一种图像隐蔽通信的安全模型

丁一军[1,2] 郑雪峰[1] 于桂荣[2]

(北京科技大学信息工程学院 北京 100083)[1] (沈阳航空工业学院计算机学院 沈阳 110136)[2]

摘 要 安全性是图像隐蔽通信应用的前提条件。基于香农信息熵和相对熵的安全约束条件还存在不足,隐藏信息不能抵抗利用图像相关性的密写分析。深入分析了图像相邻像素的相关性,给出了基于像素相关的广义信息熵、相对熵和概率分布。提出了广义信息度量的信息隐藏模型,该模型满足隐藏信息的不可检测性,适应于图像隐蔽通信。给出了安全约束条件和信息隐藏方法,并进行了验证实验,给出了实验数据。实验结果表明,该安全模型具有理论和实用价值。

关键词 信息隐藏,图像隐蔽通信,广义信息,信息隐藏安全

中图法分类号 TP391.1 **文献标识码** A

Security Model for Image Hidden Communication

DING Yi-jun[1,2] ZHENG Xue-feng[1] YU Gui-rong[2]

(School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China)[1]

(School of Computer Science and Technology, Shenyang Institute of Aeronautical Engineering, Shenyang 110136, China)[2]

Abstract Security is precondition for application of Image Hidden Communication. There is lack of constraint conditions in security based on Shannon information entropy and relative entropy, because of steganalysis by image spatial correlativity. We presented generalized information entropy, relative entropy and probability distribution, by means of analysis for correlativity of adjacency pixels of image. A security model for data hiding based on generalized information measure was proposed. The model is suitable for Image Hidden Communication and the hidden data can't be detected. Security constraint conditions and a method of steganography were derived, and we gave experimental data to verify the model. The experiment results indicate that the security model has values of theory and application.

Keywords Data hiding, Image hidden communication, Generalized information, Data hiding security

信息隐藏技术的安全性问题是一个热门话题,有些研究者用传统信息论的方法得到了一些重要的结论[1,2]。然而,基于传统信息论的信息隐藏安全方案还存在不足。我们经过分析、实验发现,Christian Cachin 提出的基于香农信息熵和相对熵的安全约束条件还不能满足图像信息隐藏的相关分析。因此,研究图像信息隐藏安全模型的前提条件是,必须给出新的信息度量方法。我们通过对图像相邻像素的相关分析,提出了一种具有相关语义的广义信息熵和相对熵,在此基础上给出了一种图像隐蔽通信的安全模型。

1 信息隐藏的安全性

信息隐藏技术具有广泛的应用前景,因此受到许多研究者的关注并得到较快的发展。信息隐藏技术若要进一步发展和实际应用,必须解决一个共同的问题,即信息隐藏技术的安全性问题。安全性是信息隐藏技术理论研究的一个重点问题,但到目前为止学术界在安全性定义、安全性评测标准等方面还未形成共识。信息隐藏技术的应用目的不同,对安全性的要求也会有所不同。本文研究的内容是隐蔽通信的安全性,下面给出相关的信息隐藏安全性定义。

定义 1(S1 安全性) 是指攻击者没有足够的信息证明经过传输信道的通信信息 X 中隐藏有秘密信息 S[3]。

该类安全性就是要求隐蔽通信满足不可检测性。隐蔽通信与数字水印等其它信息隐藏技术有所不同,如果攻击者有方法检测到秘密信息的存在,可认为这种隐蔽通信方案是失败的。在这种情况下,通信已经失去了隐蔽特性。所以,S1 安全性是所有安全的隐蔽通信方案的前提条件。

定义 2(S2 安全性) 是指通信信息 X 受到主动攻击(更广泛一些,可看成某种噪声干扰)的情况下仍然能够正确接收到秘密信息 S。

该类安全性很容易被理解为攻击者无法损坏经过传输信道的通信信息中所隐藏的秘密信息,即受到攻击者攻击的情况下仍然能够从通信信息中恢复秘密信息 S。实际上,这仅仅是实现 S2 安全性的一种方案。满足 S2 安全性的隐蔽通信要比这广泛。例如,在公共信道中实现隐蔽通信而受到主动攻击的情况下,可以通过申请重发的方案解决等,都属于这类安全性问题。

