批量二值图像的隐写研究

陈够喜[1,2] 陈俊杰[1]

(太原理工大学计算机与软件学院 太原 030024)[1] (中北大学电子与计算机科学技术学院 太原 030051)[2]

摘 要 信息隐藏的核心是隐写容量和隐秘信息的安全性。采用批量二值图像和图像分块技术,提出了一种符合Cachin安全性定义的批量二值图像隐写模型。在满足静态Markov链和独立嵌入的条件下,分析了批量二值图像隐写的容量,并证明了基于K-L散度的批量二值图像隐写的安全性。批量二值图像隐写的容量与载体数、图像分块等相关性实验的验证和分析表明,本模型具有一定的理论和应用价值。

关键词 信息隐藏,批量隐写,二值图像,安全性

中图法分类号 TP309 **文献标识码** A

Steganographic Research for Batch Binary Images

CHEN Gou-xi[1,2] CHEN Jun-jie[1]

(School of Computer and Software, Taiyuan University of Technology, Taiyuan 030024, China)[1]

(School of Computer Science and Technology, North University of China, Taiyuan 030051, China)[2]

Abstract The core of steganographic research is capacity and security of hiding information. According to Cachin' definition of security and properties of binary image block of host image, batch steganographic model of binary images was presented. Batch steganographic capacity of binary images was summarized, when satisfying static markov chain and mutually independent of embedding in covers. Security of the model was proved under certainly condition. The experimental results and analysis show that the model satisfies steganographic requirement for security. The research results are helpful for theory and application.

Keywords Information hiding, Batch steganography, Binary image, Security

1 引言

随着全球数字化进程的日益加速,二值图像在金融票据、保险记录、个人档案、各类证书、数字图书、医疗记录、手写签名、文件传真复印以及数字化形式保存的各类纸质文档中已广泛应用,包括在电子商务和电子政务中的数字化手写签名。二值图像的检测认证以及秘密信息的隐蔽传输显得尤为重要,信息隐藏技术为其提供了有效的实现手段。

信息隐藏主要针对彩色和灰度图像的隐写与分析进行研究[1],其算法普遍不适合二值图像隐写。二值图像即黑白图像,没有丰富的灰度分级,只有"0"和"1"分别代表黑白像素。目前,基于二值图像的隐写算法较少,可以归纳为分块嵌入法、游程修改嵌入法、边界修改法、基于半色调图像的嵌入算法以及文本行或字符移位法等[2]。对于通用的二值图像,目前具有代表性的两种算法是文献[3,4]提出的二值图像的隐写算法。文献[3]根据图像的连通性和平滑性的要求,根据分块分值进行数据隐藏,隐写容量和安全性与具体的图像有关。文献[4]允许在二值图像的任何位置进行黑白像素修改,所以该方法的特点是隐写容量大,但安全性较差。上述算法虽然提高了二值图像的隐写容量,但仅从密码学的安全性角度来分析了隐秘信息的安全性,而且研究的隐写载体全部针对单二值图像。文献[5]提出了一种图像隐蔽通信的安全模型,给出了安全约束条件。文献[6]提出了批量隐写与分析的隐写思路。文献[7]展开对批量隐写的嵌入容量和假设进行研究,重点是通用隐写策略,未针对二值图像的特点提出批量二值图像的隐写容量和安全性分析,未对批量二值图像隐写的隐秘信息的安全性进行深入研究,更未提出批量二值图像隐写模型。

针对彩色和灰度图像的隐写模型与二值图像隐写的不同特点的研究,基于K-L散度和Cachin的隐写安全性定义[8],本文提出批量二值图像的隐写模型和广义批量隐写模型,对隐写容量和安全性进行讨论,围绕批量二值图像及图像分块进行批量隐写理论研究。

本文第2节介绍基本定义与假设;第3节阐述批量二值图像隐写的容量分析及实现算法;第4节论证批量二值图像隐写的安全性;第5节为实验结果分析和讨论;最后为结束语。

2 符号定义与假设

定义1(批量二值图像隐写系统) 假设六元组 $\Gamma_m=(C_i,$

到稿日期:2010-12-10 返修日期:2011-03-22 本文受国家自然科学基金(60773004),山西省科技攻关项目(20090322004)资助。

陈够喜(1966—),男,博士生,副教授,CCF高级会员,主要研究方向为信息隐藏和图像处理,E-mail:chengouxicgx@163.com;陈俊杰(1956—),男,教授,博士生导师,CCF高级会员,主要研究方向为数据库与智能信息处理。

