取秘密信息；含密圆形图像的随机转角认证用于对提取秘密信息的准确性进行检验，同时与用户密钥绑定的认证策略保证了只有由掌握密钥的用户才能进行认证，从而保证了认证策略的安全性。与 Hou 等人(2016)，Lai 和 Tsai(2011)，Lee 和 Tsai(2014)，Lin 和 Tsai(2004)，刘小凯等人(2018)，Zhai 等人(2015)和张梦等人(2016)的方法缺少认证策略相比，本文方法不仅具备良好的认证能力且能有效地保证认证策略的安全性。本文生成的含密掩体为非自然载体，原始掩体不在信道中传输，因而可抵抗传统基于自然图像统计的密写分析方法。

2 完整算法

结合第1节完成的工作，可给出如下完整的算法1和算法2。

算法1 结合块旋转和马赛克拼图的生成式伪装算法。

1)输入密钥 k_0,k_1,k_2，分辨率为 $m_0\times n_0$ 像素，灰度掩体图像 $\boldsymbol{T}=(t_{i,j})_{m_0\times n_0}$，$t_{i,j}\in\{0,1,\cdots,255\}$，秘密比特序列 $\boldsymbol{B}=(b_i)_{l_{\mathrm{B}}}$，两两不等分辨率为 $(2r-1)\times(2r-1)$ 像素的灰度图像 $\boldsymbol{H}_k$，$k=0,1,\cdots,l-1$，其中 $m_0n_0 > l_0$，$l_0 = \lceil l_{\mathrm{B}}/\log_2 l\rceil$。

2)由 k_0 产生随机整数 in_k，$k=0,1,\cdots,l-1$，按式(2)将其映射为 α_{in}^k，$k=0,1,\cdots,l-1$，并按式(1)将 $\boldsymbol{H}_k$ 转化为 $\boldsymbol{H}_k'$，$k=0,1,\cdots,l-1$。

3)由 k_1 生成随机整数坐标序列 $\boldsymbol{T}_0$，k_2 生成随机整数矩阵 $\boldsymbol{R}=(r_{i,j})_{m_0\times n_0}$，初始化掩体图像 $\boldsymbol{M}=(0)_{m_2\times n_2}$。循环执行步骤4)～6)，直至枚举完 $m_0\times n_0$ 范围内的全部坐标 (x,y)。

4)若 $(x,y) \in \boldsymbol{T}_0$，按式(9)截取 $\boldsymbol{B}_{\mathrm{cu}}$ 作为 X_{cu}，将 X_{cu}，(x,y)，$r_{x,y}$ 代入式(10)生成 $\hat{k}$，通过式(14)计算 $in_{\hat{k}}$，通过式(2)计算 $\alpha_{\mathrm{in}_{\hat{k}}}$，将 $\boldsymbol{H}'_{\hat{k}}$ 按式(1)旋转 $\alpha_{\mathrm{in}_{\hat{k}}}$ 后，放入 $\boldsymbol{M}$ 中对应为 (x,y) 的网格位置上。

5)若 $(x,y) \notin \boldsymbol{T}_0$，按式(11)选取 $\boldsymbol{H}'_{\hat{k}}$，通过式(14)计算 $in_{\hat{k}}$，通过式(2)计算 $\alpha_{in_{\hat{k}}}$，然后按式(1)对 $\boldsymbol{H}'_{\hat{k}}$ 赋予随机转角 $\alpha_{in_{\hat{k}}}$，并将 $\boldsymbol{H}'_{\hat{k}}$ 放置在 $\boldsymbol{M}$ 中对应为 (x,y) 的网格位置上。

6)按式(12)计算 $\boldsymbol{H}'_{\hat{k}}$ 放入后的偏差 Δ_{x_i,y_i}，按式(13)扩散。

7)输出 $\boldsymbol{M}$。

与算法 1 对应的恢复算法记为算法 2。

算法 2 结合块旋转和马赛克拼图的秘密信息恢复算法

1)输入密钥 k_0,k_1,k_2，含密马赛克图像 $\boldsymbol{M}'$，两两不等分辨率为 $(2r-1)\times(2r-1)$ 像素的灰度图像 $\boldsymbol{H}_k$，$k=0,1,\cdots,l-1$ 和秘密信息占用的网格数量 l_0。

2)由 k_0 产生随机整数 in_k，$k=0,1,\cdots,l-1$，按式(2)将其映射为 α_{in}^{k}，$k=0,1,\cdots,l-1$，由式(1)将 $\boldsymbol{H}_k$ 转化为 $\boldsymbol{H}'_k$，并按式(17)得到 $\boldsymbol{H}'''_k$，其中 $k=0,1,\cdots,l-1$。

3)由 k_1 生成 $\boldsymbol{T}_0=(p_i^0)_{l_0}$，利用 k_2 生成 $\boldsymbol{R}=(r_{i,j})_{m_0\times n_0}$，初始化恢复信息序列 $\boldsymbol{B}'=\phi$ 和认证序列 $\boldsymbol{A}=\phi$。