到稿日期:2009-03-04 返修日期:2009-05-22 本文受国家自然科学基金项目(90412012)资助。

丁一军 男,博士生,副教授,主要研究方向为信息安全、图像处理,E-mail:ding_yi_jun@yahoo.com;郑雪峰 男,教授,博士生导师,主要研究方向为信息安全;于桂荣 女,副教授,主要研究方向为应用数学。

2 广义信息熵的引入

Christian Cachin 提出的安全约束条件是基于香农信息熵和相对熵的，其安全约束条件为 $D(P(C)||P(X))\leqslant\varepsilon$，当 $\varepsilon=0$ 时，信息隐藏方案为理论安全的。因而，理想的信息隐藏方案的安全约束条件就是隐藏秘密信息 S 前后图像具有相等的概率分布，两者的信息熵相等。但是，香农信息熵是基于客观概率的，并不考虑图像中像素间的相关关系。

用集合 A 表示图像的像素集合，用集合 B 表示隐蔽通信的符号集合（对图像来说，就是像素可能取的灰度值），有 A 到 B 的映射：映射函数为原像 x_i 取灰度值 y_j。

所有具有相同灰度值的像素形成子集：

$A_j, j\in B, A_0, A_1, \cdots, A_{|B|-1}$

是集合 A 的一个划分。因此，香农信息熵[4]

$$H(Y)=-\sum_i P(y_i)\log P(y_i)=-\sum_j Q(A_j)\log Q(A_j)$$

概率分布为

$$P(Y)=P(y_j)=Q(A_j)=\frac{|A_j|}{|A|}, j\in B$$

从上边的映射函数可以看出，y_j 的所有原像只有取值上的要求，对像素所在位置并没有要求。因而，隐藏 1bit 信息可以选择任何一对不等像素位置互换（假设在满足视觉不可感知的前提下）。但是，如果考虑相邻像素的相关性，那么上述的隐藏方法隐藏秘密信息前后图像广义的概率分布可能会不等，也就是说攻击者可以通过像素的相关分析检测到隐藏信息的存在。

我们先考虑简单的情况，像素 x_i 的相关区域为 8 邻域，区域中的像素记为 x_t，则广义映射函数 $y_j=f(x_i)$ 为原像 x_i 取灰度值 y_j 或原像为满足 $|\bar{x}_i-\bar{x}_t|\leqslant\delta$ 的 $x_i, \bar{x}_i, \bar{x}_t$ 分别表示 x_i, x_t 的灰度取值。$y_j, j\in B$ 的原像子集为

$A_j, j\in B, A_0\cap A_1\cap\cdots\cap A_{|B-1}\neq\Phi$

这些子集构成 A 的一个覆盖。概率分布为

$\widehat{P}(Y)=Q(A_j)=\frac{|A_j|}{|A|}, j\in B$，是广义的。

由于广义的概率分布与图像的位置有关，上述满足客观概率分布的隐藏方法就不一定成立。我们对标准测试图像 lena 进行了实验，实验条件为：测试图像为 512×512，8 bit 灰度图像，相邻像素相关域为 8 邻域，$\delta=1$，图像像素互换前后的图像频度变化如表 1 所列。

表 1 互换前后图像频度变化表

灰度值	频度	
7	$f_c=3040$	$f_x=3039$
8	$f_c=3525$	$f_x=3523$
9	$f_c=4314$	$f_x=4314$
10	$f_c=4826$	$f_x=4827$

lena 图像中，互换的两个像素 $x(21,15)$ 的灰度值为 9，$x(10,9)$ 的灰度值为 8，由于 $\delta=1$，因此表 1 中给出的灰度值之外的其它灰度值频度不受影响。由表 1 可知，图像像素互换前后图像的广义概率分布是不等的。通过上述分析，可以看出考虑像素相关性是必要的。下面给出图像相邻像素相关的广义信息熵。

设 W 表示以 x_i 为中心的相关区域，广义映射函数 $y_j=f(x_i)$ 为原像 x_i 取灰度值 y_j 或原像为满足 $|\bar{x}_i-\bar{x}_t|\leqslant\delta, x_t\in W$ 的 x_t，得到 A 的一个覆盖 $A_j, j\in B$。