$S,K,C_S,E_K,D_K\,|\,1<i\leqslant N)$满足下列条件：

(1)$C_1,C_2,\cdots,C_{n1}$为二值图像的序列集，记为$\{C_{n1}\}$，$n1$为$\{C_{n1}\}$的基。其中$C_i=\{c_i^j\,|\,1<i\leqslant n1,1<j\leqslant n2\}$，且$\forall i(1<i\leqslant n1),C_i\in\{C_{n1}\}$，$n2$为$C_i$中的二值图像载体数量。

(2)S为隐秘信息块集合，记为$S=\{s_1,s_2,\cdots,s_{n3}\}$，$S$的容量大小表示为$|S|=\sum_{i=1}^{n3}|s_i|$，$n3$为隐秘信息块的数量，并且$|C_i|\ \forall i(1<i\leqslant N|>|S|$。

(3)K是所有密钥的集合，$K=[k_1,k_2,\cdots,k_v]$，v为密钥数量。

(4)C_S为包含S和K的携密载体。

(5)E_K为嵌入算法：$C_i\times S\times K_j\rightarrow C_S(1<j\leqslant v)$。

(6)D_K为隐秘信息提取算法：$C_S\times K\rightarrow S$，若$\forall s_i\in S|1\leqslant i\leqslant v$且$c_j\in C_i\,|\,(1\leqslant j\leqslant N,1<i\leqslant n1)$，都有$D_K(E_K(c_j,s_i,k))=s_i$。则六元组$\Gamma_m$为批量二值图像隐写系统。

批量二值图像隐写系统就是基于多个二值图像进行多个隐秘块的隐写系统，是实现多载体多隐秘的信息隐藏的有效手段。

定义 2(批量二值图像的最大有效载荷)　假设批量二值图像隐写系统Γ_m能满足下列3个必要条件$\mathcal{R}_m$：

(1)不可感知性：包括视觉统计不可见；

(2)密钥安全性：满足 Kerckhoffs 准则；

(3)鲁棒性：具备抵抗各类攻击与信号处理的能力。

批量二值图像隐写系统Γ_m最大有效载荷M定义为：

$$|M|=\max\{m\,|\,m\in M,M|(R_m,\Gamma_m)\}\tag{1}$$

且满足下列条件：

(1)载体集$C_i(1<i\leqslant n1)$为$|C_i|=\sum|c_i^j|,1<j\leqslant N,N$为隐写目标二值图像载体数；

(2)载体集$C_i(1<i\leqslant n1)$作为整体满足最大有效载荷的隐藏条件$\mathcal{R}_m$；

(3)$|M|=\sum_{j=1}^{n3}|m_j|$，$n3$为最大有效载荷构成的隐秘信息块的数量。

因此，可得批量二值图像隐写系统Γ_m的最大有效载荷的对应关系模型为：

当$\forall i,j(1<i\leqslant N,1\leqslant j\leqslant 4)$时，有：

$$|M|=g(C_i,E_K,D_K,R_j)$$

式中，$|M|$为Γ_m的最大有效载荷；R_1为载体c_i^m和$c_i^{m'}(1\leqslant m,m'\leqslant N,m\neq m')$间的相关系数，$R_2$为不同载体嵌入算法间的相关系数；$R_3$为隐秘信息块间的相关系数；$R_4$为密钥间的相关系数；$g$为映射。且满足：

$$(C_i,E_K,D_K)\times(R_j)\rightarrow|M|$$

从上面的定义可证明[9]定理1的存在。

定理 1　对于批量二值图像系统Γ_m，假设：

(1)各二值图像$c_1,c_2,\cdots,c_i(0\leqslant i\leqslant p)$之间关系符合静止 Markov 链；

(2)$M=\sum_{j=1}^{q}m_j$，M为$\{C_i\}$的最大有效载荷，$\{C_i\}$的基为N；

(3)$\{e_{p1},e_{p2}\,|R(p1,p2)=0\}$，$p1$和$p2$为任意两个嵌入方法，$R(p1,p2)$表示$p1$和$p2$的相关系数。

