多版本备份和限制性双重认证主密钥(t,s,k,n)图像分存

邵利平,乐志芳
(陕西师范大学计算机科学学院, 陕西西安 710119)

摘 要: 传统影子图像连接的(t,s,k,n)分存易导致分发影子图像大小不等,基于伯克霍夫插值的(t,s,k,n)分存不能高效恢复;而双认证自修复图像分存对密图和备份图恢复能力十分有限.针对以上问题,采用随机参与值通过(k,s)和$(k\text{-}t,n\text{-}s)$分存来构造主密钥(t,s,k,n)分存并通过第 3 方公信方存储的 MD5 值以防止作弊.所提策略由主密钥对密图 *LL* 子带置乱来形成对显著比特多备份、对非显著比特少备份和经主密钥不同程度置乱的多版本备份图;引入限制性双重认证在保持认证精度的同时,将尽可能多的备份比特通过 GF(2^8)域(k,n)分存嵌入来形成嵌密掩体.理论和实验表明,主密钥(t,s,k,n)分存可高效求解;随机参与值可避免参与者编号泄露,分发信息的篡改和认证比特的揣测;多版本备份可对备份图高置信度地恢复;而限制性双重认证在认证能力上不低于双认证自修复图像分存.

关键词: 图像分存; 限制性双重认证; 有限域; 多版本备份; (t,s,k,n)分存; (k,n)分存; 模 p 逆矩阵
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112(2019)02-0390-14
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2019.02.019

(t,s,k,n) Image Sharing Sheme with Multi-Version Backups and Restricted Double Authentications

SHAO Li-ping, LE Zhi-fang
(*School of Computer Science, Shaanxi Normal University, Xi' an, Shaanxi* 710119, *China*)

Abstract: Conventional shadow image connection based (t,s,k,n) sharing is prone to different size shadow images and Birkhoff interpolation based (t,s,k,n) sharing leads to low recovery efficiency, while in double authentications based self-recovery image sharing, the recovery capabilities of secret image and backup image are very limited. To address these problems, random participation values were used to construct master key based (t,s,k,n) sharing by means of (k,s) and $(k\text{-}t,n\text{-}s)$ schemes and MD5 values stored in the third party were used to prevent cheating. The proposed scheme scrambled *LL* subband of secret image by master key and formed multi-version backup images with different scrambling degrees where more backups for more significant bits. Restricted double authentication strategy can embed as many backup bits as possible while maintaining authentication accuracy by (k,n) sharing over GF(2^8) field to form stego carriers. Theoretical and experimental results show, master key based (t,s,k,n) scheme can be solved efficiently. Random participation values avoid the disclosure of participant numbers and prevent tampering distributed information or guessing authentication bits. Multi-version backup strategy can restore backup images with high confidence while authentication capability of restricted double authentication strategy is no less than that of double authentications based self-recovery image sharing scheme.

Key words: image sharing; restricted double authentications; Galois field; multi-version backups; (t,s,k,n) sharing; (k,n) sharing; inverse matrix modulus p

收稿日期:2017-10-26;修回日期:2018-09-05;责任编辑:马兰英
基金项目:国家自然科学基金(No. 61100239);陕西省自然科学基金(No. 2011JQ8009, No. 2016JM6065);中央高校基本科研业务费支持项目(No. GK201402036, No. GK201703057)

1 引言

图像分存源自秘密共享,最简单秘密共享是(k,n)门限共享[1,2],即将秘密拆分为n个子秘密,当可用子秘密数大于等于门限k,秘密可完整重构. 而借助秘密共享对密图重构,则构成图像分存.

在(k,n)分存中[3],模数通常为251,像素为[0,255],会导致大于等于251像素重构损失. 文献[4]按循环移位将最不重要比特位前置清零来减少重构损失,但文献[3,4]不存在认证,无法检验恢复密图的真实性. 文献[5]将密图像素调整到[0,251)并调整掩体2×2分块右上角像素的奇偶来进行1位认证. 为避免密图视觉质量下降,文献[6]将(k,n)分存由GF(p)域拓展到GF(2^8)域,但依然只进行1位认证使得参与者容易逃脱检验. 文献[7]用中国剩余定理生成4位分存信息认证位,但需改变掩体2×2分块像素的低3位. 文献[8]将像素转换为模31余数和乘数,将分存信息减少为5位并添加3位认证信息,需改变掩体2×2分块像素的低2位. 文献[9]将密图转换为位置图和差值图分存,通过分块增强策略来严格认证. 以上文献[5~9]无法识别重构像素的准确性. 为认证密图像素,文献[10]在GF(2^3)域对密图像素分存且用4位认证位直接认证,但GF(2^3)域空间有限,无法提供足够认证精度. 同时文献[5~10]仅依据k恢复,恢复能力较低.

为提高恢复能力,文献[11,12]将密图像素及其配对像素分存,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,定位和恢复能力十分有限. 为提高修复能力,文献[13]将密图LL子带备份2份,构造与密图等大且每像素4比特的备份图,采用可逆元胞自动机来分存密图和备份图,利用备份图修复密图,但至少需3编号连续的分存单元才能恢复出2个密图和2个备份图像素,若2×4分块任一像素遭受攻击,将导致24位密图和备份图像素无法恢复. 针对此问题,文献[14]将密图LL子带按比特重要程度分组构造非等量备份,通过双重认证(对分存信息的后向认证和对分存重构信息的前向认证)和OPAP(Optimal pixel adjustment process)[15]嵌入来保证认证能力和嵌密掩体视觉质量. 文献[14]将大部分嵌入比特用于密图和备份图像素认证,综合认证比特数为$7k-12$,但仅对备份像素分配5比特嵌入空间,导致认证精度过高而恢复能力较低.

同时以上分存[3~14],参与者重要程度都相同,然而在特殊场景下,一些参与者由于身份特殊需拥有更高分存权限. 针对此问题,文献[16,17]将(k,n)分存扩展为(t,s,k,n)分存,引入重要参与者数量s和阈值t,要求参与恢复的影子图像数量至少为k且至少包含t个重要影子图像. 其中文献[16]通过$(k,s+k-t)$分存和门限1到$k-t$的秘密共享来形成(t,s,k,n)分存;文献[17]则结合$(k,s+k-t)$和$k-t$个(k,n)分存来构造(t,s,k,n)分存. 这两者都是通过中间影子图像连接来形成重要和非重要分发影子图像且在很大程度上分发影子图像大小不等,使得攻击者可检测出重要影子图像并实施攻击,同时影子图像连接也增加了密图重构复杂度. 文献[18]不进行影子图像连接,通过Lagrange多项式及其t阶导数多项式分存来构造重要和非重要影子图像,但该方案不能借助Lagrange插值高效恢复且涉及求导和有限域满秩方程组求解,计算代价十分高昂,文献[18]仅验证了完备性而未给出恢复方法,同时文献[16~18]不存在认证措施,无法鉴别传输影子图像及重构密图的真实性,而仅借助分存恢复,恢复能力较低.

针对以上问题[11~14,16~18],结合随机参与值,将(t,s,k,n)分存由影子图像转换为密钥,构造基于主密钥的密图(k,n)分存策略,所构造的重要和非重要子密钥都是模p整数且无法区分,同时主密钥(t,s,k,n)分存策略可根据参与恢复的重要参与者数量选择不同策略高效恢复. 所提方法在GF(2^8)域构造密图和备份图分存策略,采用限制性双重认证在保持较高认证精度的同时,将尽可能多的嵌入比特用于备份并形成多版本备份图,在每个版本内进一步依据显著、不显著和最不显著比特构造不同数量的备份,由多版本协同恢复来提高抗攻击能力,使得最终重构密图具有更高的视觉恢复质量.

2 Shamir-(k,n)门限秘密共享

目前大多数图像分存是建立在Shamir-(k,n)门限[1]的基础上,即构建式(1):

$$f(x)=(r_0+r_1x+r_2x^2+\cdots+r_{k-1}x^{k-1})\bmod p \quad (1)$$

式(1)中,$r_0,r_1,\cdots,r_{k-1}\in\{0,1,\cdots,p-1\}$为GF$(p)$域系数,其中$p$为素数用以保证模$p$非零整数存在乘法逆元,$r_0$为秘密信息嵌入位置[1,5],$r_1,r_2,\cdots,r_{k-1}$为随机整数,因此式(1)容量仅为1个$p$进制数;文献[3-4,8,11-12]将$r_1,\cdots,r_{k-1}$也用于分存,从而嵌入容量最多为$k$个$p$进制数.

将$x=1,2,\cdots,n,\ n\in[k,p)$代入式(1)可得$S_1=f(1),S_2=f(2),\cdots,S_n=f(n)$,若从中任取$l(l\geq k)$个,记为$S_{num_i}=f(num_i),num_i\in\{1,2,\cdots,n\},i\in1,2,\cdots,l$,则可按式(2)Lagrange插值恢复$f(x)$并提取秘密信息. 式(2)中,$(num_i-num_j)_p^{-1}$为模$p$乘法逆元,当$l<k$时,式(2)欠定无法恢复.

$$f(x)=\Big(\sum_{i=1}^{l}\Big(f(num_i)\prod_{j=1,j\neq i}^{l}(x-num_j)\cdot(num_i-num_j)_p^{-1}\Big)\Big)\bmod p \quad (2)$$

由于式(1)仅能共享素数进制数 p,若取 $p<256$,会导致像素损失[3,5],取 $p>256$[9,11,12],会使像素膨胀造成浪费.