广义信息熵：$\widehat{H}(Y)=-\sum_{j\in B}P(y_j)\log Q(A_j)$

广义相对熵：$\widehat{D}(\widehat{P}(U)||\widehat{P}(V))=\sum_{j\in B}\widehat{P}(U)|_{u=j}\log\frac{\widehat{P}(U)|_{u=j}}{\widehat{P}(V)|_{v=j}}$

广义概率分布：$\widehat{P}(Y)=Q(A_j)=\frac{|A_j|}{|A|}, j\in B$

3 信息隐藏方案

3.1 信息隐藏模型

我们的信息隐藏模型如图 1 所示。假设攻击者 Eve 进行被动攻击，即我们要解决 S1 安全性的问题。C 是掩盖图像，S 是秘密信息，K 是信息隐藏密钥，X 是编码器的输出，可能是 C 也可能是含密图像。

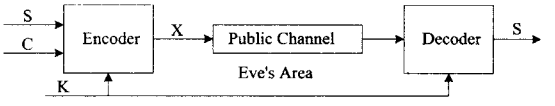

图 1 信息隐藏模型

我们要解决的问题就是使 Eve 没有信息能够检测传输的信息 X 中存在秘密信息。该模型满足如下基本约束：

(1) $H(X|CSK)=0$ 已知 C, S, K 的情况下，可以确定 X；

(2) $H(S|XK)=0$ 已知 S, K 的情况下，可以解出 S；

(3) $H(E|CX)=0$ E 是二值随机变量，0 表示 Eve 判断 X 不含密，否则判断为含密。Eve 已知 C, X 的情况下，可以准确检测出 X 是否隐藏秘密信息。因而，该模型要求 Eve 不能获得 C。

3.2 安全约束条件和信息隐藏的方法

按照 Christian Cachin 使用假设检验所得出的结论[1]，有如下定义。

定义 3 如果信息隐藏系统是安全的，当且仅当 $D(P(C)||P(X))\leqslant\varepsilon$ 且 $\widehat{D}(\widehat{P}(C)||\widehat{P}(X))\leqslant\varepsilon, \varepsilon=0$，信息隐藏系统是理论安全的。

因此，如果要获得理想的信息隐藏系统，必须隐藏信息前后图像的香农信息熵和广义信息熵是相等的，即隐藏信息前后图像的客观概率以及广义概率分布均是相等的。但在实际应用中，往往希望知道怎样做才能保证满足上述的安全条件。即使知道方法，每隐藏 1bit 信息都要计算香农信息熵和广义信息熵，判断是否满足安全约束条件也是很费时间的。我们对信息隐藏系统进行了进一步的分析，给出如下满足实际应用的一些安全约束条件。由于如果知道如何隐藏 1bit 信息，就可以用类似的方法隐藏秘密信息的其它比特，因此下面的叙述中都假设隐藏 1bit 信息。

引理 1 信息隐藏系统是 S1 安全的必要条件是满足 $|x_i-x_j|\leqslant\delta$ 的两个像素 x_i, x_j 的位置互换。

(x_i, x_j) 称为互换对。引理比较直接，下面给出简要说明。客观概率的计算不考虑像素的所在位置，如第 2 小节所述。位置互换隐藏信息前后图像的客观概率不变，香农信息熵也是相等的。该引理给出的互换是必要条件，这是因为互换还要满足广义信息熵的约束条件，因而不是所有的互换都满足 S1 安全性。

下面给出满足定义 3 的互换对所应具备的条件。在进行

互换后，图像的相关区域中心点之外的其它像素必然受到影响。影响有两种：一是原来不相关的像素变成了相关的像素，它所对应的符号(像素取值)称之为增加符号；二是原来相关的像素变成了不相关的像素，它所对应的符号称之为减少符号，统称为变化符号。

定义 4 集合 $X_k^+(k\in[-\delta,\delta],k\neq 0)$表示像素 x 被灰度值为$(\bar{x}+k)$的像素替换后增加符号的集合；集合 X_k^- 表示减少符号的集合。

定义 5 x_j 与相关区域 W 中心像素 x_i 相关，除 x_i 之外，不存在 x_j 的相关像素的取值等于 $\bar{x}_i$，称 x_j 为 x_i 的依赖像素，x_i 依赖像素个数记为 $DC_W(x_i)$。

