

BSP 二维块交织算法结合 RS 纠错码在水印中的应用*

易琛, 张天骐, 胡然, 曹亮

(重庆邮电大学 信号与信息处理重庆市重点实验室, 重庆 400065)

摘要: 针对数字水印抗突发错误弱鲁棒性的特点,研究了 SP(successive packing)二维交织算法,并根据 RS 纠错码的特性提出一种改进后的二维块交织 BSP(block successive packing)算法。首先构造出低阶的 SP 交织矩阵,然后根据 RS 码每个码字分量的长度构造出单位块矩阵,将单位块矩阵按照低阶 SP 交织矩阵内元素的顺序排列构造出 BSP 交织矩阵。BSP 交织矩阵能将多比特的 RS 码字分量分散开来提升其纠错能力。实验表明, BSP 二维交织与 RS 纠错码相结合在二维空间上的抗突发错误的能力要优于相同码率的 BCH 码加 SP 二维交织,将其应用于水印系统能明显提升水印抗剪切攻击的鲁棒性。

关键词: 数字水印; 二维交织; 二维块交织; 里德—所罗门码; 二维离散余弦变换; 剪切攻击

中图分类号: TN919.8 **文献标志码:** A **文章编号:** 1001-3695(2012)08-3029-04

doi:10.3969/j.issn.1001-3695.2012.08.058

Application of BSP two dimensional block interleaving algorithm and RS coding in digital watermark

YI Chen, ZHANG Tian-qi, HU Ran, CAO Liang

(Chongqing Key Laboratory of Signal & Information Processing, Chongqing University of Posts & Telecommunications, Chongqing 400065, China)

Abstract: This paper studied two dimensional SP interleaving algorithm according to the weak robustness of digital watermark in anti cut attack, proposed an improved BSP interleaving algorithm according to the characters of Reed Solomon code. Firstly, it constructed a low rank SP interleaving matrix and unit matrices respectively, the number of elements in each unit matrix equaled to that in each RS code component. Then it arranged all unit matrices into a new BSP interleaving matrix according to the arrangement of elements in low rank SP interleaving matrix. BSP interleaving matrix could improve RS code error correcting capability via dispersing multi-bit RS code components. Simulation shows that the combination of BSP interleaving and RS code is more robust in anti burst errors than that of SP interleaving and BCH code in two dimensional space, greatly improves the robustness of digital watermark in anti cut attack.

Key words: digital watermark; successive packing two dimensional interleaving; block successive packing two dimensional interleaving; Reed Solomon code; two dimensional discrete cosine transform(2-D DCT); cut attack

0 引言

数字水印作为数字版权保护的一种重要手段目前已成为信息安全领域的一个重要的研究方向。研究人员考虑到数字水印系统跟通信系统相似的情况,将纠错码应用于水印系统中来提升水印的鲁棒性。然而,在实际的普通通信信道中,纠错码常常与交织技术相结合,交织技术能够将突发集中的错误均匀分散开,可以显著地提升纠错码的纠错性能。在数字水印技术中,同样也可以利用交织技术与纠错编码来提升水印的鲁棒性,然而普通的一维度交织技术并不适合二维空间的水印系统。

文献[1]研究了构造二(多)维交织技术的方法,文献[2]创造性地提出了一种 SP 二维交织算法,它能把二维空间上的任意连通封闭区域分散开来,将成块的突发错误分散到不同的码字中,提升纠错码的纠错性能。以往的二维交织在水印系统中的应用研究^[3~7]都只是将 SP 二维交织算法与 BCH 编码相结合,虽然能有效提升水印抗剪切攻击的鲁棒性,但其性能有限。实际上,在一维信道中,RS 码与交织技术相结合能使信息具有更好的抗突发错误的能力,如果能将 RS 码与合适的交织技术相结合应用于水印系统,其抗突发错误的能力将更优。

本文针对这一特点,提出了改进后的 BSP 二维交织算法,此算法以 SP 二维交织算法为基础,对 RS 码字分量进行交织。改进后的 BSP 二维交织能与 RS 纠错码很好地结合提升二维

