第44卷 第6期 西 安 交 通 大 学 学 报 Vol. 44 №6
2010年6月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Jun. 2010

应用细粒度分块重构的多信道图像信息分存算法

张选平，李春枚，邵利平
（西安交通大学计算机科学与技术系，710049，西安）

摘要：针对传统图像信息分存方法存在的抵御信道攻击能力有限、分发子信息利用率不高以及要求恢复秘密图像必须无损等问题，提出了一种基于细粒度分块重构的多信道图像信息分存算法.利用拉格朗日分存算法对秘密图像进行分存，以形成分发子信息；对每个分发子信息进行细粒度分块，并依次通过雪崩图像置乱变换获得分块甄别信息；将分发子信息与甄别信息用LSB法隐藏到掩体图像中，并通过多个信道传送.对接收到的每个分发子信息进行细粒度分块甄别，利用所有分发子信息中未受损部分对秘密图像进行重构.实验结果表明，所提算法能够精确地甄别攻击，提高各分发子信息的利用率，高效地重构秘密图像，即使在所有分发子信息受到一定攻击的情况下，也能充分利用各分发子信息重构出秘密图像.

关键词：图像信息分存；分发子信息；图像置乱变换；拉格朗日分存算法
中图分类号：TP391 **文献标志码**：A **文章编号**：0253-987X(2010)06-0078-05

A Sharing Scheme of Multi-Channel Image Information in Small Granularity Block Reconstruction

ZHANG Xuanping, LI Chunmei, SHAO Liping
(Department of Computer Science and Technology, Xi′an Jiaotong University, Xi′an 710049, China)

Abstract: A sharing scheme of multi-channel image information in small granularity block reconstruction is proposed to improve the problems existing in conventional sharing schemes of image information, such as the limited ability in resisting channel attacks, the low utilization of distributed sub-information, and the requirement of the lossless restored secret image. Firstly, the secret image is shared to generate distributed sub-information using the Lagrange interpolation sharing algorithm. Then the avalanche image scrambling transformation algorithm is utilized to transform each block of distributed sub-information to gain authentication information. The LSB method is used to embed authentication information and distributed sub-information into host images, and then the host images are transmitted in multi-channel. The proposed method uses the embedded authentication information to identify the distributed sub-information in small granularity block, and makes full use of the undamaged blocks of the distributed sub-information to reconstruct the secret image. Experimental results show that the proposed scheme can identify attacks effectively, raise the utilization rate of the distributed sub-information, and reconstruct the secret image efficiently. Even when all of the distributed sub-information are subject to certain attacks, it can also make full use of the undamaged blocks of distributed sub-information to reconstruct the secret image.

Keywords: image information sharing; distributed sub-information; image scrambling transformation; Lagrange interpolation sharing algorithm

收稿日期：2009-09-16. 作者简介：张选平(1963—)，男，博士，副教授. 基金项目：国防“十一五”预研基金资助项目(282660008，570851613)；国家高技术研究发展计划资助项目(2008AA01Z131).

随着计算机、网络的发展和图像编辑、处理软件的使用，一方面使图像的修改、编辑变得简单，另一方面给图像安全带来严重威胁. 针对图像信息安全[1]，已提出数字图像水印[2]、图像信息分存[3]和图像置乱[4]等一系列安全技术方法，其中图像信息分存作为一种保护图像信息的有效技术手段已成为研究热点.

现有图像信息分存算法一般结合秘密共享算法提出，最简单的秘密共享方案是(t,n)门限秘密共享，由 Shamir 和 Blakley 分别结合 Lagrange 插值算法和矢量空间点的性质提出[5-6]. Thien 等[7]将 Shamir 的(t,n)门限方案用于图像的共享分存，Chang[8]将秘密图像划分为不重叠的块并量化像素块的值，使秘密图像被更好地隐藏，但文献[7-8]中的方法不能防止欺诈. Zhao[9]将防欺诈用于秘密图像分存机制，但生成的分发子信息没有进行伪装，在不安全信道中易引起恶意攻击. Lin 等[10]、Yang 等[11]及 Lin Peiyu[12]将分发子信息隐藏到有意义的掩体图像中，降低了潜在的攻击风险，并通过分发子信息的数字摘要算法或数字签名[13]来检测欺诈，但检测粒度为整份分发子信息，抵御信道的攻击能力有限. 文献[9-12]的算法要求恢复的图像无损在实际中很难达到，由于图像本身是离散采样编码而不是连续编码，因此图像会损失部分质量，而在视觉重建质量上峰值信噪比 PSNR(设为$R_{\mathrm{p,sn}}$)值不低于 30 dB，其视觉质量依然可接受[14].