定理 1 互换对(x,y)，$x\in W_1$，$y\in W_2$ 满足：

(1)$(\bar{x}-\bar{y})=k,(k\in[-\delta,\delta],k\neq 0)$，$X_{-k}^+\subseteq Y_K^-$，$X_{-k}^+\supseteq Y_K^-$ 且 $X_{-k}^-\subseteq Y_K^+$，$X_{-k}^-\supseteq Y_K^+$

(2)$DC_{w1}(x)=DC_{w2}(x)$，$DC_{w1}(y)=DC_{w2}(y)$

则 x,y 互换信息隐藏系统满足理论安全性。

证明：(1) 因(x,y)是互换对，$(\bar{x}-\bar{y})=k\leqslant\delta$，根据引理 1，有 $P(C)=P(X)$，故 $D(P(C)||P(X))=0$。

(2) 假设掩盖图像 C 的像素集合为 A，符号集为 B，广义映射对应的覆盖 $A_j,j=1,2,\cdots,n$，则 X 的广义概率分布 $\hat{P}(X)=Q(A_j),j\in B$，由已知条件 $X_{-k}^+\subseteq Y_K^-$，$X_{-k}^+\supseteq Y_K^-$ 且 $X_{-k}^-\subseteq Y_K^+$，$X_{-k}^-\supseteq Y_K^+$，得：

$$\hat{P}(j)=\frac{|A_j|+1-1}{|A|}\quad j\in X_{-k}^+$$

$$\hat{P}(j)=\frac{|A_j|-1+1}{|A|}\quad j\in X_{-k}^-$$

由已知条件 $DC_{w1}(x)=DC_{w2}(x)$，$DC_{w1}(y)=DC_{w2}(y)$，得：

$\hat{P}(j)=\frac{|A_j|}{|A|}$ $j=\bar{x}$ 或 $j=\bar{y}$，故

$$\hat{P}(X)=\begin{cases}\dfrac{|A_j|}{|A|} & j\in(B-X_{-k}^+\cap X_{-k}^-)\\ \dfrac{|A_j|+1-1}{|A|} & j\in X_{-k}^+\\ \dfrac{|A_j|-1+1}{|A|} & j\in X_{-k}^-\end{cases}$$

$\hat{P}(X)=\hat{P}(C)$，$\hat{D}(\hat{P}(C)||\hat{P}(X))=0$

综上，x,y 互换信息隐藏系统满足理论安全性。证毕。

由引理 1 和定理 1 可以求出满足安全约束条件的所有互换对的集合 EX。由于图像中可与一个像素交换的像素不唯一，一个像素又不能被互换多次，因此需要找到方法在多个互换对中选择出一个可进行互换的像素。我们用像素作为顶点，互换对作为边，则图像中可能的互换就构成一无向图。在图像中找一互换对等价于无向图删除一条边，并将该边加入到互换集中。希望求解出最多的互换对，因此选择要删除的边，按如下算法进行：

1) 在无向图中查找度最小的顶点；

2) 在该顶点邻接顶点集中找度最小的顶点；

3) 删除这两个顶点的连接边，加入互换对集。修改与这两个顶点邻接顶点的度，删除这两个顶点；

4) 重复前 3 步，直到无向图为空。

将上述求解出的集合 EX 分成 EX_1 和 EX_2 两个集合，其长度满足：

$|EX_1|=|EX_2|=\lfloor|EX|/2\rfloor$。需要隐藏 bit 0 选择 EX_1 集合中的互换对；否则，选择 EX_2 集合中的互换对。对 EX_1 和 EX_2 两个集合进行自然数索引，得到两个所引集合 EXN_1 和 EXN_2，信息隐藏问题变成如何通过 S 和 K 确定互换对的索引值。这样的信息隐藏方法可用下式描述：

$X=C\Leftrightarrow K$ 记号$\Leftrightarrow$表示互换

由 S 和 K 确定互换对索引值的方法与 $S2$ 安全性的实现方案有关，将在后续的文章中再加以介绍。

3.3 验证实验

实验图像为 512×512，8 bit 灰度的 lena 图像，相邻像素相关区域为 8 邻域，$\delta=1$。lena 图像被分成 8 个 64×64 的图像块分别进行运算。验证实验做了如下 3 项工作。