4)依次枚举 $p_i^0=(x_i,y_i)\in\boldsymbol{T}_0$，执行步骤 5)～7)。

5)按式(19)截取含密圆形图像 $\boldsymbol{M}_t$，并通过式(17)将 $\boldsymbol{M}_t$ 旋转为 $\boldsymbol{M}'_t$。

6)按式(18)获取 $\boldsymbol{M}'_t$ 对应的索引 $\hat{k}$，按式(20)提取二次转角索引 in_{re}，按式(21)提取 X_{cu}，将其转化为 $\boldsymbol{B}_{\mathrm{cu}}$ 并添加至 $\boldsymbol{B}'$ 中。

7)将 $\boldsymbol{M}_t$，$\boldsymbol{H}'_{\hat{k}}$，$X_{\mathrm{cu}}$，$(x_i,y_i)$，$r_{x_i,y_i}$ 代入式(22)中生成认证信息 a 并添加至 $\boldsymbol{A}$ 中。

8)输出 $\boldsymbol{B}'$，$\boldsymbol{A}$。

与现有的基于搜索的无载体信息隐藏算法相比，以上方法可将构成图像马赛克的基本组成单元圆形图像作为编码单元来表达秘密信息，通过生成单幅马赛克图像来传递秘密信息，避免了搜索式无载体信息隐藏存在的单载体隐藏容量低和涉及大量载体的信道密集传输等问题。

与生成简单质地纹理图像的纹理合成式无载体信息隐藏相比，以上方法可直接生成与给定掩体图像外观相似的有意义马赛克图像。

与传统修改式嵌入的马赛克拼图信息隐藏方法相比，以上方法仅涉及圆形图像的放置角度而不涉及任何以嵌入为目的的修改，因此可避免传统马赛克信息隐藏由于修改引发的密写异常问题。

所添加的随机转角认证也为特定用户提取秘密信息和进行角度认证提供了必要的安全保证，避免了 Hou 等人(2016)，Lai 和 Tsai(2011)，Lee 和 Tsai(2014)，刘小凯等人(2018)，Zhai 等人(2015)和张梦等人(2016)的方法因不具备提取信息的认证能力，从而无法对秘密信息的真实性进行检验的缺陷。

由于所提方法构造的认证策略是基于圆形图像的放置角度，并且是通过有意义的圆形图像纹理结合用户密钥和放置位置来表达秘密信息，而非 Hou 等人(2016)，Lai 和 Tsai(2011)，Lee 和 Tsai(2014)，刘小凯等人(2018)，Zhai 等人(2015)和张梦等人(2016)采用的基于 LSB 的嵌入策略，从而在遭受攻击时，所表达的秘密信息和放置角度可容易地通过质心旋转匹配和基于密钥的随机转角策略来提取和识别，从而不仅具备较强的抗攻击鲁棒性，也具备较好的认证精度；同时所提策略完全依赖于用户密钥，原始掩体不在信道中传输且无法获取，生成的含密掩体为非自然图像载体，可抵抗传统基于自然图像统计特性的密写分析方法，具有较高的安全性。

3 实　验

实验测试环境为 Windows 10 系统，CPU 为 Intel(R) Core(TM) i5-6600，主频为 3.31 GHz，内存为 8.00 GB，实验编程语言为 JAVA jdk 1.8.0_65。

实验选取 4 幅 128 × 128 像素的灰度图像 man、woman、cameraman 和 Lena 作为掩体图像，1 幅分辨率为 300 × 60 像素的二值秘密信息图像(如图 3 所示)，以及 32 幅分辨率为 65 × 65 像素的灰度样本图像(如图 4 所示)，这些灰度样本图像将进一步转换为圆形图像，用于秘密信息的表达和形成含密马赛克图像。

实验采用峰值信噪比(PSNR)来验证含密马赛克图像与攻击后马赛克图像之间的差异度，其具体计算为

(a) man (b) woman (c) cameraman (d) Lena (e) 二值秘密信息

图 3 实验测试图像

Fig. 3 The experimental images ((a) man; (b) woman; (c) cameraman; (d) Lena; (e) secret bit information)

图 4 实验用到的样本图像

Fig. 4 The experimental sample images

$$PSNR = 10\log\frac{255^2}{MSE} \tag{23}$$

式中，MSE 为攻击前后含密马赛克图像上的圆形图像均值的均方误差(mean square error)，其具体计算为

$$MSE = \frac{\sum_{i=0}^{m_c-1}\sum_{j=0}^{n-1}(p_{i,j}-p'_{i,j})^2}{m\times n} \tag{24}$$