针对以上问题，本文提出基于细粒度分块重构的多信道图像信息分存算法，对原始秘密图像进行分存形成若干份分发子信息，通过对分发子信息进行雪崩图像置乱变换[15]构造甄别信息，再将分发子信息与甄别信息一起用最低有效位(LSB)法嵌入到掩体图像中，分别在多个信道中传输，接收到的分发子信息参与秘密图像的恢复，通过甄别信息对分发子信息进行细粒度地甄别攻击，确定每份中可用部分，最大可能地重构秘密图像.

1　基于细粒度分块重构的多信道图像信息分存算法

基于细粒度分块重构的多信道图像信息分存方案包括秘密信息的分发与重构两个阶段.

1.1　秘密信息的分发

为了完成秘密信息的分发，首先要构造分发子信息，同时为检测攻击，还需构造甄别信息对每份分发子信息进行分块认证，并将构造出的分发子信息和甄别信息隐藏到掩体图像中形成有意义的图像，以避免引起攻击者注意从而提高安全性.

1.1.1　*分发子信息的构造*　利用拉格朗日插值多项式将秘密信息分成 n 份，其中任意 $t(t<n)$份合作可重构出秘密信息，而小于 t 份则不能得到秘密信息，t 为门限值，即

$$F(x)=(s+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1})\bmod m \quad (1)$$

式中：s 为秘密信息；系数 a_1，a_2，…，a_{t-1}是随机生成的 0 到 $m-1$ 间的整数. 记 $y_1=F(1)$，$y_2=F(2)$，…，$y_n=F(n)$为 n 份分发子信息.

由于拉格朗日分存算法在恢复秘密信息时要用到模逆运算，m 须为素数，为防止失真，m 取图像像素值范围(0～255)中最大素数 251. 在此情况下，须将秘密图像像素值预处理到 0 至 $m-1$ 间后再进行分存. 本文将秘密图像像素值进行了进制转换和压缩处理，以避免图像失真. 对于灰度图像，选取 m 为小于等于 251 的素数，再将像素值转换到 m 进制下的一组值，这组值在 0 至 $m-1$ 间；对于二值图像，选取 $m=251$，将像素值转用 0、1 代替，再将每行中连续 7 个像素值压缩成一个 0～127 之间的值，不足 7 位时补 0 后再处理.

利用拉格朗日插值多项式对预处理后的秘密图像进行分存，得到$(x_i,F(x_i))$，$y_i=F(x_i)$为分发子信息. 预处理后的秘密图像像素值记为 $S=\{s_i\mid i=1,2,\cdots,M_SN_S\}$，分发步骤如下：

步骤 1　秘密图像持有者选择一个像素值 s_i；

步骤 2　秘密图像持有者利用 $t-1$ 次多项式

$$F_i(x)=(s_i+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1})\bmod m \quad (2)$$

计算得到 n 组值$(x_k,F_i(x_k))$，其中 x_k 是一组序列号，$k=1,2,\cdots,n$；

步骤 3　重复步骤 1、2，直到处理完所有秘密图像值.