为避免此问题,可将式(1)拓展为式(3),其中 $\dot{r}_0,\dot{r}_1,\dot{r}_2,\cdots,\dot{r}_{k-1}\in GF(2^m)$ 为 $GF(2^m)$ 域多项式整数[14],$\dot{p}_g\in GF(2^{m+1})$ 为本原多项式整数,例如 $GF(2^8)$ 域本原多项式整数有:$\dot{285}=x^8+x^4+x^3+x^2+1$,$\dot{299}=x^8+x^5+x^3+x+1$ 和 $\dot{301}=x^8+x^5+x^3+x^2+1$ 等. 若将式(3)部分或全部系数用于分存,则式(3)最大嵌入容量为 k 个 $[0,2^m)$ 范围整数,对应为 km 比特,当 $m=8$ 时,对应为 k 个像素,对于 $GF(2^8)$ 域,约定 $\dot{p}_g=\dot{285}$.

$$f_{GF}(\dot{x})=(\dot{r}_0+\dot{r}_1\dot{x}+\dot{r}_2\dot{x}^2+\cdots+\dot{r}_{k-1}\dot{x}^{k-1})\bmod \dot{p}_g \tag{3}$$

将 $x=1,2,\cdots,n,n\in[k,2^m)$ 代入式(3)可得:$\dot{S}_1=f_{GF}(\dot{1}),\dot{S}_2=f_{GF}(\dot{2}),\cdots,\dot{S}_n=f_{GF}(\dot{n})$. 若收集到 $l(l\geq k)$ 个$(\dot{num}_i,f_{GF}(\dot{num}_i))$,$num_i\in\{1,2,\cdots,n\}$,$i=1,2,\cdots,l$,则可按式(4)恢复 $f_{GF}(\dot{x})$ 并提取秘密信息,而当 $l<k$ 时,式(4)欠定而无法恢复.

$$f_{GF}(\dot{x})=\Big(\sum_{i=1}^{l}\Big(f_{GF}(\dot{num}_i)\prod_{j=1,j\neq i}^{l}(\dot{x}-\dot{num}_j)\cdot(\dot{num}_i-\dot{num}_j)_{\dot{p}_g}^{-1}\Big)\Big)\bmod \dot{p}_g \tag{4}$$

式(4)中,$(\dot{num}_i-\dot{num}_j)_{\dot{p}_g}^{-1}$ 是 $\dot{num}_i-\dot{num}_j$ 模 $\dot{p}_g$ 乘法逆元,由于 $\dot{p}_g$ 为本原多项式整数,则模 $\dot{p}_g$ 非零多项式整数都存在乘法逆元.

3 随机参与值主密钥(t,s,k,n)分存策略

由主密钥 *key* 产生 $k-1$ 个随机数 $a_1,a_2,\cdots,a_{k-1}\in\{1,2,\cdots,p-1\}$,按式(5)计算 $a_0\in\{1,2,\cdots,p-1\}$. 由于 p 为素数且 $a_1a_2\cdots a_{k-1}\bmod p\neq 0$,故存在 $(a_1a_2\cdots a_{k-1})_p^{-1}$,可按式(6)恢复 *key*.

$$a_0=(a_1a_2\cdots a_{k-1}key+\sum_{i=1}^{k-2}a_ia_{i+1})\bmod p \tag{5}$$

$$key=((a_1a_2\cdots a_{k-1})_p^{-1}(a_0+(p-1)\sum_{i=1}^{k-2}a_ia_{i+1}))\bmod p \tag{6}$$

式(5)和式(6)使得 $a_0,a_1,\cdots,a_{k-1}$ 恢复时才能恢复 *key*,从而对 *key* 起保护作用. 将 $a_0,a_1,\cdots,a_{k-1}$ 按式(7)分存产生重要子密钥 $subkey_0,subkey_1,\cdots,subkey_{s-1}$,然后将 $a_t,a_{t+1},\cdots,a_{k-1}$ 按式(8)产生非重要子密钥 $subkey_s,subkey_{s+1},\cdots,subkey_{n-1}$,其中 $P_u\in\{1,2,\cdots,p-1\}$ 是由 *key* 生成的随机参与值且满足 $P_0\bmod 256,P_1\bmod 256,\cdots,P_{n-1}\bmod 256$ 两两不等,通过 P_u 取代参与者编号 u 可避免 u 泄露.

$$f_0(P_u)=(a_0+a_1P_u+\cdots+a_tP_u^{\,t}+a_{t+1}P_u^{\,t+1}+\cdots+a_{k-1}P_u^{\,k-1})\bmod p,u=0,1,\cdots,s-1 \tag{7}$$

$$g_0(P_u)=(a_tP_u+a_{t+1}P_u^{\,2}+a_{t+2}P_u^{\,3}+\cdots+a_{k-1}P_u^{\,k-t})\bmod p,u=s,s+1,\cdots,n-1 \tag{8}$$

将分发密钥 $(subkey_u,P_u)$,$u=0,1,\cdots,s-1$ 和 $(subkey_u,P_u)$,$u=s,1,\cdots,n-1$ 分别分发给重要和非重要参与者,并将分发密钥 MD5 值公布到第 3 方公信方以防止作弊. 由式(7)和式(8)知:重要和非重要子密钥都是模 p 整数,无法区分. 式(8)也避免了文献[18]t 阶导数求导,在 $k=2$ 时,依然可构造分存方案.

记 m_1,m_2 是参与恢复的重要和非重要子密钥数,上述按式(5)、式(7)和式(8)将 *key* 转换为重要和非重要子密钥的方案是(t,s,k,n)方案,原因是:

①当 $m_1\leq t,m_2\geq k-t$ 时,由非重要子密钥按式(2)可恢复出 $a_t,a_{t+1},\cdots,a_{k-1}$,然后和重要子密钥一起可构造包含 $a_0,a_1,\cdots,a_{t-1}$ 的 m_1 个方程,此时仅有当 $m_1=t$ 时,才能得到 $a_0,a_1,\cdots,a_{t-1}$,从而按式(6)恢复 *key*.

②当 $m_1>t,m_2\geq k-m_1$ 时,由重要子密钥可构造包含 k 个未知数 $a_0,a_1,\cdots,a_{k-1}$ 的 m_1 个方程,非重要子密钥可构造包含 $k-t$ 个未知数 $a_t,a_{t+1},\cdots,a_{k-1}$ 的 m_2 个方程,因此能得到包含 k 个未知数 $a_0,a_1,\cdots,a_{k-1}$ 且具有 $m_1+m_2\geq k$ 个方程的方程组,从而可恢复出 $a_0,a_1,\cdots,a_{k-1}$ 并按式(6)恢复 *key*.

由①和②可看出,仅有当 $m_1\geq t,m_1+m_2\geq k$ 时才能恢复 *key*,因此是(t,s,k,n)方案.

文献[18](t,s,k,n)分存不满足门限秘密共享的恢复条件,涉及求导和满秩方程组求解,恢复策略十分复杂,文献[18]仅证明了(t,s,k,n)方案的完备性而未给出具体求解方法. 而本文主密钥(t,s,k,n)分存不依赖于影子图像,当 $m_1=t$ 时,可通过 Lagrange 插值恢复,当 $m_1>t$ 时,可通过模 p 矩阵求逆高效求解.

当 $m_1=t,m_2\geq k-t$ 时,首先由式(2)恢复出 $a_t,a_{t+1},\cdots,a_{k-1}$,将其代入式(7)可得式(9),其中 $IP_0,IP_1,\cdots,IP_{t-1}$ 为重要随机参与值.

$$\begin{cases}f_0(IP_0)=(a_0+a_1IP_0+\cdots+a_{t-1}IP_0^{\,t-1}+a_tIP_0^{\,t}+a_{t+1}IP_0^{\,t+1}+\cdots+a_{k-1}IP_0^{\,k-1})\bmod p\\ f_0(IP_1)=(a_0+a_1IP_1+\cdots+a_{t-1}IP_1^{\,t-1}+a_tIP_1^{\,t}+a_{t+1}IP_1^{\,t+1}+\cdots+a_{k-1}IP_1^{\,k-1})\bmod p\\ \vdots\\ f_0(IP_{t-1})=(a_0+a_1IP_{t-1}+\cdots+a_{t-1}IP_{t-1}^{t-1}+a_tIP_{t-1}^{t}+a_{t+1}IP_{t-1}^{t+1}+\cdots+a_{k-1}IP_{t-1}^{k-1})\bmod p\end{cases} \tag{9}$$

将 $G_i=(f_0(IP_i)+a_t(p^t-IP_i^{\,t})+a_{t+1}(p^{t+1}-IP_i^{\,t+1})+\cdots+a_{k-1}(p^{k-1}-IP_i^{\,k-1}))\bmod p$,$i=0,1,\cdots,t-1$ 代入式(9),可得式(10):

$$\begin{cases} G_0 = (a_0 + a_1 IP_0 + \cdots + a_{t-1} {IP_0}^{t-1}) \bmod p \\ G_1 = (a_0 + a_1 IP_1 + \cdots + a_{t-1} {IP_1}^{t-1}) \bmod p \\ \vdots \\ G_{t-1} = (a_0 + a_1 IP_{t-1} + \cdots + a_{t-1} IP_{t-1}^{t-1}) \bmod p \end{cases} \tag{10}$$

式(10)等价为已知(G_0, IP_0),(G_1, IP_1),…,(G_{t-1}, IP_{t-1})求解 $a_0, a_1, \cdots, a_{t-1}$,此时仅需将($G_0, IP_0$),($G_1, IP_1$),…,($G_{t-1}, IP_{t-1}$)代入式(2),即可通过 Lagrange 插值恢复出 $a_0, a_1, \cdots, a_{t-1}$,按式(6)恢复 *key*.

当 $m_1 > t, m_2 \geq k - m_1$ 时,此时由式(7)可得式(11),式(8)可得式(12),其中 $NP_0, NP_1, \cdots, NP_{m_2-1}$ 为非重要随机参与值.

$$\begin{cases} f_0(IP_0) = (a_0 + a_1 IP_0 + \cdots + a_{k-1} {IP_0}^{k-1}) \bmod p \\ f_0(IP_1) = (a_0 + a_1 IP_1 + \cdots + a_{k-1} {IP_1}^{k-1}) \bmod p \\ \vdots \\ f_0(IP_{m_1-1}) = (a_0 + a_1 IP_{m_1-1} + \cdots + a_{k-1} IP_{m_1-1}^{k-1}) \bmod p \end{cases} \tag{11}$$

$$\begin{cases} g_0(NP_0) = (a_t NP_0 + a_{t+1} {NP_0}^2 + \cdots + a_{k-1} {NP_0}^{k-t}) \bmod p \\ g_0(NP_1) = (a_t NP_1 + a_{t+1} {NP_1}^2 + \cdots + a_{k-1} {NP_1}^{k-t}) \bmod p \\ \vdots \\ g_0(NP_{m_2-1}) = (a_t NP_{m_2-1} + a_{t+1} NP_{m_2-1}^2 + \cdots + a_{k-1} NP_{m_2-1}^{k-t}) \bmod p \end{cases} \tag{12}$$

令 $\boldsymbol{FP} = (f_0(IP_0), f_0(IP_1), \cdots, f_0(IP_{m_1-1}), g_0(NP_0), g_0(NP_1), \cdots, g_0(NP_{m_2-1}))^{\mathrm{T}}$, $\boldsymbol{a} = (a_0, a_1, \cdots, a_{t-1}, a_t, a_{t+1}, \cdots, a_{k-1})^{\mathrm{T}}$,则由式(11)和式(12)可得式(13),其中 $\boldsymbol{M}_T$ 维数为 $(m_1 + m_2) \times k$.