则下列结论成立：

(1)当$N\rightarrow\infty$，$|M|/\sqrt{N}\rightarrow\infty$时，$\Gamma_m$是不安全的；

(2)$\forall i,j(0\leqslant i,j\leqslant N),R(E_i,E_j)=0$，当$N\rightarrow\infty$时，$|M|/\sqrt{N}\rightarrow 0$，则$\Gamma_m$是安全的。

根据二值图像的特点，对于一幅较大尺寸的二值图像进行等份分块。当分块数足够大时，基于该批分块的批量隐写同样符合定理1，显见下列推论。

推论 1　基于单幅大尺寸的二值图像的批量隐写的安全性取决于该图像分块的数量，而且图像的最大有效载荷由分块数决定。

所以，在对二值图像进行批量隐写时，隐写的载体总数等于载体数和分块数之积。载体越多，分块越多，隐写的载体总数就越大，隐写安全性将越高。

定义 3(复合批量二值图像隐写系统)　假设$\Gamma_m^j=(C_i^j,S^j,K^j,C_S^j,E_K^j,D_K^j\,|\,1<i\leqslant N)$为批量二值图像隐写系统，其中$1\leqslant j\leqslant N$，则

$$\Omega=\sum_{j=1}^{N'}\bigcup\Gamma_m^j(N'\leqslant N)\tag{2}$$

上述式(2)称为复合批量二值图像隐写系统，记为Ω。

定义 4(通用批量隐写系统)　假设六元组$\Gamma_m=(C_i,S,K,C_S,E_K,D_K\,|\,1<i\leqslant N)$是批量二值图像隐写系统。当载体集中的所有元素均为任意数字载体时，称Γ_m为通用批量隐写系统，记为G。

定义 5(复合通用批量隐写系统)　假设$G_m^j=(C_i^j,S^j,K^j,C_S^j,E_K^j,D_K^j\,|\,1<i\leqslant N)$为批量通用隐写系统，其中$1\leqslant j\leqslant N$，则

$$\Xi=\sum_{j=1}^{N'}\bigcup G_m^j(N'\leqslant N)\tag{3}$$

上述式(3)称为复合通用批量隐写系统，记为Ξ。

复合通用批量隐写系统Ξ中的各隐写系统G_i和G_{i+1}之间不仅具有相关性，而且较为复杂。

3　批量二值图像隐写的容量分析

3.1　容量分析

当批量二值图像隐写系统满足定理1的两个假设条件时，根据定理1和文献[9]可推出定理2。

定理 2　设$\Gamma=(C,M,K,E_K,D_K)$为批量二值图像隐藏系统，其中：

(1)$C=\sum_{i=1}^{p}c_i,c_1,c_2,\cdots,c_i(0\leqslant i\leqslant p)$之间关系符合静止 Markov 链；

(2)$M=\sum_{j=1}^{q}m_j,\forall E_i,E_j(i,j\in N),R(E_i,E_j)=0$。

那么，该二值图像隐写系统Γ的最大有效载荷可由下式表示：

$$|M|=\omega\sqrt{|p|},0<\omega<1\tag{4}$$

从定理2可以说明，对于批量二值图像隐写系统，当载体数足够大时，最大有效载荷与载体数的平方根成正比，与载体的大小无关。

在式(4)中，ω大小的作用有两个方面：其一决定批量隐写系统Γ的隐写检出率或系统的安全程度；其二与系统的最大有效载荷$|M|$成正比。这两方面也反映出隐写系统的安全

性与鲁棒性的矛盾关系。

3.2 嵌入容量计算

二值图像均可分割为若干分块，在分块之内嵌入操作可以互相独立，分块之间符合静态 Markov 链。设隐写时采用的二值图像载体的大小均为 $2R\times 2T$，载体数为 p，将每个图像分割为 q 个 $k\times l$ 图像块。将所有的载体组合成为一个大的隐写载体 C^*，计算步骤如下：