式中，$p_{i,j}$，$p'_{i,j}$ 为待比较 2 个圆形图像像素均值，$m\times n$ 为对应马赛克图像中的圆形图像个数。

由于在实验中，每个圆形图像可隐藏 1 个 5 bit 秘密信息，即 32 进制数，因此所提方法使用误码率(ER)衡量恢复的 32 进制序列与原 32 进制序列之间的差异，其具体计算为

$$E = \frac{l_{er}}{l_{to}}\times 100\% \tag{25}$$

式中，E 是误码率，l_{er} 是发生错误的 32 进制数的个数，l_{to} 是总 32 进制数的个数。

使用认证成功率(ASR)衡量所提策略的认证成功概率，其具体计算为

$$A = \frac{l_{su}}{l_{TO}}\times 100\% \tag{26}$$

式中，A 是认证成功率，l_{su} 为认证成功的数量，l_{TO} 是总认证数量。

使用攻击占比(AR)来标记遭受攻击的圆形图像占比，其具体计算为

$$a = \frac{l_{at}^{C}}{l_{to}^{C}}\times 100\% \tag{27}$$

式中，a 是攻击占比，l_{to}^{C} 为马赛克图像中含密圆形图像的总数，l_{at}^{C} 为遭受攻击的含密圆形图像数量。

3.1 正确性实验

为验证所提策略的正确性，以图 3(e)为秘密信息，图 3(a)—(d)为掩体图像，选取图 4 作为样本图像，按不同密钥参数(线性同余映射的随机数种子)由算法 1 生成含密马赛克图像，然后按算法 2 从含密马赛克图像中提取秘密信息。其中，图 5 是含密马赛克图像，图 6 是提取的二值秘密信息和与之对应的认证图，表 1 给出了实验参数。由于图 5(a)—(d)对应的含密马赛克图像分辨率高达 8 320 × 8 320 像素，无法显示局部细节，通过图 5(e)—(h)给出 5(a)—(d)的局部细节。对于图 6 的认证图，约定黑和白分别表示认证通过和失败，认证图的分辨率为 60 × 60 像素。

由表 1、图 5 和图 6 可以看出，所提方法可生成有意义含密马赛克图像，并能通过正确密钥提取秘密信息，且提取秘密信息相对于原秘密信息的 ER 为 0%，秘密信息完整恢复，正确性得以验证。

3.2 密钥依赖性实验

为验证所提策略对密钥的依赖性，对表 1 的密钥参数进行修改，然后按算法 2 从含密马赛克图像图 5(a)—(d)中恢复出秘密信息。表 2 给出了密钥依赖性实验数据，对应的恢复信息和认证图如图 7 所示。

表 2 中前两组数据误码率为 0，ASR 低于 50%，原因是：k_0 是通过旋转转角对放置的圆形图像所表达的秘密信息进行角度认证，因此当 k_0 发生错误时，会导致认证策略失效，从而影响认证的准确度。k_0 和圆形图像所表示的秘密信息无关，从而不会对秘密信息的提取产生任何影响。

从表 2 和图 7 实验结果可看出，只有提供正确的密钥才能获取正确的秘密信息和认证信息，而错误的密钥参数将无法提取秘密信息或对其进行正确认证。

3.3 抗攻击与认证实验

为验证本文方法的抗攻击性能和认证精度，分

表 1　正确性验证实验参数

Table 1　Correctness verification experiment variables

掩体图像	密钥		马赛克图像	恢复信息	认证图	测试结果	
	参数	值				E/%	A/%
图 3(a)	k_1	4	图 5(a)	图 6(a)	图 6(e)	0	100
	k_2	7					
	k_3	2					
图 3(b)	k_1	9	图 5(b)	图 6(b)	图 6(f)	0	100
	k_2	5					
	k_3	3					
图 3(c)	k_1	5	图 5(c)	图 6(c)	图 6(g)	0	100
	k_2	1					
	k_3	6					
图 3(d)	k_1	11	图 5(d)	图 6(d)	图 6(h)	0	100
	k_2	15					
	k_3	14					

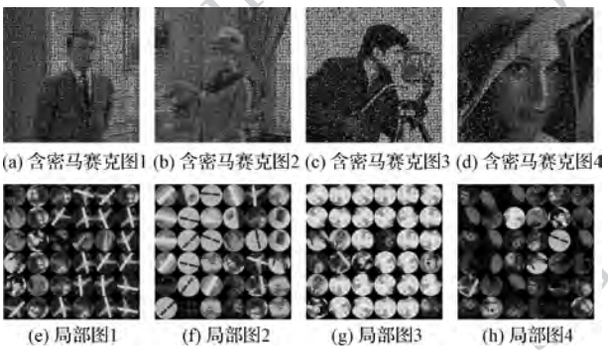


图 5　正确性实验的含密马赛克图像和局部细节图像

Fig. 5　The generated stego mosaic images and their parts in the correctness verification experiment ((a)—(d) stego mosaic images 1～4; (e)—(h) stego mosaic image parts 1～4)