$$\boldsymbol{FP} = (\boldsymbol{M}_T \boldsymbol{a}) \bmod p;$$

$$\boldsymbol{M}_T = \begin{bmatrix} 1 & IP_0 & \cdots & IP_0^{t-1} & IP_0^t & IP_0^{t+1} & \cdots & IP_0^{k-1} \\ 1 & IP_1 & \cdots & IP_1^{t-1} & IP_1^t & IP_1^{t+1} & \cdots & IP_1^{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & IP_{m_1-1} & \cdots & IP_{m_1-1}^{t-1} & IP_{m_1-1}^t & IP_{m_1-1}^{t+1} & \cdots & IP_{m_1-1}^{k-1} \\ & & & & NP_0 & NP_0^2 & \cdots & NP_0^{k-t} \\ & & & & NP_1 & NP_1^2 & \cdots & NP_1^{k-t} \\ & & & & \vdots & \vdots & \ddots & \vdots \\ & & & & NP_{m_2-1} & NP_{m_2-1}^2 & \cdots & NP_{m_2-1}^{k-t} \end{bmatrix} \bmod p \tag{13}$$

式(13)两端乘以 $\boldsymbol{M}_T^{\mathrm{T}}$ 可得式(14):

$$\boldsymbol{M}_T^{\mathrm{T}} \boldsymbol{FP} = (\boldsymbol{M}_T^{\mathrm{T}} \boldsymbol{M}_T \boldsymbol{a}) \bmod p \tag{14}$$

式(13)包含 k 元 1 次线性无关方程的数量为 $m_1 + m_2$ 且 $m_1 + m_2 \geq k$,因此 $\mathrm{rank}(\boldsymbol{M}_T) = \mathrm{rank}(\boldsymbol{M}_T^{\mathrm{T}}) = rank(\boldsymbol{M}_T^{\mathrm{T}} \boldsymbol{M}_T) = k$,而 $\boldsymbol{M}_T^{\mathrm{T}}$ 维数为 $k \times (m_1 + m_2)$,故 $\boldsymbol{M}_T^{\mathrm{T}} \boldsymbol{M}_T$ 维数为 $k \times k$,因此 $\boldsymbol{M}_T^{\mathrm{T}} \boldsymbol{M}_T$ 存在模 p 逆阵 $(\boldsymbol{M}_T^{\mathrm{T}} \boldsymbol{M}_T)_p^{-1}$,从而可按式(15)求解 $\boldsymbol{a}$,其中 $(\boldsymbol{M}_T^{\mathrm{T}} \boldsymbol{M}_T)_p^{-1}$ 可按文献[19-20]模 p 逆阵求解算法高效求解.

$$\boldsymbol{a} = ((\boldsymbol{M}_T^{\mathrm{T}} \boldsymbol{M}_T)_p^{-1} \boldsymbol{M}_T^{\mathrm{T}} \boldsymbol{FP}) \bmod p \tag{15}$$

相对于文献[16~18],主密钥(t,s,k,n)分存避免了影子图像连接; *key* 仅需计算 1 次;所构造的重要和非重要子密钥都是 GF(p)域整数,重要程度无法区分;子密钥相对于影子图像减小了信道负载,保管起来也更为方便,可选择不同策略对 *key* 恢复.

4　多版本备份策略

文献[14]和本文备份图 $\boldsymbol{S}^p$ 都是由密图 $\boldsymbol{S} = (s_{i,j})_{w \times h}$ 按 *key* 置乱的 *LL* 置乱子带 $\boldsymbol{S'}_{LL}$ 生成,如式(16)和式(17)所示.

$$\begin{cases} s_{i,j}^p = (l_7 l_6 l_5 l_3 l_2)_2 \\ s_{i+w/2,j}^p = (l_7 l_6 l_5 l_4 l_1)_2 \\ s_{i,j+h/2}^p = (l_7 l_6 l_4 l_3 l_2)_2 \\ s_{i+w/2,j+h/2}^p = (l_7 l_6 l_5 l_4 l_0)_2 \end{cases} \tag{16}$$

$$\begin{cases} s_{i,j}^p = (l_7 l_6 l_5 l_4 l_3 l_2)_2 \\ s_{i+w/2,j}^p = (l_7 l_6 l_5 l_4 l_3 l_2)_2 \\ s_{i,j+h/2}^p = (l_7 l_6 l_5 l_4 l_3 l_1)_2 \\ s_{i+w/2,j+h/2}^p = (l_7 l_6 l_5 l_4 l_3 l_0)_2 \end{cases} \tag{17}$$

式(16)将 $\boldsymbol{S'}_{LL}$ 像素 $s'^{LL}_{i,j} = (l_7 l_6 l_5 l_4 l_3 l_2 l_1 l_0)_2$ 按比特重要程度均分为 4 组:$l_7 l_6$, $l_5 l_4$, $l_3 l_2$ 和 $l_1 l_0$ 并依次备份 4、3、2 和 1 次,从而构造了 5 比特 $\boldsymbol{S}^p$ 像素. 式(17)将子带像素比特划分为显著比特 $l_7 l_6 l_5 l_4 l_3$,不显著比特 l_2 和最不显著比特 $l_1 l_0$,并依次备份 4、2 和 1 次,从而形成与 $\boldsymbol{S}$ 等大且每像素 6 比特的备份图 $\boldsymbol{S}^p$. 式(17)尽管增加 1 比特备份,但相对于式(16)提高了 $l_5 l_4 l_3$ 恢复能力,其中 $l_5 l_4$ 和 l_3 分别多备份了 1 次和 2 次.

文献[14]将 8 比特 $\boldsymbol{S}$ 和 5 比特 $\boldsymbol{S}^p$ 像素按式(3)分存,由于 $\boldsymbol{S}^p$ 像素只存放 1 次,导致恢复能力较低. 为避免该问题,本文将 1 个 $\boldsymbol{S}$ 像素和多个 $\boldsymbol{S}^p$ 备份像素在 GF(2^8)域分存,并依据 k 来确定 $\boldsymbol{S}^p$ 像素的备份数量.

在 GF(2^8)域,式(3)嵌入比特最大为 $8k$,其中 $\boldsymbol{S}$ 和 $\boldsymbol{S}^p$ 像素分别消耗 8 比特和 6 比特,因此当 $k=2$ 时,只能嵌入 1 个 $\boldsymbol{S}^p$ 像素;当 $k=3$ 时,为保持足够认证精度依然只备份 1 次 $\boldsymbol{S}^p$ 像素;当 $k>3$ 时,将备份数控制为 $k-2$,从而 $\boldsymbol{S}$ 和 $\boldsymbol{S}^p$ 像素总共消耗 $6k-4$ 比特. 为保证 $\boldsymbol{S}^p$ 安全性和攻击后恢复概率,将 $\boldsymbol{S}^p$ 置乱为不同版本以降低同位置像素被同时攻击的可能性,将其称为多版本备份策略. 这里可将 *key* 与 $\boldsymbol{S}^p$ 置乱绑定,当 $k \geq 3$ 时,由 *key* 产生随机数 $key_0, key_1, \cdots, key_{k-3}$ 将 $\boldsymbol{S}^p$ 置乱为不同版本 $\boldsymbol{S}^{p_0}, \boldsymbol{S}^{p_1}, \cdots, \boldsymbol{S}^{p_{k-3}}$;当 $k=2$ 时,则由 *key* 将 $\boldsymbol{S}^p$ 置乱为 $\boldsymbol{S}^{p_0}$. 表 1 给出了备份策略对比.

表 1 多版本备份同文献[14]单备份的对比

门限 k	文献[14]								本文							
	l_7	l_6	l_5	l_4	l_3	l_2	l_1	l_0	l_7	l_6	l_5	l_4	l_3	l_2	l_1	l_0
2	4	4	3	3	2	2	1	1	4	4	4	4	4	2	1	1
3									4	4	4	4	4	2	1	1
4									8	8	8	8	8	4	2	2
5									12	12	12	12	12	6	3	3

从表 1 可看出,多版本备份明显好于单备份,且随 k 增加,备份比特数明显增加,具备更好的密图重建和恢复能力.

5 限制性双重认证和多版本备份恢复策略

本文在保持 $\boldsymbol{S}^p$ 充分备份的前提下,仅保留有限认证精度,但依然保持同文献[14]同等或相近的认证精度,将其称为限制性双重认证策略.

这里按式(18)将 key 映射为与 $s_{i,j}$ 和 $s_{i,j}^{p_0}, s_{i,j}^{p_1}, \cdots s_{i,j}^{p_z}$ 及 (i,j) 相关的密钥 $key_{i,j}$,其中 $k=2$ 时,$z=0$;$k\geq 3$ 时,$z=k-3$,目的是只有正确的 $\boldsymbol{S}$ 和 $\boldsymbol{S}^p$ 像素及坐标才能产生正确的前向认证信息. 这里以 $key_{i,j}$ 为种子生成随机数 $r_{i,j}^0, r_{i,j}^1, \cdots, r_{i,j}^{k-3}, r_{i,j}^{k-2}$ 并按式(19)生成 $s_{i,j}$ 和 $s_{i,j}^{p_0}, s_{i,j}^{p_1}, \cdots s_{i,j}^{p_z}$ 前向认证信息 $check_{i,j}^0, check_{i,j}^1, \cdots, check_{i,j}^{k-2}$.

$$key_{i,j}=\begin{cases} s_{i,j}\times s_{i,j}^{p_0}+s_{i,j}+s_{i,j}^{p_0}+key+i+j+i\times j, & k=2 \\ s_{i,j}\times(s_{i,j}^{p_0}+s_{i,j}^{p_1}+\cdots+s_{i,j}^{p_{k-3}})+key+i+j+i\times j, & k\geq 3 \end{cases} \tag{18}$$

$$\left.\begin{array}{l} check_{i,j}^0=r_{i,j}^0(\bmod 2^2) \\ check_{i,j}^1=r_{i,j}^1(\bmod 2^2) \\ \cdots \\ check_{i,j}^{k-3}=r_{i,j}^{k-3}(\bmod 2^2) \\ check_{i,j}^{k-2}=r_{i,j}^{k-2}(\bmod 2^8) \end{array}\right\}\begin{array}{l} k=2 \\ k\geq 3 \end{array} \tag{19}$$

在式(19)中,当 $k=2$ 时,前向认证信息 $check_{i,j}^0$ 共 2 比特;当 $k\geq 3$ 时,前向认证信息 $check_{i,j}^0, check_{i,j}^1, \cdots, check_{i,j}^{k-2}$ 共 $2k+4$ 比特. 按式(20)对前向认证信息、$\boldsymbol{S}$ 和 $\boldsymbol{S}^p$ 像素比特重组,从而按式(3)在 GF(2^8)域得到分存信息 $f_{GF}^{i,j}(\dot{S}_u)$,$u=0,1,\cdots,n-1$,$S_u=P_u \bmod 2^8$.