(1)二值图像 $c_i(1\leqslant i\leqslant p)$组合变换。设组合函数为：

$$\{c_j \mid 0\leqslant j\leqslant i\}=F(c_i \mid 0\leqslant i\leqslant p) \tag{5}$$

式中，对已知二值图像 c_i 进行组合变换，将得到数量不等的一些新图像。当 p 为偶数时，组合为 $2\times\frac{p}{2}$ 的矩阵；当 p 为奇数时，顺序排列；

(2)将每个二值图像分割为 q 个 $k\times l$ 图像块；

(3)计算组合后的载体的总图像块数量 pq；

(4)二值图像的最大有效载荷为：

$$|M|=\omega\sqrt{pq}\ (0<\omega<1) \tag{6}$$

上述步骤(1)－(4)是在一个批量隐写系统 Γ 中完成隐写的。在步骤(1)和(2)时，将二值图像或分块再次进行组合，将得到一个复合批量隐写系统 Ω，包括若干批量隐写系统，可表示为：

$$\Omega=\sum_{i=1}^{p'}\bigcup\Gamma_i\ (1\leqslant p'\leqslant p) \tag{7}$$

由式(7)可得新隐写系统 Ω 的最大有效载荷为：

$$|M'|=|M_1|+|M_2|+\cdots+|M_{P'}|$$
$$=\omega_1\sqrt{q_1}+\omega_2\sqrt{q_2}+\cdots+\omega_{p'}\sqrt{q_{p'}}$$

式中，隐写检出率 $\omega_i(1\leqslant i\leqslant p')$的不同分布将形成更为复杂的批量隐写系统。

由于各批量隐写系统的不同特点和其间相关的复杂性，无法对定义 4 和定义 5 进行定量分析，因此很难得到复合批量隐写系统的最大有效载荷的定量描述。

4 批量二值图像的安全性分析

隐写系统的安全性主要体现在攻击者无法发现或证明隐秘信息的存在性，可以说该系统在理论上是安全的。

设在同一集合上的分布 P_1 和 P_2 的 K-L 散度定义为：

$$D_{KL}(P_1\parallel P_2)=\int p_1(x)\log\frac{p_1(x)}{p_2(x)}\mathrm{d}x$$

Cachin 在文献[8]从信息论的角度给出了一个隐写系统的安全性定义。设 P_s 为隐秘信息的概率分布，P_c 为载体数据的概率分布。如果 $D_{KL}(P_c\mid P_s)=0$，那么隐写系统就是完备保密的；如果 $D_{KL}(P_c\mid P_s)\leqslant\varepsilon$，那么隐写系统就称为 ε-安全。

假设批量二值图像的隐写策略为简单组合等份分拆策略，那么隐写概率为：

$$p_b=\frac{|M|}{pq|c_i|}\quad(1\leqslant i\leqslant p)$$

设两连续的随机变量 Q_1 和 Q_2 及对应的概率密度函数 q_1 和 q_2，批量二值图像隐写分析发生Ⅰ型或Ⅱ型错误的概率[10]分别为 α 或 β，可得：

$$D_{KL}(Q_1\parallel Q_2)=\int q_1(x)\log\frac{q_1(x)}{q_2(x)}\mathrm{d}x$$

$$D_{KL}(\alpha,\beta)=\alpha\log_2\frac{\alpha}{1-\beta}+\beta\log_2\frac{\beta}{1-\alpha}(\alpha+\beta<1)$$

由于决定性过程不能增加两种分布情况的 K-L 散度，即有 $g:Q\to T$，则：

$$D_{KL}(T_1\parallel T_2)\leqslant D_{KL}(Q_1\parallel Q_2)$$

批量二值图像的隐写过程可视为基于载体的概率 p_b 的均匀分布。

设 $f_1=\inf\{\alpha_1,\alpha_2,\cdots,\alpha_p\}$，$f_2=\sup\{\beta_1,\beta_2,\cdots,\beta_p\}$。其中 f_1 和 f_2 对应的分布函数分别为 F_1 和 F_2，则：

$$D_{KL}(F_1\parallel F_2)=p\int f_1(x)\log_2\frac{f_1(x)}{f_2(x)}\mathrm{d}x$$
$$=p\int f_1(x)\log_2\frac{f_1(x)}{f_1(x-p_b)}\mathrm{d}x$$