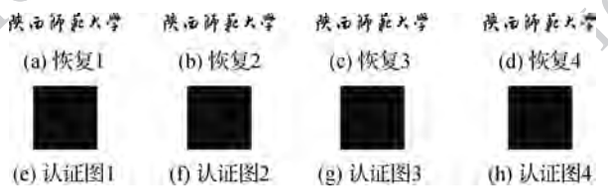


图 6　正确性实验恢复信息以及认证图

Fig. 6　The recovered information and their authentication images in the correctness verification experiment ((a)—(d) recovered secret 1～4; (e)—(h) authentication images 1～4)

别对正确性实验中生成的含密马赛克图像进行下列攻击:1)JPEG 压缩:对选中的含密马赛克图像进行不同质量因子的 JPEG 压缩;2)加噪攻击:对选中的马赛克图像添加不同强度的随机噪声;3)剪切攻击:对选中的马赛克图像进行不同占比的剪切;4)替换攻击:将选中的马赛克图像中的部分含密圆形图像替换为其他圆形图像;5)转角攻击:将选中的马赛克图像中的部分含密圆形图像施加随机转角扰动。

图 7　密钥依赖性实验恢复信息及认证图

Fig. 7　The recovered secrets and their authentication images in the key dependency verification experiment ((a)—(h) recovered secret 1～8; (i)—(p) authentication images 1～8)

3.3.1　抗 JPEG 压缩实验

为验证本文方法抗 JPEG 的压缩性能，对

图5(b)和图5(c)进行不同质量因子的JPEG压缩，并利用正确密钥按算法2提取秘密信息，表3给出了抗JPEG压缩的实验参数，图8为对应的压缩后含密马赛克图像，对应的恢复信息和认证图如图9所示。

表2　密钥依赖性实验参数

Table 2　Key dependency verification experiment variables

马赛克图像	密钥原值			密钥修改值			重构密图	认证图	测试结果	
	k_0	k_1	k_2	k_0	k_1	k_2			E/%	A/%
图5(a)	4	7	2	25	–	–	图7(a)	图7(i)	0	47.28
图5(a)	4	7	2	3	–	–	图7(b)	图7(j)	0	45.46
图5(b)	9	5	3	–	15	–	图7(c)	图7(k)	96.90	84.60
图5(b)	9	5	3	–	4	–	图7(d)	图7(l)	96.97	84.56
图5(c)	5	1	6	–	–	13	图7(e)	图7(m)	83.00	83.59
图5(c)	5	1	6	–	–	4	图7(f)	图7(n)	84.55	83.92
图5(d)	11	15	14	10	18	9	图7(g)	图7(o)	97.19	86.76
图5(d)	11	15	14	3	5	1	图7(h)	图7(p)	97.29	86.65

注：“–”表示未修改。

表3　抗JPEG压缩实验参数

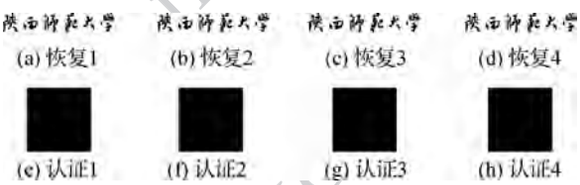
Table 3　Anti-JPEG verification experiment variables

马赛克图像	质量因子	压缩后图像	重构密图	认证图	测试结果		
					$PSNR$/dB	E/%	A/%
图5(b)	50	图8(a)	图9(a)	图9(e)	27.391	0	100
图5(b)	80	图8(b)	图9(b)	图9(f)	32.688	0	100
图5(c)	50	图8(c)	图9(c)	图9(g)	28.247	0	100
图5(c)	80	图8(d)	图9(d)	图9(h)	33.184	0	100

(a) 压缩图1　(b) 压缩图2　(c) 压缩图3　(d) 压缩图4

图8　JPEG压缩攻击后的含密马赛克图像

Fig. 8　Mosaic images with JPEG compressed ((a)—(d) JPEG compressed images 1～4)



(a) 恢复1　(b) 恢复2　(c) 恢复3　(d) 恢复4

(e) 认证1　(f) 认证2　(g) 认证3　(h) 认证4

图9　JPEG压缩实验恢复信息及认证图

Fig. 9　The recovered secrets and their authentication images in anti-JPEG verification experiment ((a)—(d) recovered secret 1～4; (e)—(h) authentication images 1～4)

由表3、图8和图9可看出，尽管经历较大质量因子的JPEG压缩攻击，按算法2提取出的恢复信息与原秘密信息的ER依然为0%，ASR为100%，表明所提方法具备良好的抗JPEG压缩性能并能对恢复的秘密信息进行正确性认证。

3.3.2　抗加噪攻击实验

为验证本文方法抵抗随机噪声的性能，对图5(c)和图5(d)添加不同强度的随机噪声，并利用正确密钥按算法2提取秘密信息。

表4给出了加噪攻击的实验参数，对应的攻击后含密马赛克图像如图10所示，图11是对应的恢复信息和认证图。

从表4、图10和图11的实验结果可看出，尽管遭受到不同比例的噪声攻击，本文方法提取的秘密信息与原信息的ER低于5%，表明本文方法可抵抗噪声攻击；由ASR为100%知，本文方法依然可对恢

