软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2017,28(12):3306−3346 [doi: 10.13328/j.cnki.jos.005234]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

非等量备份和双认证自修复有限域图像分存*

欧阳显斌[1,2], 邵利平[1,2], 乐志芳[1,2]

[1](现代教学技术教育部重点实验室(陕西师范大学),陕西 西安 710062)

[2](陕西师范大学 计算机科学学院,陕西 西安 710119)

通讯作者: 邵利平, E-mail: slpmaster@163.com

摘 要: 传统有意义图像分存方案存在认证能力偏低、攻击后不具备修复能力或修复能力整体较弱以及嵌入掩体视觉质量不高等问题.针对以上问题,提出一种结合非等量备份和双认证自修复有限域图像分存方案,包含分存和恢复阶段.在分存阶段,首先对密图做 1 级离散小波变换,取 LL 子带按密钥置乱,并对置乱后 LL 子带每个系数比特按比特位重要程度分组进行非等量备份来构造与密图等大备份图;然后对密图和备份图每个像素及其对应 7*K*-13 位认证信息在 GF(2^7)有限域进行(*K*,*N*)分存,将产生的 7 位分存信息和使用密钥产生的 1 位认证信息使用优化 LSB 法嵌入到 *N* 个掩体 2×2 分块中;最后对密钥进行(*K*,*N*)分存,将子密钥对应的 MD5 值公开到第 3 方公信方并将子密钥和嵌入掩体分发给参与者.在恢复阶段,首先对参与者提供的子密钥真实性进行检验,利用检验通过子密钥对密钥进行恢复;其次对分发掩体 2×2 分块嵌入的分存信息和 1 位认证信息使用密钥进行第 1 重认证,利用第 1 重认证通过分存信息重建 GF(2^7)有限域分存多项式,提取出密图和备份图每个像素及其对应的 7*K*-13 位认证信息并对其进行第 2 重检验和构造初步密图、备份图以及认证图;再次由备份图和认证图重构密图 LL 子带,然后对其做逆置乱和逆离散小波变换得到密图修复参考图;最后对认证图每一个认证不通过秘密像素,根据其周围像素认证情况选择多项式插值拟合或进行修复参考图像素替代修复.理论和实验结果表明,与现有方法相比,所提方法具备更好的认证能力,并能充分使用双认证和自然图像邻近像素相关性来提升其攻击后修复能力,且分发掩体具备较高视觉质量.

关键词: 图像分存;有意义图像;(*K*,*N*)门限方案;有限域;备份图;非等量备份;比特位分组;双认证;自修复;多项式插值拟合

中图法分类号: TP309

中文引用格式: 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.软件学报,2017,28(12):3306−3346. http://www.jos.org.cn/1000-9825/5234.htm

英文引用格式: Ou-Yang XB, Shao LP, Le ZF. Gloise field self-recovery image sharing scheme with non-equivalent backup and double authentications. Ruan Jian Xue Bao/Journal of Software, 2017,28(12):3306−3346 (in Chinese). http://www.jos.org.cn/1000-9825/5234.htm

Gloise Field Self-Recovery Image Sharing Scheme with Non-Equivalent Backup and Double Authentications

OU-YANG Xian-Bin[1,2], SHAO Li-Ping[1,2], LE Zhi-Fang[1,2]

[1](Key Laboratory of Modern Teaching Technology of Ministry of Education (Shaanxi Normal University), Xi'an 710062, China)

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

* 基金项目: 国家自然科学基金(61100239); 陕西省科技新星计划(2011kjxx17); 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)

Foundation item: National Natural Science Foundation of China (6110239); Science and Technology New Star Project of Shaanxi Province (2011kjxx17); Natural Science Foundation of Shaanxi Province (2011JQ8009, 2016JM6065); Fundamental Research Fund for the Central Universities of China (GK201402036, GK201703057)

收稿时间: 2016-04-11; 修改时间: 2016-09-20; 采用时间: 2016-12-10; jos 在线出版时间: 2017-03-24

CNKI 网络优先出版: 2017-03-24 16:29:44, http://kns.cnki.net/kcms/detail/11.2560.TP.20170324.1629.007.html

Abstract: In conventional meaningful image sharing schemes, there exist some shortages such as low authentication ability, weak to no repair or recovery ability after being attacked, and low visual quality in embedded carriers. To address these problems, this paper proposes a Gloise field self-recovery image sharing scheme with non-equivalent backup and double authentication. The proposed scheme includes both distributing and recovery stages. The distributing stage include three steps. First, the LL subband of the secret image is obtained by one layer DWT and then the LL subband coefficients is scrambled by a secret key to generate the non-equivalent backup image according to different bit important degree groups where both the backup image and the secret image are in same size. Second, each pixel in both the secret image and the backup image are shared with their 7*K*-13 authentication bits into 7 bits distributed information on GF(2^7), and then the distributed 7 bits information with its 1 bit authentication generated by the secret key is embedded into 2×2 blocks of *N* distributed carriers by the optimized LSB embedding method. Finally, the secret key used to scramble LL subband and generate 1 bit authentication is also shared into *N* sub-keys by (*K*,*N*)-threshold scheme, and then the sub-keys' MD5 values are published into the third reliable party and the *N* sub-keys and embedded carriers are distributed to *N* participants. The recovery stage has four steps. First, the facticity of participants' sub-keys is verified, and then the sub-keys are used to recovery the secret key. Second, the embedded distributed information with its 1 bit authentication is checked by the first authentication, the checked distributed information is used to reconstruct GF(2^7) interpolation polynomial, and then the pixels in the secret image and the backup image with their 7*K*-13 authentication bits are recovered to construct the preliminary secret image, backup image and authentication image. Third, the backup image and authentication image are used to reconstruct the LL subband of the secret image and then to build the repair reference image by the descramble method and inverse DWT. Finally, the unpassed secret image pixels in the authentication image are self-recovered by the polynomial interpolation fitting and pixel replacement in repair reference image. The theory and experiment show the proposed method has a superb authentication ability and can make full use of double authentication ability and the adjoin pixels to improve its self-recovery ability, and the embedded carriers have better visual qualities.

Key words: image sharing; meaningful image; (*K*,*N*)-threshold scheme; Gloise field; backup image; non-equivalent backup; bit grouping; double authentications; self-recovery; polynomial interpolation fitting

现有图像分存主要源自密码学秘密共享.最简单秘密共享是(*K*,*N*)门限秘密共享,最早由 Shamir 和 Blakley 分别结合 Lagrange 插值公式和矢量空间点性质提出[1,2].在(*K*,*N*)门限秘密共享方案中,任何包含至少 *K* 个参与者的集合都是许可集,反之则是禁止集.其基本思想是:将秘密信息分成 *N* 个子秘密,并且当收集到任意 *t*(*t*≥*K*)个子秘密,则可计算出原秘密;反之则无法恢复.这里的*K*就是门限共享方案门限.当前已提出的秘密共享算法除了 Shamir 和 Blakley 方案外,还有基于中国剩余定理的 Asmuth-Bloom 共享算法[3]和使用矩阵乘法的 Karnin-Greene-Hellman 共享算法[4]等.

将密图借助秘密共享算法拆分为影子图像,通过分发影子图像对密图重构,即为图像信息分存.文献[5–9]分别将 Shamir 门限方案、中国剩余定理和 Blakley 方案用于(*K*,*N*)图像分存,文献[10,11]还给出了基于元胞自动机的图像分存方法.

但文献[5–9]仅具备基本图像分存功能,为提高图像分存适用面,文献[12–17]给出了渐进图像分存,随着参与者数量增加,恢复密图视觉质量也逐渐提高;为减少信道传输负载,文献[18–20]给出了更小影子图像分存方法;为分存多密图,文献[21]给出基于 Lagrange 插值多项式和中国剩余定理的多密图分存方案;为使部分分发影子图像更为重要,文献[22]给出了基于关键影子图像分存;结合可逆嵌入,文献[23–25]给出了可逆图像分存,在密图恢复的同时,可高质量或无损地恢复掩体;结合双变量单向函数和可撤销门限,文献[26]实现了门限可改变图像分存.除了渐进分存、小影子分存、多密图分存、关键影子分存、可逆分存和门限可改变分存以外,带认证能力的有意义图像分存也成为分存研究重点.

文献[27]将密图像素 8 位分存信息和 1 位奇偶校验位嵌入到掩体 2×2 分块左下、右下和右上像素中,并调整 2×2 分块左上像素作为 Lagrange 插值公式输入.但由于 Lagrange 插值多项式模数是 251,不可避免地带来密图失真,且认证位只有 1 位奇偶校验位,起不到丝毫认证作用.对于 2×2 分块,需至少修改 9 个比特位,带来掩体失真.为减少模数 251 对密图溢出像素影响,文献[28]将密图像素 LSB 位循环右移至 MSB 位,通过对溢出像素 MSB 位置 0 使得处理后密图像素最多仅损失 1 个低位 LSB 位,相对于传统直接将大于等于 251 像素截断处理,减少密图失真.针对文献[27]存在密图有损和掩体失真等问题,文献[29]用 GF(2^8)替代 GF(251)、采用 1 位 HMAC 消息认证位替代奇偶校验位并调整 2×2 分存信息嵌入结构来提升认证能力和提高嵌入掩体视觉质量.然而对每

个分块,文献[29]只有 1 个嵌入认证位,每个分块篡改通过认证概率高达 1/2,存在较大安全隐患.为解决文献[27,29]的弱认证问题,文献[30]通过中国剩余定理生成 4 个认证位,并基于文献[5]的(*K*,*N*)分存策略,获得较好的认证能力和掩体视觉质量.但它依然采用传统 LSB 法,直接将 8 位分存信息和 4 位认证位嵌入到掩体 2×2 分块像素低 3 位.文献[30]使用多项式将多个系数进行分存,相对于文献[27,29],有更好的嵌入视觉质量,但掩体视觉质量依然偏低.为提高掩体的视觉质量,文献[31]对文献[30]的 LSB 嵌入法进行改进,通过调整像素第 4 个低位来减小嵌入信息后像素与原像素的差值,以获得更高的视觉嵌入质量.为进一步提升嵌入后掩体视觉质量,文献[10]仅对掩体所有 2×2 分块 1/2 分块的低 2 位按 LSB 法嵌入分存信息,并通过对秘密像素认证来取代对密图分存信息[27,29−31]认证以提高认证准度,将每 2 个秘密像素和对应的 8 位认证信息作为初始 3 时刻 8 元胞,按可逆元胞自动机进行分存,然后将 8 位分存信息嵌入到掩体 2×2 分块低 2 位比特中.文献[10]相比文献[27,29–31]嵌入分存信息后,掩体具有很高的视觉质量,但对于每个分存单元,需至少 K 个编号连续参与者才能恢复密图,并不是真正意义的(*K*,*N*)分存.为减少认证位嵌入并进一步提高掩体视觉质量,文献[32]采用认证锁链,即,用 2 位认证位来认证前一个像素分存信息和当前像素分存信息,使得每个像素分存信息可被 4 位认证信息认证,而每个分块却仅嵌入 2 位认证信息和当前像素分存信息.文献[33]给出了双变量对称多项式分存,通过对称多项式来实现认证且不嵌入任何认证信息到掩体,以提高掩体视觉质量.以上文献[27,29–31]都存在像素扩张且都将分存信息嵌入到掩体 2×2 分块中.

针对有意义图像分存[27,29−31]存在像素扩张的现象,文献[34]使用调整差值变换将密图转变为位置图和差值图分存,所提方案具备较好视觉质量且不存在任何像素扩张,并通过分块增强策略来弥补使用严格认证存在的不足.所提策略尽管不存在像素扩张,但不能识别像素攻击位置,更无法对攻击像素进行修复.文献[35]对密图像素进行 GF(2^3)有限域分存,且对秘密像素进行直接认证,不仅避免了像素扩张,而且提高了对秘密像素的认证准度.但 GF(2^3)分存多项式提供的存储空间十分有限,导致秘密像素认证能力整体偏低.

文献[10,27,29–35]都是带认证有意义图像分存并有较大概率检测攻击,但不能充分使用其认证能力对认证失败像素进行修复,其中,文献[10]用 8 位认证位认证 2 个秘密像素,文献[33,34]分别用多项式对称性和 MD5 来检验掩体是否遭受攻击.为提高修复能力,文献[36,37]使用 Lagrange 多项式的多个系数来分存密图像素和配对像素,并分别将分存信息和 4 位或 3 位认证信息通过调整模数的方法嵌入到掩体 2×2 分块中.文献[36,37]通过像素配对使得方案具备一定攻击后修复能力,但所提方案认证位较少,秘密像素分存信息最多存储两份,且用最小覆盖矩形来确定攻击区域,导致所提策略恢复能力偏低.为获得更强攻击后修复能力,文献[11]对密图做 1 级离散小波变换,取其 LL 子带备份 2 份,从而构造出与原密图等大且每个像素只有 4 位的备份图,若原秘密像素遭受攻击,则可通过恢复出备份图对应位置像素进行修复,从而获得了相对于文献[36,37]更好的修复能力.但文献[11]是将 2 个 8 位秘密像素和 2 个 4 位备份图像素总计 24 位作为初始 3 时刻 8 元胞来构造可逆元胞自动机进行分存,将分存信息和对应的 8 位认证信息用 LSB 法嵌入到掩体 2×4 分块的低 2 位中,这样导致的问题是:① 它不是真正意义的(3,*N*)门限方案,需至少 3 个编号连续的分存单元才能恢复出 2 个秘密像素和 2 个备份图像素;② 2×4 分块中任意一个像素被攻击,即导致 2 个秘密像素及其 2 个备份图像素总共 24 位信息不可用,从而无法抵制任意微小噪声攻击;③ 对 LL 子带,每个像素低位比特和高位比特采用等量备份策略,即,每个像素比特备份两次,但像素高位比特重要性显然高于低位比特,从而影响该方案在大面积攻击下的修复能力;④ 该方案依然使用传统 LSB 法嵌入分存信息和认证信息,从而导致嵌入分存信息的掩体视觉质量依然偏低.

文献[27,28,30–32,34,36,37]用模为素数的 Lagrange 插值多项式来分存秘密信息,而计算机中,数据以 2 进制进行存储,用素数分存不可避免地造成像素截断[27,28,30−32]或多项式模数空间浪费[34,36,37].而文献[29,33]用 GF(2^8)有限域的 Lagrange 插值多项式分存,可有效避免该问题,但其分存信息仅为 2^8 范围内的整数,使掩体无法嵌入过多分存认证信息.文献[29]仅嵌入 1 位认证信息位,而文献[33]没有嵌入任何认证位,导致所提策略认证能力偏低.而使用较小有限域空间只能分存较小的秘密信息,文献[35]采用 GF(2^3)对密图进行分存,虽可有效减少像素扩张和提高掩体视觉质量,但其分存多项式只能存储较少信息,因而本文采用基于 GF(2^7)有限域 Lagrange 多项式进行分存.

文献[11,27,29–33,36,37]都是对分存信息进行认证,这种认证方式可有效地发现掩体是否被攻击及其被攻击的大致轮廓,但每个掩体都要嵌入认证信息.若认证位较多,则会导致嵌入分存信息后掩体视觉质量偏低.为保证嵌入掩体视觉质量,文献[27,29–33]都采用较少的认证位进行认证,这样会导致较高误判概率;若参与者了解认证信息生成和嵌入规则,则有较高的概率伪造能通过认证的分存信息,同时,文献[27,29–33]仅对分存信息进行认证,也无法对重构出的秘密像素的真实性进行检验.而文献[10,30,33]仅对秘密像素进行认证并将认证信息和秘密信息分存嵌入至掩体中,而不对分存信息进行认证,这种认证方式可用少量认证位实现对秘密信息较可靠的认证,因为每个恶意参与者篡改分存信息都无法预知重构结果.该方法虽有较高的概率识别被篡改的秘密信息,但无法识别恶意篡改掩体.因此,本文将两种认证方式结合起来进行双认证,使得对秘密信息拥有较强认证能力的同时,也能粗略地识别出遭到攻击掩体以及攻击的大致轮廓.

针对文献[10,27,29–35]不具备攻击后修复能力和文献[11,36,37]修复能力偏低且嵌入掩体视觉质量下降等问题,本文结合非等量备份和双认证,提出一种基于 GF(2^7)有限域的有意义自恢复(K,N)图像分存方案.

在分存阶段,与文献[11]直接将LL 子带所有系数比特进行等量备份生成备份图策略不同,所提策略是将LL子带上所有系数比特,按比特位由高至低的重要程度分组来构造不同数量备份,对高位比特分组进行多备份,对低位比特分组进行少备份,以形成与密图等大且每个像素为 5 比特的备份图,从而相对于文献[11]备份策略更为合理,所创建备份图也更耐受攻击.所提策略可对同一位置 1 个秘密像素和 1 个备份像素生成 7K-13 位认证比特,然后将秘密像素、备份像素和对应认证比特使用 GF(2^7)有限域的 Lagrange 插值多项式进行(K,N)分存,产生 7 位分存信息,避免了传统 Lagrange(K,N)分存方案[27,28,30–32,34,36,37]由于模为素数所造成的比特位嵌入空间浪费.由 7 位分存信息计算 1 位认证信息,并使用优化 LSB 法嵌入到掩体 2×2 分块的低 2 位比特中,从而相对于文献[11,36,37]的嵌入掩体具有更高视觉质量.在上述分存阶段,包含对分存信息的第 1 重认证和对秘密像素的第 2 重认证,其中,第 1 重认证用 1 比特认证信息来验证掩体是否遭到攻击以及识别被攻击大致轮廓,第 2 重认证用 7K-13 位认证信息来验证秘密像素是否被准确恢复.

在恢复阶段,首先,通过第 1 重认证对参与恢复的分存信息是否被攻击进行检验,若存在不少于 K 个分存信息认证通过,则进行第 2 重认证,即:对这些通过第 1 重认证的分存信息用 GF(2^7)有限域 Lagrange 插值多项式恢复出秘密像素、备份像素和与之对应的秘密像素认证信息,从而得到认证图、备份图和初步密图.通过双认证,被攻击像素在理论上最多有$(1/2)^{7K-12}$的综合概率通过认证,相比于文献[11,36,37]的 1/256,1/16 和 1/8 的篡改通过概率具备更高的认证精度;其次,根据备份图和认证图重建出密图 LL 子带,并通过逆离散小波变换、逆置乱变换生成修复参考图;最后,对初步恢复的密图未通过认证像素进行自恢复操作,若其 8 邻域有 4 个以上像素通过认证,则对认证通过像素来进行多项式拟合,重建出秘密像素;否则,用修复参考图对应位置像素作为秘密像素修复值.

与文献[11,27,29–37]相比,所提策略具备较高的嵌入掩体视觉质量;而与此同时,又能充分使用双认证结果对密图认证失败的像素进行准确定位,并能充分利用其相关性对密图进行有效的自恢复,因而相对文献[11,36,37]具有更强的攻击后修复能力和较高的实际应用价值.

本文第 1 节为准备工作:对 Lagrange 分存模型和基于 GF(2^7)的有限域分存模型进行介绍,为简化描述 GF(2^7)有限域的性质,本文引入 GF(2^7)有限域的多项式整数,使得 GF(2^7)有限域的多项式与一个[0,127]范围内的整数直接对应.第 2 节对传统的有意义图像分存方案进行简介和剖析,包括基于像素配对和元胞自动机的有意义图像分存.第 3 节给出非等量备份和双认证自修复有限域图像的分存方案,包括基于像素比特位分组的非等量备份图生成策略、基于 GF(2^7)有限域的密图与备份图的分存认证策略、结合优化 LSB 法的分存信息认证和嵌入策略以及完整的分存方法.第 4 节在第 3 节的基础上进一步给出恢复方案,包括双认证、基于非等量备份的修复参考图构建策略、对密图的自修复策略以及完整恢复算法.第 5 节对所提策略进行实验验证,并与相关文献进行实验比较.第 6 节对全文总结,并给出进一步工作.

1 准备工作

1.1 Lagrange分存模型

目前,绝大多数(*K*,*N*)有意义图像分存都是建立在 Shamir-(*K*,*N*)门限方案[1]的基础上,其思想是构建形如公式(1)的多项式:

$$f(k)=(s+r_1k+r_2k^2+\ldots+r_{K-1}k^{K-1}) \bmod p \tag{1}$$

其中,s 是常数项,通常为秘密值嵌入位置;$r_1,r_2,\ldots,r_{K-1}$ 是高次项系数,通常为随机整数;p 为素数,且满足 $s,r_1,r_2,\ldots,r_{K-1}\in\{0,1,\ldots,p-1\}$.

记 N 为[K,p)范围内整数,将 k=1,2,…,N 依次代入 $f(k)$,从而形成 N 个分发信息$(1,f(1)),(2,f(2)),\ldots,(N,f(N))$.若从中任取 $t(t\geqslant K)$个分发信息$(num_i,f(num_i)),num_i\in\{1,2,\ldots,N\},i=1,2,\ldots,t$,则可按公式(2)的 Lagrange 插值公式对 $f(k)$进行恢复,从而按 $s=f(0)$恢复出秘密值.

$$f(k)=\left(\sum_{i=1}^{t}\left(f(num_i)\prod_{j=1,j\neq i}^{t}(k-num_j)(num_i-num_j)_p^{-1}\right)\right)\bmod p \tag{2}$$

其中,$(num_i-num_j)_p^{-1}$ 为(num_i-num_j)的模 p 的乘法逆元.

经典 Lagrange 分存模型通常只利用常数项 s 作为秘密值嵌入位置,仅能嵌入 1 个[0,p)范围内的整数,所提供的嵌入容量十分有限.文献[5,30]进一步将Lagrange分存模型的多个系数用于分存,即 $r_1,r_2,\ldots,r_{K-1}$ 都可用于嵌入信息,则公式(1)可用于 K 个[0,p)范围内的整数嵌入.然而 Shamir-(*K*,*N*)门限方案[1]模数 p 为素数,在计算机中,数据通常使用二进制存储,因此需对秘密信息进行截断处理[27,30−32]或采用 LSB 位置 0[28]或选择大于秘密值上界的模数来进行分存[34,36,37],由此不可避免地导致嵌入秘密信息损失一定精度或对模数空间造成较大的浪费[27,28,30−32,34,36,37],从而降低嵌入掩体的视觉质量.

1.2 GF(2^7)有限域多项式整数和Lagrange分存模型

为避免素数域Lagrange分存模型存在精度损失,文献[29,33]将Shamir-(*K*,*N*)分存拓展到GF(2^8)有限域,可在一定程度上缓解上述问题.但所提方法并未充分利用 Lagrange 多项式的多个系数进行分存,导致掩体嵌入的分存信息过多,从而嵌入掩体的视觉质量偏低.文献[35]在 GF(2^3)有限域分存,分存多项式存储空间较小,导致秘密像素认证位较少,因而认证能力偏低.为获得较好的视觉质量和充分使用模数空间,本文将 Shamir-(*K*,*N*)门限方案约束在 GF(2^7)有限域,并充分使用多项式的多个系数来进行分存.为简化 GF(2^7)有限域的性质描述,本文引入GF(2^7)有限域多项式整数,使得 GF(2^7)有限域的多项式与一个[0,127]范围内的整数直接对应.以下首先给出GF(2^7)有限域多项式整数的定义,在此基础上,对 GF(2^7)有限域多项式整数的运算性质以及逆元进行约定.

定义 1(GF(2^7)有限域多项式整数). 任何处于[0,2^7)的整数 x,都可将其转换为二进制数 $x=(a_6a_5a_4a_3a_2a_1a_0)_2$,从而对应为 $\dot{x}=a_0t^0+a_1t^1+\ldots+a_6t^6$,这里,称 $\dot{x}$ 为 GF(2^7)有限域多项式整数,简称多项式整数.