$$\left.\begin{array}{l} r_0=s_{i,j} \\ r_1=2^6\cdot check_{i,j}^0+s_{i,j}^{p_0} \\ \vdots \\ r_{k-2}=2^6\cdot check_{i,j}^{k-3}+s_{i,j}^{p_{k-3}} \\ r_{k-1}=check_{i,j}^{k-2} \end{array}\right\}\begin{array}{l} k=2 \\ k\geq 3 \end{array} \tag{20}$$

记 $f_{GF}^{i,j}(\dot{S}_u)$ 对应的 2 进制数为 $o_{i,j}^u=(o_7^{i,j,u}\ o_6^{i,j,u}\ o_5^{i,j,u}\ o_4^{i,j,u}\ o_3^{i,j,u}\ o_2^{i,j,u}\ o_1^{i,j,u}\ o_0^{i,j,u})_2$,$u=0,1,\cdots,n-1$,对每个 $o_{i,j}^u$ 按式(21)映射为 $key_{i,j}^u$ 并生成 1 位随机数作为 $o_{i,j}^u$ 后向认证比特 $v_{i,j}^u$,将 $o_{i,j}^u$ 和 $v_{i,j}^u$ 划分为 4 组:$o_0^{i,j,u}o_1^{i,j,u}$,$o_2^{i,j,u}o_3^{i,j,u}$,$o_4^{i,j,u}o_5^{i,j,u}$ 和 $o_6^{i,j,u}o_7^{i,j,u}v_{i,j}^u$ 按 OPAP[15] 嵌入掩体 $\boldsymbol{C}^u$ 像素 $c_{2i,2j}^u$,$c_{2i,2j+1}^u$,$c_{2i+1,2j}^u$,$c_{2i+1,2j+1}^u$ 的低位比特上作为嵌密掩体 $\boldsymbol{C}'^u$.

$$key_{i,j}^u=(o_{i,j}^u\times key\times P_u+o_{i,j}^u+key+P_u+i+j+i\times j)\bmod p \tag{21}$$

式(21)将 P_u 和 key 及 (i,j) 用于后向认证比特生成,避免了用户对分发信息篡改和对认证比特的揣测. 式(18)~式(21)即构成了限制性双重认证比特分配策略,当 k 较小时,优先保证 $\boldsymbol{S}$ 和 $\boldsymbol{S}^p$ 像素的精确认证,当 k 较大时,则限制认证精度,保证 $\boldsymbol{S}$ 和 $\boldsymbol{S}^p$ 像素的恢复能力. 表 2 给出了认证能力对比. 从表 2 可看出,在 $k=2$,3 时,本文认证比特数高于文献[14],综合认证能力更高,当 $k\geq 4$ 时,本文认证比特尽管少于文献[14],但综合认证能力已趋于 100%,从而与文献[14]相当.

表 2 限制性双重认证同文献[14]双重认证的对比

门限 k	方法	认证比特数		区分度		综合认证能力
		前向	后向	密图备份图像素	分存信息	
2	文献[14]	1	1	$1/2^1$	$1/2^1$	$75\%=1-1/2^2$
	本文	2	1	$1/2^2$	$1/2^1$	$87.5\%=1-1/2^3$
3	文献[14]	8	1	$1/2^8$	$1/2^1$	$99.80\%\approx 1-1/2^9$
	本文	10	1	$1/2^{10}$	$1/2^1$	$99.95\%\approx 1-1/2^{11}$
4	文献[14]	15	1	$1/2^{15}$	$1/2^1$	$100.00\%\approx 1-1/2^{16}$
	本文	12	1	$1/2^{12}$	$1/2^1$	$99.99\%\approx 1-1/2^{13}$
5	文献[14]	22	1	$1/2^{22}$	$1/2^1$	$100.00\%\approx 1-1/2^{23}$
	本文	14	1	$1/2^{14}$	$1/2^1$	$100.00\%\approx 1-1/2^{15}$

限制性双重认证在使用方式上同文献[14]一致.由于限制性双重认证取决于 *key* 能否重构,并进一步和主密钥(t,s,k,n)分存策略绑定,使得满足(t,s,k,n)约束的参与者才能进行双重认证并检验真实性.

由于本文是将 $s_{i,j}$ 和 $s_{i,j}^{p}$ 涉及的多版本 $s_{i,j}^{p_0},s_{i,j}^{p_1},\cdots,s_{i,j}^{p_z}$ 按式(3)分存,因此式(4)恢复出的 $s_{i,j}^{p}$ 涉及(i_0,j_0),(i_1,j_1),$\cdots$,(i_z,j_z)位置的多个版本 $s_{i_0,j_0}^{p},s_{i_1,j_1}^{p},\cdots,s_{i_z,j_z}^{p}$,为标识认证情况,按算法 1 构建 $\boldsymbol{S}_{init}$ 和 $\tilde{\boldsymbol{S}}^{p_0},\tilde{\boldsymbol{S}}^{p_1},\cdots,\tilde{\boldsymbol{S}}^{p_z}$ 并生成认证图 $\boldsymbol{A},\tilde{\boldsymbol{A}}^{p_0},\tilde{\boldsymbol{A}}^{p_1},\cdots,\tilde{\boldsymbol{A}}^{p_z}$,其中 $\boldsymbol{A}=(a_{i,j})_{w\times h}$.

算法 1　$\boldsymbol{S}_{init},\tilde{\boldsymbol{S}}^{p_0},\tilde{\boldsymbol{S}}^{p_1},\cdots,\tilde{\boldsymbol{S}}^{p_z}$及$\boldsymbol{A},\tilde{\boldsymbol{A}}^{p_0},\tilde{\boldsymbol{A}}^{p_1},\cdots,\tilde{\boldsymbol{A}}^{p_z}$构建算法

第 1 步:初始化 $\boldsymbol{A},\tilde{\boldsymbol{A}}^{p_0},\tilde{\boldsymbol{A}}^{p_1},\cdots,\tilde{\boldsymbol{A}}^{p_z}$ 全为$(0)_{w\times h}$,其中 0 和 1 表示认证通过和失败.

第 2 步:对参与者嵌密掩体提取的分存信息和认证比特进行第 1 重认证,若(i,j)位置分存信息通过认证的数量大于等于 k,则标记 $a_{i,j}=1$.

第 3 步:对 $\boldsymbol{A}$ 标记 1 位置的分存信息按式(4)重构 S_{init} 和 $\tilde{\boldsymbol{S}}^{p_0},\tilde{\boldsymbol{S}}^{p_1},\cdots,\tilde{\boldsymbol{S}}^{p_z}$,若重构 $s_{i,j}^{init}$ 和 $\tilde{s}_{i,j}^{p_0},\tilde{s}_{i,j}^{p_1},\cdots,\tilde{s}_{i,j}^{p_z}$ 未通过第 2 重认证,则标记 $a_{i,j}=0$.

第 4 步:将 $\boldsymbol{A}$ 赋值给 $\tilde{\boldsymbol{A}}^{p_0},\tilde{\boldsymbol{A}}^{p_1},\cdots,\tilde{\boldsymbol{A}}^{p_z}$,由 *key* 产生随机数种子 $key_0,key_1,\cdots,key_z$,将 $key_z,z=0,1,\cdots,k-3$ 用作对 $\tilde{\boldsymbol{S}}^{p_z},\tilde{\boldsymbol{A}}^{p_z}$ 同样逆置乱,当 $k=2$ 时,则直接由 *key* 将 $\tilde{\boldsymbol{S}}^{p_0},\tilde{\boldsymbol{A}}^{p_0}$ 逆置乱为 $\tilde{\boldsymbol{S}}'^{p_0},\tilde{\boldsymbol{A}}'^{p_0}$.

第 5 步:将 $\tilde{\boldsymbol{S}}'^{p_0},\tilde{\boldsymbol{S}}'^{p_1},\cdots,\tilde{\boldsymbol{S}}'^{p_z}$ 和 $\tilde{\boldsymbol{A}}'^{p_0},\tilde{\boldsymbol{A}}'^{p_1},\cdots,\tilde{\boldsymbol{A}}'^{p_z}$ 重新作为 $\tilde{\boldsymbol{S}}^{p_0},\tilde{\boldsymbol{S}}^{p_1},\cdots,\tilde{\boldsymbol{S}}^{p_z}$ 和 $\tilde{\boldsymbol{A}}^{p_0},\tilde{\boldsymbol{A}}^{p_1},\cdots,\tilde{\boldsymbol{A}}^{p_z}$,然后和 $\boldsymbol{S}_{init},\boldsymbol{A}$ 一起输出.

记 $cnt_q,q\in[0,7]$ 为 $\tilde{s}_{i,j}^{p_z},\tilde{s}_{i+w/2,j}^{p_z},\tilde{s}_{i,j+h/2}^{p_z},\tilde{s}_{i+w/2,j+h/2}^{p_z}$ 存储的 $s'^{LL}_{i,j}$ 第 q 比特 l_q 累计认证通过次数,$sum_q,q\in[0,7]$ 为第 q 比特累计值,这里按式(22) sum_q 对 cnt_q 的统计均值来对 l_q 高置信度重建,其中[ ]为四舍五入取整,$cnt_q=0$ 是所有备份比特认证失败的极端情况. $s'^{LL}_{i,j}$ 重建过程记为算法 2.

$$l_q=\begin{cases}[sum_q/cnt_q], & cnt_q\neq 0\\ 1, & cnt_q=0\end{cases}\tag{22}$$

算法 2　$s'^{LL}_{i,j},i=0,1,\cdots,w/2-1,j=0,1,\cdots,h/2-1$ 重建算法

第 1 步:初始化 $cnt_q=sum_q=0,q\in[0,7]$,依次扫描(i,j),$(i+w/2,j)$,$(i,j+h/2)$,$(i+w/2,j+h/2)$位置 $\tilde{\boldsymbol{S}}^{p_0},\tilde{\boldsymbol{S}}^{p_1},\cdots,\tilde{\boldsymbol{S}}^{p_z}$ 元素,若其通过 $\tilde{\boldsymbol{A}}^{p_0},\tilde{\boldsymbol{A}}^{p_1},\cdots,\tilde{\boldsymbol{A}}^{p_z}$ 认证,则将其转换为 6 比特 $bit_0,bit_1,\cdots,bit_5$.

第 2 步:若 $bit_0,bit_1,\cdots,bit_5$ 中存在 l_q,则按式(23)更新 sum_q 和 $cnt_q,q\in[0,7]$.

$$\begin{aligned}sum_q&=sum_q+l_q\\ cnt_q&=cnt_q+1\end{aligned}\tag{23}$$

第 3 步:反复执行第 1 步~第 2 步,直至扫描完 $\tilde{\boldsymbol{S}}^{p_0},\tilde{\boldsymbol{S}}^{p_1},\cdots,\tilde{\boldsymbol{S}}^{p_z}$ 所有位置,按式(22)重建并输出 $s'^{LL}_{i,j}=(l_7l_6l_5l_4l_3l_2l_1l_0)_2$.