表 4　抗加噪攻击实验参数

Table 4　Anti-noise verification experiment variables

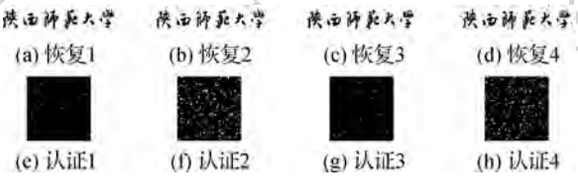
马赛克图像	噪声强度/%	加噪后图像	重构密图	认证图	测试结果		
					PSNR/dB	*E*/%	*A*/%
图 5(c)	8	图 10(a)	图 11(a)	图 11(e)	15.277	0.30	100
图 5(c)	20	图 10(b)	图 11(b)	图 11(f)	11.563	3.57	100
图 5(d)	8	图 10(c)	图 11(c)	图 11(g)	15.384	0.28	100
图 5(d)	20	图 10(d)	图 11(d)	图 11(h)	12.015	3.96	100

(a) 加噪攻击1　(b) 加噪攻击2　(c) 加噪攻击3　(d) 加噪攻击4

图 10　加噪攻击后的含密马赛克图像

Fig. 10　Mosaic images with noise

((a)—(d) noise attacked images 1～4)



(a) 恢复1　(b) 恢复2　(c) 恢复3　(d) 恢复4

(e) 认证1　(f) 认证2　(g) 认证3　(h) 认证4

图 11　加噪攻击实验恢复信息及认证图

Fig. 11　The recovered secrets and their authentication images in anti-noise verification experiment ((a)—(d) recovered secret 1～4; (e)—(h) authentication images 1～4)

复的秘密信息进行高效认证。

3.3.3　抗剪切攻击实验

为验证本文方法抵抗剪切攻击的性能，对图 5(a)和图 5(b)进行不同占比的剪切攻击，并利用正确密钥按算法 2 进行秘密信息提取。表 5 给出了抗剪切攻击的实验数据，与之对应的剪切攻击后的马赛克图像如图 12 所示，对应的恢复信息和认证图如图 13 所示。

由表 5、图 12 和图 13 的实验数据可看出，对含密马赛克图像进行剪切攻击尽管会降低秘密信息的恢复质量，但本文方法的 ER 和剪切占比趋于一致，ASR 始终高于 90%，说明本文方法对剪切攻击具有较高的认证准度。

3.3.4　抗替换攻击实验

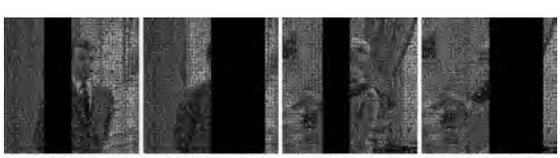
为验证本文方法抵抗替换攻击的性能，将图 5(c)和图5(d)中不同数量的圆形图像替换为其他圆形图像并赋予随机角度。然后由正确密钥按算法 2 提取秘密信息。表 6 给出了替换攻击的实验数据，图 14 是经替换攻击的马赛克图像，与之对应的恢复信息和认证图如图 15 所示。

由表 6、图 14 和图 15 的实验数据可看出，尽管替换攻击会导致秘密信息遭到破坏，但本文方法的 ER 和替换占比趋于一致，ASR 始终高于 90%，说明

表 5　抗剪切攻击实验参数

Table 5　Anti-cut verification experiment variables

马赛克图像	剪切占比/%	剪切后图像	重构密图	认证图	测试结果		
					PSNR/dB	*E*/%	*A*/%
图 5(a)	20	图 12(a)	图 13(a)	图 13(e)	13.595	18.29	90.39
图 5(a)	40	图 12(b)	图 13(b)	图 13(f)	10.448	38.97	90.16
图 5(b)	20	图 12(c)	图 13(c)	图 13(g)	13.249	19.78	91.11
图 5(b)	40	图 12(d)	图 13(d)	图 13(h)	10.444	39.40	90.83



(a) 剪切攻击1　(b) 剪切攻击2　(c) 剪切攻击3　(d) 剪切攻击4

图 12　剪切攻击后含密马赛克图像

Fig. 12　Mosaic images with cropping

((a)—(d) cropping attacked images 1～4)

图 13　剪切攻击实验恢复信息及认证图

Fig. 13　The recovered secrets and their authentication images in anti-cut verification experiment ((a)—(d) recovered secret 1～4; (e)—(h) authentication images 1～4)