例如:$105\in[0,2^7)$且 $105=(1101001)_2$,故 $\dot{105}=t^0+t^3+t^5+t^6$.类似地,$3\in[0,2^7)$且 $3=(11)_2$,故 $\dot{3}=t^0+t^1$.

定义 2(多项式整数加法运算). 记多项式整数 $\dot{a}=a_0t^0+a_1t^1+\ldots+a_6t^6$ 和 $\dot{b}=b_0t^0+b_1t^1+\ldots+b_6t^6$,则多项式整数加法 $\dot{a}+\dot{b}$ 定义为 $\dot{a}+\dot{b}=((a_0+b_0)t^0+(a_1+b_1)t^1+\ldots+(a_6+b_6)t^6)(\bmod 2)$,即:

$$\dot{a}+\dot{b}=(a_0\oplus b_0)t^0+(a_1\oplus b_1)t^1+\ldots+(a_6\oplus b_6)t^6,$$

其中,⊕为异或操作,即模 2 加运算.

由定义 2 知,多项式整数加法运算具有封闭性.即,多项式整数加法运算结果依然是多项式整数.

例如:若 $\dot{a}=t^0+t^1+t^6$ 和 $\dot{b}=t^0+t^5$,有 $\dot{a}+\dot{b}=(2t^0+t^1+t^5+t^6)\bmod 2=t^1+t^5+t^6$,则 $t^1+t^5+t^6$ 是多项式整数.

定义 3(多项式整数减法运算). 记多项式整数 $\dot{a}=a_0t^0+a_1t^1+\ldots+a_6t^6$ 和 $\dot{b}=b_0t^0+b_1t^1+\ldots+b_6t^6$,则多项式整数 $\dot{a}-\dot{b}$ 减法定义为 $\dot{a}-\dot{b}=((2+a_0-b_0)t^0+(2+a_1-b_1)t^1+\ldots+(2+a_6-b_6)t^6)(\bmod 2)$.

由定义 2 可知,多项式整数减法运算具有封闭性.即,多项式整数减法运算结果依然是多项式整数.

例如:若 $\dot{a}=t^0+t^1+t^6$ 和 $\dot{b}=t^0+t^5$,由 $\dot{a}-\dot{b}=((2+1-1)t^0+(2+1)t^1+(2-1)t^5+(2+1)t^6)\bmod 2=t^1+t^5+t^6$,则 $t^1+t^5+t^6$ 依然是多项式整数.

定理 1. 多项式整数加法运算等价为多项式整数减法运算,即 $\dot{a}+\dot{b}=\dot{a}-\dot{b}$.

证明:记 $\dot{a}=a_0t^0+a_1t^1+...+a_6t^6$ 和 $\dot{b}=b_0t^0+b_1t^1+...+b_6t^6$,则有:

$$\begin{aligned}\dot{a}-\dot{b}&=((2+a_0-b_0)t^0+(2+a_1-b_1)t^1+...+(2+a_6-b_6)t^6)(\bmod 2)\\&=((a_0+2-b_0)t^0+(a_1+2-b_1)t^1+...+(a_6+2-b_6)t^6)(\bmod 2)\\&=((a_0+b_0)t^0+(a_1+b_1)t^1+...+(a_6+b_6)t^6)(\bmod 2).\end{aligned}$$

而由 $\dot{a}+\dot{b}=((a_0+b_0)t^0+(a_1+b_1)t^1+...+(a_6+b_6)t^6)(\bmod 2)$,故 $\dot{a}-\dot{b}=\dot{a}+\dot{b}$. □

定义 4(多项式整数乘法运算). 记多项式整数 $\dot{a}=a_0t^0+a_1t^1+...+a_6t^6$ 和 $\dot{b}=b_0t^0+b_1t^1+...+b_6t^6$, 则多项式整数乘法 $(\dot{a}\dot{b})_{\dot{p}}$ 定义为 $(\dot{a}\dot{b})_{\dot{p}}=((a_0t^0+a_1t^1+...+a_6t^6)(b_0t^0+b_1t^1+...+b_6t^6))(\bmod \dot{p})$, 其中,多项式整数 $\dot{p}$ 为 GF(2^7)有限域本原多项式.由于 GF(2^7)有限域本原多项式不唯一,在本文中,约定 $\dot{p}=t^0+t^3+t^7$, 将 $(\dot{a}\dot{b})_{\dot{p}}$ 简记为 $\dot{a}\dot{b}$.

例如:若 $\dot{a}=t^0+t^1+t^6$ 和 $\dot{b}=t^2$,则有 $\dot{a}\dot{b}=(t^2+t^3+t^8)(\bmod \dot{p})$.

由 $t^7(\bmod \dot{p})=t^0+t^3$, 故:

$$\dot{a}\dot{b}=(t^2+t^3)(\bmod \dot{p})+t(t^7 \bmod \dot{p})=(t^2+t^3+t^1+t^4)(\bmod \dot{p})=(t^1+t^2+t^3+t^4)(\bmod \dot{p}).$$

定义 5(多项式整数幂次运算). 多项式整数幂次运算 $\dot{a}^k$ 定义为 $\dot{a}^k=\overbrace{\dot{a}\dot{a}...\dot{a}}^{k}$.

定义 6(多项式整数逆元). 对于任意 GF(2^7)有限域非零多项式整数 $\dot{a}$ 的逆元记为 $\dot{a}_{\dot{p}}^{-1}$,且满足 $\dot{a}_{\dot{p}}^{-1}\dot{a}=1$.

例如: $\dot{a}=t^2+t^6$, 则 $\dot{a}_{\dot{p}}^{-1}=t$, 因为 $\dot{a}_{\dot{p}}^{-1}\dot{a}=(t^3+t^7)(\bmod \dot{p})=1$.

结合以上定义和约定,可给出 GF(2^7)有限域 Lagrange 分存模型,即公式(3):

$$f_{GF}(\dot{k})=(\dot{s}+\dot{r}_1\dot{k}+\dot{r}_2\dot{k}^2+...+\dot{r}_{K-1}\dot{k}^{K-1})\bmod \dot{p} \tag{3}$$

其中, $\dot{s},\dot{r}_1,\dot{r}_2,...,\dot{r}_{K-1}$ 为 GF(2^7)有限域多项式整数,记 N 为[K,2^7)范围内的整数,将 k=1,2,…,N 依次代入 $f_{GF}(\dot{k})$,从而形成 N 个分发信息 $(1,f_{GF}(\dot{1})),(2,f_{GF}(\dot{2})),...,(N,f_{GF}(\dot{N}))$,而对于每个 $f_{GF}(\dot{k}),k=1,2,...,N$,可通过[0,$2^7$)范围内整数进行存储.若从中任取 $t(t\geqslant K)$个分发信息 $(\dot{num}_i,f_{GF}(\dot{num}_i)),num_i\in\{1,2,...,N\},i=1,2,...,t$,则可按 GF($2^7$)有限域 Lagrange 插值公式,即公式(4)对 $f_{GF}(\dot{k})$ 进行恢复,然后将 $f_{GF}(\dot{k})$ 系数转换为对应整数即可提取出秘密信息.

$$f_{GF}(\dot{k})=\left(\sum_{i=1}^{t}(f_{GF}(\dot{num}_i)\prod_{j=1,j\neq i}^{t}(\dot{k}-\dot{num}_j)(\dot{num}_i-\dot{num}_j)_{\dot{p}}^{-1})\right)\bmod \dot{p} \tag{4}$$

同样,对于 GF(2^7)有限域 Lagrange-(K,N)分存模型公式(3),其实际提供嵌入容量最大为 K 个[0,2^7)范围内整数,即能存储 7K 个 2 进制比特.

2 传统有意义图像分存方案

2.1 基于像素配对的有意义图像分存

文献[36,37]给出了基于像素配对的有意义图像分存,引入像素配对来增加攻击后的修复能力.其中,文献[36]用密钥生成序列〈0,1,…,mn−1〉上的排列〈q_0,q_1,…,q_{mn-1}〉,对于 $i\in\{0,1,...,mn-1\}$,有索引配对(i,q_i)和与之对应的像素配对(P_x,P_y)且x=i,y=q_i.将(P_x,P_y)表示为二进制序列〈$P_x^0,P_x^1,...,P_x^7,P_y^0,P_y^1,...,P_y^7$〉.由于任意像素通常存在于2个不同配对中,若其中一个遭受破坏,则可用另一个恢复,从而具备一定攻击后修复能力.

令 $a=P_y^7P_x^7P_x^6P_x^5,b=P_y^6P_x^4P_x^3P_x^2,c=P_y^5P_y^4P_x^1P_x^0$,对 a,b,c 使用公式(5)分存:

$$f_1(k)=(a+bk+ck^2) \bmod 17 \tag{5}$$

公式(5)仅分存了像素配对中 P_y 高 4 位和 P_x.记第 k 个掩体分存值 $f_1(k)\in\{0,1,...,16\}<2^5$,它可用 5 位二进制位表示,将这 5 位二进制位串和 i 作为参数用 Hash 函数映射成 4 位认证码 a_x,然后用公式(6)计算 D_x.

$$D_x = 17\times 2\times f_1(k) + 2\times a_x + P_y^3 \tag{6}$$

公式(6)中,D_x包括第 k 个掩体分存值 $f_1(k)$,对应认证码 a_x 以及像素配对中 P_y 第 5 位 P_y^3,其中,$D_x\in\{0,1,\ldots,575\}<5^4$ 可用 4 位五进制串表示.基于此,文献[36]通过调整 1 个掩体 2×2 分块每个像素值,使其分别嵌入 1 个 5 进制数,从而将密图分存值存储到掩体中.公式(6)还原时,可先提取出 D_x,然后通过 D_x 模 2、除以 2 后模 17 以及除以 34,依次求得 P_y^3,a_x 和 $f_1(k)$.将 $f_1(k)$再次用 Hash 函数可映射出 4 位认证码与 a_x 比较:若相等,则标记该像素通过认证;否则,标记该像素未通过认证.由于文献[36]分存信息只有 4 位认证信息,因而攻击后逃过认证的概率高达 1/16.在处理完所有像素后,对认证图用最小矩形来修正认证结果,即:找到包含所有认证未通过像素最小覆盖矩形,并置该矩形所有像素不通过认证.若认证通过分存值$f_1(k)$不小于 K,则可按公式(2)恢复出 a,b,c,得到密图在(i,q_i)配对位置上 P_y 高 5 位以及 P_x,然后标记对应位置密图通过认证;否则,标记不通过认证.对密图认证不通过像素采用配对像素修复.文献[36]使用最小矩形修正认证结果不合理,对于分布较为均匀的随机噪声攻击,该方案将认定整张图像遭受攻击.

为提高文献[36]的修复效率,文献[37]对文献[36]的策略进行了改进,将(i,q_i)位置像素配对分别用 3 位 7 进制数表示为$(a_1b_1c_1)_7$和$(a_2b_2c_2)_7$,然后将公式(5)转换为公式(7)分存:

$$f_2^r(k) = (a_r + b_r k + c_r k^2) \bmod 7; r = 1,2 \tag{7}$$

对于每个分发掩体 k,可由公式(7)得到分存值 $f_2^1(k)$ 和 $f_2^2(k)$,再由这两个值以及 k 和当前块编号作为参数,使用 HMAC 产生 3 位验证码 a_x,然后用公式(8)取代公式(6),生成 D_x.

$$D_x = 8\times 7\times a_x + 7\times f_2^1(k) + f_2^2(k) \tag{8}$$

公式(8)中,$D_x\in\{0,1,\ldots,440\}<5^4$,同样可用 4 位五进制数来表示,从而通过调整掩体 2×2 像素块每个像素模 5 值嵌入 1 个五进制数.文献[36,37]尽管具备一定的修复能力,但整体修复能力偏低,且由于模数 17 和模数 7 的限制,使得 K 不小于 3,而 N 的可选范围仅能为[K,16]和[K,6]范围内的整数,这将严重影响该方案适用性;另外,每个像素使用模 5 来嵌入分存信息,使得该方案嵌入掩体视觉质量整体偏低.

2.2 基于可逆元胞自动机和离散小波变换的有意义图像分存方案

针对文献[36,37]修复能力偏低,文献[11]对文献[36,37]的备份策略进行改进,提出了基于可逆元胞自动机和离散小波变换的有意义图像分存,其中,离散小波变换用于构造备份图,可逆元胞自动机用于构造(3,N)分存,使用掩体依然是密图大小的 2×2 倍.记密图为 $\boldsymbol{S}=(s_{i,j})_{m\times n}$ 且 m 和 n 均为偶数,对其做一级离散小波变换取其 LL 子带,记为 $\boldsymbol{S}_{LL}=(s_{i,j}^{LL})_{m/2\times n/2}$,将其置乱为 $\boldsymbol{S}'_{LL}=(s_{i,j}'^{LL})_{m/2\times n/2}$,记 $\boldsymbol{S}^p=(s_{i,j}^p)_{m\times n}$ 是 $\boldsymbol{S}$ 的备份图,嵌入分存信息前的掩体为 $\boldsymbol{C}^k=(c_{i,j}^k)_{2m\times 2n}, k=1,2,...,N$.

文献[11]对 $\boldsymbol{S}'_{LL}$ 上的每个低频系数 $s_{i,j}'^{LL}=(l_7l_6l_5l_4l_3l_2l_1l_0)_2$ 按公式(9)构造备份图 $\boldsymbol{S}^p$ 上的像素.

$$\begin{cases} s_{i,j}^p = (l_6l_4l_2l_0)_2 \\ s_{i+m/2,j}^p = (l_7l_5l_3l_1)_2 \\ s_{i,j+n/2}^p = (l_7l_5l_3l_1)_2 \\ s_{i+m/2,j+n/2}^p = (l_6l_4l_2l_0)_2 \end{cases} \tag{9}$$

公式(9)中:若 $s_{i,j}^p$ 和 $s_{i+m/2,j+n/2}^p$ 有一个通过认证,则可恢复偶数比特 $l_6l_4l_2l_0$;若 $s_{i+m/2,j}^p$ 和 $s_{i,j+n/2}^p$ 有一个通过认证,则可恢复奇数比特 $l_7l_5l_3l_1$.由公式(9),可构造与 $\boldsymbol{S}$ 等大且像素比特为 4 比特的备份图 $\boldsymbol{S}^p=(s_{i,j}^p)_{m\times n}$.文献[11]的 $\boldsymbol{S}'_{LL}$ 中,所有系数比特都同等程度备份了两次,但高位比特的重要程度是高于低位比特的.

文献[11]通过可逆元胞自动机将 $\boldsymbol{S}$ 和 $\boldsymbol{S}^p$ 分存,具体方法是:

- 首先,将分辨率为 $m\times n$ 的 $\boldsymbol{S}$ 和 $\boldsymbol{S}^p$ 划分成 $m\times n/2$ 个不重叠 1×2 小块;
- 然后,对每个 1×2 小块,将 $s_{i,2\times j}^p$ 和 $s_{i,2\times j+1}^p$ 连接成 8 位比特,即 $16\times s_{i,2\times j}^p + s_{i,2\times j+1}^p$,将其加密后作为 0 时刻 8 元胞 $C^{(0)}$,而 $s_{i,2\times j}$ 和 $s_{i,2\times j+1}$ 分别作为 1 时刻和 2 时刻 8 元胞 $C^{(1)}$和 $C^{(2)}$;

- 最后,通过可逆元胞自动机迭代 N 次得到 3,4,…,2+N 时刻元胞 $C^{(3)},C^{(4)},\ldots,C^{(N+2)}$,将其分发和嵌入到对应的 N 个掩体中.

对于第 k 个掩体,可获得 2+k 时刻元胞状态 $C^{(k+2)}$作为分存信息,将 $C^{(k+2)}$记为$(c_7c_6c_5c_4c_3c_2c_1c_0)_2$,然后,以 $C^{(k+2)}$所在小块的位置坐标(i,j)、随机序列和对应掩体 2×4 小块的每个像素高 6 位作为参数,生成 8 位认证信息$(a_7a_6a_5a_4a_3a_2a_1a_0)_2$,并将$(c_7c_6c_5c_4c_3c_2c_1c_0)_2$和$(a_7a_6a_5a_4a_3a_2a_1a_0)_2$用 LSB 法嵌入到掩体 2×4 分块的每个像素的低 2 位中.文献[11]采用简单 LSB 法嵌入分存信息和认证信息,会导致嵌入掩体视觉质量下降.而将 2 个秘密像素和 2 个备份像素分存信息嵌入到一个 2×4 分块中,若 2×4 分块任意一个像素被攻击,则嵌入到同 1 个分块中的 2 个秘密像素和 2 个备份像素不可用,从而导致文献[11]策略对噪声攻击修复能力依然较弱.

在恢复时,文献[11]首先从掩体的 2×4 分块的所有像素低 2 位中提取出 $(c_7'c_6'c_5'c_4'c_3'c_2'c_1'c_0')_2$ 和认证信息 $(a_7'a_6'a_5'a_4'a_3'a_2'a_1'a_0')_2$,并再次生成认证信息 $(a_7''a_6''a_5''a_4''a_3''a_2''a_1''a_0'')_2$,通过对比 $(a_7'a_6'a_5'a_4'a_3'a_2'a_1'a_0')_2$ 和 $(a_7''a_6''a_5''a_4''a_3''a_2''a_1''a_0'')_2$,验证该分块是否被攻击过:

- 若被攻击,则在认证图中标记为 0;
- 反之,若存在 3 个连续掩体在该分块通过认证,则可通过可逆元胞自动机迭代获得 $s'_{i,2\times j},s'_{i,2\times j+1}$ 和 $s'^{p}_{i,2\times j},s'^{p}_{i,2\times j+1}$,进而可获得认证图、攻击后密图 $\hat{\boldsymbol{S}}$ 和攻击后备份图 $\hat{\boldsymbol{S}}^p$,然后,按公式(9)对 $\hat{\boldsymbol{S}}^p$ 上的偶数比特 $l_6'l_4'l_2'l_0'$ 和奇数比特 $l_7'l_5'l_3'l_1'$ 分别进行恢复.若对应比特分组无法恢复,则将其置为$(1000)_2$,以此对置乱后的 $\hat{\boldsymbol{S}}'_{LL}$ 进行恢复.
- 最后,对 $\hat{\boldsymbol{S}}'_{LL}$ 做逆置乱和逆离散小波变换后,可得近似密图 $\hat{\boldsymbol{S}}'$,并通过 $\hat{\boldsymbol{S}}'$ 修复 $\hat{\boldsymbol{S}}$ 中的认证不通过像素.

文献[11]相比文献[36,37]提高了修复能力,同时对分存信息采用等长认证码进行认证,提高了对分存信息的认证精度.然而,它是借用可逆元胞自动机进行分存,并不是真正意义的(3,N)门限方案.对于每个分块,需至少 3 个连续参与者才能按可逆元胞自动机恢复出秘密像素和备份像素,其适用条件过于苛刻,严重影响方案适用性.同时,由于仅对分存信息进行认证,并不能对重构秘密像素进行精确认证.尽管认证码达到了 8 位,恶意用户依然有 1/256 的篡改概率逃脱检验,而将 2 个秘密像素和 2 个备份像素分存信息嵌入到一个 2×4 分块中,若 2×4 分块任意一个像素被攻击,将导致嵌入到同一个分块中的所有秘密像素和备份像素不可用.因而,文献[11]对噪声攻击的实际修复能力依然偏弱.

与文献[11]不同,本文给出的是建立在 GF(2^7)有限域的真正意义的(K,N)图像分存方法,并在该方法中融入了双认证能力,既能对分发分存信息进行简单认证,也能对重构密图进行高精度精确认证.备份图按低频系数比特位的重要程度分组,进行由多到少的非等量备份,相对于文献[11]的等量备份策略,性能有了大幅度提高;同时,也引入了多项式拟合来增强重构图像的自修复能力.相对于传统方法[10,11,27,29–37],不仅具备更好的修复能力,嵌入分存信息后,掩体也具备更高的视觉质量,还可对随机噪声攻击具有一定的迭代抵抗能力.

3 结合非等量备份和双认证有限域图像分存方案

本文所给出的结合非等量备份和双认证有限域图像分存方案主要包括 3 个环节.

- 首先,由密钥 *Key* 置乱的密图 LL 子带按子带像素比特位的重要程度分组构建出每像素 5 比特备份图;
- 然后,将密图 8 比特像素和备份图 5 比特像素以及对应的 7K-13 个认证比特在 GF(2^7)有限域上进行(K,N)分存;
- 最后,为 7 比特分存信息添加 1 比特认证信息,按优化 LSB 嵌入策略嵌入到掩体划分的不重叠 2×2 小块中.

其中,7K-13 个认证比特会随着(K,N)门限的增长而增加,因此,可对备份像素和秘密像素提供高精度认证.图 1 给出了分存方案流程图.图 1 中,箭头方向表示输入/输出,实线框表示输入信息或处理环节,虚线框表示所涉及的具体处理细节.以下对该流程图中所涉及的基于比特位分组的非等量备份图生成策略、GF(2^7)有限域的密图和备份图认证和分存策略以及结合优化 LSB 法分存信息认证和嵌入策略进行具体说明.

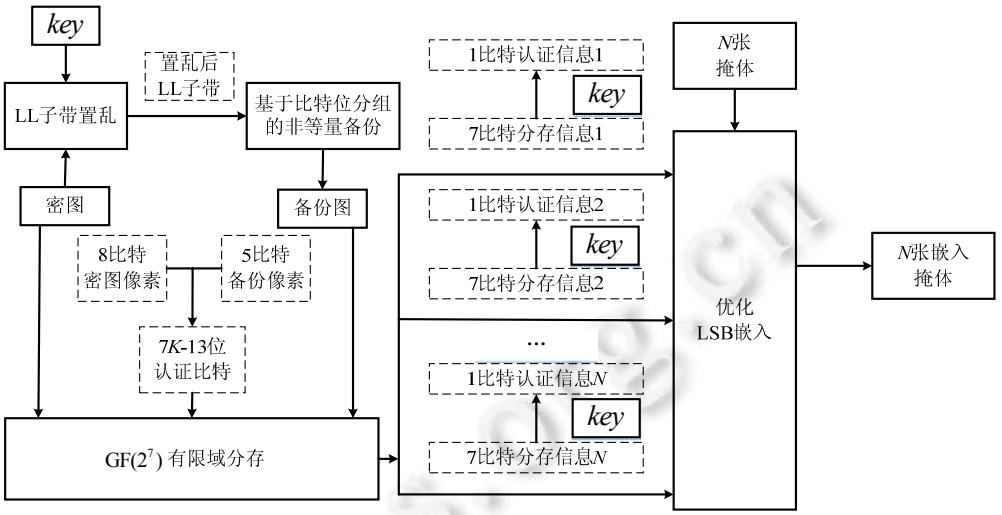


Fig.1 Flow chart of image sharing scheme

图 1 图像分存方案流程图

3.1 基于比特位分组的非等量备份图生成策略

文献[11]尽管用密图 $\boldsymbol{S}=(s_{i,j})_{m\times n}$ 的 LL 置乱子带 $\boldsymbol{S}'_{LL}=(s'^{LL}_{i,j})_{m/2\times n/2}$ 构建备份图 $\boldsymbol{S}^p=(s^p_{i,j})_{m\times n}$ 提升了重构密图的修复能力,但所提策略是直接将 $\boldsymbol{S}'_{LL}$ 每个系数比特备份了 2 份.但在实际中,像素高位比特相对于像素低位比特对图像的视觉质量影响更大,也更为重要,以 $\boldsymbol{S}'_{LL}=(s'^{LL}_{i,j})_{m/2\times n/2}$ 上的系数 $s'^{LL}_{i,j}=(l_7l_6l_5l_4l_3l_2l_1l_0)_2$ 为例,记 $\xi(l_i)$ 为 l_i 的重要程度,则有 $\xi(l_7)=2\xi(l_6)=4\xi(l_5)=8\xi(l_4)=16\xi(l_3)=32\xi(l_2)=64\xi(l_1)=128\xi(l_0)$,而文献[11]将重要程度不同的比特同等对待,是有失偏颇的.