相对于文献[14],本文可充分利用不同位置备份的同一比特对备份图高置信度地恢复.同时备份比特分散在不同备份图的不同位置,具备较好的抗攻击能力.尽管本文后向认证比特数较少,但高置信度的 $\boldsymbol{S}'_{LL}$ 重建策略会纠正误判概率.

6　所提算法

以下给出完整分存算法,记为算法 3.

算法 3　多版本备份和限制性双重认证主密钥(t,s,k,n)图像分存算法

第 1 步:输入 t,s,k,n 且满足 $0<t\leq s\leq k\leq n$,$\boldsymbol{S}=(s_{i,j})_{w\times h}$,$\boldsymbol{C}^u=(c^u_{i,j})_{2w\times 2h},u=1,2,\cdots,n,key\in\{1,2,\cdots,p-1\}$,由 *key* 生成 $P_0,P_1,\cdots,P_{n-1}\in\{1,2,\cdots,p-1\}$ 且满足 $P_0 \bmod 256,P_1 \bmod 256,\cdots,P_{n-1} \bmod 256$ 两两不等.

第 2 步:由 *key* 将 $\boldsymbol{S}$ 的 *LL* 子带置乱为 $\boldsymbol{S}'_{LL}$ 并按式(17)构造 $\boldsymbol{S}^p$,若 $k\geq 3$ 时,由 *key* 产生随机数 $key_0,key_1,\cdots,key_{k-3}$ 将 $\boldsymbol{S}^p$ 置乱为 $\boldsymbol{S}^{p_0},\boldsymbol{S}^{p_1},\cdots,\boldsymbol{S}^{p_{k-3}}$,当 $k=2$ 时,则由 *key* 将 $\boldsymbol{S}^p$ 置乱为 $\boldsymbol{S}^{p_0}$.

第 3 步:将 *key* 按式(18)映射为 $key_{i,j}$,由式(19)生成 $check^0_{i,j},check^1_{i,j},\cdots,check^{k-2}_{i,j}$.

第 4 步:将 $s_{i,j},s_{i,j}^{p_0},s_{i,j}^{p_1},\cdots,s_{i,j}^{p_{k-3}}$ 以及 $check^0_{i,j},check^1_{i,j},\cdots,check^{k-2}_{i,j}$ 按式(20)重组并按式(3)在 GF(2^8)域分存产生 $f^{i,j}_{GF}(\dot{\boldsymbol{S}}_u)$,$u=0,1,\cdots,n-1$,$\boldsymbol{S}_u=P_u \bmod 2^8$(当 $k=2$ 时,则仅有 $s^{p_0}_{i,j}$).

第 5 步:将 $f^{i,j}_{GF}(\dot{\boldsymbol{S}}_u)$ 对应的 2 进制数 $o^u_{i,j}=(o_7^{i,j,u}o_6^{i,j,u}o_5^{i,j,u}o_4^{i,j,u}o_3^{i,j,u}o_2^{i,j,u}o_1^{i,j,u}o_0^{i,j,u})_2,u=0,1,\cdots,n-1,key$ 以及 $P_0,P_1,\cdots,P_{n-1}$ 按式(21)映射为 $key^u_{i,j}$ 并产生 $o^u_{i,j}$ 后向认证比特 $v^u_{i,j}$.

第 6 步:将 $o^u_{i,j}$ 和 $v^u_{i,j}$ 划分为 4 组:$o_0^{i,j,u}o_1^{i,j,u}$,$o_2^{i,j,u}o_3^{i,j,u}$,$o_4^{i,j,u}o_5^{i,j,u}$ 和 $o_6^{i,j,u}o_7^{i,j,u}v^u_{i,j}$ 并利用 OPAP 嵌入到掩体 $\boldsymbol{C}^u$ 像素 $c^u_{2i,2j},c^u_{2i,2j+1},c^u_{2i+1,2j},c^u_{2i+1,2j+1}$ 低位比特上.

第 7 步:重复第 3 步~第 6 步直至处理完所有密图像素,可得 $\boldsymbol{C}'^u,u=0,1,\cdots,n-1$.

第 8 步:将 *key* 及其产生的 $a_1,a_2,\cdots,a_{k-1}$ 按式(5)映射为 a_0,其中 $a_0,a_1,\cdots,a_{k-1}\in\{1,2,\cdots,p-1\}$,将 $a_0,a_1,\cdots,a_{k-1}$ 和 $a_i,a_{i+1},\cdots,a_{k-1}$ 分别按式(7)和式(8)得到重要子密钥 $subkey_0,subkey_1,\cdots,subkey_{s-1}$ 和非重要子密钥 $subkey_s,subkey_{s+1},\cdots,subkey_{n-1}$.

第 9 步:将 $\boldsymbol{C}'^u,(subkey_u,P_u),u=0,1,\cdots,n-1$ 前 s 个和后 $n-s$ 分发给重要和非重要参与者,将$(subkey_u,P_u),u=0,1,\cdots,n-1$ 的 MD5 值公布到第 3 方公信方以防止参与者作弊并销毁中间参数.

与之对应的恢复算法记为算法 4.

算法 4　多版本备份和限制性双重认证主密钥(t,s,k,n)图像恢复算法

第 1 步:配置 t,s,k,n,输入重要分发密钥和嵌密掩体$(subkey_{IP_v},IP_v)$,$\boldsymbol{C}'^{IP_v}=(c'^{IP_v}_{i,j})_{2w\times 2h},v=0,1,\cdots,m_1-1$ 以及非重要分发密钥和嵌密掩体$(subkey_{NP_r},NP_r)$,$\boldsymbol{C}'^{NP_r}=(c'^{NP_r}_{i,j})_{2w\times 2h},r=0,1,\cdots,m_2-1$.

第 2 步:若分发密钥 MD5 值与第 3 方存储的 MD5 值不一致,则拒绝恢复,记通过检验的重要和非重要参与者数量分别为 m'_1,m'_2,若不满足 $m'_1\geq t,m'_1+m'_2\geq k$,则失败退出,不失一般性,假设 $m'_1=m_1,m'_2=m_2$.

第 3 步:若 $m_1=t$,则按式(2)对式(8)和式(10)系数恢复,反之按式(15)对式(7)全部系数恢复,然后按式(6)计算 *key*.

第 4 步:由算法 1 得到 $\boldsymbol{S}_{init},\tilde{\boldsymbol{S}}^{p_0},\tilde{\boldsymbol{S}}^{p_1},\cdots,\tilde{\boldsymbol{S}}^{p_z}$ 以及 $\boldsymbol{A},\tilde{\boldsymbol{A}}^{p_0},\tilde{\boldsymbol{A}}^{p_1},\cdots,\tilde{\boldsymbol{A}}^{p_z}$.

第 5 步:由算法 2 得到 $\boldsymbol{S}'_{LL}$ 像素 $s'^{LL}_{i,j}$,其中 $i=0,1,\cdots,w/2-1,j=0,1,\cdots,h/2-1$.

第 6 步:由 key 对 $\boldsymbol{S}'_{LL}$ 逆置乱并产生 $\boldsymbol{S}_{ref}$,结合邻近像素点插值拟合和修复参考图像素替代修复[14]重建并输出 $\boldsymbol{S}_{final}$.

同现有方法相比,所提方法避免了中间影子图像连接[16~17],恢复的高复杂度[18];可利用 Lagrange 插值或模 p 矩阵求逆高效求解[19~20];所提出的多版本备份可高置信度地恢复备份图,而限制性双重认证综合认证能力趋近或等同于文献[14].

7 实验

实验选取(1,2,2,5)和(2,3,4,5)方案进行测试,取 $key=131819$, $p=1000000007$. 图 1 是分辨率 256×256 和 512×512 的测试图像. 实验按式(24)和式(25)计算图像差异和衡量图像恢复质量,按攻击识别率[14]评判认证能力. 表格中的"–"为不存在.

(a) Boats (b) Baboon (c) F16 (d) Sailboat (e) Lena (f) Peppers

图 1 测试图像

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

$$\mathrm{PSNR}=10\times\log_{10}\frac{255^2}{\mathrm{MSE}} \tag{25}$$

式(24)中,$p_{i,j}$,$p'_{i,j}$为像素值,$w\times h$ 为图像分辨率.

7.1 主密钥(t,s,k,n)方案的验证和对比实验

对 key 按算法 3 第 8 步~第 9 步进行(t,s,k,n)分存,并按算法 4 第 1 步~第 3 步重构 key,然后和文献[16~18]对比. 表 3 和表 4 分别给出了分发密钥分配表和 key 恢复结果.

表 4 除了分组 4~7 和 10 以外,都能恢复 key. 原因这些分组都不满足(t,s,k,n)约束,因此正确性得以验证.