所提方法可识别替换攻击,同时具备较高的认证准度。

3.3.5　抗转角攻击实验

为验证本文方法抵抗转角攻击的性能,对图 5(a)和图 5(b)中的部分含密圆形图像施加攻击参数相同的随机转角扰动,然后由正确密钥按算法 2 提取秘密信息。

表 7 给出了转角攻击的实验数据,图 16 是经转角攻击的马赛克图像,对应的恢复信息和认证图如图 17 所示。

由表 7、图 16 和图 17 可以看出,本文方法可以很好地抵抗转角攻击。尽管施加了不同转角占比的攻击,提取秘密信息的 ER 始终为 0,ASR 始终为 100%,说明借助圆形图像所表达的秘密信息可准确提取,并且任何转角攻击所导致的随机转角变化均可被本文的认证策略准确识别,从而具有非常高的认证精度。

表 6　抗替换攻击实验参数

Table 6　Anti-replace verification experiment variables

马赛克图像	替换占比/%	替换后图像	重构密图	认证图	测试结果		
					PSNR/dB	*E*/%	*A*/%
图 5(c)	20	图 14(a)	图 15(a)	图 15(e)	16.178	19.97	90.60
图 5(c)	40	图 14(b)	图 15(b)	图 15(f)	13.149	38.75	90.86
图 5(d)	20	图 14(c)	图 15(c)	图 15(g)	16.088	19.24	92.39
图 5(d)	40	图 14(d)	图 15(d)	图 15(h)	13.197	38.53	92.59

图 14　替换攻击后的含密马赛克图像

Fig. 14　Mosaic images with replace attack ((a)—(d) replacing attacked images 1～4)

图 15　替换攻击实验恢复信息及认证图

Fig. 15　The recovered secrets and their authentication images in anti-replacement verification experiment ((a)—(d) recovered secret 1～4; (e)—(h) authentication images 1～4)

3.4　与传统文献的对比

传统基于搜索的无载体信息隐藏主要通过检索数据库中包含指定秘密矢量的自然无修改载体来传递秘密信息。由于图像和文本等自然载体对与之不相关的秘密信息的表达能力十分有限,导致这类方法单载体嵌密容量极低,涉及大量载体在信道中密集传输,从而容易诱发攻击,导致传输的秘密信息遭受破坏。同时这类方法为找到合适的自然载体,需构建大数据库。随着数据库文本和图像信息表现能力的增强,需搜索的数据量也呈几何级数增加,即使借助倒排索引,搜索、存储和维护也将是一个沉重的负担。

表 8 给出了 Yuan 等人(2017),Zhang 等人(2018),Zheng 等人(2017)和 Zhou 等人(2015,2017)的方法中公开的实验数据,由于 Zhou 等人(2018)的方法利用发送图像的图像小块来重构密图,而图像块的大小未知,同时未给出数据库中具体样本数量,因而表 8 未列出其相关数据。

由表 8 可知,Yuan 等人(2017),Zhang 等人(2018),Zheng 等人(2017)和 Zhou 等人(2015,2017)方法中的单载体嵌密容量较低,而对应数据库则较为庞大,其中Zheng等人(2017)方法中的数

表 7　抗转角攻击实验参数

Table 7　Anti-rotation verification experiment variables

马赛克图像	转角占比/%	转角后图像	重构密图	认证图	测试结果		
					PSNR/dB	*E*/%	*A*/%
图 5(a)	20	图 16(a)	图 17(a)	图 17(e)	26.476	0	100
图 5(a)	40	图 16(b)	图 17(b)	图 17(f)	22.499	0	100
图 5(b)	20	图 16(c)	图 17(c)	图 17(g)	26.446	0	100
图 5(b)	40	图 16(d)	图 17(d)	图 17(h)	23.492	0	100

(a) 转角攻击1　(b) 转角攻击2　(c) 转角攻击3　(d) 转角攻击4

图 16　转角度攻击后的含密马赛克图像

Fig. 16　Mosaic images with rotation attack ((a)—(d) rotation attacked images 1～4)

(a) 恢复1　(b) 恢复2　(c) 恢复3　(d) 恢复4

(e) 认证1　(f) 认证2　(g) 认证3　(h) 认证4

图 17　转角攻击实验恢复信息及认证图

Fig. 17　The recovered secrets and their authentication images in anti-rotation verification experiment ((a)—(d) recovered secret 1～4; (e)—(h) authentication images 1～4)

表 8　搜索无载体信息隐藏实验数据

Table 8　Search-based coverless information hiding data

方法	单载体嵌密容量/B	样本图像数量
Zhou 等人(2015)	1	–
Yuan 等人(2017)	1	–
Zhou 等人(2017)	2.5	2 000 万
Zhang 等人(2018)	*M*/8	–
Zheng 等人(2017)	2.25	2 000

注:“–”代表该数据未公开。

据库样本数量尽管相对较少,但需利用修改式嵌密的方法将参与信息重构的边信息嵌入至额外载体中,违背了无载体信息隐藏的基本原则。与传统基于搜索的无载体信息隐藏方法相比,本文所提方法通过圆形图像的索引来表达秘密信息,以本文实验数据为例,一个圆形图像可隐藏 5 bit 信息,而对应的样本图像集合中只有 32 幅图像,在提升嵌密容量的同时避免了 Yuan 等人(2017),Zhang 等人(2018),Zheng 等人(2017)和 Zhou 等人(2015,2017,2018)方法中存在的高昂数据库创建与检索代价;此外,本文方法通过结合参数映射和误差扩散的马赛克图像生成策略将含密圆形图像放入对应位置并生成一张含密马赛克图像,避免了大量载体的信道密集传输。