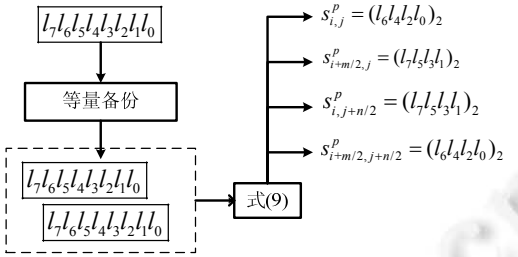
与文献[11]不同,这里将 $s'^{LL}_{i,j}=(l_7l_6l_5l_4l_3l_2l_1l_0)_2$ 上的比特位分为 4 组,并分别进行非等量备份,其中,第 0 组 l_7l_6 备份 4 次,第 1 组 l_5l_4 备份 3 次,第 2 组 l_3l_2 备份 2 次,第 3 组 l_1l_0 备份 1 次;然后,按公式(10)将 $\boldsymbol{S}'_{LL}=(s'^{LL}_{i,j})_{m/2\times n/2}$ 上的 $s'^{LL}_{i,j}=(l_7l_6l_5l_4l_3l_2l_1l_0)_2$ 转换为备份图 $\boldsymbol{S}^p$ 上的备份像素 $s^p_{i,j}$,$s^p_{i+m/2,j}$,$s^p_{i,j+n/2}$ 和 $s^p_{i+m/2,j+n/2}$,对 $\boldsymbol{S}'_{LL}$ 置乱密钥 Key 由分存发起者选取,并在分存方案完成后销毁.

$$\begin{cases} s^p_{i,j}=(l_7l_6l_5l_3l_2)_2 \\ s^p_{i+m/2,j}=(l_7l_6l_5l_4l_1)_2 \\ s^p_{i,j+n/2}=(l_7l_6l_4l_3l_2)_2 \\ s^p_{i+m/2,j+n/2}=(l_7l_6l_5l_4l_0)_2 \end{cases} \tag{10}$$

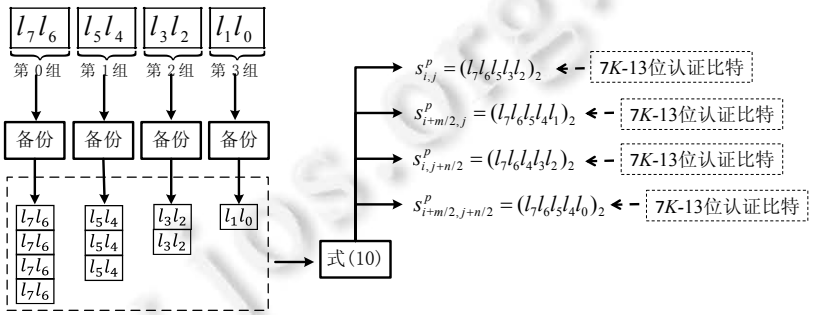
公式(10)即对应为基于比特位分组的非等量备份图生成策略.这里需要说明的是:若严格按比特位的重要程度进行非等量备份并且满足 $l_0,l_1,\ldots,l_7$,至少需备份 1,2,…,8 份,此时需存储 36 个备份比特;若将其均匀分为 4 份,则需存储 9 个备份比特.而过多备份比特会限制对备份像素和密图像素的认证能力,从而降低认证精度.为保证对秘密像素和备份像素高精度认证,本文采用的是按比特位的重要程度分组来进行非等量备份.图 2 是对文献[11]的等量备份策略和本文所给出的非等量备份策略进行的对比,其中,虚线箭头表示认证关系.

在图2中,尽管本文所提策略的备份像素相对于文献[11]仅增加1个备份比特,却具有较高性能:本文对每个备份像素都有 7*K*-13 位认证比特,因而可进行高精度认证;而同等情况下,文献[11]由于仅对分存信息进行认证,从而不能对重构出的秘密像素和备份像素的真假进行准确鉴别,因此会存在一定的误判概率.

表 1 给出了本文和文献[11]的密图 LL 子带像素比特的所有恢复情况,表 2 则给出了本文和文献[11]的密图 LL 子带像素每一位比特攻击后的恢复概率.



(a) 文献[11]的等量备份策略



(b) 本文基于比特位分组的非等量图像备份策略

Fig.2 Equivalent backup strategy and none-equivalent backup strategy

图 2 等量备份策略与非等量图像备份策略

Table 1 LL sub-band bit recovery status in the proposed scheme and scheme[11]

表 1 本文和文献[11]的 LL 子带像素比特恢复情况

编号	参与恢复的正确备份像素	本文的恢复比特	本文的恢复位数	文献[11]的恢复比特	文献[11]的恢复位数
1	$s_{i,j}^p,s_{i+m/2,j}^p,s_{i,j+n/2}^p,s_{i+m/2,j+n/2}^p$	$l_7l_6l_5l_4l_3l_2l_1l_0$	8	$l_7l_6l_5l_4l_3l_2l_1l_0$	8
2	$s_{i,j}^p,s_{i+m/2,j}^p,s_{i,j+n/2}^p$	$l_7l_6l_5l_4l_3l_2l_1$	7	$l_7l_6l_5l_4l_3l_2l_1l_0$	8
3	$s_{i,j}^p,s_{i,j+n/2}^p,s_{i+m/2,j+n/2}^p$	$l_7l_6l_5l_4l_3l_2l_0$	7	$l_7l_6l_5l_4l_3l_2l_1l_0$	8
4	$s_{i,j}^p,s_{i+m/2,j}^p,s_{i+m/2,j+n/2}^p$	$l_7l_6l_5l_4l_3l_2l_1l_0$	8	$l_7l_6l_5l_4l_3l_2l_1l_0$	8
5	$s_{i+m/2,j}^p,s_{i,j+n/2}^p,s_{i+m/2,j+n/2}^p$	$l_7l_6l_5l_4l_3l_2l_1l_0$	8	$l_7l_6l_5l_4l_3l_2l_1l_0$	8
6	$s_{i,j}^p,s_{i+m/2,j}^p$	$l_7l_6l_5l_4l_3l_2l_1$	7	$l_7l_6l_5l_4l_3l_2l_1l_0$	8
7	$s_{i,j}^p,s_{i,j+n/2}^p$	$l_7l_6l_5l_4l_3l_2$	6	$l_7l_6l_5l_4l_3l_2l_1l_0$	8
8	$s_{i,j}^p,s_{i+m/2,j+n/2}^p$	$l_7l_6l_5l_4l_3l_2l_0$	7	$l_6l_4l_2l_0$	4
9	$s_{i+m/2,j}^p,s_{i,j+n/2}^p$	$l_7l_6l_5l_4l_3l_2l_1$	7	$l_7l_5l_3l_1$	4
10	$s_{i+m/2,j}^p,s_{i+m/2,j+n/2}^p$	$l_7l_6l_5l_4l_1l_0$	6	$l_7l_6l_5l_4l_3l_2l_1l_0$	8
11	$s_{i,j+n/2}^p,s_{i+m/2,j+n/2}^p$	$l_7l_6l_5l_4l_3l_2l_0$	7	$l_7l_6l_5l_4l_3l_2l_1l_0$	8
12	$s_{i,j}^p$	$l_7l_6l_5l_3l_2$	5	$l_6l_4l_2l_0$	4
13	$s_{i+m/2,j}^p$	$l_7l_6l_5l_4l_1$	5	$l_7l_5l_3l_1$	4
14	$s_{i,j+n/2}^p$	$l_7l_6l_4l_3l_2$	5	$l_7l_5l_3l_1$	4
15	$s_{i+m/2,j+n/2}^p$	$l_7l_6l_5l_4l_0$	5	$l_6l_4l_2l_0$	4
16	0	无	0	无	0

Table 2 LL sub-band pixel bit recovery probability in the proposed scheme and scheme[11]

表 2 本文与文献[11]的 LL 子带像素比特恢复概率

比特	l_7	l_6	l_5	l_4	l_3	l_2	l_1	l_0
本文恢复概率	15/16	15/16	7/8	7/8	3/4	3/4	1/2	1/2
文献[11]恢复概率	3/4	3/4	3/4	3/4	3/4	3/4	3/4	3/4

从表 1 可看出:若 $s^p_{i,j},s^p_{i+m/2,j},s^p_{i,j+n/2}$ 和 $s^p_{i+m/2,j+n/2}$ 只有 1 个通过认证,则至少可恢复 l_7l_6,除此以外还可精确地恢复其他比特中的 3 个,而文献[11]却只能恢复 4 个且 l_7l_6 有一个无法恢复;若其中有 2 个通过认证,则至少可恢复 $l_7l_6l_5l_4$,除此以外还可精确地恢复其他比特中的 2 个或 3 个,而文献[11]则有 2/3 的概率全部修复和 1/3 的概率修复 4 个且 l_7l_6 有一个无法恢复;若其中有 3 个通过认证,则至少可恢复 $l_7l_6l_5l_4l_3l_2$,除此以外还可精确地恢复其他比特中的 1 个或 2 个,而文献[11]可正确修复;若全部通过认证,则本文和文献[11]备份像素所有比特都可恢复.

表 2 是对表 1 中每位比特恢复概率进行统计的结果.从表 2 可看出:本文所构造的备份像素恢复策略,高位比特分组中比特具有较高恢复概率,低位分组比特中比特具有较低恢复概率,但所有比特被恢复概率不低于 1/2 且最大恢复概率可达到 15/16;而文献[11]对所有比特具有一样修复概率都为 3/4.相比之下,本文对 $l_7l_6l_5l_4$ 的正确修复概率要大于文献[11],l_3l_2 要等于文献[11],l_1l_0 要小于文献[11].而高位比特的重要程度显然高于低位比特,因此,本文基于比特位分组的非等量备份图生成策略在整体性能上优于文献[11].

3.2 GF(2^7)有限域密图与备份图认证和分存策略

第 3.1 节可由密图 $\boldsymbol{S}$ 产生与之等大且像素比特为 5 比特的备份图 $\boldsymbol{S}^p=(s^p_{i,j})_{m\times n}$.

与文献[11,27,29–32,34,36,37]仅对分存信息进行认证和文献[10,33,35]仅对秘密像素进行认证不同,本文不仅对分存密图和备份图进行认证,也对分存后分存信息进行认证.文献[11,36,37]尽管使用 Hash 或 HMAC 来生成认证信息,但对认证信息如何生成未做具体说明,这个认证信息非常重要.在本文中,$s_{i,j}$ 和 $s^p_{i,j}$ 的认证信息由连续生成的 K–1 个伪随机数构成,伪随机数种子 $ke_{i,j}$ 由 $s_{i,j}$、$s^p_{i,j}$ 以及对应的坐标(i,j)按公式(11)产生.

$$ke_{i,j}=i+j+i\times j+s_{i,j}+s^p_{i,j}+s^p_{i,j}\times s_{i,j} \tag{11}$$

公式(11)可设计得更为复杂,例如同给定的密钥绑定,从而提供足够安全性.

使用 $ke_{i,j}$ 可得到伪随机序列 $\boldsymbol{R}_{i,j}=\langle r^0_{i,j},r^1_{i,j},r^2_{i,j},...,r^k_{i,j},...\rangle$,发起者可根据实际需要来约定 $\boldsymbol{R}_{i,j}$ 选取规则.这里,按公式(12)生成 $s_{i,j}$ 和 $s^p_{i,j}$ 的认证信息 $a^0_{i,j},a^1_{i,j},...,a^{K-2}_{i,j}$.

$$\begin{cases} a^0_{i,j}=r^1_{i,j}(\mathrm{mod}\,2)\\ a^1_{i,j}=r^2_{i,j}(\mathrm{mod}\,128)\\ a^2_{i,j}=r^3_{i,j}(\mathrm{mod}\,128)\\ ...\\ a^{K-2}_{i,j}=r^{K-1}_{i,j}(\mathrm{mod}\,128) \end{cases} \tag{12}$$

其中,$r^0_{i,j}$ 不使用.公式(12)中,认证信息 $a^0_{i,j},a^1_{i,j},...,a^{K-2}_{i,j}$ 被划分为 2 部分:1 比特 $a^0_{i,j}$ 和 7K-14 比特 $a^1_{i,j},a^2_{i,j},...,a^{K-2}_{i,j}$,因此,$a^0_{i,j},a^1_{i,j},...,a^{K-2}_{i,j}$ 总共包含 7K-13 位认证比特.公式(12)引入 $a^0_{i,j}$ 的目的是将 $s_{i,j}$ 和 $s^p_{i,j}$ 转换为 2 个 7 比特,从而作为 GF(2^7)有限域分存多项式分存系数. $a^0_{i,j},a^1_{i,j},...,a^{K-2}_{i,j}$ 用于恢复阶段的第 2 重认证,即,对恢复出秘密像素和备份像素真实性进行检验.

文献[36,37]采用的分存模数分别为 17 和 7 的 Lagrange 分存模型,由于模数 17 和模数 7 的限制,使得 Shamir-(K,N)门限方案的 K 不小于 3;同时,N 的可选范围仅能为[K,16]和[K,6]范围内的整数,从而严重制约了此类方法的实际适用面.且由于模数 p 为素数的限制作用,导致文献[36,37]的分存方案只能选取大于实际分存值上界的模数 p 进行分存,从而对有限分存空间造成浪费,导致嵌入掩体视觉质量下降.

为避免文献[36,37]采用 Lagrange 分存模型不能有效地利用模数空间进行嵌入,文献[10,11]分别采用可逆元胞自动机进行(K,N)或(3,N)分存.尽管没有浪费有限分存空间,对于每个分块,需至少 K 个或 3 个连续的参与者

才能按可逆元胞自动机恢复出秘密像素和备份像素,其适用条件过于苛刻,同样影响该方案的适用面.在本文中,为避免文献[10,11,30,31]存在的问题,采用 GF(2^7)有限域的 Lagrange 插值多项式对 $s_{i,j}$, $s_{i,j}^p$ 和认证信息 $a_{i,j}^0,a_{i,j}^1,...,a_{i,j}^{K-2}$ 按公式(13)进行分存.

$$f_{GF}^{i,j}(\dot{k})=(\dot{a}+\dot{b}\dot{k}+\dot{a}_{i,j}^1\dot{k}^2+...+\dot{a}_{i,j}^{K-2}\dot{k}^{K-1})\bmod \dot{p} \tag{13}$$

公式(13)即为 GF(2^7)有限域分存多项式,其中,a,b 可由公式(14)计算得到:

$$\begin{aligned} a&=s_{i,j}/2\in\{0,1,...,127\}\\ b&=64\times(s_{i,j}\bmod 2)+2\times s_{i,j}^p+a_{i,j}^0\in\{0,1,...,127\}\end{aligned} \tag{14}$$

故在公式(13)中, $a,b,a_{i,j}^0,a_{i,j}^1,...,a_{i,j}^{K-2}$ 都为 7 比特.因此, $\dot{a},\dot{b},\dot{a}_{i,j}^0,\dot{a}_{i,j}^1,...,\dot{a}_{i,j}^{K-2}$ 都为 GF(2^7)有限域多项式整数,不浪费任何模数空间.图 3 给出了 GF(2^7)有限域密图与备份图认证和分存流程图.

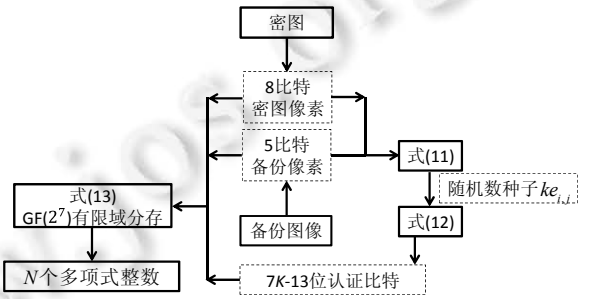


Fig.3 Flow chart of secret and backup image authentication and sharing scheme on GF(2^7)

图 3 基于 GF(2^7)有限域的密图和备份图认证与分存流程图

由于所构造(K,N)门限方案在 GF(2^7)有限域,因此 N 为[K,2^7)范围内的整数.K 还可为 2,因此相对于文献[11,36,37]具有更广泛的适用面,同时也避免了文献[11]提出的必须至少 3 个参与者才能按可逆元胞自动机恢复出秘密像素和备份像素的不适用性,并且本文方案随着 K 的增大,认证信息越来越长,从而可对秘密像素和备份像素提供足够高的认证精度,具备更高的适用面.表 3 给出了不同门限 K 下的认证信息位数.

Table 3 Proposed scheme authentication bits with different threshold K

表 3 所提策略在不同门限 K 下的认证信息位数

门限 K	2	3	4	5	6	7	8	9	10
认证位长度	1	8	15	22	29	36	43	50	57

从表 3 可看出:当 K=2 时,有 1 位认证比特作为秘密像素和备份像素认证信息,认证比特虽然少,但相对于文献[10,11,36,37]的 K 不能为 2 具有更好的适用性;而当 K 大于 2 时,有 7K−13 个认证比特,恶意篡改秘密像素或备份像素通过认证的概率低至$(1/2)^{7K-13}$,相比文献[10,35]秘密像素认证概率 1/256 和 1/16 具有更强的认证能力,而文献[11,27,29−32,34,36,37]不具备对秘密像素的认证能力,而只具备对分存信息的认证能力.

3.3 结合优化LSB的分存信息认证和嵌入策略

在本文中,与文献[11,36,37]一样,掩体 $\boldsymbol{C}^k=(c_{i,j}^k)_{2m\times 2n},k=1,2,...,N$ 为密图 $\boldsymbol{S}$ 和备份图 $\boldsymbol{S}^p=(s_{i,j}^p)_{m\times n}$ 各自分辨率的 2×2 倍.将 k=1,2,…,N 分别代入公式(13),可得到 GF(2^7)有限域多项式整数 $f_{GF}^{i,j}(\dot{k}),k=1,2,...,N$,将其转换为 7 位 2 进制数 $v_k^{i,j}=(v_6^{i,j,k}v_5^{i,j,k}v_4^{i,j,k}v_3^{i,j,k}v_2^{i,j,k}v_1^{i,j,k}v_0^{i,j,k})_2,k=1,2,...,N$.对其可分别产生 1 位认证信息,从而将 7 比特 2 进制数和 1 比特认证信息嵌入到掩体划分的 1 个不重叠 2×2 小块中.

$v_k^{i,j}$ 的 1 比特认证信息 $va_k^{i,j}$ 同样由伪随机序列生成,伪随机序列密钥 $Ke_{i,j}^k$ 按公式(15)确定.

$$Ke_{i,j}^k=i+j+i\times j+v_k^{i,j}+Key+v_k^{i,j}\times Key \tag{15}$$

使用 $Ke_{i,j}^k$ 可生成伪随机序列 $\boldsymbol{RR}_{i,j,k}=\langle rr_{i,j,k}^0, rr_{i,j,k}^1, rr_{i,j,k}^2,...,rr_{i,j,k}^k,...\rangle$,发起者可根据实际需要选取 $\boldsymbol{RR}_{i,j,k}$ 使用规则,这里按公式(16)产生 1 比特认证信息 $va_k^{i,j}$.

$$va_k^{i,j}=rr_{i,j,k}^1 \bmod 2 \tag{16}$$

其中,$va_k^{i,j}$ 用于恢复阶段第 1 重认证,对提取到的分存信息真实性进行检验.与文献[11,36,37]仅对分存信息进行 Hash 认证方法不同,本文只对分存信息做简单认证,而对重构出的秘密信息进行高精度认证,从而不仅能够充分地利用分发信息进行重构,同时也能提高密图和备份图的重构精度,还可进一步提高攻击后密图的修复能力.

将 $v_6^{i,j,k},v_5^{i,j,k},v_4^{i,j,k},v_3^{i,j,k},v_2^{i,j,k},v_1^{i,j,k},v_0^{i,j,k}$ 和 $va_k^{i,j}$ 总共 8 比特划分为 4 组,即 $v_0^{i,j,k}v_1^{i,j,k}$,$v_2^{i,j,k}v_3^{i,j,k}$,$v_4^{i,j,k}v_5^{i,j,k}$ 和 $v_6^{i,j,k}va_k^{i,j}$,然后将其嵌入到掩体 $\boldsymbol{C}^k$ 像素 $c_{2i,2j}^k,c_{2i,2j+1}^k,c_{2i+1,2j}^k,c_{2i+1,2j+1}^k$ 低 2 位比特上,其中,k=1,2,…,N.

文献[11]采用的是普通 LSB 法,会导致嵌入掩体视觉质量偏低;而本文引入文献[31]的优化 LSB 法来嵌入分存和认证信息,可有效保障掩体嵌入视觉质量.

假设需要嵌入的信息比特为$(s_1s_2)_2$,被嵌入像素记为 $ps=(p_7p_6p_5p_4p_3p_2p_1p_0)_2$,普通 LSB 法嵌入$(s_1s_2)_2$后的载体像素为 $ps'=(p_7p_6p_5p_4p_3p_2s_1s_2)_2$,而优化 LSB 法通过公式(17)进行调节,使得嵌入分存信息后的 ps''离原像素 ps 更为接近.

$$ps''=\begin{cases} ps'-4, & ps'>4, 2<ps'-ps<4 \\ ps'+4, & ps'\leqslant 251, -4<ps'-ps<-2 \\ ps', & \text{其他情况} \end{cases} \tag{17}$$

按公式(17)可将 $c_{2i,2j}^k,c_{2i,2j+1}^k,c_{2i+1,2j}^k,c_{2i+1,2j+1}^k$ 转换为 $c_{2i,2j}'^k,c_{2i,2j+1}'^k,c_{2i+1,2j}'^k,c_{2i+1,2j+1}'^k$,当处理完密图 $\boldsymbol{S}=(s_{i,j})_{m\times n}$ 和备份图 $\boldsymbol{S}^p=(s_{i,j}^p)_{m\times n}$ 上所有 $s_{i,j}$ 和 $s_{i,j}^p$,可得嵌入分存信息后掩体 $\boldsymbol{C}'^k=(c_{i,j}'^k)_{2m\times 2n}, k=1,2,...,N$.

图 4 给出了结合优化 LSB 的分存信息认证和嵌入策略流程图,其中,虚线箭头表示具体嵌入位置.与文献[11]相比,采用优化 LSB 法可得到更高的嵌入视觉质量;同时,每个 2×2 小块嵌入的分存信息数量更少.因此,相对于文献[36,37],也具备更高的视觉质量.

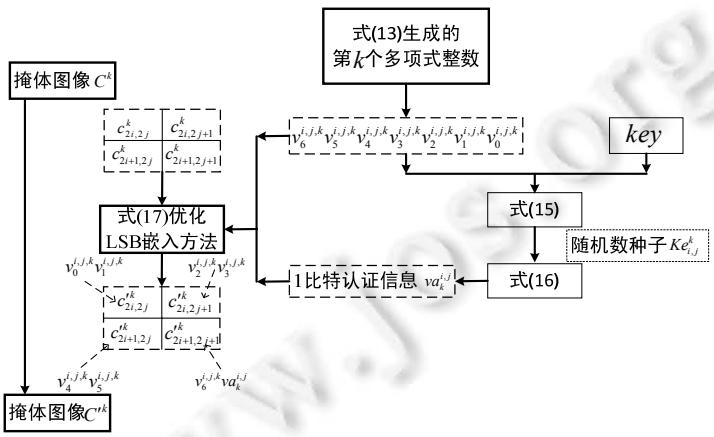


Fig.4 Flow chart of distributed information authentication and embedding strategy

图 4 分存信息认证和嵌入策略流程图

在以上所给出的分存策略中,还涉及到密钥 *Key*.在本文中,*Key* 被用来置乱 $\boldsymbol{S}_{LL}=(s_{i,j}^{LL})_{m/2\times n/2}$ 和生成公式(15)的密钥 $Ke_{i,j}^k$,若不恰当保管,将威胁到整个分存方案安全.文献[11,36,37]同样存在十分重要的密钥 *Key*,但文献[11,36,37]并未说明如何保护密钥.这里,将 *Key* 按公式(1)分存成 N 个子密钥 $subkey_1,subkey_2,...,subkey_N$ 分发给 N 个参与者,并将子密钥对应的 MD5 值公布到第 3 方公信方,以防止参与者恶意篡改子密钥.当收集到至少 K 个未被篡改的子密钥,则可无损地恢复出密钥 *Key*.