1) 求出每个图像块中满足安全约束条件的互换对集合 EXC。为了将互换对集合用图形表示，对互换对集合做如下处理：

n 个像素的图像块中可能的互换总数为：

$$n-1+n-2+\cdots+2+1=\frac{n(n-1)}{2}$$

对其按顺序进行索引，像素 i,j 互换对应的索引值为$(2n-i)\times(i-1)/2+j$，构成的索引集合称为互换全集。

EXC 是互换全集的子集，EXC 的互换对与互换全集索引值的对应关系可看成 EXC 的互换对在互换全集的一种分布，称为互换对分布(ECD Exchange couple distribution)。lena 图像第 1 图像块的互换对分布如图 2 所示。索引值取值范围很大，因此用对数表示。

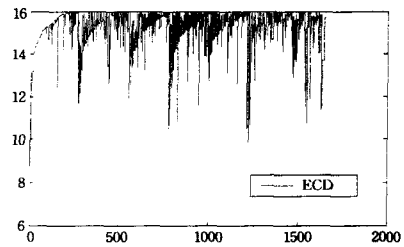

图 2 互换对分布(ECD)

2) 我们做了广义概率分布与互换对关系的统计实验。为了进行比较，需要统计出满足安全约束条件的相同灰度值的像素互换对个数，即频度。因而，同一灰度值的像素互换对频度与广义概率就可以做对比。lena 图像第 1 图像块的对比结果如图 3 所示。

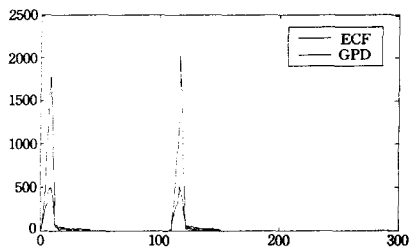

图 3 ECF 与 GPD 对比

图中，ECF(Exchange Couple Frequency)为互换对频度，GPD(generalized Probability Distribution) 为广义概率分布。如图 3 所示，广义概率大，对应互换对频度高。这个规律有较大的实际意义，即在求互换对时，忽略广义概率小的灰度值对

(下转第 130 页)

缩小 20%	0.7921	添加椒盐噪声	0.8579
放大 25%	0.8661	添加乘性噪声	0.8645
条状剪切	0.8532	中值滤波	0.6452
块状剪切	0.8379	维纳滤波	0.6673

从表 3 的测试结果中可以看出，嵌入水印之后，无任何攻击的情况下，提取出的水印相关系数为 0.9999，基本与原图相同。之后对图像进行了常见的几何攻击，包括不同形式的旋转、缩放、剪切和平移，以及一些加噪、滤波处理。从测试结果中可以发现，带剪切的旋转效果明显弱于不带剪切的旋转结果；缩小的结果弱于放大的结果，这些都是由于一些几何攻击在攻击过程中丢失了部分原始数据而造成的。鉴于随着数据的丢失，图像的实际意义也会跟着下降，失去使用价值，所以实验结果还是可以接受的。

结束语 本文从构造几何攻击不变域抵抗几何攻击的思路出发，提出了一种改进的基于奇异值分解的抗几何攻击的数字图像水印算法。

通过对图像奇异值分解的特性进行分析和研究，提出了以奇异值矩阵中次大值点作为水印的最优嵌入位置。并改进现有的分块奇异值分解嵌入方法，提出了一套在 DFT 变换域的类之字形采样方案，详细设计了采样起始和终止位置、采样顺序及数据矩阵的构建方式，有效提高了水印系统的安全性，并解决了分块后无法抵抗旋转攻击的问题，降低了水印检测过程的复杂度。并且，本方案与原有的奇异值分解方法相比，彻底消除了对 U,V 矩阵的依赖，抗干扰能力更强。实验证明，本文提出的水印算法，对于抵抗常见的几何攻击是有效的。

参 考 文 献

[1] Liu R Z, Tan T N. An SVD-based watermarking scheme for protecting rightful ownership[J]. IEEE Transaction on Multimedia, 2002, 4(1): 121-128

[2] Shieh Jieh-Ming, Lou Der-Chyuan, Chang Ming-Chang. A semi-blind digital watermarking scheme based on singular value decomposition[J]. Computer Standards and Interfaces, 2005, 28(4): 428-440

[3] Zhang Zhi-Ming, Wang Lei. A novel SVD watermarking method with turbo code enhanced robustness[C]// Proc. of the Intl. Computer Congress 2004 on Wavelet Analysis and its Applications, and Active Media Technology. v1, 2004