传统基于纹理合成的无载体信息隐藏将给定的样例纹理划分为纹理小块,并建立纹理小块与秘密信息之间的映射关系,通过样例纹理合成来生成与之相似的含密纹理。但这类方法只能生成简单质地的非自然纹理图像。

与传统基于纹理合成的无载体信息隐藏方法相比,本文方法则是利用图像马赛克这一特殊、有意义图像作为载体图像,避免了无意义纹理图像的产生。

传统基于马赛克拼图的信息隐藏方法的本质是修改式嵌密方法,难免会在掩体图像中遗留下修改痕迹,且 Hou 等人(2016),Lai 和 Tsai(2011),Lee 和 Tsai(2014),Lin 和 Tsai(2004),刘小凯等人(2018),Zhai 等人(2015)和张梦等人(2016)的方法不具备提取信息的认证能力,从而无法对秘密信息的真实性进行检验。另外这类方法为提高嵌密容量,通常采用的是对攻击较为敏感的基于 LSB 的嵌入策略,从而在遭受攻击时嵌入的信息容易丢失。

与传统基于马赛克拼图的信息隐藏方法相比,本文方法是通过有意义的圆形图像纹理结合用户密钥和放置位置来表达秘密信息,所构造的认证策略是基于圆形图像的放置角度的认证策略,从而在遭受攻击时,所表达的秘密信息和放置角度不容易丢失,可通过质心旋转匹配和基于密钥的随机转角策

略来提取和识别,不仅具备较强的抗攻击鲁棒性,也具备较好的认证精度,同时所提策略完全依赖于用户密钥,具有较高的安全性。

4 结 论

传统基于搜索的无载体信息隐藏方法单载体容量低且涉及大量载体在信道中密集传输;基于纹理合成的无载体信息隐藏方法只能生成简单质地的非自然纹理图像;传统基于马赛克拼图的信息隐藏方法尽管可生成有意义图像,但需借助修改式嵌入的方式嵌入变换参数,难免会遗留下修改痕迹从而无法躲避密写分析者的检验。针对以上问题,本文给出了一种基于块旋转和马赛克拼图的生成式伪装方法,采用参数映射方法将二值秘密信息比特串借助样本图像进行表达。本文方法首先将多个灰度图像转换为具有伪随机转角的圆形图像,利用与密钥和位置有关的参数映射方法将所选圆形图像放置在由密钥生成的二值秘密信息比特位串在掩体图像中的隐藏位置中,并对圆形图像添加与密钥、位置和秘密信息有关的二次随机转角,以便在提取过程中对秘密信息的正确性进行认证。对于非隐藏位置则通过选择与掩体图像中对应位置像素点最接近的圆形图像以形成掩盖,最后通过误差扩散将放置过程中产生的偏差传递掩体周围未处理的像素,从而生成马赛克图像。在提取过程中,可通过质心旋转匹配从马赛克图像中提取秘密信息比特串并通过随机转角认证策略对其进行认证。与马赛克拼图的信息隐藏方法相比,所提策略仅通过随机放置位置的圆形图像来表达秘密信息而不涉及对圆形图像的任意修改式嵌入,且通过质心旋转匹配和随机转角认证不仅具有较好的抗攻击容忍能力和认证精度,还具备较高的安全性。本文方法嵌密和提取过程完全依赖于密钥。与纹理合成的无载体信息隐藏方法相比,本文方法可生成有意义含密掩体图像。与基于搜索的无载体信息隐藏方法相比,本文方法嵌密容量高,避免了载体的信道密集传输。

但本文生成马赛克图像分辨率过大,且由于马赛克拼图只能依据给定的样本图像来逼近掩体图像,其视觉质量如何有效提升还有待进一步研究。

参考文献(References)

Adeli A and Broumandnia A. 2018. Image steganalysis using improved particle swarm optimization based feature selection. Applied Intelligence, 48(6): 1609-1622 [DOI: 10.1007/s10489-017-0989-x]

Coltuc D and Jean-Marc C. 2007. Very fast watermarking by reversible contrast mapping. IEEE Signal Processing Letters, 14(4): 255-258 [DOI: 10.1109/LSP.2006.884895]

Holub V and Fridrich J. 2015. Low-complexity features for JPEG steganalysis using undecimated DCT. IEEE Transactions on Information Forensics and Security, 10(2): 219-228 [DOI: 10.1109/tifs.2014.2364918]

Hou D D, Zhang W M and Yu N H. 2016. Image camouflage by reversible image transformation. Journal of Visual Communication and Image Representation, 40: 225-236 [DOI: 10.1016/j.jvcir.2016.06.018]