3.4 结合非等量备份和双认证有限域图像分存算法

结合第 3.1 节~第 3.3 节的工作,可给出结合非等量备份和双认证有限域图像的分存算法,记为算法 1:

算法 1. 结合非等量备份和双认证有限域图像分存算法.

输入:密钥 Key,密图 $\boldsymbol{S}=(s_{i,j})_{m\times n}$ 和 N 份掩体 $\boldsymbol{C}^k=(c_{i,j}^k)_{2m\times 2n},k=1,2,...,N$;

输出:嵌入分存信息后掩体 $\boldsymbol{C}'^k=(c_{i,j}'^k)_{2m\times 2n},k=1,2,...,N$ 和子密钥 $subkey_1,subkey_2,\ldots,subkey_N$.

第 1 步:对密图 $\boldsymbol{S}=(s_{i,j})_{m\times n}$ 做 1 级离散小波变换取 LL 子带 $\boldsymbol{S}_{LL}=(s_{i,j}^{LL})_{m/2\times n/2}$ 并用密钥 Key 将 $\boldsymbol{S}_{LL}=(s_{i,j}^{LL})_{m/2\times n/2}$ 置乱为 $\boldsymbol{S}'_{LL}=(s'^{LL}_{i,j})_{m/2\times n/2}$;

第 2 步:根据 $\boldsymbol{S}_{LL}=(s_{i,j}^{LL})_{m/2\times n/2}$ 系数比特位重要程度分组,按公式(10)构造备份图 $\boldsymbol{S}^p=(s_{i,j}^p)_{m\times n}$;

第 3 步:对 $s_{i,j}$ 和 $s_{i,j}^p$ 使用公式(11)和公式(12)计算认证信息 $a_{i,j}^0,a_{i,j}^1,...,a_{i,j}^{K-1}$,并用公式(13)分存 $s_{i,j},s_{i,j}^p$ 和 $a_{i,j}^0$,$a_{i,j}^1,...,a_{i,j}^{K-1}$,得到分存信息 $f_{GF}^{i,j}(\dot{k}),k=1,2,...,N$;

第 4 步:通过公式(16)计算 $f_{GF}^{i,j}(\dot{k}),k=1,2,...,N$ 对应分存信息 $v_k^{i,j}$ 的认证信息 $va_k^{i,j}$;

第 5 步:按公式(17)将 $v_k^{i,j}$ 和 $va_k^{i,j}$ 嵌入到 $\boldsymbol{C}^k=(c_{i,j}^k)_{2m\times 2n}$ 像素 $c_{2i,2j}^k,c_{2i,2j+1}^k,c_{2i+1,2j}^k,c_{2i+1,2j+1}^k$ 上,得到 $c_{2i,2j}'^k$,$c_{2i,2j+1}'^k$,$c_{2i+1,2j}'^k,c_{2i+1,2j+1}'^k$;

第 6 步:反复执行第 3 步~第 5 步,直至处理完所有秘密像素,得到 $\boldsymbol{C}'^k=(c_{i,j}'^k)_{2m\times 2n},k=1,2,...,N$;

第 7 步:将 Key 按公式(1)分存成 N 个子密钥 $subkey_1,subkey_2,\ldots,subkey_N$,将其和 $\boldsymbol{C}'^k=(c_{i,j}'^k)_{2m\times 2n},k=1,2,...,N$ 分发给 N 个参与者保管,销毁中间计算数据.

在算法 1 中,

- 步骤 1、步骤 2 用于构造非等量备份图.相对于文献[11]基于等量备份的备份图生成策略,具备更好的自恢复和抗攻击能力;
- 步骤 3~步骤 5 用于生成秘密像素和备份像素第 2 重认证信息,然后将 GF(2^7)有限域秘密像素和备份像素以及第 2 重认证信息进行分存,并将分存信息和由分存信息产生的第 1 重认证信息使用优化 LSB 法嵌入到掩体分块中.相比文献[10,11,27,29–34,36,37]只对秘密像素进行认证或只对分存信息进行认证,具备更好的认证能力,且使用优化 LSB 法嵌入信息后的掩体具备更好的视觉质量;
- 步骤 7 用于对密钥 Key 进行分存保护.相对于文献[11,29,36,37]不对密钥 Key 进行任何处理,具备更高的安全性.

4 结合非等量备份和双认证有限域图像恢复方案

与第 3 节图像分存方案相对应的恢复方案主要包括 4 个环节:首先,对参与者提供子密钥通过第 3 方存储 MD5 值进行检验,若检验通过子密钥数大于等于 K,则可重构出 Key;其次,对参与恢复掩体像素中分存信息进行第 1 重认证,并对恢复出秘密像素和备份像素进行第 2 重认证,对双认证结果进行标记来构建认证图;再次,通过认证图和恢复出备份图构建修复参考图;最后,结合认证图和邻近像素插值拟合以及修复参考图像素替代策略来对认证不通过秘密像素进行恢复.图 5 给出了密图恢复方案流程图.

为便于描述,假设参与恢复的 $t(t\geqslant K)$张分发掩体标号为 $num_1,num_2,\ldots,num_t\in\{1,2,\ldots,N\}$且两两不同,将它们分别记为 $\boldsymbol{C}'^{num_k}=(c_{i,j}'^{num_k})_{2\times 2n},k=1,2,...,t$,对应的子密钥记为 $subkey_{num_1},subkey_{num_2},...,subkey_{num_t}$,并假设所有用户提供的子密钥都正确,此时,可通过 $(num_1,subkey_{num_1}),(num_2,subkey_{num_2}),...,(num_t,subkey_{num_t})$ 按公式(2)还原出公式(15)中的 Key.以下主要对上述密图恢复方案中的双认证策略、修复参考图构建策略以及结合邻近像素插值拟合和修复参考图像素替代的密图自恢复策略进行说明.

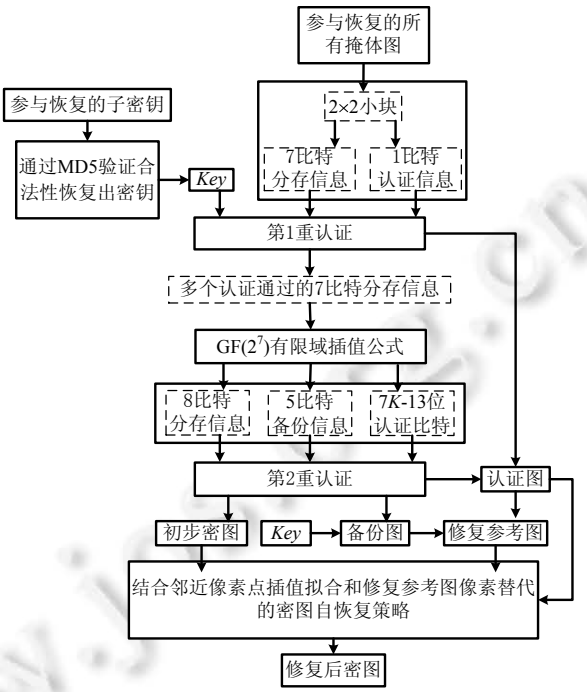


Fig.5 Flow chart of secret image recovery scheme

图 5 密图恢复方案流程图

4.1 用于分存信息和恢复秘密像素以及备份像素的双认证策略

文献[11,36,37]只对分存信息进行认证,用于对掩体是否遭受攻击进行认证.相对于掩体,用户更关心密图的攻击情况,因而本文用更多的认证比特来对恢复秘密像素是否遭受攻击进行第 2 重认证.第 2 重认证相对于第 1 重认证更为安全也更为重要,它至少需 K 幅分发掩体对应位置的分存信息才可恢复出分存多项式,而第 1 重认证信息和分存信息存储在同一个掩体当中,由于掩体容量所限,导致分存信息认证的比特数较少,例如,文献[11,29−32,36,37]存在恶意用户篡改掩体而不被发现的风险,甚至有很大的概率逃脱检验.所以本文采用双认证:首先,利用第 1 重认证来检验掩体是否被攻击和确定攻击的大致范围;然后,对第 1 重认证通过的分存信息恢复出秘密像素和备份像素以及认证信息,进行第 2 重认证.

对掩体 $\boldsymbol{C}'^{num_k}=(c'^{num_k}_{i,j})_{2m\times 2n}$ 的 2×2 分块 $\boldsymbol{B}'^{num_k}_{i,j}$ 的 4 个像素 $c'^{num_k}_{2i,2j},c'^{num_k}_{2i,2j+1},c'^{num_k}_{2i+1,2j},c'^{num_k}_{2i+1,2j+1}$ 依次提取每个像素低 2 位,可得到分存信息 $v^{i,j}_{num_k}=(v^{i,j,num_k}_6v^{i,j,num_k}_5v^{i,j,num_k}_4v^{i,j,num_k}_3v^{i,j,num_k}_2v^{i,j,num_k}_1v^{i,j,num_k}_0)_2$ 和 1 比特认证信息 $va^{i,j}_{num_k}$.

结合 Key 和提取到的 $v^{i,j}_{num_k}$,使用公式(15)再次计算伪随机生成序列密钥 $Ke^{num_k}_{i,j}$,然后生成伪随机序列 $\boldsymbol{RR}_{i,j,num_k}=\langle rr^0_{i,j,num_k},rr^1_{i,j,num_k},rr^2_{i,j,num_k},...,rr^k_{i,j,num_k},...\rangle$,并可验证提取到的认证信息 $va^{i,j}_{num_k}$ 是否和 $rr^1_{i,j,num_k}\bmod 2$ 相等:若相等,则表示 $\boldsymbol{B}'^{num_k}_{i,j}$ 提取到的 $v^{i,j}_{num_k}=(v^{i,j,num_k}_6v^{i,j,num_k}_5v^{i,j,num_k}_4v^{i,j,num_k}_3v^{i,j,num_k}_2v^{i,j,num_k}_1v^{i,j,num_k}_0)_2$ 通过认证;否则,表示不通过认证.上述对分存信息的认证策略,即第 1 重认证策略.图 6 给出了第 1 重认证处理流程.

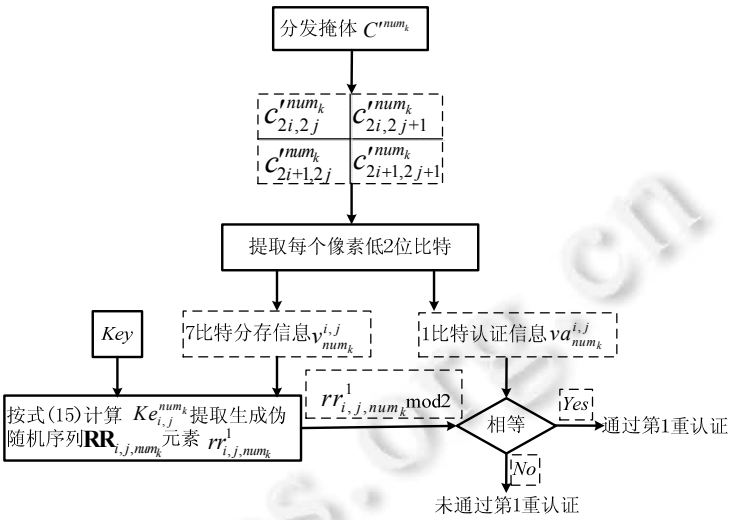


Fig.6 Flow chart of the first authentication

图 6 第 1 重认证流程图

通过第 1 重认证,可判断参与恢复的掩体是否遭受攻击或恶意篡改,并可根据认证比特得到每张掩体的攻击或篡改轮廓.若 $v^{i,j}_{num_k}, k=1,2,...,t$ 中不少于 K 个通过第 1 重认证,则可进行进一步恢复;否则,标记认证图 $\boldsymbol{A}=(a_{i,j})_{m\times n}$ 的 $a_{i,j}$=0,即,密图和备份图的第(i,j)位置像素未通过第 1 重认证.第 1 重认证仅用于筛选可参于恢复的秘密像素和备份像素的分存值,不做精确认证,尽管会带来误判,但会在第 2 重对秘密像素和备份像素的高精度认证时得以纠正.

为便于描述,不失一般性,假设 $v^{i,j}_{num_k}, k=1,2,...,t$ 都通过第 1 重认证且不少于 K 个.对于 $v^{i,j}_{num_k}, k=1,2,...,t$,可将它们转换为 GF(2^7)有限域多项式整数,得到 $(\dot{num}_1, f^{i,j}_{GF}(\dot{num}_1)),(\dot{num}_2, f^{i,j}_{GF}(\dot{num}_2)),...,(\dot{num}_t, f^{i,j}_{GF}(\dot{num}_t))$;然后,通过公式(4)还原公式(12) $f^{i,j}_{GF}(\dot{k})=(\dot{a}+\dot{b}\dot{k}+\dot{a}^1_{i,j}\dot{k}^2+...+\dot{a}^{K-2}_{i,j}\dot{k}^{K-1}) \bmod \dot{p}$,从而提取出有限域多项式整数 $\dot{a},\dot{b},\dot{a}^1_{i,j},...,\dot{a}^{K-2}_{i,j}$,并转换为对应的整数 $a,b,a^1_{i,j},...,a^{K-2}_{i,j}$.

通过 a,b 可还原得到 $s_{i,j}$=2×a+b/128, $s^p_{i,j}=(b/2) \bmod 32$ 和 $a^0_{i,j}=b \bmod 2$,从而恢复出秘密像素 $s_{i,j}$ 和备份像素 $s^p_{i,j}$ 及对应的 7K-13 位认证信息 $a^0_{i,j},a^1_{i,j},...,a^{K-2}_{i,j}$.在认证时,对秘密像素 $s_{i,j}$ 和备份像素 $s^p_{i,j}$ 再次按公式(11)和公式(12)计算认证信息 $a'^0_{i,j},a'^1_{i,j},...,a'^{K-2}_{i,j}$,并验证它们是否与恢复出的认证信息 $a^0_{i,j},a^1_{i,j},...,a^{K-2}_{i,j}$ 一致:若 $a'^0_{i,j},a'^1_{i,j},...,a'^{K-2}_{i,j}$ 和 $a^0_{i,j},a^1_{i,j},...,a^{K-2}_{i,j}$ 全部相等,则表明秘密像素 $s_{i,j}$ 和备份像素 $s^p_{i,j}$ 通过第 2 重认证,并在认证图 $\boldsymbol{A}=(a_{i,j})_{m\times n}$ 上标记 $a_{i,j}$=1;否则,不通过认证,标记 $a_{i,j}$=0.上述对秘密像素 $s_{i,j}$ 和备份像素 $s^p_{i,j}$ 的认证策略,即为第 2 重认证策略.

图 7 给出了第 2 重认证流程图.

由于第 1 重认证只有 1 位认证比特,认证能力较弱,可能导致 $(\dot{num}_1, f^{i,j}_{GF}(\dot{num}_1)),(\dot{num}_2, f^{i,j}_{GF}(\dot{num}_2)),...,(\dot{num}_t, f^{i,j}_{GF}(\dot{num}_t))$ 存在第 1 重认证通过的被攻击像素,然而第 2 重认证包含 7K–13 位认证信息可对秘密像素 $s_{i,j}$ 和备份像素 $s^p_{i,j}$ 进行高精度认证,从而第 1 重认证结果得以纠正.

若 $(\dot{num}_1, f^{i,j}_{GF}(\dot{num}_1)),(\dot{num}_2, f^{i,j}_{GF}(\dot{num}_2)),...,(\dot{num}_t, f^{i,j}_{GF}(\dot{num}_t))$ 中存在大于等于 K 个像素没被攻击,此时可对参与恢复的任意 K 个分存值对进行枚举,直至确定其是否可以通过第 2 重认证.对分存信息的第 1 重认证和对秘密像素和备份像素的第 2 重认证,构成了本文的双认证策略.通过双认证,分存信息认证通过概率为 1/2,秘密像素被恶意攻击通过认证的最大可能概率仅为$(1/2)^{7K-13}$,对秘密像素 7K-13 位认证位会随着门限 K 的增长而增大,从而本文策略的认证能力也在增强.若同时考虑对分存信息和秘密像素的认证比特,则本文的综合认证能力可达$(1/2)^{7K-12}$.因此,相对于文献[10,35]仅对秘密像素有 8 位、4 位认证位和文献[11,36,37]仅对分存信息有 8 位、

4 位和 3 位认证位,所提策略具备更强的认证能力.文献[10,11,35−37]的门限 K 至少为 3 且不会随着门限改变而增强其认证能力,而本文策略在 K=3 时,综合认证能力至少为 $1/2^9$,因此在同等情况下,相对于文献[10,11,35−37],认证策略更优.

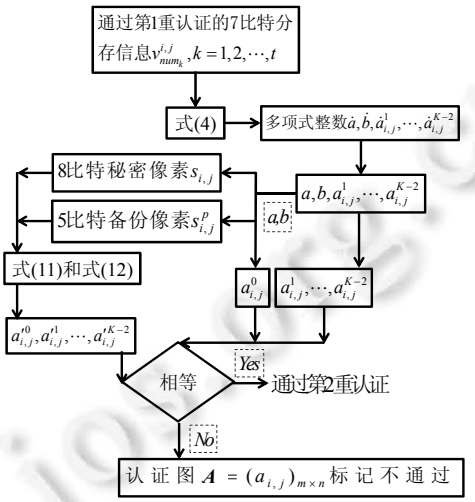


Fig.7 Flow chart of the second authentication

图 7 第 2 重认证流程图

4.2 结合非等量备份的修复参考图构建策略

通过第 4.1 节可得初步密图 $\boldsymbol{S}=(s_{i,j})_{m\times n}$、备份图 $\boldsymbol{S}^p=(s_{i,j}^p)_{m\times n}$ 和认证图 $\boldsymbol{A}=(a_{i,j})_{m\times n}$.这里,可利用 $\boldsymbol{S}^p$ 和 $\boldsymbol{A}$ 重建子带 $\boldsymbol{S}_{LL}=(s_{i,j}^{LL})_{m/2\times n/2}$,并对 $\boldsymbol{S}_{LL}$ 做一级逆离散小波变换,来得到修复参考图 $\boldsymbol{S}'=(s_{i,j}')_{m\times n}$,然后用于第 4.3 节的密图修复.记 $\boldsymbol{S}_{LL}$ 置乱恢复前子带为 $\boldsymbol{S}'_{LL}=(s_{i,j}'^{LL})_{m/2\times n/2}$,子带像素 $s_{i,j}'^{LL}$ 由 $\boldsymbol{S}^p$ 中的 $s_{i,j}^p,s_{i+m/2,j}^p,s_{i,j+n/2}^p$ 和 $s_{i+m/2,j+n/2}^p$ 以及 $\boldsymbol{A}$ 中的 $a_{i,j},a_{i+m/2,j},a_{i,j+n/2}$ 和 $a_{i+m/2,j+n/2}$ 共同确定,其中,$0\leqslant i<m/2, 0\leqslant j<n/2$.由于本文采用基于比特位重要程度分组的非等量备份策略,因此置乱恢复前子带像素 $s_{i,j}'^{LL}$ 中的每位比特被分别以不同的数量存储于备份像素 $s_{i,j}^p,s_{i+m/2,j}^p,s_{i,j+n/2}^p$ 和 $s_{i+m/2,j+n/2}^p$ 的不同位置.考虑到即使进行第 2 重高精度认证也依然存在一定误判概率,因此,本文是通过认证备份像素同一比特的平均值来对 $s_{i,j}'^{LL}$ 中的每个比特进行恢复.记 $cnt_k,k=0,1,\ldots,7$ 表示 $s_{i,j}^p,s_{i+m/2,j}^p,s_{i,j+n/2}^p$ 和 $s_{i+m/2,j+n/2}^p$ 存储的子带像素 $s_{i,j}'^{LL}$ 的第 k 个比特位通过认证的次数,$sum_k,k=0,1,\ldots,7$ 表示 $s_{i,j}'^{LL}$ 通过认证的第 k 个比特位的累计值.初始化 $cnt_k=0,sum_k=0,k=0,1,\ldots,7$,本文计算 $s_{i,j}'^{LL}$ 的具体方法为:对 $s_{i,j}'^{LL}$ 第 k 位 bit_k,可通过 $s_{i,j}^p,s_{i+m/2,j}^p,s_{i,j+n/2}^p$ 和 $s_{i+m/2,j+n/2}^p$ 与 $a_{i,j},a_{i+m/2,j},a_{i,j+n/2}$ 和 $a_{i+m/2,j+n/2}$ 计算其通过认证的次数 cnt_k 和对应的认证累计值 sum_k,若 $cnt_k>0$,取 sum_k/cnt_k 的四舍五入值作为 bit_k 的值.图 8 给出了修复参考图构建流程.

例如:以 $s_{i,j}^p$ 和 $a_{i,j}$ 为例,对于 $s_{i,j}^p$,

- 若 $a_{i,j}=1$,由公式(10)可知 $s_{i,j}^p=(l_7l_6l_5l_3l_2)_2$,则可分别为 $cnt_7,cnt_6,cnt_5,cnt_3,cnt_2$ 增加 1,然后,通过下列公式更新 $sum_7,sum_6,sum_5,sum_3,sum_2$:

$$sum_7=sum_7+(\lfloor s_{i,j}^p/16\rfloor \bmod 2),$$
$$sum_6=sum_6+(\lfloor s_{i,j}^p/8\rfloor \bmod 2),$$
$$sum_5=sum_5+(\lfloor s_{i,j}^p/4\rfloor \bmod 2),$$
$$sum_3=sum_3+(\lfloor s_{i,j}^p/2\rfloor \bmod 2),$$
$$sum_2=sum_2+(s_{i,j}^p \bmod 2).$$

同样,$s^p_{i+m/2,j}$ 和 $a_{i+m/2,j}$ 用来更新 $cnt_7,cnt_6,cnt_5,cnt_4,cnt_1$ 和 $sum_7,sum_6,sum_5,sum_4,sum_1$,对 $s^p_{i,j+n/2},a_{i,j+n/2}$ 和 $s^p_{i+m/2,j+n/2},a_{i+m/2,j+n/2}$ 也做类似处理;

- 反之,若 $a_{i,j}$=0,则不做任何处理.