表 3 主密钥(t,s,k,n)分存分发密钥分配表

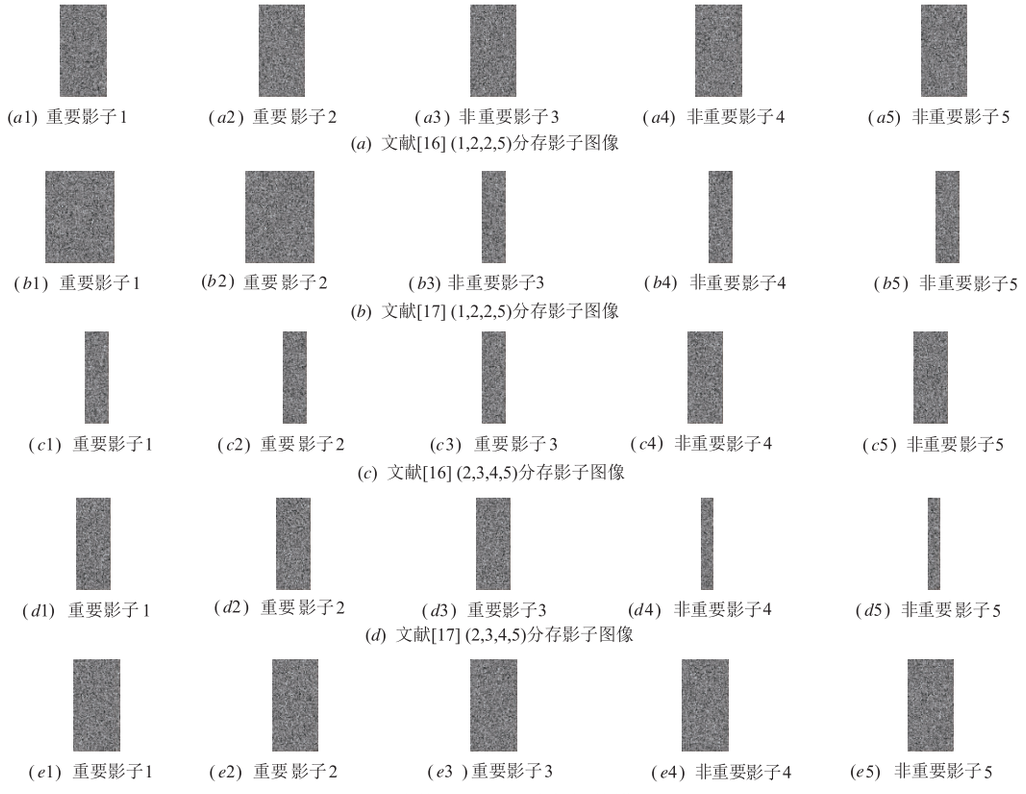
分存方案	参与者类型	参与者编号	分发密钥		MD5 值
			子密钥	随机参与值	
(1,2,2,5)	重要	1	523700256	29	0xed86707769098ce8985486a379d0a88e
		2	523712172	32	0x3f570025b758d1151ca618daadc70053
	不重要	3	258180	65	0x51e247b12047203e98b5cf8cf3362285
		4	131076	33	0x1f7d5777559c4ee758b842e1a577e0a8
		5	492528	124	0x2b37e86b9bd44c83033bd9ba9b832a8c
(2,3,4,5)	重要	1	140081739	29	0x5550e2ee2527f3fbaa2bf54ea0234a3d
		2	162716440	32	0xc8e3de51628e427778c8141666f4c975
		3	546152121	65	0xd0ea6a6f28c8a2c4e390796e3195359a
	不重要	4	133502952	33	0xf851b9080e70a771c9a99f7fc9d26f31
		5	862904073	124	0x1f4efd5c98b730cef4d3779061f04a95

表 4 主密钥(t,s,k,n)分存恢复结果

分存方案	分组编号	参与者编号	数量		是否满足(t,s,k,n)	主密钥	
			重要	非重要		实际	恢复
(1,2,2,5)	1	1,2	2	0	是	131819	131819
	2	1,3	1	1	是	131819	131819
	3	2,4,5	1	2	是	131819	131819
	4	3,4,5	0	3	否	131819	–
	5	1	1	0	否	131819	–

续表

分存方案	分组编号	参与者编号	数量		是否满足(t,s,k,n)	主密钥	
			重要	非重要		实际	恢复
(2,3,4,5)	6	1,2	2	0	否	131819	–
	7	1,2,3	3	0	否	131819	–
	8	1,2,3,4	3	1	是	131819	131819
	9	2,3,4,5	2	2	是	131819	131819
	10	4,5	0	2	否	131819	–



(a) 文献[16] (1,2,2,5)分存影子图像

(b) 文献[17] (1,2,2,5)分存影子图像

(c) 文献[16] (2,3,4,5)分存影子图像

(d) 文献[17] (2,3,4,5)分存影子图像

(e) 文献[18] (2,3,4,5)分存影子图像

图2　文献[16~18] (t,s,k,n)分存策略分发影子图像

图2是以图1(a)为密图按文献[16~18]构造的影子图像,由于文献[18]$k\neq2$,因此仅给出了(2,3,4,5)影子图像. 表5给出了影子图像大小.

从图2和表5可看出,文献[16]除$k-t=1$时,重要和非重要影子图像大小相等;文献[17]则所有情况下重要和非重要影子图像大小不等. 文献[18]影子图像大小相等,但$k\neq2$. 另外文献[16~18]都是通过影子图像来构造(t,s,k,n)方案,计算量大. 文献[18]不能借助Lagrange插值恢复,涉及大量满秩方程组求解和求导,计算代价较高.

表5　文献[16~18]重要和非重要影子图像大小

文献	分存方案	重要影子图像		非重要影子图像		影子大小相等
		图像	分辨率	图像	分辨率	
文献[16]	(1,2,2,5)	图2(a1)~图2(a2)	128×256	图2(a3)~图2(a5)	128×256	是
文献[17]	(1,2,2,5)	图2(b1)~图2(b2)	192×256	图2(b3)~图2(b5)	64×256	否
文献[16]	(2,3,4,5)	图2(c1)~图2(c3)	64×256	图2(c4)~图2(c5)	96×256	否
文献[17]	(2,3,4,5)	图2(d1)~图2(d3)	96×256	图2(d4)~图2(d5)	32×256	否
文献[18]	(2,3,4,5)	图2(e1)~图2(e3)	128×256	图2(e4)~图2(e5)	128×256	是

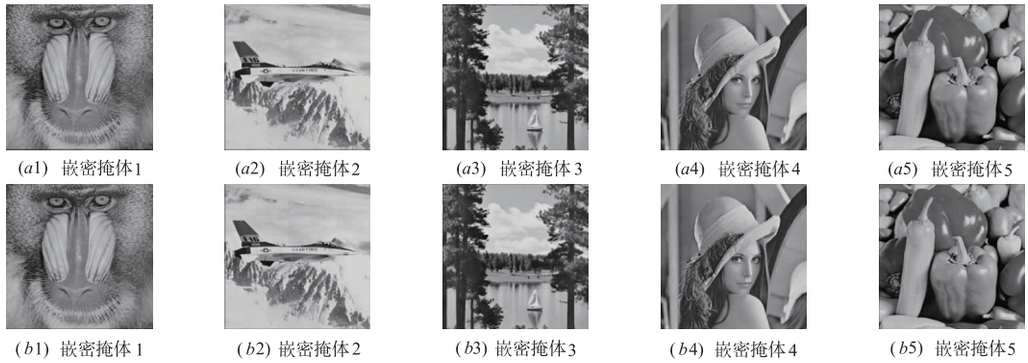
从表3和表4可看出,本文将影子图像转换为子密钥,且子密钥都是模 p 整数无法区分,以更小代价来构造更安全的分存策略且适用于 (t,s,k,n) 分存的各种情况.

从第3节可看出,本文相对于文献[16~18]在计算和恢复代价,安全性和普适性上具有更好的性能.

7.2 嵌密掩体视觉质量和密图恢复质量验证实验

在7.1节的基础上,以图1(a)为密图,图1其他图像为掩体,按算法3分存并按算法4重构,然后对嵌密掩体和最终重构密图的视觉质量进行测试. 图3为嵌密掩体,表6衡量了嵌密掩体视觉质量,表7为密图重构结果,图4是重构密图.

从图3和表6可看出,无论是(1,2,2,5),还是(2,3,4,5)分存,嵌密掩体PSNR大约为44.75dB左右,视觉质量普遍较好,隐藏密图难以发现.



(a1) 嵌密掩体1 (a2) 嵌密掩体2 (a3) 嵌密掩体3 (a4) 嵌密掩体4 (a5) 嵌密掩体5

(b1) 嵌密掩体1 (b2) 嵌密掩体2 (b3) 嵌密掩体3 (b4) 嵌密掩体4 (b5) 嵌密掩体5

图3 主密钥(1,2,2,5)和(2,3,4,5)分存嵌密掩体

结合图4、表6和表7并对比表4可看出,仅有满足 (t,s,k,n) 约束的分组才能完整重构密图. 图4、表6和表7与表4一一对应,原因是只有当 key 通过 (t,s,k,n) 重构,密图才能恢复,因此结合主密钥 (t,s,k,n) 方案,对密图的分存和恢复也是 (t,s,k,n) 方案,从而相对于文献[16~18]具有最小的 (t,s,k,n) 构造代价.

表6 主密钥 (t,s,k,n) 分存嵌密掩体视觉质量(PSNR:dB)

分存方案	掩体1:图1(b)		掩体2:图1(c)		掩体3:图1(d)		掩体4:图1(e)		掩体5:图1(f)	
	嵌密掩体	PSNR	嵌密掩体	PSNR	嵌密掩体	PSNR	嵌密掩体	PSNR	嵌密掩体	PSNR
(1,2,2,5)	图3(a1)	44.75	图3(a2)	44.75	图3(a3)	44.76	图3(a4)	44.75	图3(a5)	44.75
(2,3,4,5)	图3(b1)	44.75	图3(b2)	44.74	图3(b3)	44.75	图3(b4)	44.75	图3(b5)	44.74

从图2和图3可看出,文献[16~18]传输的是无意义影子图像,而本文分发掩体都是有意义的且具备较高视觉质量,从而传输中不易引起怀疑,减少攻击的可能性.

(a) 1组 (b) 2组 (c) 3组 (d) 8组 (e) 9组

图4 主密钥(t,s,k,n)分存重构结果

7.3 多版本备份策略有效性验证实验

按算法3第2步取图1(a)LL子带分别按 $k=2$ 和 $k=4$ 构造多版本备份图,并施加强度为5%、20%、30%和50%的随机噪声,然后计算 LL 子带各比特位面的正确重建概率并按MSE衡量重建质量. 表8是与文献[14]的对比.

从表8可看出,当 $k=2$ 时,本文略优于文献[14],原因是 $k=2$ 时,本文与文献[14]都仅有1个备份图,只是 l_5 和 l_4 多备份了1次,l_3 多备份了2次,使得 l_5,l_4 和 l_3 恢复能力好于文献[14];当 $k=4$ 时,本文远好于文献[14],原因是本文2张备份图多于文献[14]1张备份图.

7.4 限制性双重认证策略有效性验证实验

对图3施加图5攻击,然后按算法4第3步~第6步恢复,计算认证图并和文献[14]对比. 图5是攻击模板,其中图5(g)~5(i)的噪声强度为8%、20%和50%. 表9是与文献[14]的对比,图6为本文和文献[14]认证图.