Lai I J and Tsai W H. 2011. Secret-fragment-visible mosaic image—a new computer art and its application to information hiding. IEEE Transactions on Information Forensics and Security, 6(3): 936-945 [DOI: 10.1109/TIFS.2011.2135853]

Lee Y L and Tsai W H. 2014. A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations. IEEE Transactions on Circuits and Systems for Video Technology, 24(4): 695-703 [DOI: 10.1109/tcsvt.2013.2283431]

Lin W L and Tsai W H. 2004. Data hiding in image mosaics by visible boundary regions and its copyright protection application against print-and-scan attacks//Proceedings of International Computer Symposium, Taipei, China: Tatung University: 449-454

Liu X K, Yao H and Qin C. 2018. Improved reversible image camouflage method based on image block classification threshold optimization, Journal of Applied Sciences, 36(2): 237-246 (刘小凯, 姚恒, 秦川. 2018. 基于图像块分类阈值优化的改进可逆图像伪装. 应用科学学报, 36(2): 237-246) [DOI: 10.3969/j.issn.0255-8297.2018.02.003]

Qin Z C, Li M and Wu B. 2017. Robust steganography via patch-based texture synthesis//Proceedings of the 9th International Conference on Internet Multimedia Computing and Service. Qingdao, China: Springer, 429-439 [DOI: 10.1007/978-981-10-8530-7_42]

Qian Z X, Zhou H, Zhang W M and Zhang X P. 2016. Robust steganography using texture synthesis//Proceedings of the 12th International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Taiwan, China: Springer: 25-33 [DOI: 10.1007/978-3-319-50209-0_4]

Song X F, Liu F L, Zhang Z G, Yang C F, Luo X Y and Chen L J. 2017. 2D Gabor filters-based steganalysis of content-adaptive JPEG steganography. Multimedia Tools and Applications, 76(24): 26391-26419 [DOI: 10.1007/s11042-016-4157-9]

Wu K C and Wang C M. 2015. Steganography using reversible texture synthesis. IEEE Transactions on Image Processing, 24(1): 130-139 [DOI: 10.1109/TIP.2014.2371246]

Xu J Y, Mao X Y, Jin X G, Jaffer A, Liu S F, Li L and Toyoura M. 2015. Hidden message in a deformation-based texture. The Visual Computer, 31(12): 1653-1669 [DOI: 10.1007/s00371-014-1045-z]

Yuan C S, Xia Z H and Sun X M. 2017. Coverless image steganography based on SIFT and BOF. Journal of Internet Technology, 18(2): 435-442 [DOI: 10.6138/JIT.2017.18.2.20160624c]

Zhai S Y, Li F, Chang C C and Mao Q. 2015. A meaningful scheme for sharing secret images using mosaic images. International Journal of Network Security, 17(5): 643-649 [DOI: 10.6633/IJNS.201509.17(5).16]

Zhang M, Zhai S Y and Su D Q. 2016. Improved algorithm of secret image sharing based on mosaic technique. Application Research of Computers, 33(11): 3480-3484 (张梦, 翟圣云, 苏栋骐. 2016. 基于马赛克技术的秘密图像共享改进算法. 计算机应用研究, 33(11): 3480-3484)

Zhang X, Peng F and Long M. 2018. Robust coverless image steganography based on DCT and LDA topic classification. IEEE Transactions on Multimedia, 20(12): 3223-3238 [DOI: 10.1109/TMM.2018.2838334]

Zheng S L, Wang L, Ling B H and Hu D H. 2017. Coverless information hiding based on robust image hashing//Proceedings of the 13th International Conference on Intelligent Computing Methodologies. Liverpool, United Kingdom: Springer, 536-547 [DOI: 10.1007/978-3-319-63315-2_47]

Zhou Z L, Jonathan W Q M, Yang C N and Sun X M. 2017. Coverless image steganography using histograms of oriented gradients-based hashing algorithm. Journal of Internet Technology, 18(5): 1177-1184 [DOI: 10.6138/JIT.2017.18.5.20160815b]

Zhou Z L, Mu Y and Wu Q M J. 2018. Coverless image steganography using partial-duplicate image retrieval. Soft Computing, 23(13): 4927-4938 [DOI: 10.1007/s00500-018-3151-8]

Zhou Z L, Sun H Y, Harit R, Chen X Y and Sun X M. 2015. Coverless image steganography without embedding //Proceedings of the 1st International Conference on Cloud Computing and Security. Nanjing, China: Springer, 123-132. [DOI: 10.1007/978-3-319-27051-7_11]

作者简介

王洋，1992 年生，女，硕士，主要研究方向为马赛克拼图无载体信息隐藏。
E-mail: 2465250489@qq.com

邵利平，通信作者，男，副教授，主要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。
E-mail: slpmaster@163.com

陆海，男，硕士，主要研究方向为无载体信息隐藏。
E-mail: m15063732825@163.com