经上述处理后,可得到更新后的 cnt_i,sum_i,i=0,1,…,7.最后,用公式(18)和公式(19)确定 $\boldsymbol{S}'_{LL}$ 中 $s'^{LL}_{i,j}$ 的值:

$$f(k,cnt_k,sum_k)=\begin{cases}[sum_k/cnt_k]\times 2^k, & cnt_k>0\\ \lfloor 2^k/2\rfloor, & cnt_k=0\end{cases} \tag{18}$$

$$s'^{LL}_{i,j}=\sum_{k=0}^{7} f(k,cnt_k,sum_k) \tag{19}$$

公式(18)中,[]表示四舍五入取整,而⌊⌋表示向下取整.对 $s'^{LL}_{i,j}$ 的第 $k(0\leqslant k\leqslant 7)$位,若 cnt_k>0,表示该位认证通过 cnt_k 个,在这种情况下,可能存在较小概率使得认证通过值不全相等,所以本文取平均认证结果作为该位最终值,即,把 sum_k/cnt_k 的四舍五入值作为该位值.而对于 cnt_k=0,本文取其期望值 1/2,以减少与像素真实值之间的误差.当处理完所有像素得到 $\boldsymbol{S}'_{LL}$,对其使用 *Key* 做逆置乱,得到 $\boldsymbol{S}$ 的 1 级离散小波变换的 LL 子带部分 $\boldsymbol{S}_{LL}$,此时,可将其他子带置为 0,做 1 次逆离散小波变换,得到密图修复参考图 $\boldsymbol{S}'=(s'_{i,j})_{m\times n}$,并用于恢复密图修复.

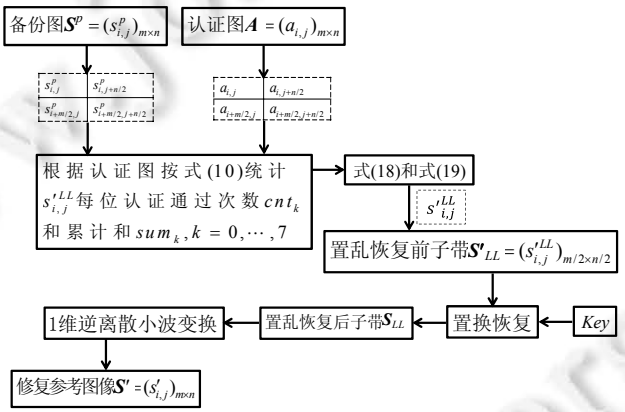


Fig.8 Flow chart of repaired reference image construction

图 8 修复参考图构建流程图

4.3 结合邻近像素点插值拟合和修复参考图像素替代的密图自恢复策略

经第 4.1 节和第 4.2 节的处理,可得到初步密图 $\boldsymbol{S}=(s_{i,j})_{m\times n}$、认证图 $\boldsymbol{A}=(a_{i,j})_{m\times n}$ 和密图修复参考图 $\boldsymbol{S}'=(s'_{i,j})_{m\times n}$.文献[11]是直接用修复参考图的对应位置像素来替代密图中未通过认证的像素,而未考虑自然图像的邻近相关性导致密图修复质量偏低.为提高密图的自恢复能力,本文充分考虑自然图像的邻近像素相关性来对未通过认证的像素进行插值拟合修复,在无法进行插值拟合的情况下,再使用修复参考图对应的位置像素对密图进行自恢复操作.

对于任意位置,

- 若认证图元素 $a_{i,j}$=1,则表示 $s_{i,j}$ 认证通过,此时不需要进行修复,将 $s_{i,j}$ 作为最终密图同位置像素;
- 若 $a_{i,j}$=0,此时表示 $s_{i,j}$ 未通过认证,需对其进行修复,记位置(i,j)的 8-邻域为$(i-1,j-1),(i-1,j),(i-1,j+1),(i,j-1),(i,j+1),(i+1,j-1),(i+1,j),(i+1,j+1)$,统计这 8 个位置通过认证的位置个数,将其记为 $cntt_{i,j}$.若 8-邻域中某个位置坐标不存在,则认为其认证不通过.

这里,根据 $cntt_{i,j}$<4 或 $cntt_{i,j}\geqslant 4$ 两种情况来对秘密像素进行修复.

① $cntt_{i,j}$<4,令 $s_{i,j}=s'_{i,j}$,即,直接使用修复参考图 $\boldsymbol{S}'=(s'_{i,j})_{m\times n}$ 对应的位置像素来修复 $s_{i,j}$;

② 若 $cntt_{i,j}\geqslant 4$,表示 $s_{i,j}$ 周围的大部分 8-邻域像素没有遭受攻击,而自然图像的邻近像素相关性强,因此可使用 8-邻域像素认证通过的像素来逼近 $s_{i,j}$,将比直接使用修复参考图 $\boldsymbol{S}'=(s'_{i,j})_{m\times n}$ 上对应的位置像素 $s'_{i,j}$ 对 $s_{i,j}$ 进行替代具有更好的修复效果.原因是将除 LL 子带的其他子带值全设为 0,通过逆离散小波变换,等价为用 2×2 小块均值进行替代.记 $s_{i,j}$ 的 8-邻域认证通过的像素位置和像素值分别为 (x_0+i,y_0+j), $(x_1+i,y_1+j),...,(x_{cntt_{i,j}}+i,y_{cntt_{i,j}}+j)$ 和 $z_0,z_1,...,z_{cntt_{i,j}}$,若 $cntt_{i,j}\geqslant 4$,此时可用多项式 $h(x,y)=h_0+h_1x+h_2y+h_3xy$ 来拟合这些认证通过的像素.为防止拟合结果和真实值相差较大,这里将 $cntt_{i,j}\geqslant 4$ 和 $|h_0-s'_{i,j}|\leqslant 4$ 作为限制条件,若 $|h_0-s'_{i,j}|\leqslant 4$,则令 $s_{i,j}=h_0$;否则,令 $s_{i,j}=s'_{i,j}$.

求拟合多项式 $h(x,y)=h_0+h_1x+h_2y+h_3xy$ 的方法主要有两种:一种是最小二乘法,另一种是经典梯度下降法.这里按梯度下降法来拟合多项式,主要步骤是:先初始化 $h_0^{(0)},h_1^{(0)},h_2^{(0)},h_3^{(0)}$ 为 0,然后用公式(20)对 $h_0^{(0)},h_1^{(0)},h_2^{(0)},h_3^{(0)}$ 进行迭代,直至拟合多项式趋于稳定或迭代次数超过指定迭代次数.

$$\left.\begin{aligned}
h_0^{(t+1)}&=h_0^{(t)}-\theta\sum_{l=0}^{cntt_{i,j}}(h^{(t)}(x_l,y_l)-z_l)\times 1\\
h_1^{(t+1)}&=h_1^{(t)}-\theta\sum_{l=0}^{cntt_{i,j}}(h^{(t)}(x_l,y_l)-z_l)\times x_l\\
h_2^{(t+1)}&=h_2^{(t)}-\theta\sum_{l=0}^{cntt_{i,j}}(h^{(t)}(x_l,y_l)-z_l)\times y_l\\
h_3^{(t+1)}&=h_3^{(t)}-\theta\sum_{l=0}^{cntt_{i,j}}(h^{(t)}(x_l,y_l)-z_l)\times x_ly_l
\end{aligned}\right\} \tag{20}$$

其中,θ为迭代步长,通常设置为较小数值或随迭代次数的增加而逐渐变小;而 $h^{(t)}(x_l,y_l)=h_0^t+h_1^tx_l+h_2^ty_l+h_3^tx_ly_l$. 利用公式(20)可得到 h_0,h_1,h_2,h_3 的拟合值 $\hat{h}_0,\hat{h}_1,\hat{h}_2,\hat{h}_3$,然后令 $s_{i,j}=h(0,0)=\hat{h}_0$,并把 $s_{i,j}$ 约束为 0~255 间的整数,若满足 $|s_{i,j}-s'_{i,j}|\leqslant 4$,则保留 $s_{i,j}$;否则,令 $s_{i,j}=s'_{i,j}$ 作为 $s_{i,j}$ 的最终修复值.当处理完密图所有认证未通过像素,即可得到自恢复后的密图 $\boldsymbol{S}=(s_{i,j})_{m\times n}$.图 9 给出了结合邻近像素插值拟合和修复参考图像素替代的密图自恢复流程.

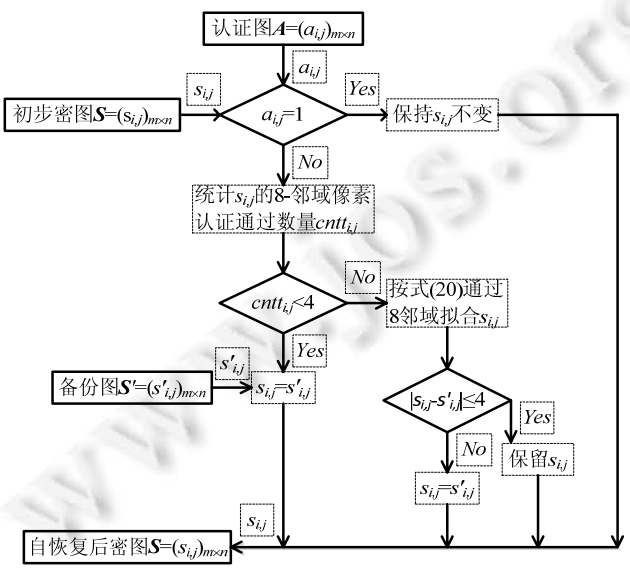


Fig.9 Flow chart of self-recovered secret image

图 9 密图自恢复流程图

与文献[11]相比,所述策略不仅用备份图来修复密图认证不通过的像素,还充分考虑了自然图像邻近像素

的相关性,对于认证不通过的像素,若其周围大多数像素通过认证,则可通过这些像素来对认证不通过的像素进行拟合修复.

4.4 结合非等量备份和双认证有限域图像恢复算法

结合第 4.1 节~第 4.3 节的工作,可得到结合非等量备份和双认证有限域图像恢复算法,记为算法 2.

算法 2. 结合非等量备份和双认证有限域图像恢复算法.

输入:子密钥 $subkey_{num_1},subkey_{num_2},...,subkey_{num_t}$ 和嵌入分存信息后掩体 $\boldsymbol{C}'^{num_k}=(c'^{num_k}_{i,j})_{2m\times 2n},k=1,2,...,t$;

输出:修复后密图 $\boldsymbol{S}=(s_{i,j})_{m\times n}$ 和认证图 $\boldsymbol{A}=(a_{i,j})_{m\times n}$.

第 1 步:若合法子密钥小于 K,则恢复失败;反之,通过子密钥 $subkey_{num_1},subkey_{num_2},...,subkey_{num_t}$ (为便于描述,假设所有子密钥均合法),用公式(2)恢复出密钥 Key;

第 2 步:提取掩体 $\boldsymbol{C}'^{num_k}=(c'^{num_k}_{i,j})_{2m\times 2n},k=1,2,...,t$ 上的 2×2 分块 $\boldsymbol{B}'^{num_k}_{i,j}$ 嵌入分存信息 $v^{i,j}_{num_k}$ 和它的 1 位认证信息 $va^{i,j}_{num_k}$,并检验第 1 重认证结果;

第 3 步:若存在大于等于 K 个 $v^{i,j}_{num_k},k=1,2,...,t$ 通过第 1 重认证,则使用公式(4)还原 $s_{i,j}$, $s^p_{i,j}$ 和 $a^0_{i,j},a^1_{i,j},...,a^{K-1}_{i,j}$ 并检验第 2 重认证结果;

第 4 步:若 $s_{i,j}$ 和 $s^p_{i,j}$ 通过双认证,则设置认证结果 $a_{i,j}$=1;否则,$a_{i,j}$=0;

第 5 步:重复第 1 步~第 4 步,直至处理完所有位置,得到初步密图 $\boldsymbol{S}=(s_{i,j})_{m\times n}$、备份图 $\boldsymbol{S}^p=(s^p_{i,j})_{m\times n}$ 和认证图 $\boldsymbol{A}=(a_{i,j})_{m\times n}$;

第 6 步:使用认证图 $\boldsymbol{A}=(a_{i,j})_{m\times n}$ 和备份图 $\boldsymbol{S}^p=(s^p_{i,j})_{m\times n}$ 重建出 $\boldsymbol{S}'_{LL}=(s'^{LL}_{i,j})_{m/2\times n/2}$,并对其用 Key 做逆置乱和逆离散小波变换,得到密图修复参考图 $\boldsymbol{S}'=(s'_{i,j})_{m\times n}$;

第 7 步:对于密图像素 $s_{i,j}$,若 $a_{i,j}$=1,则不修改其值;否则,转第 8 步;

第 8 步:统计 $s_{i,j}$ 周围 8-邻域像素通过的认证数量 $cntt_{i,j}$:若 $cntt_{i,j}$<4,则用 $\boldsymbol{S}'=(s'_{i,j})_{m\times n}$ 的 $s'_{i,j}$ 作为 $s_{i,j}$;否则,转第 9 步;

第 9 步:按公式(20)使用 $s_{i,j}$ 周围 8-邻域像素认证通过的像素来对 $s_{i,j}$ 拟合,将拟合出的 $s_{i,j}$ 约束为 0-255 间的整数,若 $|s_{i,j}-s'_{i,j}|\leqslant 4$,则保留 $s_{i,j}$;否则,令 $s_{i,j}=s'_{i,j}$;

第 10 步:处理完所有位置之后,可得修复后密图 $\boldsymbol{S}=(s_{i,j})_{m\times n}$.

在算法 2 中:

- 步骤 1 用于验证每个参与者子密钥的合法性,以防止参与者恶意篡改子密钥;
- 步骤 2~步骤 5 由掩体提取出分存信息进行第 1 重认证,若能恢复出秘密像素,则进行第 2 重认证,从而得到初步密图、备份图和认证图.相比文献[11,36,37],双认证具备更好的认证能力;
- 步骤 6 通过认证图和备份图做逆置乱和逆离散小波变换,得到密图修复参考图.通过非等量备份,相比于文献[11]等量备份策略具备更好的修复能力和抗攻击能力.
- 步骤 7~步骤 10 用于密图自修复,相对文献[11,36,37]的直接像素替代策略,所提策略进一步考虑利用自然图像邻近像素的相关性来对密图进行恢复,从而进一步提高了密图恢复质量.

此外,上述算法的步骤 3、步骤 4 还可充分使用第 2 重认证能力,即枚举任意 K 个 $v^{i,j}_{num_k},k=1,2,...,t$ 来进一步提高 $s_{i,j}$ 和 $s^p_{i,j}$ 的成功恢复概率.

5 实 验

以下对本文所提策略进行实验验证,并将所提策略与文献[10,11,27,29,30,36,37]进行实验比较.实验测试环境为 Windows 7 操作系统,CPU 为 AMD FX(tm)-8320 8 核 CPU,单处理核心主频为 3.50GHz,内存为 16.00GB,实验编码语言为 JAVA jdk1.8.0_20.取密钥 Key=131819,密钥分存 Lagrange 多项式模数为 1 000 000 007.

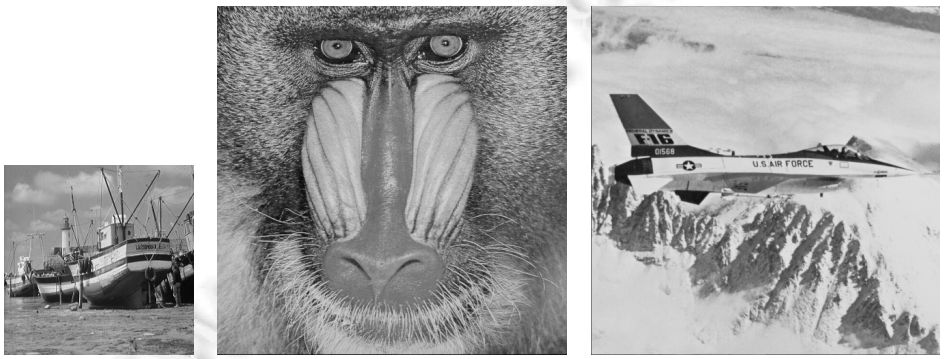
实验测试图像为 USC-SIPI 标准测试图样,采用图 10(a),分辨率为 256×256 灰度图像 Boats 作为密图,图

10(b)~图 10(f)所示,分辨率为 512×512 灰度图像 Baboon,F16,Sailboat,Lena 和 Peppers 作为掩体图像.为客观评价图像,用公式(21)的 MSE 度量图像差异,用公式(22)的 PSNR 衡量图像视觉质量:

$$MSE=\frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(p_{i,j}-p'_{i,j})^2}{m\times n} \tag{21}$$

$$PSNR=10\log_{10}\frac{255^2}{MSE} \tag{22}$$

公式(21)中, $p_{i,j},p'_{i,j}$ 为待比较两幅图像像素值.此外,本文还采用攻击识别率衡量所提策略的认证能力,攻击识别率定义为密图正确识别被攻击像素数占密图被攻击像素总数的比率.



(a) Boats (b) Baboon (c) F16

(d) Sailboat (e) Lena (f) Peppers

Fig.10 Experimental images

图 10 实验测试图像

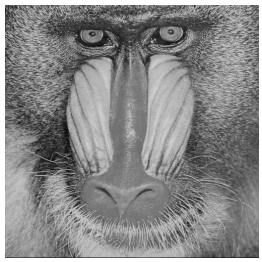
5.1 密图分存与恢复验证实验

将图 10(a)按算法 1 进行(3,5)门限分存,得到分发掩体如图 11(a)~图 11(e)所示,相对于图 10(b)~图 10(f)的 PSNR 分别为 46.35dB,46.36dB,46.36dB,46.38dB,46.38dB.表明分发掩体具有较高视觉质量,攻击者难以发现嵌入分存信息.

对图 11 分发掩体可按算法 2 恢复,这里按参与者提供正确子密钥和分发掩体进行恢复,恢复参数和恢复结果如表 4 和图 12 所示.表中"–"表示不存在.从表 4 和图 12 结果可看出:只有参与恢复掩体和子密钥数量不小于门限 3,才能无损恢复出密图;若子密钥数量小于门限 3 时,将无法恢复出 *Key*,从而恢复失败.

表 5 给出了参与者保管的子密钥、分发掩体和第 3 方公信方存储的 MD5 值.

表 6 是以参与者 1 为恶意参与者,对子密钥进行篡改的 MD5 值.


(a) 分发掩体 1


(b) 分发掩体 2


(c) 分发掩体 3


(d) 分发掩体 4

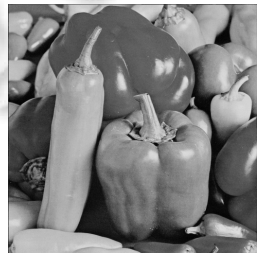

(e) 分发掩体 5

Fig.11 Distributed cover images

图 11 分发掩体

Table 4 Secret image recovery variables

表 4 密图的恢复参数

编号	参与图像	恢复密图	密图	MSE
1	图 11(a)~图 11(c)	图 12(a)	图 10(a)	0
2	图 11(b)~图 11(d)	图 12(b)		0
3	图 11(a)、图 11(c)、图 11(e)	图 12(c)		0
4	图 11(a)~图 11(d)	图 12(d)		0
5	图 11(b)~图 11(e)	图 12(e)		0
6	图 11(a)~图 11(e)	图 12(f)		0
7	图 11(a)、图 11(b)	–		–
8	图 11(a)	–		–


(a) 第 1 组恢复结果


(b) 第 2 组恢复结果


(c) 第 3 组恢复结果


(d) 第 4 组恢复结果


(e) 第 5 组恢复结果


(f) 第 6 组恢复结果

Fig.12 Recovered images

图 12 恢复图样

Table 5 Participant distributed information

表 5 参与者分发信息

参与者标号	分发子密钥	掩体	第 3 方存储的 MD5
1	1845480	图 11(a)	0xf17a011ceba20886dbcd8b2ac3695c12
2	3559167	图 11(b)	0xe2a7bcc2df75fcca1918be812d40e541
3	5272880	图 11(c)	0x63e80f9cb22816ec36c9b54f11b75e93
4	6986619	图 11(d)	0xfe69be6a745b8b3f3df3b9effc7d1bd1
5	8700384	图 11(e)	0x5eaa34c8e66cc5c4958e069ef9b4e57b

Table 6 Verify results of the sub-key's validity

表 6 子密钥认证有效性验证结果

篡改后的子密钥	子密钥对应的 MD5	第 3 方存储的 MD5
1845479	0x51085133a086258f7162f776e10a6949	0xf17a011ceba20886dbcd8b2ac3695c12
1845481	0x4f4a2433fd13d00f36ae84398e6fe27f	0xf17a011ceba20886dbcd8b2ac3695c12
18454800	0x1d0c8f13dfdeee8d690783fdaa2c01a0	0xf17a011ceba20886dbcd8b2ac3695c12
11845480	0xe743befd638042a41b4be901240cbb9d	0xf17a011ceba20886dbcd8b2ac3695c12
118454	0xfd4ffd379afdd5afb5a0bb28ba1169cc	0xf17a011ceba20886dbcd8b2ac3695c12
11	0x6512bd43d9caa6e02c990b0a82652dca	0xf17a011ceba20886dbcd8b2ac3695c12
666666	0xf379eaf3c831b04de153469d1bec345e	0xf17a011ceba20886dbcd8b2ac3695c12
1324354353	0x6d34fe122a255af207b2034f6e45789b	0xf17a011ceba20886dbcd8b2ac3695c12

从表 6 可看出,参与者篡改子密钥将会被第三方存储的 MD5 值直接鉴别出来.

5.2 非等量备份策略有效性验证实验

为验证非等量备份策略的有效性,对图 10(a)进行小波变换,取其 LL 子带置乱后,分别按文献[11]的等量备份策略构造备份图 1 和本文的非等量备份策略构造备份图 2.然后,对备份图 1 和备份图 2 分别施加强度为 1%,5%,10%,20%,30%,50%的随机噪声,对备份图 1 和备份图 2 正确重构出的 LL 子带的各比特位面概率以及对应的 *MSE* 进行统计.表 7 和表 8 给出了具体实验结果.

Table 7 Recovery results of Ref.[11]'s backup image construction method

表 7 文献[11]的备份图构造方法的恢复结果

攻击力度(%)	l_7 (%)	l_6 (%)	l_5 (%)	l_4 (%)	l_3 (%)	l_2 (%)	l_1 (%)	l_0 (%)	MSE
0	100	100	100	100	100	100	100	100	0
1	99.99	100	99.99	100	99.99	100	99.99	100	0.55
5	99.93	99.79	99.91	99.85	99.88	99.87	99.91	99.86	16.60
10	99.75	99.20	99.68	99.43	99.61	99.53	99.63	99.53	54.96
20	98.87	96.90	98.65	97.91	98.27	98.04	98.24	98.09	223.05
30	97.25	92.89	96.67	95.21	95.87	95.54	95.64	95.59	527.16
50	92.19	80.69	90.97	86.74	87.82	87.80	87.74	87.75	1461.53

Table 8 Recovery results of the proposed non-equivalent backup image construction method

表 8 本文备份图构造方法的恢复结果

攻击力度	l_7 (%)	l_6 (%)	l_5 (%)	l_4 (%)	l_3 (%)	l_2 (%)	l_1 (%)	l_0 (%)	MSE
0	100	100	100	100	100	100	100	100	0
1	100	100	100	100	99.99	99.99	99.45	98.51	0.02
5	100	100	99.98	99.97	99.85	99.87	96.98	92.64	0.19
10	100	100	99.91	99.84	99.39	99.49	93.95	85.87	0.71
20	99.92	99.93	99.50	98.89	97.37	98.05	86.36	73.63	4.90
30	99.48	99.45	98.34	96.84	93.52	95.36	78.35	63.75	21.14
50	95.83	95.32	92.47	87.75	81.28	87.54	62.11	50.00	145.86

从表 7 和表 8 可看出:针对随机噪声攻击,本文的 LL 子带恢复 MSE 远小于文献[11]对应方法的 LL 子带恢复 MSE.本文对 LL 子带高位比特 l_7,l_6,l_5 和 l_4 的恢复概率总是高于文献[11],说明对高位比特分组备份更多次的非等量备份策略是有效的;而本文的低位比特分组中,l_3,l_2,l_1 和 l_0 的恢复概率略低于文献[11],原因是由公式(18)累加恢复像素值的低位进位问题所导致的.但总体上,本文给出的非等量备份策略优于文献[11]的构造方法.