1.1.2　*甄别信息的形成*　传统防欺诈方案主要结合数字摘要或数字签名来防欺诈，保护对象为整份分发子信息，检测粒度较大. 雪崩图像置乱算法中对置乱图像的任意一个微小攻击都将导致受损的图像无法恢复为原始图像，本文将雪崩图像置乱变换用于构造能够甄别攻击及篡改定位的甄别信息. 分发子信息受到任意的攻击或篡改等，都会导致某些分块计算出的甄别信息与原始甄别信息不同，因而这些分块认证不通过，步骤如下：

步骤 1　选取一个 key，确定分发子信息分块的大小；

步骤2 秘密图像持有者根据分块的大小，用key生成雪崩置乱变换的逆变换阵；

步骤3 把一个分发子信息的一个分块记为 $\boldsymbol{S}_{k_i}$，其经过雪崩置乱的逆变换阵变换后，生成一个新的矩阵，即甄别信息，记为 $\boldsymbol{Z}_{k_i}$，其中 $k=1,2,\cdots,n,i$ 为块号；

步骤4 重复步骤3，直到一个分发子信息所有分块处理完毕；

步骤5 重复步骤1～4，直到所有的分发子信息处理完毕.

1.1.3 隐藏 选取合适大小的掩体图像，对分发子信息的每个分块，采用LSB嵌入到彩色掩体图像对应分块的 R 分量最低位中. 将对应分块的甄别信息用LSB嵌入到彩色掩体图像对应分块的 G 分量最低位中.

分块的大小由秘密图像持有者选取，分块越小则认证的粒度越细，重构的效果越好. 无论分块大小，秘密图像像素值总数不变，每个像素值按照式(2)进行分存，因此分发的计算代价不变；对任意一份分发子信息，无论分块大小，分发子信息总量不变，得到的甄别信息总量也保持不变. 一个秘密图像为 $M\times N$ 大小的二值图像，预处理后为 $M\times\lceil N/7\rceil$ 大小的灰度图像. 分发得到的每个分发子信息大小为 $M\times\lceil N/7\rceil$，共有 $M\times\lceil N/7\rceil\times 8$ b，若分块大小为 $B_m\times B_n$，共有 $M\times\lceil N/7\rceil/(B_m\times B_n)$ 个分块，每个分块的甄别信息大小为 $B_m\times B_n$，则甄别信息总量为 $M\times\lceil N/7\rceil\times 8$ b.

1.2 秘密信息的重构

分发子信息在传输过程中可能会受到攻击，因此需要对接收的每份分发子信息进行分块认证. 将接收到的彩色图像记为 $\boldsymbol{O}'_k$，其中 $k=1,2,\cdots,n^*$（n^* 为实际接收端收到的分发子信息的份数）. $\boldsymbol{O}'_k$ 分块后每个块记为 $\boldsymbol{O}'_{k_i}$，R 分量中嵌入的分发子信息块记为 $\boldsymbol{S}'_{k_i}$，G 分量中嵌入的甄别信息记为 $\boldsymbol{Z}'_{k_i}$，认证过程如下：

步骤1 从 O'_{k_i} 的 R 分量的每个像素值的最低位提取出 S'_{k_i}；

步骤2 用key生成雪崩置乱变换的逆变换阵，$\boldsymbol{S}'_{k_i}$ 经过雪崩置乱的逆变换阵变换后，生成甄别信息 $\boldsymbol{Z}''_{k_i}$；

步骤3 从 $\boldsymbol{O}'_{k_i}$ 的G分量的每个像素值的最低位提取出 $\boldsymbol{Z}'_{k_i}$ 并与 $\boldsymbol{Z}''_{k_i}$ 比较，相同则此块认证通过，否则不通过；

步骤4 重复步骤1～3，直到所有的分发子信息认证完毕.

认证完所有 $\boldsymbol{S}'_{k_i}$ 后，如果同一块号的 $\boldsymbol{S}'_{k_i}$ 通过认证的数量超过门限值 t，则利用Lagrange插值公式

$$F(x)=\sum_{j=1}^{t}y_j\prod_{i\neq j}\frac{x-x_i}{x_j-x_i}\bmod m \tag{3}$$

计算秘密像素值 $s=F(0)$. 通过此方法计算出该块所对应的原始像素值后，原始图像对应块号的分块可无损失地恢复；反之，则无法重构出原始图像对应块号的分块. 按此法处理完所有分块后，可重构出秘密图像.