对 $\log_2 f_1(x)$和 $\log_2 f_1(x-p_b)$进行泰勒展开，有：

$$D_{KL}(F_1\parallel F_2)=p\int f_1(x)\left[p_b\frac{f_1'(x)}{f_1(x)}-\frac{p_b^2}{2}f_1(\xi)''\right]\mathrm{d}x$$
$$=-\frac{p_b^2p}{2}f''_1(\xi)=-\frac{|M|^2}{p|C^*|^2}$$

$$D_{KL}(F_1\parallel F_2)=-\frac{|M|^2}{p|C^*|^2}f_1''(\xi)\leqslant C_1\frac{|M|^2}{N|C|^2}$$

令 $C^1\geqslant-\frac{f_1''(\xi)}{2}$，$x-p<\xi<x$，由定理 1 可得：

当 $\sqrt{|M|}/N\to 0$，$\lim\limits_{N\to\infty}D_{KL}(F_1\parallel F_2)\to 0$。

因为 $D_{KL}(F_1\parallel F_2)\geqslant 0$($F_1=F_2$ 时等号成立)且 $D_{KL}(F_1\parallel F_2)$为凸函数，所以当 $N\to 0$ 且 $\sqrt{|M|}/N\to 0$ 时，

$$D_{KL}(F_1\parallel F_2)=0$$

可见，当满足定理 1 的两个假设条件时，批量二值图像隐写系统符合 Cachin 的 ε-安全性定义，故可称为 ε-安全的批量二值图像隐写系统。

5 实验结果与分析

目前基于二值图像的隐写主要用于数字签名、有价票据和纸质文档的数字化管理以及隐蔽通信等领域之中。分别对手写体文稿、纸质文档和二值卡通图像进行实验。图 1 是一个英文纸质文稿，图像大小为 500×500，分块尺寸为 20×20；图 2 为卡通图片，图像大小为 768×1024，分块尺寸为 20×20。隐秘信息为文本文件。

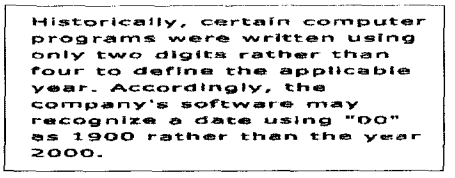
Historically, certain computer programs were written using only two digits rather than four to define the applicable year. Accordingly, the company's software may recognize a date using "00" as 1900 rather than the year 2000.

图 1 纸质文档中的批量隐写

图 2 二值卡通图像中的批量隐写

基于 3 种载体进行批量隐写，隐写策略为等份分拆和独立嵌入，分别对检出率、最大有效载荷、最大有效载荷与载体

数或分块数的关系以及安全性进行实验。

为了取得最大的隐写容量，分块采用大小为 1×1，2×2，…，20×20，共进行 20 次实验，隐写算法采用文献[11]的方法。分块数与隐写容量的关系如图 3 所示。分块越大，载体隐写容量越小。采用 2×2 分块将取得最大的隐写容量。

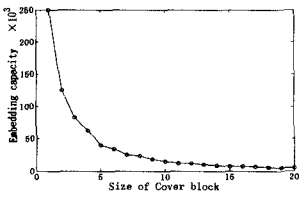

图 3　载体分块的数量与隐写

当 ω 取不同值时，隐写系统的嵌入容量呈现规律性变化，如图 4 所示。当 ω 取值一定时，隐写的最大有效载荷与载体数的平方根成正比；当 ω 取值越大，最大载体有效也随之增大，系统的安全性将变低。

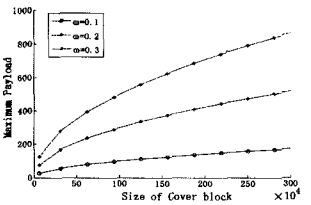

图 4　批量二值图像的隐写容量与载体数的相关性

采用图 2 的载体设计批量隐写系统，载体数采用隐写载体总数计算，隐秘信息采用文本信息，基于 D_{KL} 的理论描述公式，计算批量二值图像的载体数变化下的 D_{KL}，实验如图 5 所示。批量隐写满足定理 1 的两个假设条件。