[4] 吕英华，王巍，孔俊，等. 基于 SVD 和神经网络的鲁棒水印算法[J]. 计算机科学，2005，32(12)：232-235

[5] Ganic E, Eskicioglu A M. Robust DWT-SVD domain inage watermarking: embedding data in all frequencies[C]// Proc. of the 2004 Multimedian and Security Workshop on Multimedian and Security. 2004: 166-174

[6] 刘峰，孙林军. 一种基于 DCT 和 SVD 的数字图像水印技术[J]. 计算机应用，2005，25(8)：1944-1946

[7] 黄松，张伟，陈军，等. 一个基于 DWT 的自适应数字水印算法[J]. 计算机科学，2006，33(7)：155-157

[8] 周波，陈健. 基于奇异值分解的抗几何失真的数字水印算法[J]. 中国图像图形学报，2004，9(4)：507-509

[9] 李海峰，王树勋，温泉，等. 基于分块 SVD 和 Zernike 矩的鲁棒图像水印[J]. 模式识别与人工智能，2005，18(3)：359-365

(上接第 122 页)

应像素的计算，不会对互换集有太大影响，但可以显著提高计算时间性能。

3) 用互换集对 lena 图像进行像素互换，进行了互换前后的图像块广义概率分布比较实验，验证了互换前后的图像块广义概率分布不发生变化。由于 $\delta=1$，互换前后的图像在视觉上没有任何变化。将 lena 图像第 1 图像块 EXC 集合的 1653 个互换对都进行像素位置互换，这是图像块失真的极限，对应的峰值信噪比为

$$PSNR=-10\lg\left\{\frac{1}{255^2MN}\sum_{m=1}^{M}\sum_{n=1}^{N}[d(m,n)]^2\right\}$$

$$=-10\lg\left\{\frac{2\times1653}{255^2\times64\times64}\right\}=112.97\text{dB}$$

人眼只能判别出 $PSNR\leqslant38$dB 失真的图像[5]，所以人眼无法判断出互换所产生的图像失真。

为了使以后的研究者能进行数据比较，将 lena 图像第 1 图像块的前几个互换对的数据按顺序给出，如表 2 所列。

表 2 互换对的数据表

互换对	像素	依赖像素数	变化符号集
x(1,45) x(14,46)	x(1,45)=3	1,0,1	{1} - - -
	x(14,46)=4	0,1,2	- {6} - {3}
x(1,52) x(2,47)	x(1,52)=1	1,0,1	- - - -
	x(2,47)=2	0,1,2	- - - {1}
x(1,58) x(54,56)	x(1,58)=123	1,0,1	- - - -
	x(1,52)=122	1,1,0	{120} - - -

依赖像素数的 3 个值依次对应 x_{-1},x,x_{+1} 的依赖像素个数。变化符号集的 4 个值依次对应 $X_{+1}^{+},X_{+1}^{\pm},X_{-1}^{-},X_{+1}^{-}$。

结束语 通过对图像相邻像素的相关性进行分析，给出了基于广义信息熵的安全约束条件，改善了基于香农信息熵的信息隐藏安全模型的不足之处。所提出的信息隐藏的安全约束条件和方法，具有理论和实际的意义。但所提出的广义信息熵是否是理论上最佳的，还有待进一步研究。另外，δ 值的确定与图像的视觉感知模型有关，目前还没能在理论上解决，只能通过实验来确定。

参 考 文 献

[1] Cachin C. An information-theoretic model for steganography[C]// Proceeding of Second International Workshop on Information Hiding. Lecture Notes in Computer Science. 1998: 306-318

[2] Mittelholzer T. An information-theoretic approach to steganography and watermarking[C]// Preliminary Proceedings of the Third Inter-national Information Hiding Workshop. Dresden, Germany, 1999: 1-15

[3] 林代茂，胡岚，郭云彪，等. 广义信息隐藏技术的安全问题[J]. 中山大学学报，2004，43(2)：14-16

[4] 鲁晨光. 广义熵和广义互信息的编码意义[J]. 通信学报，1994，15(6)：37-44

[5] Petitcolas F A P, Anderson R J. Evaluation of Copyright Marking Systems[C]// Proc. IEEE Multimedia Systems. Italy: Florence, June 1999: 574-579