2 安全性分析

本方案的安全性是基于分存多项式的复杂性，Thien等[7]已对此进行过讨论分析. 对于拉格朗日分存算法，任意 $t(t<n)$ 份合作可重构出秘密信息，而小于 t 份则不能得到秘密信息. 由式(2)可知，$F_1(x)$ 获取秘密信息 s_1 需 t 个方程式，如果只能得到 $t-1$ 份分发子信息 $F_1(1)$，$F_1(2)$，…，$F_1(t-1)$，则只能构造 $t-1$ 个方程式

$$\left.\begin{aligned}
&F_1(1)=(s_1+a_1+a_2+\cdots+a_{t-1})\bmod m\\
&F_1(2)=(s_1+2a_1+2^2a_2+\cdots+2^{t-1}a_{t-1})\bmod m\\
&\qquad\vdots\\
&F_1(t-1)=(s_1+(t-1)a_1+(t-1)^2a_2+\\
&\cdots+(t-1)^{t-1}a_{t-1})\bmod m
\end{aligned}\right\} \tag{4}$$

式中：$F_1(1)$，$F_1(2)$，…，$F_1(t-1)$，m 是攻击者已知的，s_1，a_1，a_2，…，a_{t-1} 未知，有 t 个未知数，而只有 $t-1$ 个方程式，因此得到正确秘密信息 s_1 的概率为 $1/m$. 所以，对于1个 $M\times N$ 大小的二值图像，经过预处理后其大小变为 $M\times\lceil N/7\rceil$，$m=251$，则得到正确预处理后的信息概率为 $(1/251)^{M\times\lceil N/7\rceil}$. 因此，攻击者获取原秘密图像的可能性很小.

3 实验结果

实验中用峰值信噪比 $R_{\mathrm{p,sn}}$ 作为图像嵌入信息前后或受攻击前后质量的衡量标准，$(R_{ij}=(r_{ij},g_{ij},b_{ij}))_{M\times N}$ 是原始图像，$(\widetilde{R}_{ij}=(\tilde{r}_{ij},\tilde{g}_{ij},\tilde{b}_{ij}))_{M\times N}$ 是被处理后的图像. $R_{\mathrm{p,sn}}$ 定义为

$$R_{\mathrm{p,sn}}=(R^r_{\mathrm{p,sn}}+R^g_{\mathrm{p,sn}}+R^b_{\mathrm{p,sn}}) \tag{5}$$

$$R_{\mathrm{p,sn}}=10\lg\left\{\frac{MN\times 255^2}{\sum_{i=1}^{MN}(r_{ij}-\tilde{r}_{ij})^2}\right\} \tag{6}$$

实验选取秘密图像为64×56的二值图像(见图

1e)，预处理后变为 64×8 的灰度图像，采用(2，4)门限方案进行分发后，每个分发子信息的大小为 64×8，采用 8×1 分块认证，每个分块共 64 b，选取 64×64 的掩体图像，掩体图像按 8×8 分块，生成的分发子信息和甄别信息嵌入到掩体图像中，如图 1a～1d 所示.

图 2 为接收到的 6 组分发子信息在传输中受到攻击的情况，$R_{p,sn}$ 值表示其受攻击的强度. 图 2a～2d 为接收到的 4 份分发子信息均未受到攻击的情况，图 2e～2h 为接收到的 4 份分发子信息中无损的份数达到门限值 2 的情况，图 2i～2x 为 3 份或 4 份分发子信息都受到攻击的情况.

文献[9-12]和本文方案在收到 6 组分发子信息情况下，所有接收到的分发子信息的利用情况及重构出的秘密图像效果对比见表 1. 图 3 为采用本文方案重构出的秘密图像.

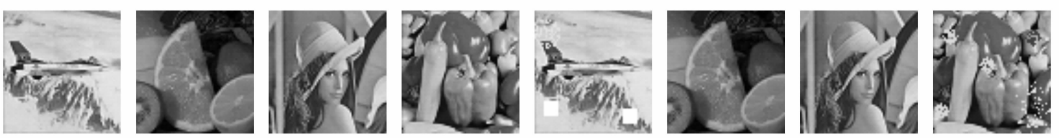
表 1　文献[9-12]和本文方案重构效果对比

编号	文献[9-12]重构效果			本文方案重构效果		
	重构的分发子信息	重构出的秘密图像	$R_{p,sn}$	重构的分发子信息	重构出的秘密图像	$R_{p,sn}$
1	图 2a、图 2b、图 2c、图 2d	图 3a	∞	图 2a、图 2b、图 2c、图 2d	图 3c	∞
2	图 2f、图 2g	图 3b	∞	图 2f、图 2g	图 3d	∞
3				图 2i、图 2j、图 2k、图 2l	图 3e	19.325 3
4				图 2m、图 2n、图 2o、图 2p	图 3f	∞
5				图 2q、图 2r、图 2s	图 3g	∞
6				图 2v、图 2w	图 3h	12.341 3