5.3 优化LSB嵌入策略有效性验证实验

这里也对本文使用的优化 LSB 嵌入策略的有效性进行实验验证,普通 LSB 法的 PSNR 与优化 LSB 法的 PSNR 对比结果见表 9.从表 9 可看出,使用优化 LSB 比普通 LSB 法嵌入掩体视觉质量平均提升 2.22dB,从而说明优化 LSB 法嵌入策略的有效性.

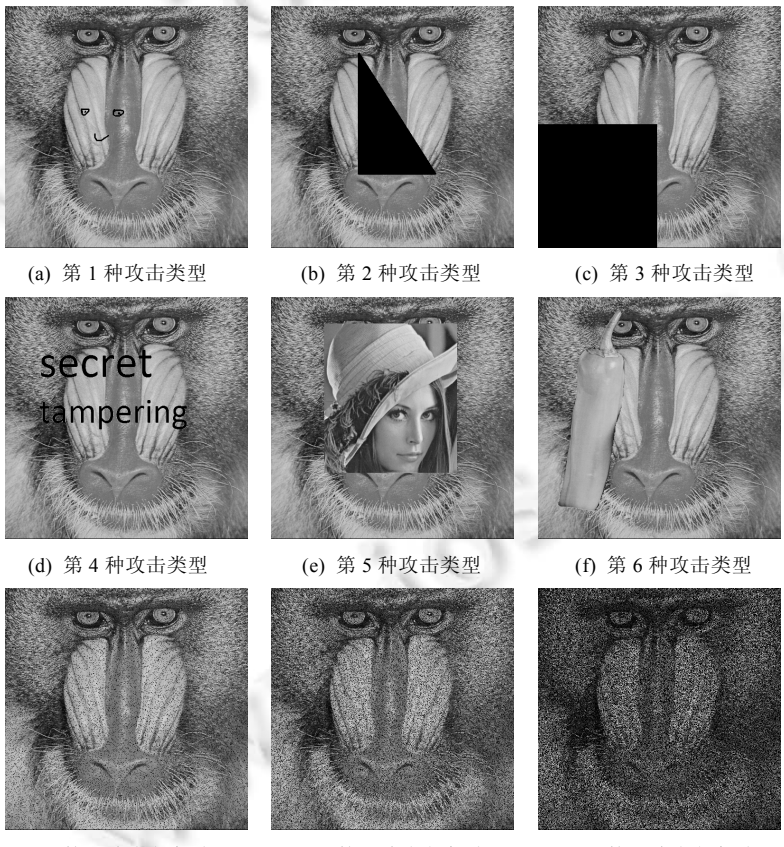
Table 9 Verify results of the optimized LSB embed strategries

表 9 优化 LSB 嵌入策略有效性验证结果

嵌入方法	掩体 1 (dB)	掩体 2 (dB)	掩体 3 (dB)	掩体 4 (dB)	掩体 5 (dB)
普通 LSB	44.14	44.19	44.15	44.16	44.14
优化 LSB	46.35	46.36	46.36	46.38	46.38
优化值	+2.21	+2.17	+2.21	+2.22	+2.24

5.4 双认证有效性验证实验

为验证双认证的有效性,以攻击图 11(a)分发掩体 1 为例,具体说明实验中所选择的攻击类型.其中,图 13(a)~图 13(d)为涂鸦或裁剪攻击,图 13(e)~图 13(f)为覆盖攻击,图 13(g)~图 13(i)为随机噪声攻击,噪声比率取 8%,20%和 50%.



(a) 第 1 种攻击类型 (b) 第 2 种攻击类型 (c) 第 3 种攻击类型

(d) 第 4 种攻击类型 (e) 第 5 种攻击类型 (f) 第 6 种攻击类型

(g) 第 7 种攻击类型 (h) 第 8 种攻击类型 (i) 第 9 种攻击类型

Fig.13 Examples of attacking and tampering images

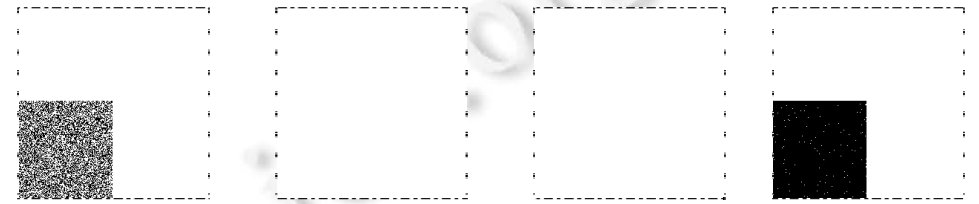
图 13 攻击和篡改图样示例

以参与者 1~参与者 3 携带的对应子密钥和掩体图 11(a)~图 11(c)参与恢复为例,对参与者 1~参与者 3 进行攻击,双认证结果如表 10 和图 14 所示.

Table 10 Double authentication results of the attacked cover images

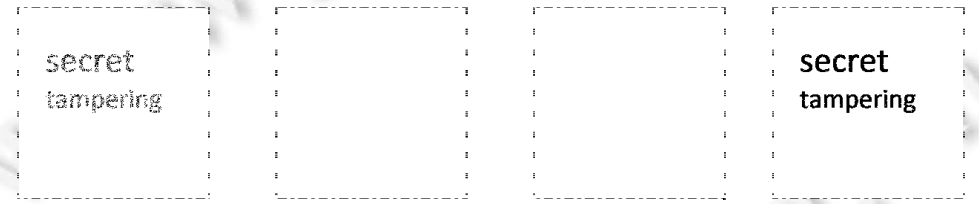
表 10 对掩体攻击的双认证结果

标号	掩体 1 攻击类型	掩体 2 攻击类型	掩体 3 攻击类型	认证图	攻击最终识别比率 (%)	第 1 重认证识别比率 (%)	第 2 重认证识别比率 (%)
1	图 13(c)	–	–	图 14(a)	99.85	50.40	49.60
2	图 13(d)	–	–	图 14(b)	99.74	50.06	49.94
3	图 13(g)	–	–	图 14(c)	99.83	53.67	46.33
4	图 13(b)	图 13(e)	–	图 14(d)	99.83	56.58	43.42
5	图 13(b)	图 13(g)	–	图 14(e)	99.85	54.87	45.13
6	图 13(g)	图 13(h)	–	图 14(f)	99.82	58.05	49.95
7	图 13(a)	图 13(b)	图 13(d)	图 14(g)	99.85	51.20	48.80
8	图 13(d)	图 13(f)	图 13(g)	图 14(h)	99.84	56.32	43.68
9	图 13(c)	图 13(e)	图 13(i)	图 14(i)	99.86	63.39	36.61



掩体 1 的第 1 重认证结果　掩体 2 的第 1 重认证结果　掩体 3 的第 1 重认证结果　最终认证图

(a) 第 1 组攻击双认证结果图

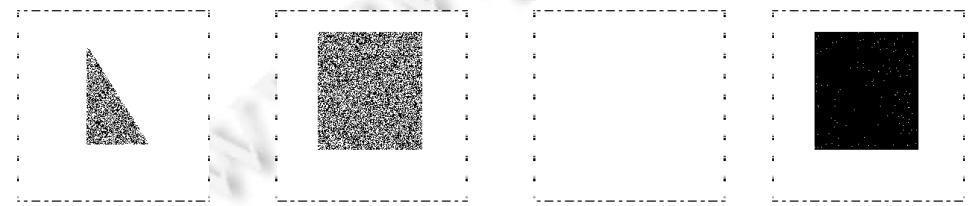


掩体 1 的第 1 重认证结果　掩体 2 的第 1 重认证结果　掩体 3 的第 1 重认证结果　最终认证图

(b) 第 2 组攻击双认证结果图

掩体 1 的第 1 重认证结果　掩体 2 的第 1 重认证结果　掩体 3 的第 1 重认证结果　最终认证图

(c) 第 3 组攻击双认证结果图

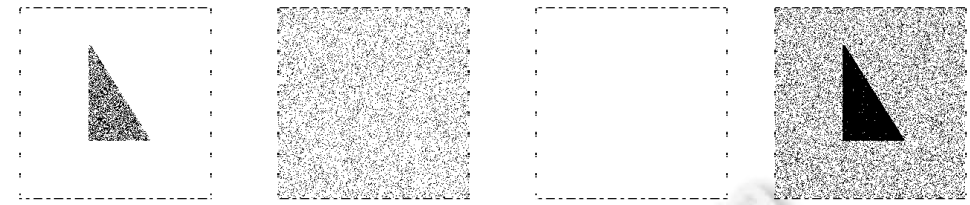


掩体 1 的第 1 重认证结果　掩体 2 的第 1 重认证结果　掩体 3 的第 1 重认证结果　最终认证图

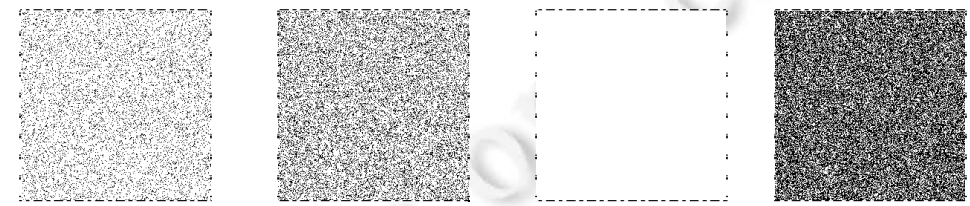
(d) 第 4 组攻击双认证结果图

Fig.14 Double authentication results

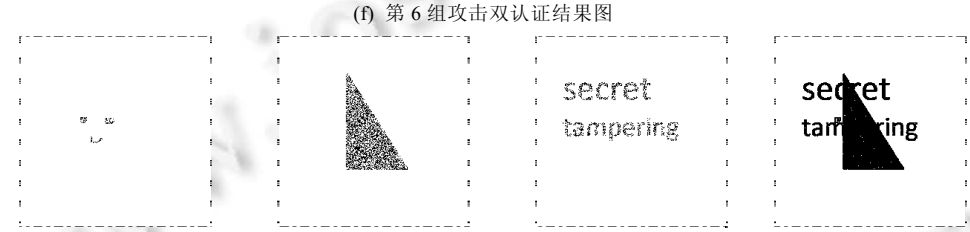
图 14 双认证结果



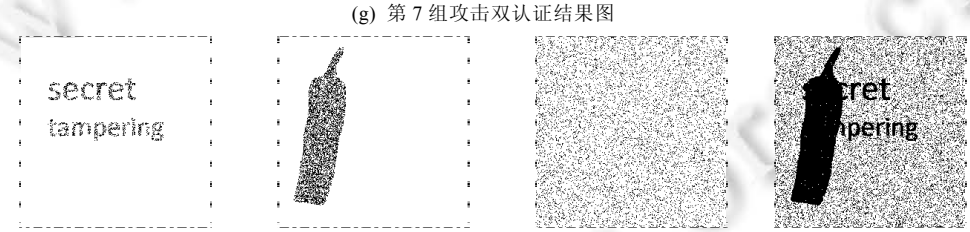
(e) 第 5 组攻击双认证结果图



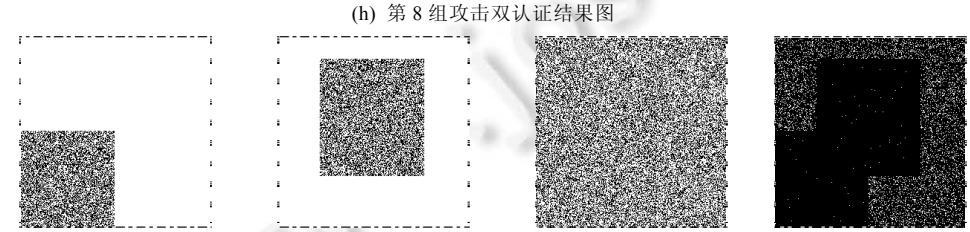
(f) 第 6 组攻击双认证结果图



(g) 第 7 组攻击双认证结果图



(h) 第 8 组攻击双认证结果图



(i) 第 9 组攻击双认证结果图

Fig.14 Double authentication results (Continued)

图 14 双认证结果(续)

从图 14 的第 1 重认证图可看出每个掩体攻击的大致轮廓,从最终认证图可清晰发现每个掩体遭受攻击的叠加图.

由表 10 可知,本文策略的攻击识别比率接近于 511/512.其中,第 1 重认证识别比率大于或接近 50%,标号 3~

标号 9 攻击样式第 1 重认证识别比率明显大于 50%.这是因为存在较多同一秘密像素多个分存信息遭受攻击.表 10 和图 14 表明,本文的双认证策略是有效的.

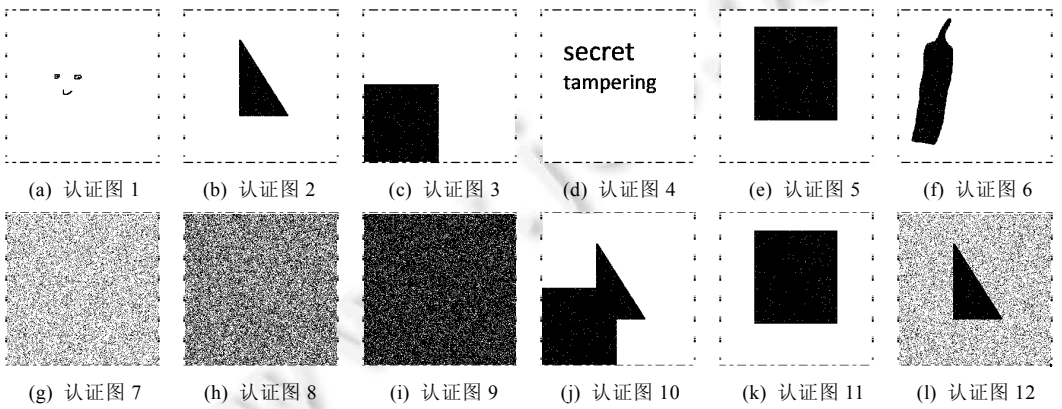
5.5 修复参考图与插值拟合有效性验证实验

为验证修复参考图与插值拟合有效性,以参与者 1~参与者 3 携带的对应子密钥和掩体图 11(a)~图 11(c)参与恢复为例,对参与者 1~参与者 3 进行攻击、认证和恢复,结果如表 11、图 15 和图 16 所示.

Table 11 Recovery results of the the attacked cover images

表 11 对掩体攻击恢复结果

标号	掩体 1 攻击	掩体 2 攻击	掩体 3 攻击	认证图	恢复密图	恢复图像 PSNR(dB)	攻击识别率 (%)
1	图 13(a)	–	–	图 15(a)	图 16(a)	49.57	100
2	图 13(b)	–	–	图 15(b)	图 16(b)	32.58	99.79
3	图 13(c)	–	–	图 15(c)	图 16(c)	29.49	99.85
4	图 13(d)	–	–	图 15(d)	图 16(d)	36.71	99.74
5	图 13(e)	–	–	图 15(e)	图 16(e)	26.87	99.84
6	图 13(f)	–	–	图 15(f)	图 16(f)	33.04	99.76
7	图 13(g)	–	–	图 15(g)	图 16(g)	30.73	99.83
8	图 13(h)	–	–	图 15(h)	图 16(h)	25.92	99.84
9	图 13(i)	–	–	图 15(i)	图 16(i)	17.56	99.82
10	图 13(b)	图 13(c)	–	图 15(j)	图 16(j)	28.48	99.83
11	图 13(b)	图 13(e)	–	图 15(k)	图 16(k)	26.88	99.83
12	图 13(b)	图 13(g)	–	图 15(l)	图 16(l)	28.84	99.85
13	图 13(d)	图 13(f)	–	图 15(m)	图 16(m)	31.89	99.82
14	图 13(d)	图 13(h)	–	图 15(n)	图 16(n)	25.23	99.78
15	图 13(g)	图 13(h)	–	图 15(o)	图 16(o)	23.37	99.82
16	图 13(a)	图 13(b)	图 13(c)	图 15(p)	图 16(p)	28.52	99.84
17	图 13(d)	图 13(e)	图 13(f)	图 15(q)	图 16(q)	26.27	99.81
18	图 13(g)	图 13(h)	图 13(i)	图 15(r)	图 16(r)	15.78	99.86
19	图 13(a)	图 13(b)	图 13(d)	图 15(s)	图 16(s)	31.63	99.85
20	图 13(a)	图 13(b)	图 13(g)	图 15(t)	图 16(t)	28.99	99.85
21	图 13(d)	图 13(f)	图 13(g)	图 15(u)	图 16(u)	28.39	99.84
22	图 13(d)	图 13(f)	图 13(h)	图 15(v)	图 16(v)	24.12	99.82
23	图 13(g)	图 13(g)	图 13(g)	图 15(w)	图 16(w)	29.74	99.95
24	图 13(c)	图 13(e)	图 13(i)	图 15(x)	图 16(x)	15.98	99.86

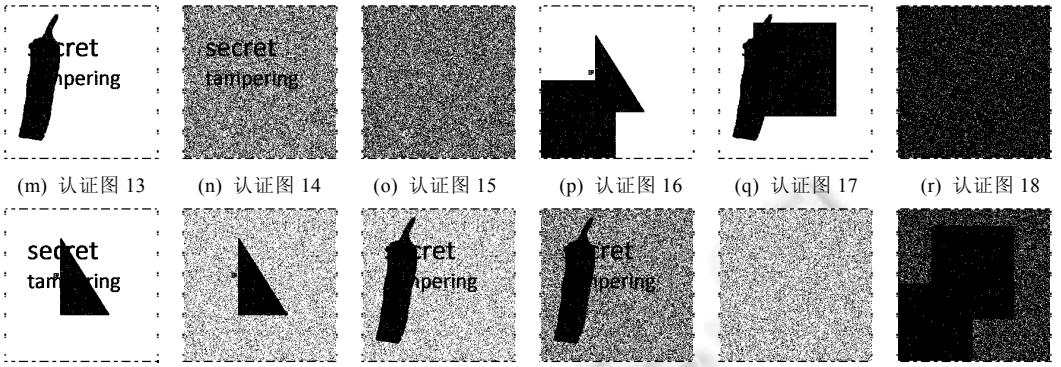


(a) 认证图 1 (b) 认证图 2 (c) 认证图 3 (d) 认证图 4 (e) 认证图 5 (f) 认证图 6

(g) 认证图 7 (h) 认证图 8 (i) 认证图 9 (j) 认证图 10 (k) 认证图 11 (l) 认证图 12

Fig.15 Authentication images of the proposed scheme after being attacked

图 15 所提策略攻击后的认证图



(m) 认证图 13 (n) 认证图 14 (o) 认证图 15 (p) 认证图 16 (q) 认证图 17 (r) 认证图 18

(s) 认证图 19 (t) 认证图 20 (u) 认证图 21 (v) 认证图 22 (w) 认证图 23 (x) 认证图 24

Fig.15 Authentication images of the proposed scheme after being attacked (Continued)

图 15 所提策略攻击后的认证图(续)

(a) 恢复图 1 (b) 恢复图 2 (c) 恢复图 3 (d) 恢复图 4 (e) 恢复图 5 (f) 恢复图 6

(g) 恢复图 7 (h) 恢复图 8 (i) 恢复图 9 (j) 恢复图 10 (k) 恢复图 11 (l) 恢复图 12

(m) 恢复图 13 (n) 恢复图 14 (o) 恢复图 15 (p) 恢复图 16 (q) 恢复图 17 (r) 恢复图 18

(s) 恢复图 19 (t) 恢复图 20 (u) 恢复图 21 (v) 恢复图 22 (w) 恢复图 23 (x) 恢复图 24

Fig.16 Recovery images of the proposed scheme after being attacked

图 16 所提策略的攻击恢复图

从表 11、图 15 可以看出攻击形状叠加,因为对每个攻击像素最多有 1/512 的概率逃脱认证,即识别比率约为 99.80%,而表 11 统计的攻击像素识别率都接近 99.80%,因而可验证这一点,说明本文策略具有较强的认证能力.从表 11 和图 16 可看出:对图 13 第 1 种~第 8 种类型攻击及其组合都具备较好的修复能力;而对图 13 第 9 种攻击类型(50%的噪声攻击),由于攻击粒度较大,几乎撒在了掩体所有 2×2 分块上,导致恢复结果较差;但总体上,本文策略具备较好的修复能力.为进一步验证修复参考图与插值拟合策略的有效性,本文对算法 2 不使用任何

修复手段得到的初步密图、只使用修复参考图替换修复和使用完整算法 2 进行修复得到的密图视觉质量进行对比,对比结果见表 12,表中用粗体标记 3 种策略的最优值.从表 12 可看出,所有攻击都是完整算法密图修复结果 PSNR 最高,若不使用任何修复手段,则恢复密图视觉质量非常低;只使用修复参考图替换修复,可较大程度提高密图的视觉质量,这说明本文的备份图构造策略十分有效.同样也可看到:使用完整算法修复的密图在没有噪声攻击情况下,PSNR 等同于只使用修复参考图替换修复 PSNR;而存在噪声攻击时,使用完整策略进行修复比只使用修复参考图替换修复 PSNR 有略微提高.这是因为在噪声攻击情况下,会有较大概率存在一个秘密像素被攻击而周围像素没有被攻击情况,这说明本文的插值拟合策略也是有效的.

Table 12 Validation results of the recovery strategies

表 12 修复策略有效性验证结果

标号	掩体 1 攻击	掩体 2 攻击	掩体 3 攻击	初步秘密图像 PSNR(dB)	只用替换修复 PSNR(dB)	完整算法 PSNR(dB)
1	图 13(a)	–	–	39.75	**49.57**	**49.57**
2	图 13(b)	–	–	23.27	**32.58**	**32.58**
3	图 13(c)	–	–	20.90	**29.49**	**29.49**
4	图 13(d)	–	–	28.32	**36.71**	**36.71**
5	图 13(e)	–	–	17.93	**26.87**	**26.87**
6	图 13(f)	–	–	24.05	**33.04**	**33.04**
7	图 13(g)	–	–	21.21	30.71	**30.73**
8	图 13(h)	–	–	17.76	25.72	**25.92**
9	图 13(i)	–	–	15.27	17.55	**17.56**
10	图 13(b)	图 13(c)	–	19.57	**28.48**	**28.48**
11	图 13(b)	图 13(e)	–	17.93	**26.88**	**26.88**
12	图 13(b)	图 13(g)	–	19.51	28.83	**28.84**
13	图 13(d)	图 13(f)	–	22.92	**31.89**	**31.89**
14	图 13(d)	图 13(h)	–	17.56	25.04	**25.23**
15	图 13(g)	图 13(h)	–	16.84	23.17	**23.37**
16	图 13(a)	图 13(b)	图 13(c)	19.56	**28.52**	**28.52**
17	图 13(d)	图 13(e)	图 13(f)	17.49	**26.27**	**26.27**
18	图 13(g)	图 13(h)	图 13(i)	14.86	**15.78**	**15.78**
19	图 13(a)	图 13(b)	图 13(d)	22.37	**31.63**	**31.63**
20	图 13(a)	图 13(b)	图 13(g)	19.53	28.95	**28.99**
21	图 13(d)	图 13(f)	图 13(g)	19.40	28.38	**28.39**
22	图 13(d)	图 13(f)	图 13(h)	17.09	23.95	**24.12**
23	图 13(g)	图 13(g)	图 13(g)	20.20	29.72	**29.74**
24	图 13(c)	图 13(e)	图 13(i)	14.87	**15.98**	**15.98**

5.6 与相关文献认证和修复能力对比实验

为验证本文策略相对其他文献的认证和修复能力,对文献[11]和文献[36]的分发掩体进行 24 种攻击(见表 11).实验结果见表 13 和如图 17~图 20 所示.