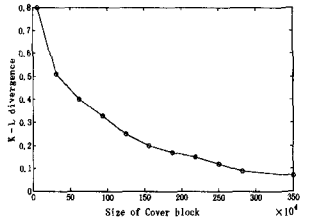

图 5　隐写系统安全性变化曲线

从图 5 可看出，隐写系统随着载体数的变大，其安全性将更高，满足批量隐写的需求。当然，图 5 中的曲线也会随 ξ 取值的不同而发生变化。

结束语　本文提出了一种批量二值图像的隐写模型，并且基于一定的假设条件，证明了隐写系统的安全性，分析了系统隐写容量与载体数变化的相关性，进行了相应的实验，分析了批量二值图像隐写。本文从理论安全方面论证秘密信息的存在性，它区别于密码学意义上的安全性分析，有助于隐写术安全性研究。今后将对本文的隐写安全性证明过程的两个假设条件进行适当放松，进一步探讨多二值图像多隐秘信息的理论规律。

参 考 文 献

[1] 傅德胜，谢永华. 基于图像的信息隐藏检测技术[J]. 信息网络安全，2008，91(7)：72-74

[2] 周琳娜，杨义先，郭云彪，等. 基于二值图像的信息隐藏研究综述[J]. 中山大学学报，2004，43(2)：72-75

[3] Wu M，Liu B. Data hiding in binary for authentica- tion and annotation [J]. IEEE Transactions on Multimedia，2004，6(4)：528-538

[4] Tseng Y-C，Chen Y-Y，Pan H-K. A secure data hiding scheme for two-color images[J]. IEEE Transac- tions on Communications，2002，50(8)：1227 -1231

[5] 丁一军，郑学峰，于桂荣. 一种图像隐蔽通信的安全模型[J]. 计算机科学，2010，37(2)：120-122，130

[6] Ker A D. Batch steganography and pooled stega- nalysis [C]// Processing of the 8th Information Hiding Workshop. Springerlink LNCS，2007(4437)：265-281

[7] Pevny T，Fridrich J. Benchmarking for stegano- graphy[C]// Information Hiding 2008. Santa Barbara，CA USA，2008：251-267

[8] Cachin C. An Information-theoretic Model for Steganography [C]// 2nd International Workshop on Information Hiding. Oregon，USA，1998，1525：306-318

[9] Ker A D，Pevny T，Kodovsky J. The Square Root Law of Steganographic Capacity[C]// Proceedings of the 10th ACM workshop on Multimedia and Security. Oxford U K，2008：107-116

[10] 吕欣，马智，冯登国. 安全隐写系统的信息理论分析[J]. 计算机科学，2006，33(6)：140-142

[11] 郭萌，张鸿斌，魏磊. 二值图像中的数据隐藏算法[J]. 电子学报，2009，37(11)：2409-2415

(上接第 266 页)

[14] 曹治国，鄢睿丞，宋喆. 利用模糊形状上下文关系的红外与可见光图像匹配方法[J]. 红外与激光工程，2008，37(6)：1095-1110

[15] 唐俊，王年，梁栋，等. 一种结合形状上下文分析的 Laplace 谱匹配算法[J]. 系统仿真学报，2009，21(14)：4345-4350

[16] 束鑫，吴小俊，潘磊. 一种新的基于形状轮廓点分布的图像检索[J]. 光电子·激光，2009，20(10)：1385-1389

[17] Alajlan N，Elrube I，Kamel M S，et al. Shape retrieval using triangle-area representation and dynamic space warping [J]. Pattern Recognition，2007，40(7)：1911-1920

[18] Petrakis E G M，Diplaros A，Milios E. Matching and retrieval of distorted and occluded shapes using dynamic programming [J]. IEEE Trans. Pattern Anal. Mach. Intell.，2002，24(11)：1501-1516

[19] Adamek T，O'Connor N. A multiscale representation method for nonrigid shapes with a single closed contour [J]. IEEE Trans. on CSVT，2004，14(5)：742-753

[20] 章毓晋. 基于内容的视觉信息检索[M]. 北京：科学出版社，2003