由表 1 可知，只有在接收到无损的分发子信息份数大于等于门限值的情况下，文献[9-12]才可重构出秘密图像，其他情况下则无法重构出秘密图像. 本文方法在 3 份甚至所有分发子信息都受攻击的情况下，也可充分利用所有分发子信息中未受损部分重构出秘密图像.

(a)掩体图像 1　(b)掩体图像 2　(c)掩体图像 3　(d)掩体图像 4　(e)秘密图像

图 1　嵌入分发子信息和甄别信息的掩体图像及秘密图像



(a)$R_{p,sn}=\infty$　(b)$R_{p,sn}=\infty$　(c)$R_{p,sn}=\infty$　(d)$R_{p,sn}=\infty$　(e)$R_{p,sn}=$20.963 3　(f)$R_{p,sn}=\infty$　(g)$R_{p,sn}=\infty$　(h)$R_{p,sn}=$18.820 9

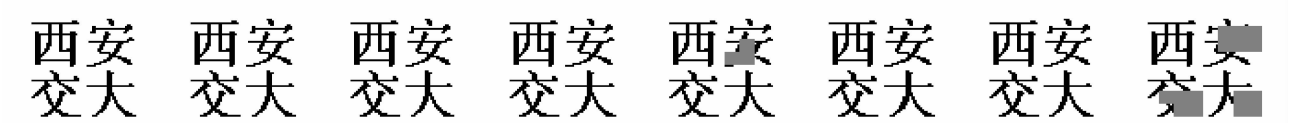
(i)$R_{p,sn}=$16.541 8　(j)$R_{p,sn}=$8.716 4　(k)$R_{p,sn}=$19.115 6　(l)$R_{p,sn}=\infty$　(m)$R_{p,sn}=$16.541 8　(n)$R_{p,sn}=$9.312 1　(o)$R_{p,sn}=$17.107 6　(p)$R_{p,sn}=\infty$

(q)$R_{p,sn}=$20.963 3　(r)$R_{p,sn}=$13.722 3　(s)$R_{p,sn}=$24.379 7　(t)$R_{p,sn}=$4.531 5　(u)$R_{p,sn}=$9.760 6　(v)$R_{p,sn}=$13.722 3　(w)$R_{p,sn}=$20.120 1　(x)$R_{p,sn}=$4.531 5

图 2　分发子信息受攻击的情况

对于表1中编号为4、5的分发子信息受攻击的情况，文献[9-12]不能利用任何分发子信息重构出秘密图像，本文方案则可充分利用所有分发子信息中未受损部分无损地重构出秘密图像，如图3f和图3g，而对于编号为3、6的分发子信息受较强攻击的情况，文献[9-12]也不能重构出秘密图像，但本文方案依然可最大限度地重构出秘密图像，如图3e和图3h，其原始秘密信息依然可见.

在不安全信道中传输时，可能所有分发子信息都受到攻击而导致无损的分发子信息份数达不到门限值，文献[9-12]对整份分发子信息进行认证，则认证通过的分发子信息份数达不到门限值，不能重构出秘密图像，而本文方案是对分发子信息进行分块检测与认证，确定出接收到的所有分发子信息中没有受到攻击的分块，并充分利用它们来最大限度地重构秘密图像，只要同一分块认证通过的份数达到门限值，秘密图像的该分块即可重构出来. 与文献[9-12]相比，本文方案提高了分发子信息的利用率，增强了抵抗攻击的能力，即使在所有分发子信息都受到一定攻击的情况下，也能较好地重构秘密图像.