Table 13 Recovery results of Ref.[11] and Ref.[36] after being attacked

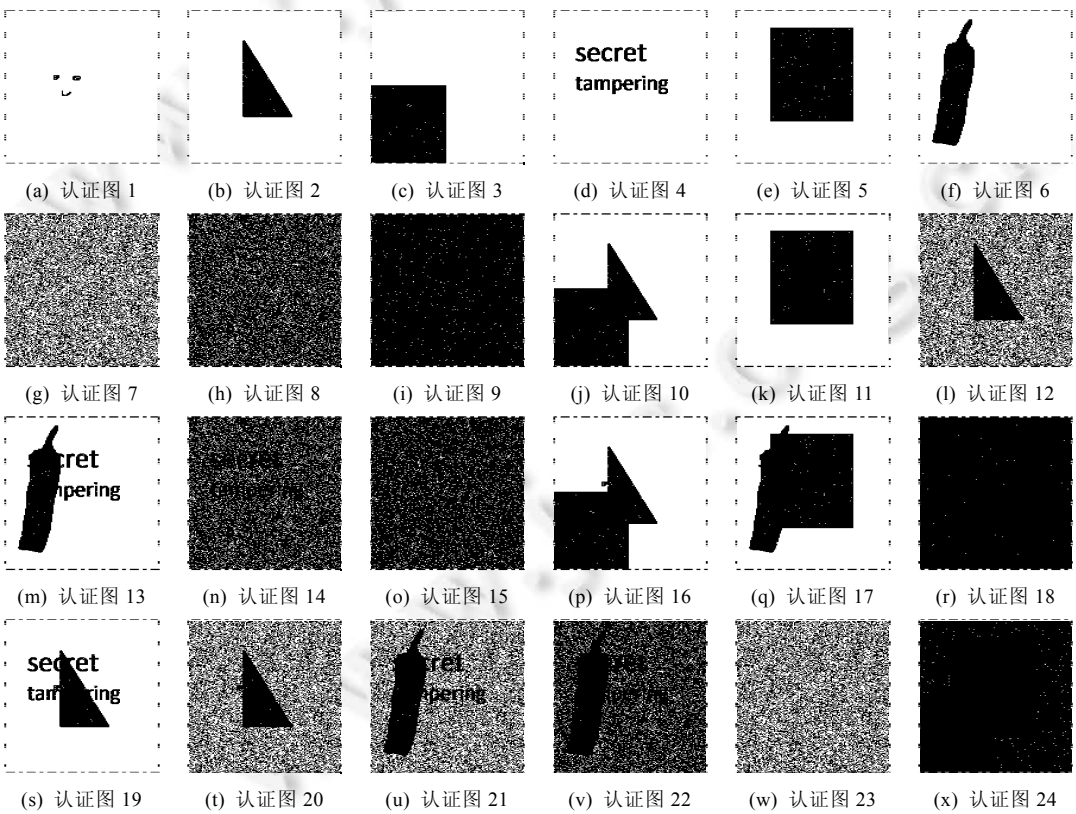
表 13 对文献[11]和文献[36]的掩体攻击及恢复结果

标号	本文恢复图像 PSNR(dB)	文献[11]			文献[36]		
		认证图	恢复密图	恢复图像 PSNR(dB)	认证图	恢复密图	恢复图像 PSNR(dB)
1	**49.57**	图 17(a)	图 18(a)	48.57	图 19(a)	图 20(a)	45.89
2	32.58	图 17(b)	图 18(b)	**32.60**	图 19(b)	图 20(b)	28.82
3	**29.49**	图 17(c)	图 18(c)	29.46	图 19(c)	图 20(c)	26.89
4	**36.71**	图 17(d)	图 18(d)	35.51	图 19(d)	图 20(d)	28.86
5	**26.87**	图 17(e)	图 18(e)	25.72	图 19(e)	图 20(e)	22.62
6	**33.04**	图 17(f)	图 18(f)	33.01	图 19(f)	图 20(f)	27.89
7	**30.73**	图 17(g)	图 18(g)	19.14	图 19(g)	图 20(g)	14.59
8	**25.92**	图 17(h)	图 18(h)	12.63	图 19(h)	图 20(h)	14.59

Table 13 Recovery results of Ref.[11] and Ref.[36] after being attacked (Continued)

表 13 对文献[11]和文献[36]的掩体攻击及恢复结果(续)

标号	本文恢复图像 PSNR(dB)	文献[11]			文献[36]		
		认证图	恢复密图	恢复图像 PSNR(dB)	认证图	恢复密图	恢复图像 PSNR(dB)
9	**17.56**	图 17(i)	图 18(i)	10.30	图 19(i)	图 20(i)	14.59
10	**28.48**	图 17(j)	图 18(j)	27.94	图 19(j)	图 20(j)	22.57
11	**26.88**	图 17(k)	图 18(k)	25.79	图 19(k)	图 20(k)	22.62
12	**28.84**	图 17(l)	图 18(l)	17.99	图 19(l)	图 20(l)	14.59
13	**31.89**	图 17(m)	图 18(m)	31.39	图 19(m)	图 20(m)	23.60
14	**25.23**	图 17(n)	图 18(n)	12.52	图 19(n)	图 20(n)	14.59
15	**23.37**	图 17(o)	图 18(o)	11.42	图 19(o)	图 20(o)	14.59
16	**28.52**	图 17(p)	图 18(p)	27.99	图 19(p)	图 20(p)	22.51
17	**26.27**	图 17(q)	图 18(q)	22.98	图 19(q)	图 20(q)	20.19
18	**15.78**	图 17(r)	图 18(r)	10.24	图 19(r)	图 20(r)	14.59
19	**31.63**	图 17(s)	图 18(s)	30.93	图 19(s)	图 20(s)	25.78
20	**28.99**	图 17(t)	图 18(t)	18.00	图 19(t)	图 20(t)	14.59
21	**28.39**	图 17(u)	图 18(u)	17.37	图 19(u)	图 20(u)	14.59
22	**24.12**	图 17(v)	图 18(v)	12.26	图 19(v)	图 20(v)	14.59
23	**29.74**	图 17(w)	图 18(w)	19.12	图 19(w)	图 20(w)	14.59
24	**15.98**	图 17(x)	图 18(x)	10.28	图 19(x)	图 20(x)	14.59



(a) 认证图 1 (b) 认证图 2 (c) 认证图 3 (d) 认证图 4 (e) 认证图 5 (f) 认证图 6

(g) 认证图 7 (h) 认证图 8 (i) 认证图 9 (j) 认证图 10 (k) 认证图 11 (l) 认证图 12

(m) 认证图 13 (n) 认证图 14 (o) 认证图 15 (p) 认证图 16 (q) 认证图 17 (r) 认证图 18

(s) 认证图 19 (t) 认证图 20 (u) 认证图 21 (v) 认证图 22 (w) 认证图 23 (x) 认证图 24

Fig.17 Authentication images of the Ref.[11] after being attacked

图 17 文献[11]的攻击后认证图

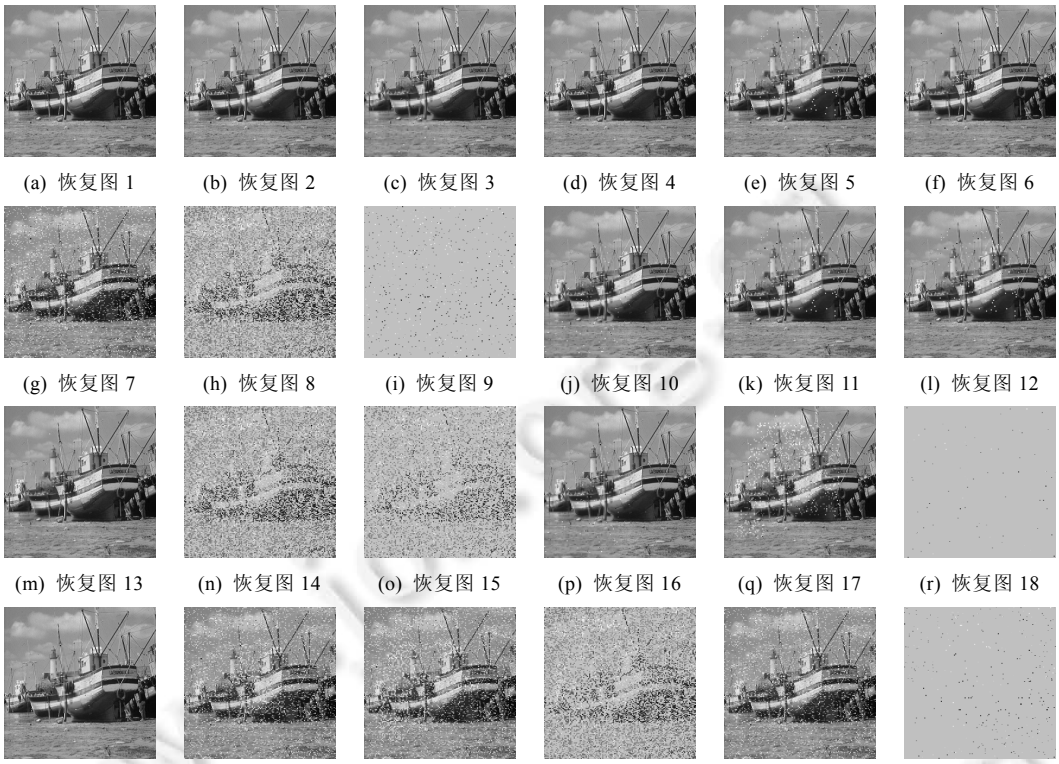


Fig.18 Recovery images of the Ref.[11] after being attacked

图 18 文献[11]的攻击后恢复图

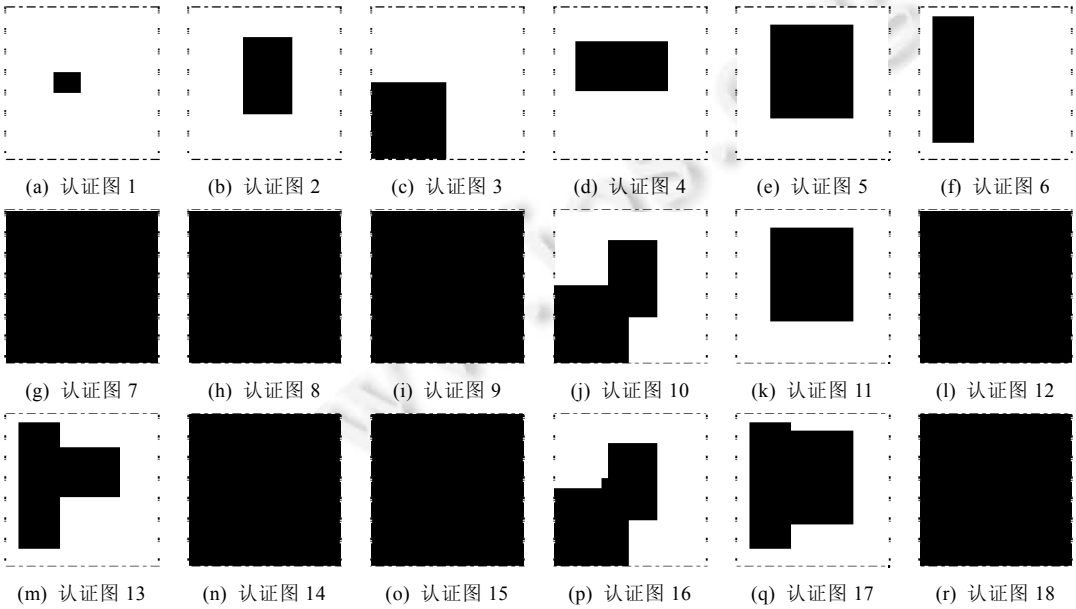


Fig.19 Authentication images of the Ref.[36] after beging attacked

图 19 文献[36]的攻击后认证图

(s) 认证图 19 (t) 认证图 20 (u) 认证图 21 (v) 认证图 22 (w) 认证图 23 (x) 认证图 24

Fig.19 Authentication images of the Ref.[36] after beging attacked (Continued)

图 19 文献[36]的攻击后认证图(续)

(a) 恢复图 1 (b) 恢复图 2 (c) 恢复图 3 (d) 恢复图 4 (e) 恢复图 5 (f) 恢复图 6

(g) 恢复图 7 (h) 恢复图 8 (i) 恢复图 9 (j) 恢复图 10 (k) 恢复图 11 (l) 恢复图 12

(m) 恢复图 13 (n) 恢复图 14 (o) 恢复图 15 (p) 恢复图 16 (q) 恢复图 17 (r) 恢复图 18

(s) 恢复图 19 (t) 恢复图 20 (u) 恢复图 21 (v) 恢复图 22 (w) 恢复图 23 (x) 恢复图 24

Fig.20 Recovery images of the Ref.[36] after being attacked

图 20 文献[36]的攻击后恢复图

表 13 中用粗体标记了恢复图像 PSNR 的最优值,可看出:除攻击样例 2,文献[11]最高且与本文的恢复值相接近;其他攻击样例都是本文的恢复效果要好于文献[11,36],尤其是对包含随机噪声攻击的攻击样例,本文的恢复密图 PSNR 要比文献[11,36]恢复密图 PSNR 高 10dB 左右,从而验证本文修复能力要好于文献[11,36],且对于随机点攻击具备较好的修复能力.此外,从表 13 和图 19 可看出,文献[36]用最小外包矩形包含认证不通过像素的认证策略会带来非常大的误判概率.从图 15 和图 17 的认证图对比可看出:文献[11]遭受随机噪声攻击时,认证图与攻击图样不符,为大面积黑点,这说明文献[11]将 2 个秘密像素绑定分存嵌入至掩体 2×4 分块策略是不合理的.从总体上看,本文策略的认证能力优于文献[11,36].

5.7 与相关文献综合性能对比实验

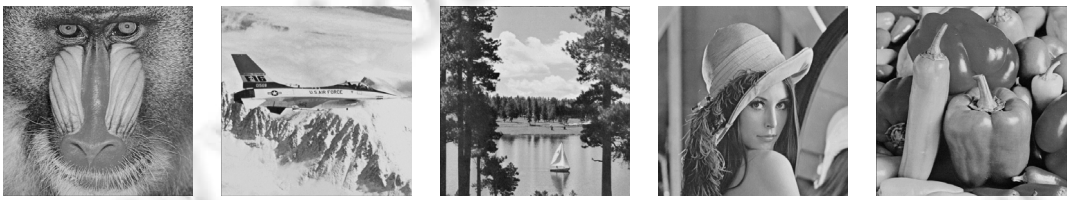
为说明本文策略的综合性能,文献[10,11,27,29,30,36,37]的分发掩体如图 21 所示,表 14 列出了文献[10,11,27,29,30,36,37]和本文综合性能.

掩体 1　掩体 2　掩体 3　掩体 4　掩体 5

(a) 文献[10]分发掩体

掩体 1　掩体 2　掩体 3　掩体 4　掩体 5

(b) 文献[11]分发掩体



掩体 1　掩体 2　掩体 3　掩体 4　掩体 5

(c) 文献[27]分发掩体

掩体 1　掩体 2　掩体 3　掩体 4　掩体 5

(d) 文献[29]分发掩体

掩体 1　掩体 2　掩体 3　掩体 4　掩体 5

(e) 文献[30]分发掩体

Fig.21　Experimental images of similar works

图 21　与同类文献对比的实验图样

(f) 文献[36]分发掩体

(g) 文献[37]分发掩体

Fig.21 Experimental images of similar works (Continued)

图 21 与同类文献对比的实验图样(续)

Table 14 Experimental results of similar works

表 14 相关文献性能对比结果

策略	恢复条件	最大嵌入容量	认证能力	认证类型	修复能力	分发掩体 PSNR(dB)					
						掩体 1	掩体 2	掩体 3	掩体 4	掩体 5	平均
文献[10]	连续 K 个掩体	1/2	1/256	认证秘密像素	无	47.22	47.18	47.18	47.16	47.17	47.18
文献[11]	连续 K 个掩体	1/4	1/256	认证分存信息	有	44.15	44.17	44.16	44.16	44.14	44.16
文献[27]	任意 K 个掩体	K/4	1/2	认证分存信息	无	39.18	39.23	39.17	39.18	39.18	39.19
文献[29]	任意 K 个掩体	1/4	1/2	认证分存信息	无	41.60	41.62	41.49	41.41	41.33	41.49
文献[30]	任意 K 个掩体	1/4	1/8	认证分存信息	无	42.72	42.60	42.18	42.00	41.79	42.26
文献[36]	任意 K 个掩体	1/4	1/16	认证分存信息	有	45.13	45.13	45.12	45.12	45.13	45.13
文献[37]	任意 K 个掩体	1/4	1/8	认证分存信息	有	45.12	45.12	45.12	45.11	45.12	45.12
所提策略	任意 K 个掩体	1/4	$1/2^{7K-12}$	双认证	有	46.35	46.36	46.36	46.38	46.38	46.37

从表 14 可看出:文献[10,11]恢复条件是需要连续 K 个掩体,适用条件过于苛刻,而本文和其他相关文献只需任意 K 个掩体即可恢复.从认证能力上看,当 K=3 时,本文策略的认证能力为 1/512,好于其他文献,并且所提策略是双认证策略.文献[10,27]的最大嵌入容量相对优于其他文献,但不具备修复能力.此外,只有所提策略和文献[11,36,37]具备修复能力,而其他文献不具备.从表 14 的 PSNR 可看出:本文所提策略具备很好的视觉质量,平均高于文献[11]约 2.21dB,高于文献[36,37]约 1.24dB,仅低于文献[10]的分发掩体 PSNR,但文献[10]仅具备认证能力而不具备修复能力.上述实验结果表明:本文策略在具备较强认证能力和修复能力的同时,分发掩体也具备较高视觉质量.

5.8 普适性验证实验

为验证本文所提算法的普适性,本文也对图 10(a)按算法 1 进行(2,5)和(4,5)门限分存,所得到的分发掩体如图 22(a)~图 22(e)和图 22(f)~图 22(m)所示.

图 22(a)~图 22(e)相对于图 10(b)~图 10(f)的 PSNR 为 46.38dB,46.36dB,46.35dB,46.37dB,46.36dB;图 22(f)~图 22(m)相对于图 10(b)~图 10(f)的 PSNR 分别为 46.37dB,46.36dB,46.36dB,46.37dB,46.39dB.这表明(2,5)和(4,5)门限分存分发掩体同样具备较高的视觉质量,攻击者难以发现嵌入的分存信息.对图 22 的分发掩体可按算法 2 进行(2,5)和(4,5)门限恢复,这里根据参与者提供的正确子密钥和分发掩体进行恢复,恢复参数和恢复结果如表 15、表 16 和图 23、图 24 所示.从这些结果可以看出:对于(2,5)或(4,5)门限,只有参与恢复的掩体和子密钥数量

不小于门限 2 或 4 时才能无损地恢复出密图.

(a) (2,5)分发掩体 1 (b) (2,5)分发掩体 2 (c) (2,5)分发掩体 3 (d) (2,5)分发掩体 4 (e) (2,5)分发掩体 5

(f) (4,5)分发掩体 1 (g) (4,5)分发掩体 2 (h) (4,5)分发掩体 3 (l) (4,5)分发掩体 4 (m) (4,5)分发掩体 5

Fig.22 Distributed cover images based on (2,5) and (4,5) threshold sharing

图 22 (2,5)和(4,5)门限分发掩体

Table 15 Secret image recovery variables based on (2,5)-threshold

表 15 基于(2,5)门限密图恢复参数

编号	参与图像	恢复密图	密图	*MSE*
1	图 22(a)~图 22(c)	图 23(a)		0
2	图 22(b)~图 22(d)	图 23(b)		0
3	图 22(a)~图 22(d)	图 23(c)		0
4	图 22(b)~图 22(e)	图 23(d)	图 10(a)	0
5	图 22(a)~图 22(e)	图 23(e)		0
6	图 22(a)、图 22(b)	图 23(f)		0
7	图 22(a)	–		–

Table 16 Secret image recovery variables based on (4,5)-threshold

表 16 基于(4,5)门限密图的恢复参数

编号	参与图像	恢复密图	密图	*MSE*
1	图 22(f)~图 22(h)	–		–
2	图 22(g),图 22(h),图 22(l)	–		–
3	图 22(f)~图 22(h), 图 22(l)	图 24(a)		0
4	图 22(g),图 22(h),图 22(l),图 22(m)	图 24(b)	图 10(a)	0
5	图 22(f)~图 22(h),图 22(l),图 22(m)	图 24(c)		0
6	图 22(g),图 22(h)	–		–
7	图 22(m)	–		–

(a) 第 1 组恢复结果 (b) 第 2 组恢复结果 (c) 第 3 组恢复结果 (d) 第 4 组恢复结果 (e) 第 5 组恢复结果 (f) 第 6 组恢复结果

Fig.23 Recovery images of (2,5)-threshold

图 23 (2,5)门限恢复图样

(a) 第 3 组恢复结果 (b) 第 4 组恢复结果 (c) 第 5 组恢复结果

Fig.24 Recovery images of (4,5)-threshold

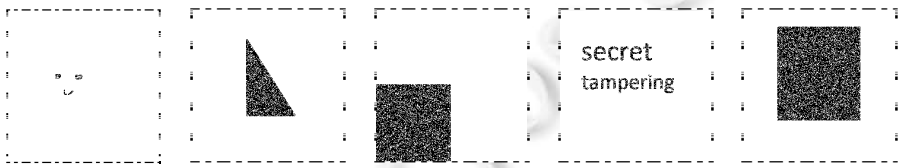
图 24 (4,5)门限恢复图样

这里,分别以前 2 个和前 3 个参与者携带的子密钥和分发掩体参与恢复为例来验证(2,5)和(4,5)门限的认证能力和恢复能力.其中:(2,5)门限对应的攻击前分发掩体如图 22(a)、图 22(b)所示,具体的攻击、认证和恢复结果如表 17、图 25 和图 26 所示;(4,5)门限对应的攻击前分发掩体如图 22(f)~图 22(h)所示,具体的攻击、认证和恢复结果如表 18、图 27 和图 28 所示.