表 7　主密钥(t,s,k,n)分存密图重构结果

分存方案	分组编号	参与者编号	数量		是否满足(t,s,k,n)	密图		
			重要	非重要		原图	重构图	MSE
(1,2,2,5)	1	1,2	2	0	是	图 1(a)	图 4(a)	0
	2	1,3	1	1	是		图 4(b)	0
	3	2,4,5	1	2	是		图 4(c)	0
	4	3,4,5	0	3	否		–	–
	5	1	1	0	否		–	–
(2,3,4,5)	6	1,2	2	0	否	图 1(a)	–	–
	7	1,2,3	3	0	否		–	–
	8	1,2,3,4	3	1	是		图 4(d)	0
	9	2,3,4,5	2	2	是		图 4(e)	0
	10	4,5	0	2	否		–	–

表 8　本文多版本备份和文献[14]单一备份密图 LL 子带恢复结果

方法	门限 k	噪声强度%	恢复%								MSE
			l_7	l_6	l_5	l_4	l_3	l_2	l_1	l_0	
本文	2	5	100	100	100	100	100	99.86	97.29	92.86	0.084
		20	99.87	99.85	99.88	99.90	99.92	98.24	87.08	74.12	3.678
		30	99.46	99.37	99.46	99.63	99.66	95.57	78.82	64.20	18.334
		50	95.77	95.39	96.03	97.14	96.86	87.86	63.75	50.54	119.678
	4	5	100	100	100	100	100	100	99.88	99.61	0.004
		20	100	100	100	100	100	99.90	97.88	94.29	0.067
		30	99.99	99.99	100	99.99	99.99	99.57	94.78	87.28	0.396
		50	99.77	99.75	99.81	99.87	99.83	97.17	83.09	69.31	5.031
文献[14]	2 和 4	5	100	100	99.99	99.98	99.86	99.87	97.43	92.88	0.146
		20	99.86	99.85	99.54	99.09	97.38	97.99	86.95	74.48	5.918
		30	99.46	99.38	98.30	96.77	93.74	95.45	78.67	64.45	24.115
		50	95.77	95.26	92.55	87.88	81.54	88.26	63.71	51.25	127.010

(a) 攻击 1　(b) 攻击 2　(c) 攻击 3　(d) 攻击 4　(e) 攻击 5　(f) 攻击 6　(g) 攻击 7　(h) 攻击 8　(i) 攻击 9

图5　攻击模板

从表 9 可看出,在认证能力上,当 $k=2$ 时,本文前向和后向认证比特分别为 2 个和 1 个,文献[14]对应的认证比特均为 1 个,本文(1,2,2,5)优于文献[14];当 $k=4$ 时,本文前向和后向认证比特分别为 12 个和 1 个,文献[14]则分别是 15 个和 1 个,本文(2,3,4,5)低于文献[14],但两者都趋近于 100%. 从图 6 可看出,当 $k=2$ 时,左边认证图比右边更为清晰,说明本文(1,2,2,5)优于文献[14];当 $k=4$ 时,各组认证图中左边和右边的区别特征不明显,因此本文(2,3,4,5)和文献[14]认证能力上相当. 表 9 和图 6 与表 2 理论分析趋于一致,且随 k 增加,综合认证能力也趋于一致,但本文所需认证比特数更少,性能更优.

表 9 限制性双重认证与文献[14]双重认证对比

对比方法	分组编号	参与恢复掩体	分发掩体攻击			限制性双重认证策略		文献[14]双重认证策略	
			掩体1攻击	掩体2攻击	掩体3攻击	攻击别比率%	认证图	攻击别比率%	认证图
本文(1,2,2,5)和文献[14](2,5)	1	掩体1：图3(*a*1)	图5(*c*)	–	–	**87.16**	图6(*a*1)	75.26	图6(*a*2)
	2		图5(*g*)	–	–	**86.07**	图6(*b*1)	77.20	图6(*b*2)
	3	掩体2：图3(*a*2)	图5(*a*)	图5(*b*)	–	**87.14**	图6(*c*1)	76.19	图6(*c*2)
	4		图5(*c*)	图5(*e*)	–	**88.29**	图6(*d*1)	76.65	图6(*d*2)
本文(2,3,4,5)和文献[14](4,5)	5	掩体1：图3(*b*1)	图5(*c*)	–	–	99.99	图6(*e*1)	**100.00**	图6(*e*2)
	6		图5(*g*)	–	–	99.99	图6(*f*1)	**100.00**	图6(*f*2)
	7	掩体2：图3(*b*2)	图5(*b*)	图5(*e*)	–	99.98	图6(*g*1)	**100.00**	图6(*g*2)
	8		图5(*b*)	图5(*g*)	–	99.99	图6(*h*1)	**100.00**	图6(*h*2)
	9	掩体3：图3(*b*3)	图5(*g*)	图5(*h*)	–	99.99	图6(*i*1)	**100.00**	图6(*i*2)
	10		图5(*a*)	图5(*b*)	图5(*d*)	100.00	图6(*j*1)	**100.00**	图6(*j*2)
	11	掩体4：图3(*b*4)	图5(*d*)	图5(*f*)	图5(*g*)	99.98	图6(*k*1)	**100.00**	图6(*k*2)
	12		图5(*c*)	图5(*e*)	图5(*i*)	99.99	图6(*l*1)	**100.00**	图6(*l*2)

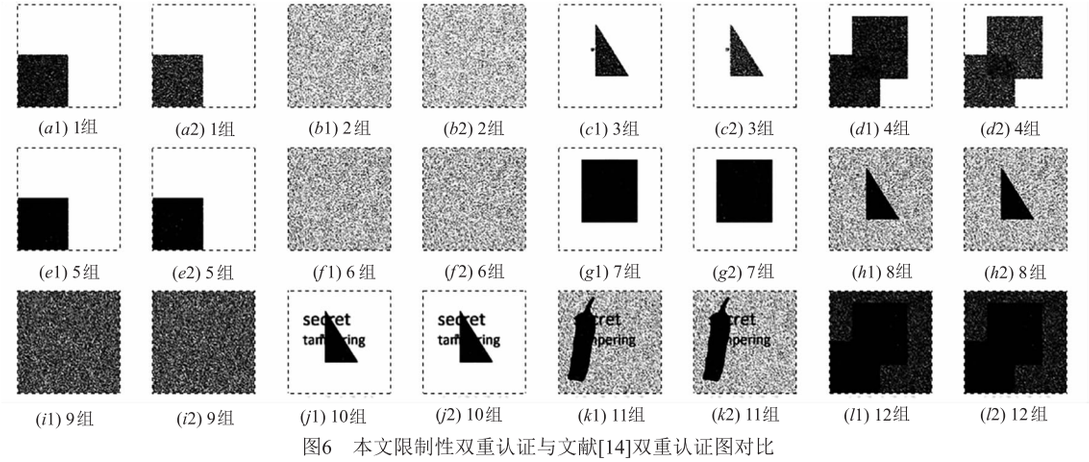


图6 本文限制性双重认证与文献[14]双重认证图对比

7.5 重构图像视觉质量对比实验

在7.4节基础上,在同等情况下,进一步对比本文和文献[14]密图重构视觉质量. 表10是与文献[14]的对比,其中PSNR列粗体表示行最大值,ΔPSNR列粗体表示PSNR差异中的最大值或最小值. 图7为修复图样.

从表10可看出,在同等情况下,本文重构密图视觉质量明显好于文献[14]. 对于(1,2,2,5)分存,PSNR提升了2.27~4.34dB;对于(2,3,4,5)分存PSNR提升为0.39~4.02dB且绝大多数样例提升都较为显著.

从图7可看出,本文第1幅比文献[14]第2幅的视觉恢复质量更为清晰. 原因是$k=2$时,本文认证精度更高且提升了中位比特l_5,l_4,l_3备份次数;当$k=4$时,本文和文献[14]认证精度都有了较大提升,视觉重构质量也明显提升,但本文在保持同等或相当的认证精度的同时,进一步增加了备份图数量,从而可联合多版本备份图的备份比特进一步增强密图重构能力.

7.6 综合性能对比

表11给出了与文献[11~14,16~18]的对比. 可看出本文相对于文献[11~14,16~18]具有更好的性能,适用面也更广.

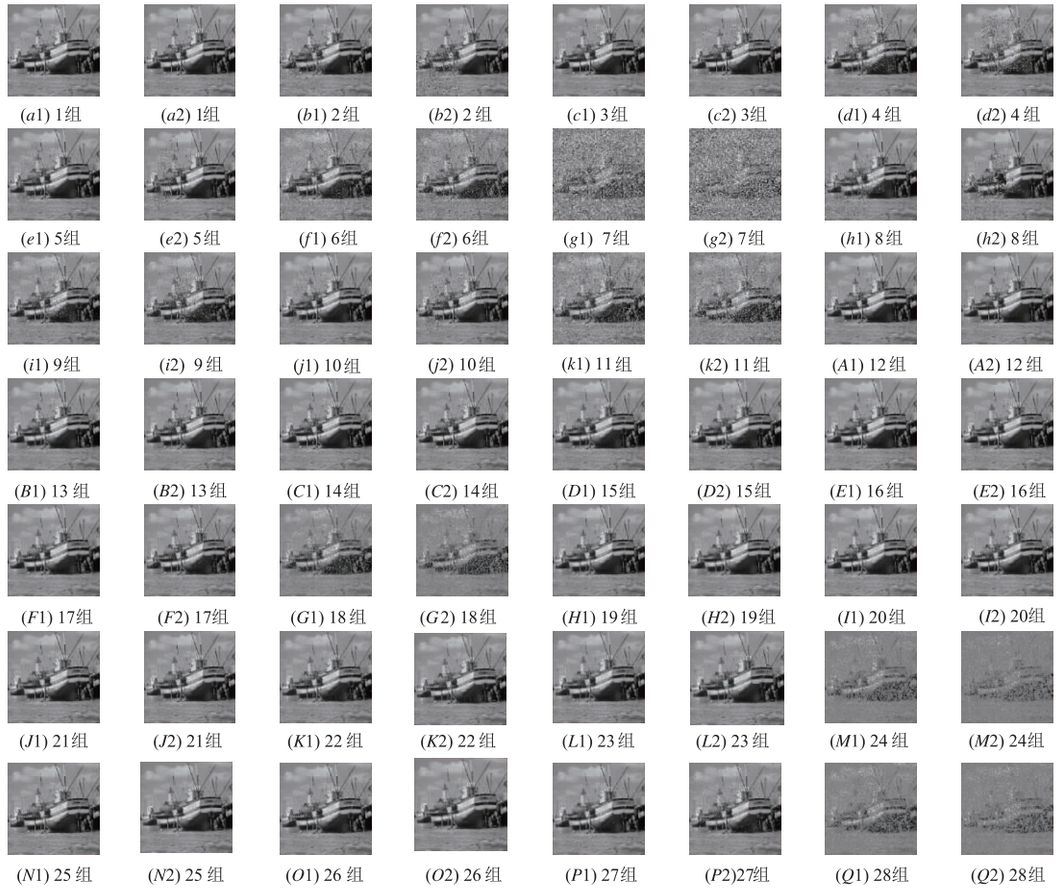


图7　本文和文献[14]最终修复图样

表 10　本文和文献[14]最终修复图像对比(PSNR:dB)