(a)重构图像1 (b)重构图像2 (c)重构图像3 (d)重构图像4 (e)重构图像5 (f)重构图像6 (g)重构图像7 (h)重构图像8

图3 重构出的秘密图像

4 结 论

图像信息分存技术是一种保护秘密图像的重要方法，目前图像信息分存领域存在对分发子信息的检测粒度过大，分发子信息利用率不高，抵御信道攻击有限等问题. 针对上述问题，本文提出一种基于细粒度分块重构的多信道图像信息分存方案. 该方案能够对分发子信息进行细粒度地甄别攻击，在所有分发子信息都受到一定攻击的情况下仍能充分利用分发子信息中未受损部分最大限度地重构出秘密图像，而已有图像信息分存方案只在接收到的无损分发子信息份数达到门限值时才能重构出秘密图像，其他情况下则无法重构秘密图像. 与传统方案相比，本文方案提高了分发子信息的利用率，增强了抵抗攻击的能力. 该方案能对剪切、篡改等攻击精确检测与定位，但不能抵抗JPEG压缩，因此还需进一步研究能抵抗一定压缩的分块重构的信息分存方案.

参考文献：

[1] PHADIKAR A, MAITY S P. A cost effective scheme for content verification and access control of quality of an image[C]// 2008 IEEE Region 10 Colloquium and Third International Conference on Industrial and Information Systems (ICIIS-2008). Kharagpur: [s. n.], 2008: 1-6.

[2] 尹浩，林闯，邱锋，等. 数字水印技术综述[J]. 计算机研究与发展，2005，42(7)：1093-1099.
YIN Hao, LIN Chuang, QIU Feng, et al. A survey of digital watermarking [J]. Journal of Computer Research and Development, 2005, 42(7): 1093-1099.

[3] 邵利平，覃征，衡星辰. 一种基于与(或)逻辑实现的信息分存算法[J]. 西安交通大学学报，2006，40(10)：1078-1082.
SHAO Liping, QIN Zheng, HENG Xingchen. Information sharing algorithm based on conjunction and disjunction logic functions [J]. Journal of Xi′an Jiaotong University, 2006, 40(10): 1078-1082.

[4] 丁玮，闫伟齐，齐东旭. 基于Arnold变换的数字图像置乱技术[J]. 计算机辅助设计与图形学学报，2001，13(4)：338-341.
DING Wei, YAN Weiqi, QI Dongxu. Digital image scrambling technology based on Arnold transformation [J]. Journal of Computer-Aided Design & Computer Graphics, 2001, 13(4): 338-341.

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

[6] BLAKLEY G R. Safeguarding cryptographic keys[C]// National Computer Conference. Montvale: [s. n.], 1979: 313-317.

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

[8] CHANG C C, LIN C Y, TSENG CS. Secret image hiding and sharing based on the (t, n)-threshold[J]. Fundamenta Informaticae, 2007, 76(4): 399-411.

[9] ZHAO Rong, ZHAO Jianjie, DAI Fang, et al. A new image secret sharing scheme to identify cheaters[J]. Computer Standards & Interfaces, 2007, 31(1): 252-257.

[10] LIN C C, TSAI W H. Secret image sharing with steg-

anography and authentication[J]. Journal of Systems and Software, 2004, 73(3): 405-414.

[11] 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.

[12] LIN P Y, LEE J S, CHANG C C. Distortion-free secret image sharing mechanism using modulus operator[J]. Pattern Recognition, 2008, 42(5):886-895.

[13] STINSON D R. Cryptography: theory and practice [M]. 3rd ed. USA: CRC Press, 2006.

[14] TAUBMAN D S, MARCELLIN M W, RABBANI M. JPEG2000: image compression fundamentals, standards and practice[J]. Journal of Electronic Imaging, 2002, 11(2):286-287.

[15] 邵利平，覃征，衡星辰，等. 基于高维矩阵变换的雪崩图像置乱变换[J]. 中国图象图形学报，2008，13(8)：1429-1436.
SHAO Liping, QIN Zheng, HENG Xingchen, et al. Avalanche image scrambling transformation based on high-dimension matrix transformation [J]. Journal of Image and Graphics, 2008, 13(8):1429-1436.

（编辑　武红江　苗凌）