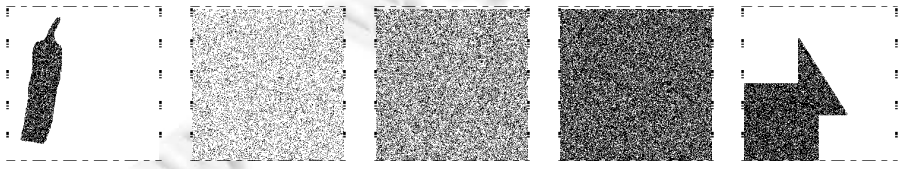
Table 17 Recovery results of the the attacked carriers based on (2,5)-threshold

表 17 对(2,5)门限分发掩体攻击的恢复结果

标号	掩体 1 攻击	掩体 2 攻击	认证图	恢复密图	恢复图像 PSNR(dB)	攻击识别率(%)
1	图 13(a)	–	图 25(a)	图 26(a)	40.42	73.26
2	图 13(b)	–	图 25(b)	图 26(b)	24.38	74.93
3	图 13(c)	–	图 25(c)	图 26(c)	20.10	75.26
4	图 13(d)	–	图 25(d)	图 26(d)	27.81	74.11
5	图 13(e)	–	图 25(e)	图 26(e)	18.77	74.98
6	图 13(f)	–	图 25(f)	图 26(f)	23.95	74.95
7	图 13(g)	–	图 25(g)	图 26(g)	21.10	77.20
8	图 13(h)	–	图 25(h)	图 26(h)	16.24	76.42
9	图 13(i)	–	图 25(i)	图 26(i)	11.20	75.65
10	图 13(b)	图 13(c)	图 25(j)	图 26(j)	19.52	75.88
11	图 13(b)	图 13(e)	图 25(k)	图 26(k)	19.25	77.99
12	图 13(b)	图 13(g)	图 25(l)	图 26(l)	20.09	77.78
13	图 13(d)	图 13(f)	图 25(m)	图 26(m)	23.00	77.50
14	图 13(d)	图 13(h)	图 25(n)	图 26(n)	16.53	77.19
15	图 13(g)	图 13(h)	图 25(o)	图 26(o)	15.27	79.18



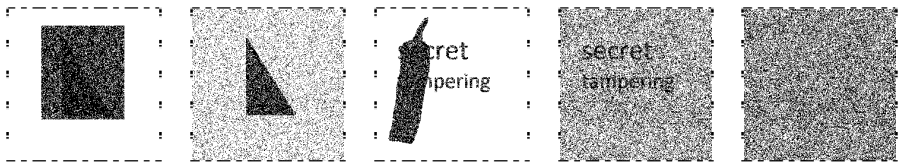
(a) 认证图 1 (b) 认证图 2 (c) 认证图 3 (d) 认证图 4 (e) 认证图 5



(f) 认证图 6 (g) 认证图 7 (h) 认证图 8 (i) 认证图 9 (j) 认证图 10

Fig.25 Authentication images of (2,5)-threshold

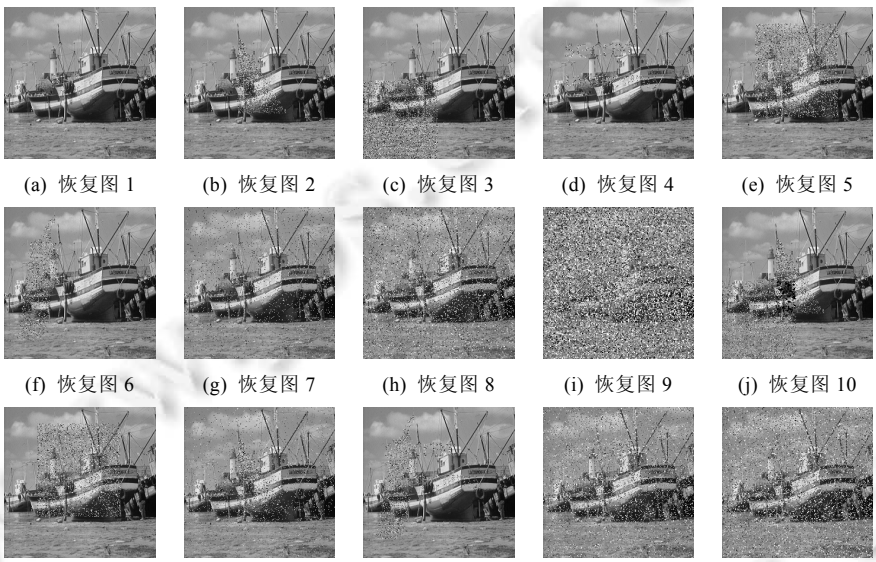
图 25 (2,5)门限攻击后的认证图



(k) 认证图 11 (l) 认证图 12 (m) 认证图 13 (n) 认证图 14 (o) 认证图 15

Fig.25 Authentication images of (2,5)-threshold (Continued)

图 25 (2,5)门限攻击后认证图(续)



(a) 恢复图 1 (b) 恢复图 2 (c) 恢复图 3 (d) 恢复图 4 (e) 恢复图 5

(f) 恢复图 6 (g) 恢复图 7 (h) 恢复图 8 (i) 恢复图 9 (j) 恢复图 10

(k) 恢复图 11 (l) 恢复图 12 (m) 恢复图 13 (n) 恢复图 14 (o) 恢复图 15

Fig.26 Recovery images of (2,5)-threshold

图 26 (2,5)门限恢复图

Table 18 Recovery results of the the attacked carriers based on (4,5)-threshold

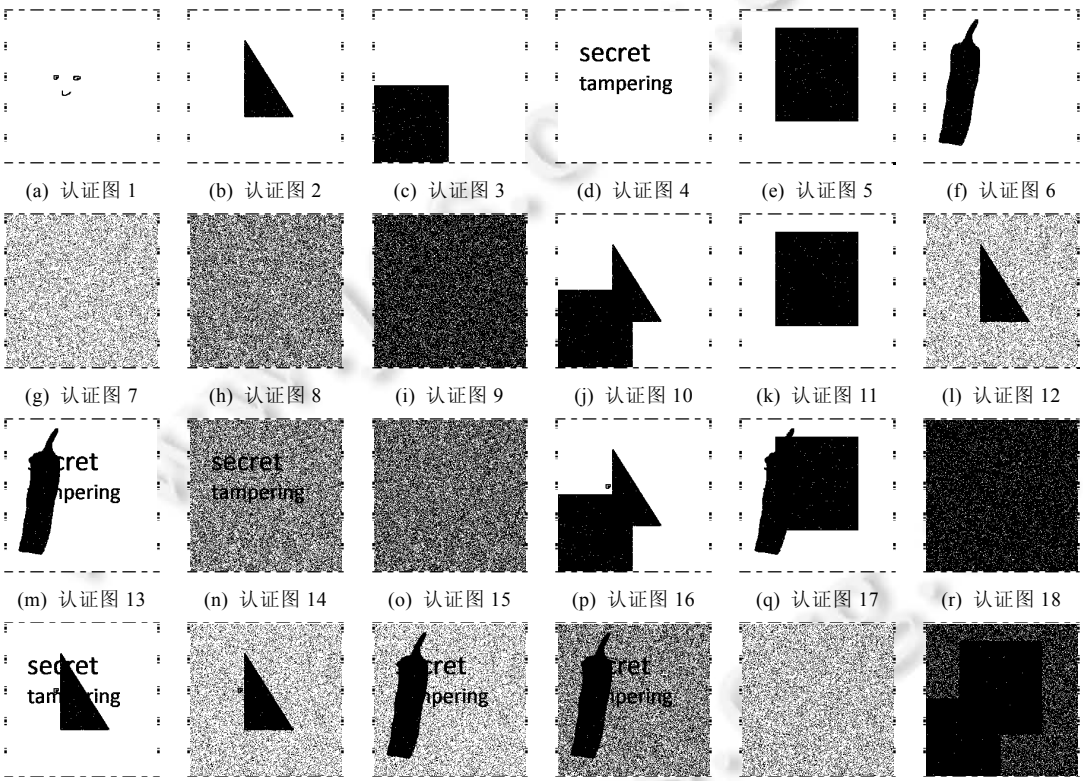
表 18 对(4,5)门限分发掩体攻击的恢复结果

标号	对掩体 1 攻击	对掩体 2 攻击	对掩体 3 攻击	认证图	恢复密图	恢复图像 PSNR(dB)	攻击识别率(%)
1	图 13(a)	–	–	图 27(a)	图 28(a)	49.53	100
2	图 13(b)	–	–	图 27(b)	图 28(b)	32.85	100
3	图 13(c)	–	–	图 27(c)	图 28(c)	29.64	100
4	图 13(d)	–	–	图 27(d)	图 28(d)	36.83	100
5	图 13(e)	–	–	图 27(e)	图 28(e)	27.04	100
6	图 13(f)	–	–	图 27(f)	图 28(f)	33.40	100
7	图 13(g)	–	–	图 27(g)	图 28(g)	30.86	100
8	图 13(h)	–	–	图 27(h)	图 28(h)	26.09	99.99
9	图 13(i)	–	–	图 27(i)	图 28(i)	17.69	100
10	图 13(b)	图 13(c)	–	图 27(j)	图 28(j)	28.75	100
11	图 13(b)	图 13(e)	–	图 27(k)	图 28(k)	27.02	100
12	图 13(b)	图 13(g)	–	图 27(l)	图 28(l)	29.01	100
13	图 13(d)	图 13(f)	–	图 27(m)	图 28(m)	32.12	100
14	图 13(d)	图 13(h)	–	图 27(n)	图 28(n)	25.35	100
15	图 13(g)	图 13(h)	–	图 27(o)	图 28(o)	23.42	100
16	图 13(a)	图 13(b)	图 13(c)	图 27(p)	图 28(p)	28.73	100
17	图 13(d)	图 13(e)	图 13(f)	图 27(q)	图 28(q)	26.46	100
18	图 13(g)	图 13(h)	图 13(i)	图 27(r)	图 28(r)	15.79	100

Table 18 Recovery results of the the attacked carriers based on (4,5)-threshold (Continued)

表 18 对(4,5)门限分发掩体攻击的恢复结果(续)

标号	对掩体 1 攻击	对掩体 2 攻击	对掩体 3 攻击	认证图	恢复密图	恢复图像 PSNR(dB)	攻击识别率(%)
19	图 13(a)	图 13(b)	图 13(d)	图 27(s)	图 28(s)	31.80	100
20	图 13(a)	图 13(b)	图 13(g)	图 27(t)	图 28(t)	28.91	100
21	图 13(d)	图 13(f)	图 13(g)	图 27(u)	图 28(u)	28.47	100
22	图 13(d)	图 13(f)	图 13(h)	图 27(v)	图 28(v)	24.12	100
23	图 13(g)	图 13(g)	图 13(g)	图 27(w)	图 28(w)	29.75	100
24	图 13(c)	图 13(e)	图 13(i)	图 27(x)	图 28(x)	15.98	100



(a) 认证图 1 (b) 认证图 2 (c) 认证图 3 (d) 认证图 4 (e) 认证图 5 (f) 认证图 6

(g) 认证图 7 (h) 认证图 8 (i) 认证图 9 (j) 认证图 10 (k) 认证图 11 (l) 认证图 12

(m) 认证图 13 (n) 认证图 14 (o) 认证图 15 (p) 认证图 16 (q) 认证图 17 (r) 认证图 18

(s) 认证图 19 (t) 认证图 20 (u) 认证图 21 (v) 认证图 22 (w) 认证图 23 (x) 认证图 24

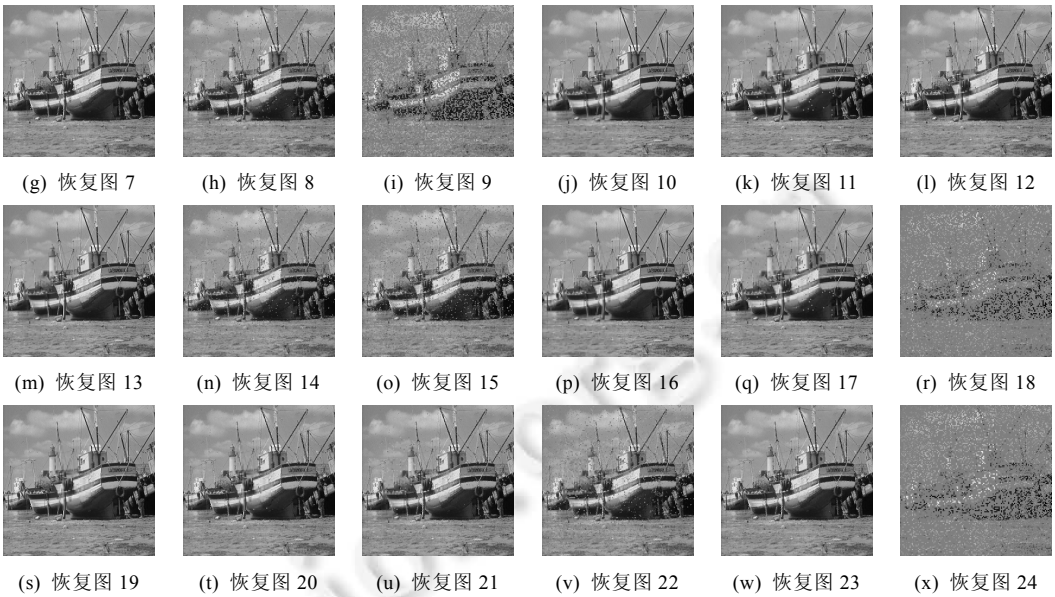
Fig.27 Authentication images of (4,5)-threshold

图 27 (4,5)门限攻击后的认证图

(a) 恢复图 1 (b) 恢复图 2 (c) 恢复图 3 (d) 恢复图 4 (e) 恢复图 5 (f) 恢复图 6

Fig.28 Recovery images of (4,5)-threshold

图 28 (4,5)门限恢复图



(g) 恢复图 7 (h) 恢复图 8 (i) 恢复图 9 (j) 恢复图 10 (k) 恢复图 11 (l) 恢复图 12

(m) 恢复图 13 (n) 恢复图 14 (o) 恢复图 15 (p) 恢复图 16 (q) 恢复图 17 (r) 恢复图 18

(s) 恢复图 19 (t) 恢复图 20 (u) 恢复图 21 (v) 恢复图 22 (w) 恢复图 23 (x) 恢复图 24

Fig.28 Recovery images of (4,5)-threshold (Continued)

图 28 (4,5)门限恢复图(续)

对比(2,5)门限、(4,5)门限和(3,5)门限可知:结合双认证,(2,5)门限每个攻击像素最多有 1/4 概率逃脱认证,即,识别比率约为 75%,因此,表 17 的攻击点识别率都接近 75%;而(4,5)门限每个攻击点最多有 $1/2^{16}$ 的概率逃脱认证,因此,表 18 的攻击点识别率接近 100%.从表 17 和图 26 以及表 18 和图 28 可看出:同(3,5)门限相类似,(2,5)门限和(4,5)门限对图 13 中的第 1 种~第 8 种类型的攻击及其组合都具备较好的修复能力;对图 13 中的第 9 种攻击类型——50%的噪声攻击,由于攻击粒度较大,因为其几乎撒在了掩体所有的 2×2 分块,导致恢复结果较差.但总体上,本文所述策略在不同门限方案上也具备较好的修复能力.

6 结束语

本文给出了一种非等量备份和双认证自修复有限域图像分存方案.在分存时,首先,通过离散小波变换和密钥 *Key* 来构造与密图等大非等量备份图;然后,在 GF(2^7)有限域将密图像素和备份像素及其第 2 重认证信息进行(*K*,*N*)分存,并通过优化 LSB 法将分存信息及第 1 重认证信息嵌入到掩体中,以提高掩体视觉质量;最后,将 *Key* 进行(*K*,*N*)分存.为防止参与者作弊,向第 3 方公信方公布子密钥对应的 MD5 值.在恢复时,首先恢复 *Key*,并用 *Key*、掩体和双认证结果恢复初步密图、认证图和备份图.为提高修复能力,所提策略根据像素认证图的认证情况,选择性地使用插值修复和替换修复.因而,本文策略具备较强的认证能力和修复能力,且分存掩体具备较好的视觉质量.但所提策略分存信息依然是嵌入空域,导致对压缩攻击没抵抗力.另外,本文所给出的备份策略是基于比特位重要程度分组的非等量备份策略,对于图像,除了像素比特位重要程度以外,不同区域像素的重要程度也是不同的,例如位于医学图像病灶区域和军事图像目标区域的像素,如何根据像素重要程度的不同来构造更好的非等量备份策略也是下一步工作重点,以提高策略修复能力,使其具有更好的修复结果.这里也特别对评审专家提供的修改建议表示感谢.

References:

[1] Shamir A. How to share a secret. Communications of the ACM, 1979,22(11):612−613. [doi: 10.1145/359168.359176]

[2] Blakley GR. Safeguarding cryptographic keys. In: Proc. of the AFIPS'79 National Computer Conf., Vol.48. New York: IEEE, 1979. 313−317. [doi: 10.1109/AFIPS.1979.98]

[3] Asmuth C, Bloom J. A modular approach to key safeguarding. IEEE Trans. on Information Theory, 1983,29(2):208−210. [doi: 10.1109/TIT.1983.1056651]

[4] Karnin ED, Green JW, Hellman ME. On sharing secret systems. IEEE Trans. on Information Theory, 1983,29(1):35−41. [doi: 10.1109/TIT.1983.1056621]

[5] Thien CC, Lin JC. Secret image sharing. Computers & Graphics, 2002,26(5):765−770. [doi: 10.1016/S0097-8493(02)00131-0]

[6] Shyu SJ, Chen YR. Threshold secret image sharing by Chinese remainder theorem. In: Proc. of the 2008 IEEE Asia-Pacific Services Computing Conf., 2008. 1332−1337. [doi: 10.1109/APSCC.2008.223]

[7] Ulutas M, Nabiyev VV, Ulutas G. A new secret image sharing technique based on Asmuth Bloom's scheme. In: Proc. of the Int'l Conf. on Application of Information and Communication Technologies. Baku: IEEE, 2009. 1−5. [doi: 10.1109/ICAICT.2009.5372571]

[8] Chen CC, Fu WY. A geometry-based secret image sharing approach. Journal of Information Science and Engineering, 2008,24(5):1567−1577. [doi: 10.6688/JISE.2008.24.5.18]

[9] Tso HK. Sharing secret images using Blakley's concept. Optical Engineering, 2008,47(7):0770011−0770013. [doi: 10.1117/1.2955502]

[10] Eslami Z, Razzaghi SH, Zarepour AJ. Secret image sharing based on cellular automata and steganography. Pattern Recognition, 2010,43(1):397−404. [doi: 10.1016/j.patcog.2009.06.007]

[11] Wu XT, Sun W. Secret image sharing scheme with authentication and remedy abilities based on cellular automata and discrete wavelet transform. The Journal of Systems and Software, 2013,86(4):1068−1088. [doi: 10.1016/j.jss.2012.11.021]

[12] Chen SK, Lin JC. Fault-Tolerant and progressive transmission of images. Pattern Recognition, 2005,38(12):2466−2471. [doi: 10.1016/j.patcog.2005.04.002]

[13] Wang RZ, Shyu SJ. Scalable secret image sharing. Signal Processing: Image Communication, 2007,22(4):363−373. [doi: 10.1016/j.image.2006.12.012]

[14] Liu YX, Yang CN, Yeh PH. Reducing shadow size in smooth scalable secret image sharing. Security & Communication Networks, 2014,7(12):2237−2244. [doi: 10.1002/sec.930]

[15] Lee JS, Chen YR. Selective scalable secret image sharing with verification. Multimedia Tools & Applications, 2017,76(1):1−11. [doi: 10.1007/s11042-015-3011-9]

[16] Liu W, Wang A, Chang CC, Li Z, Liu, L. A grouped-scalable secret image sharing scheme. Multimedia Tools & Applications, 2015, 74(17):7095−7109. [doi: 10.1007/s11042-014-1953-y]

[17] Wang ZH, Di YF, Li, JJ, Chang CC, Liu, H. Progressive secret image sharing scheme using meaningful shadows. Proc. of the Security and Communication Networks. 2016,9(17):4075−4088. [doi: 10.1002/sec.1589]

[18] Wang RZ, Su CH. Secret image sharing with smaller shadow images. Pattern Recognition Letters, 2006,27(6):551−555. [doi: 10.1016/j.patrec.2005.09.021]

[19] Wang XF, Li Z, Zhang XN, Wang SP, Chen J. (*r*,*n*)-threshold image secret sharing methods with small shadow images. In: Proc. of the 10th Int'l Workshop on Digital Forensics and Watermarking. Berlin: Springer-Verlag, 2012. 425−438. [doi: 10.1007/978-3-642-32205-1_34]

[20] Das SK, Dhara BC. An image secret sharing technique with block based image coding. In: Proc. of the 5th Int'l Conf. on Communication Systems and Network Technologies. IEEE, 2015. 648−652. [doi: 10.1109/CSNT.2015.37]

[21] Chang CC, Huynh NT, Le HD. Lossless and unlimited multi-image sharing based on Chinese remainder theorem and Lagrange interpolation. Signal Processing, 2014,99:159−170. [doi: /10.1016/j.sigpro.2013.12.022]

[22] Li P, Yang CN, Zhou Z. Essential secret image sharing scheme with the same size of shadows. Digital Signal Processing, 2016,50:51−60. [doi: 10.1016/j.dsp.2015.12.004]

[23] Lin PY, Lee JS, Chang CC. Distortion-Free secret image sharing mechanism using modulus operator. Pattern Recognition, 2009, 42(5):886−895. [doi: 10.1016/j.patcog.2008.09.014]

[24] Lin PY, Chan CS. Invertible secret image sharing with steganography. Pattern Recognition Letters, 2010,31(13):1887−1893. [doi: 10.1016/j.patrec.2010.01.019]

[25] Kim DH, Lee GJ, Park MH, Yoo KY. A reversible secret sharing scheme based on GF(2^8). In: Proc. of the 9th Int'l Conf. on Information Technology-New Generations. Las Vegas: IEEE, 2012. 425−430. [doi: 10.1109/ITNG.2012.101]

[26] Yuan L, Li M, Guo C, Hu W, Luo, X. Secret image sharing scheme with threshold changeable capability. Mathematical Problems in Engineering, 2016,(1):1−11. [doi: 10.1155/2016/9576074]

[27] Lin CC, Tsai WH. Secret image sharing with steganography and authentication. The Journal of Systems and Software, 2004,73(3): 405−414. [doi: 10.1016/S0164-1212(03)00239-5]

[28] Kanso A, Ghebleh M. An efficient (*t*,*n*)-threshold secret image sharing scheme. Multimedia Tools & Applications, 2016, 1−20. [doi: 10.1007/s11042-016-3917-x]

[29] Yang CN, Chen TS, Yu KH, Wang CC. Improvements of image sharing with steganography and authentication. The Journal of Systems and Software, 2007,80(7):1070−1076. [doi: 10.1016/j.jss.2006.11.022]

[30] Chang CC, Hsieh YP, Lin CH. Sharing secrets in stego images with authentication. Pattern Recognition, 2008,41(10):3130−3137. [doi: 10.1016/j.patcog.2008.04.006]

[31] Wu CC, Kao SJ, Hwang MS. A high quality image sharing with steganography and adaptive authentication scheme. The Journal of Systems and Software, 2011,84(12):2196−2207. [doi: 10.1016/j.jss.2011.06.021]

[32] Eslami Z, Zarepour AJ. Secret image sharing with authentication-chaining and dynamic embedding. The Journal of Systems and Software, 2011,84(5):803−809. [doi: 10.1016/j.jss.2011.01.002]

[33] Yang CN, Ouyang JF, Harn L. Steganography and authentication in image sharing without parity bits. Optics Communications, 2012,285(7):1725−1735. [doi: 10.1016/j.optcom.2011.12.003]

[34] Ouyang XB, Shao LP, Chen WX. Meaningful (*K*,*N*) image sharing scheme combined with the adjusting difference transformation. Journal of Image and Graphics, 2015,20(5):633−642 (in Chinese with English abstract). [doi: 10.11834/jig.20150506]

[35] Ouyang XB, Shao LP. Meaningful (*K*,*N*) free expansion image sharing scheme based on GF(2^3). Computer Science, 2015,42(12): 251−256 (in Chinese with English abstract).

[36] Chang CC, Chen YH, Wang HC. Meaningful secret sharing technique with authentication and remedy abilities. Information Sciences, 2011,181(14):3073−3084. [doi: 10.1016/j.ins.2011.03.002]

[37] Chen YH, Chang CC. Image tamper detection and recovery based on dual watermarks sharing strategy. Journal of Digital Information Management, 2012,10(1):39−49.

附中文参考文献:

[34] 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.中国图像图形学报,2015,20(5):633−642. [doi: 10.11834/jig.20150506]

[35] 欧阳显斌,邵利平.一种基于 GF(2^3)的(*K*,*N*)有意义无扩张图像分存方案.计算机科学,2015,42(12):251−256.

欧阳显斌(1992－),男,江西宜黄人,硕士,主要研究领域为有意义图像信息分存.

邵利平(1978－),男,副教授,CCF 专业会员,主要研究领域为图像音频信号处理,信息安全交叉.

乐志芳(1993－),女,学士,主要研究领域为图像信息渐进分存.