对比方法	分组编号	参与恢复掩体	分发掩体攻击			本文重构密图		文献[14]重构密图		ΔPSNR
			掩体1攻击	掩体2攻击	掩体3攻击	恢复图像	PSNR	恢复图像	PSNR	
本文(1,2,2,5)和文献[14](2,5)	1	掩体1:图3(a1) 掩体2:图3(a2)	图5(a)	–	–	图7(a1)	**44.76**	图7(a2)	40.42	**4.34**
	2		图5(c)	–	–	图7(b1)	**23.80**	图7(b2)	20.10	3.70
	3		图5(d)	–	–	图7(c1)	**31.76**	图7(c2)	27.81	3.95
	4		图5(e)	–	–	图7(d1)	**21.64**	图7(d2)	18.77	2.97
	5		图5(f)	–	–	图7(e1)	**27.26**	图7(e2)	23.95	3.31
	6		图5(h)	–	–	图7(f1)	**19.54**	图7(f2)	16.24	3.30
	7		图5(i)	–	–	图7(g1)	**13.92**	图7(g2)	11.20	2.72
	8		图5(b)	图5(c)	–	图7(h1)	**22.58**	图7(h2)	19.52	3.06
	9		图5(b)	图5(g)	–	图7(i1)	**22.36**	图7(i2)	20.09	**2.27**
	10		图5(d)	图5(f)	–	图7(j1)	**26.60**	图7(j2)	23.00	3.60
	11		图5(g)	图5(h)	–	图7(k1)	**18.01**	图7(k2)	15.27	2.74

续表

对比方法	分组编号	参与恢复掩体	分发掩体攻击			本文重构密图		文献[14]重构密图		ΔPSNR
			掩体1攻击	掩体2攻击	掩体3攻击	恢复图像	PSNR	恢复图像	PSNR	
本文(2,3,4,5)和文献[14](4,5)	12	掩体1：图3(*b*1) 掩体2：图3(*b*2) 掩体3：图3(*b*3) 掩体4：图3(*b*4)	图5(*a*)	–	–	图7(*A*1)	**49.92**	图7(*A*2)	49.53	**0.39**
	13		图5(*c*)	–	–	图7(*B*1)	**31.41**	图7(*B*2)	29.64	1.77
	14		图5(*d*)	–	–	图7(*C*1)	**38.57**	图7(*C*2)	36.83	1.74
	15		图5(*e*)	–	–	图7(*D*1)	**29.54**	图7(*D*2)	27.04	2.50
	16		图5(*f*)	–	–	图7(*E*1)	**35.17**	图7(*E*2)	33.40	1.77
	17		图5(*h*)	–	–	图7(*F*1)	**29.14**	图7(*F*2)	26.09	3.05
	18		图5(*i*)	–	–	图7(*G*1)	**21.31**	图7(*G*2)	17.69	3.62
	19		图5(*b*)	图5(*c*)	–	图7(*H*1)	**30.49**	图7(*H*2)	28.75	1.74
	20		图5(*b*)	图5(*g*)	–	图7(*I*1)	**30.91**	图7(*I*2)	29.01	1.90
	21		图5(*d*)	图5(*f*)	–	图7(*J*1)	**33.91**	图7(*J*2)	32.12	1.79
	22		图5(*g*)	图5(*h*)	–	图7(*K*1)	**27.19**	图7(*K*2)	23.42	3.77
	23		图5(*d*)	图5(*e*)	图5(*f*)	图7(*L*1)	**29.01**	图7(*L*2)	26.46	2.55
	24		图5(*g*)	图5(*h*)	图5(*i*)	图7(*M*1)	**18.33**	图7(*M*2)	15.79	2.54
	25		图5(*a*)	图5(*b*)	图5(*d*)	图7(*N*1)	**33.58**	图7(*N*2)	31.80	1.78
	26		图5(*a*)	图5(*b*)	图5(*g*)	图7(*O*1)	**30.90**	图7(*O*2)	28.91	1.99
	27		图5(*d*)	图5(*f*)	图5(*h*)	图7(*P*1)	**28.14**	图7(*P*2)	24.12	**4.02**
	28		图5(*c*)	图5(*e*)	图5(*i*)	图7(*Q*1)	**18.64**	图7(*Q*2)	15.98	2.66

表11 综合性能对比

比较方法	恢复条件	门限限制	认证能力	认证类型	参与者重要性	修复能力
文献[11]	(k,n)	$k\geq3$	1/16	对分存信息后向认证	无	弱
文献[12]	(k,n)	$k\geq3$	1/8	对分存信息后向认证	无	弱
文献[13]	近似(k,n),连续k个参与者	$k\geq3$	1/256	对分存信息后向认证	无	弱
文献[14]	(k,n)	$k\geq2$	$1/2^{7k-12}$	双重认证	无	强
文献[16]	(t,s,k,n)	$k\geq2$	无	无	有	无
文献[17]	(t,s,k,n)	$k\geq2$	无	无	有	无
文献[18]	(t,s,k,n)	$k\geq3$	无	无	有	无
本文	(t,s,k,n)	$k\geq2$	$k=2,1/8$ $k\geq3,1/2^{2k+5}$	限制性双重认证	有	很强

8 结论

以上,给出了一种多版本备份和限制性双重认证的主密钥(t,s,k,n)图像分存. 引入随机参与值将(t,s,k,n)分存中的影子图像构造转换为子密钥构造,通过(k,s)和$(k-t,n-s)$分存来产生重要和非重要子密钥并通过第3方公信方存储的MD5值以防止作弊. 所构造的(t,s,k,n)分存可依据参与恢复的重要参与者数量按Lagrange插值和模p矩阵求逆高效恢复. 为提高密图恢复能力,所提方案进一步通过主密钥对密图*LL*子带置乱来形成对显著比特多备份、对非显著比特少备份且经主密钥不同程度置乱的多版本备份图,引入限制性双重认证在保持一定认证精度的同时,将尽可能多的备份比特嵌入,通过GF(2^8)域(k,n)分存形成嵌密掩体.

同现有方法相比,避免影子图像参与恢复[16~18]导致的计算量大和计算复杂等问题;引入随机参与值避免了参与者编号泄露,对分发信息的篡改以及对认证比特的揣测;多版本备份可充分利用不同位置存储的比特对备份图高置信度地恢复且具备较好的抗攻击能

力,而限制性双重认证在认证能力上不低于文献[14].

参考文献

[1] Shamir A. How to share a secret[J]. Communications of the Association for Computing Machinery, 1979, 22(11): 612 – 613.

[2] Blakley G R. Safeguarding cryptographic keys[A]. Proceedings of 1979 National Computer Conference[C]. New York, USA: AFIPS, 1979. 48: 313 – 317.

[3] Thien C C, Lin J C. Secret image sharing[J]. Computers & Graphics, 2002, 26(5): 765 – 770.

[4] Kanso A, Ghebleh M. An efficient (t, n)-threshold secret image sharing scheme[J]. Multimedia Tools & Applications, 2016, 76(15): 1 – 20.

[5] Lin C C, Tsai W H. Secret image sharing with steganography and authentication[J]. Journal of Systems and Software, 2004, 73(3): 405 – 414.

[6] Yang C N, Chen T S, Yu K H, et al. Improvements of image sharing with steganography and authentication[J]. Journal of Systems and Software, 2007, 80(7): 1070 – 1076.

[7] Chang C C, Hsieh Y P, Lin C H. Sharing secrets in stego images with authentication[J]. Pattern Recognition, 2008, 41(10): 3130 – 3137.

[8] Ulutas M, Ulutas G, Nabiyev V V. Secret image sharing with enhanced visual quality and authentication mechanism[J]. The Imaging Science Journal, 2011, 59(3): 154 – 165.

[9] 欧阳显斌,邵利平,陈文鑫. 结合调整差值变换的(K,N)有意义图像分存方案[J]. 中国图象图形学报, 2015, 20(5): 633 – 642.
Ouyang Xianbin, Shao Liping, Chen Wenxin. Meaningful (K, N) image sharing scheme combined with the adjusting difference transformation[J]. Journal of Image and Graphics, 2015, 20(5): 633 – 642. (In Chinese)

[10] 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[J]. 计算机科学, 2015, 42(12): 251 – 256.
Ouyang Xianbin, Shao Liping. Meaningful (K, N) free expansion image sharing scheme based on GF(2^3)[J]. Computer Science, 2015, 42(12): 251 – 256. (in Chinese)

[11] Chang C C, Chen Y H, Wang H C. Meaningful secret sharing technique with authentication and remedy abilities[J]. Information Sciences, 2011, 181(14): 3073 – 3084.

[12] Chen Y H, Chang C C. Image tamper detection and recovery based on dual watermarks sharing strategy[J]. Journal of Digital Information Management, 2012, 10(1): 39 – 49.

[13] Wu X T, Sun W. Secret image sharing scheme with authentication and remedy abilities based on cellular automata and discrete wavelet transform[J]. Journal of Systems and Software, 2013, 86(4): 1068 – 1088.

[14] 欧阳显斌,邵利平,乐志芳. 非等量备份和双认证自修复有限域图像分存[J]. 软件学报, 2017, 28(12): 3306 – 3346.
Ouyang Xianbin, Shao Liping, Le Zhifang. Gloise field self-recovery image sharing scheme with non-equivalent backup and double authentications[J]. Journal of Software, 2017, 28(12): 3306 – 3346. (in Chinese)

[15] Chan C K, Cheng L M. Hiding data in images by simple LSB substitution[J]. Pattern Recognition, 2004, 37(3): 469 – 474.

[16] Li P, Yang C N, Wu C C, et al. Essential secret image sharing scheme with different importance of shadows[J]. Journal of Visual Communication & Image Representation, 2013, 24(7): 1106 – 1114.

[17] Yang C N, Li P, Wu C C, et al. Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach[J]. Signal Processing Image Communication, 2015, 31: 1 – 9.

[18] Li P, Yang C N, Zhou Z. Essential secret image sharing scheme with the same size of shadows[J]. Digital Signal Processing, 2016, 50: 51 – 60.

[19] 邵利平,覃征,衡星辰,等. 基于矩阵变换的图像置乱逆问题求解[J]. 电子学报, 2008, 36(7): 1355 – 1363.
Shao Liping, Qin Zheng, Heng xingchen, et al. Solution for the inverse problem of matrix transform based image scrambling[J]. Acta Electronica Sinica, 2008, 36(7): 1355 – 1363. (in Chinese)

[20] 邵利平. 数字图像置乱技术[M]. 北京:科学出版社, 2016. 56 – 94.

作者简介

邵利平(通信作者)　男,1978 年生于河南郑州. 博士,副教授,研究方向为数字图像音频置乱、加密、密写、水印、隐匿、分存、伪装和欺骗等.
E-mail: slpmaster@163.com

乐志芳　女,1993 年生于江西抚州,硕士,研究方向为数字图像分存.