收稿日期: 2012-01-12; **修回日期:** 2012-02-20 **基金项目:** 国家自然科学基金资助项目(61071196,61102131);教育部新世纪优秀人才支持计划资助项目(NCET-10-0927);信号与信息处理重庆市市级重点实验室建设资助项目(CSTC2009CA2003);重庆市杰出青年基金资助项目(CSTC2011jjjq40002);重庆市自然科学基金资助项目(CSTC2009BB2287, CSTC2010BB2398, CSTC2010BB2409, CSTC2010BB2411)

作者简介: 易琛(1984-),男,湖南岳阳人,硕士研究生,主要研究方向为信道编码及其盲识别、数字水印(yihchan@sina.com);张天骐(1971-),男,四川眉山人,教授,博士(后),主要研究方向为语音信号处理、通信信号的调制解调、盲处理、神经网络实现以及 FPGA、VLSI 实现;胡然(1987-),女,重庆大足人,硕士研究生,主要研究方数字音频水印;曹亮(1987-),男,陕西西安人,硕士研究生,主要研究方向为语音信号处理。

空间抗突发错误攻击的能力,显著提升水印系统的抗剪切攻击的鲁棒性。

1 水印的嵌入和提取

1.1 水印嵌入提取流程

图 1 为原始水印经过预处理、嵌入、提取、后处理最终恢复出水印的流程,本文的主要工作是预处理后处理的编译码和交织部分,如图 1 虚线框所示。

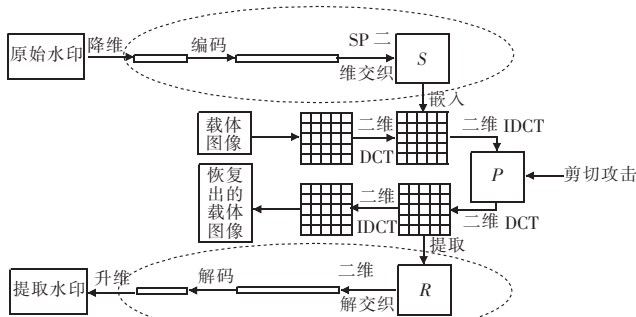


图 1 水印嵌入提取流程

图 1 中载体图像 P 中嵌入的水印由于进行了编码和交织具有抗剪切攻击的能力。

水印嵌入提取的具体步骤如下:

- 将二维水印进行降维、分段编码处理后的一维序列进行 SP 二维交织形成 S 方阵。
- 对方阵载体图像以 8×8 为单位块进行分块处理,对每个 8×8 单位块进行二维 DCT 变换。
- 将 S 方阵中的每个元素(0 或 1)嵌入到对应的经过二维 DCT 变换后的载体图像 8×8 子块中,再将所有子块进行二维离散余弦反变换(IDCT)得到嵌入水印的图像 P 。
- 对图像 P 进行二维 DCT 变换后从每个 8×8 子块中提取出 0 或 1 构成 R 方阵。
- 对 R 方阵进行二维解交织、解码、升维,最后得到恢复出水印。

1.2 二维离散余弦变换(2-D DCT)^[8]

二维 DCT 变换是信息隐藏中主要的变换域算法之一。主要思想是将水印信号嵌入到人类视觉最敏感的中低频部分,攻击者在破坏水印的过程中就不可避免地引起图像质量的严重下降。

一个 $M \times N$ 矩阵 A 的二维 DCT 定义为:

$$D_{ij} = a_i a_j \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos \frac{\pi(2m+1)i}{2M} \cos \frac{\pi(2n+1)j}{2N} \quad (1)$$

$0 \leq i \leq M-1, 0 \leq j \leq N-1$

其中:

$$a_i = \begin{cases} \frac{1}{\sqrt{M}}, & i=0 \\ \sqrt{\frac{2}{M}}, & 1 \leq i \leq M-1 \end{cases}, a_j = \begin{cases} \frac{1}{\sqrt{N}}, & j=0 \\ \sqrt{\frac{2}{N}}, & 1 \leq j \leq N-1 \end{cases} \quad (2)$$

逆 DCT 变换定义为

$$A_{mn} = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} a_i a_j D_{ij} \cos \frac{\pi(2m+1)i}{2M} \cos \frac{\pi(2n+1)j}{2N} \quad (3)$$

$0 \leq m \leq M-1, 0 \leq n \leq N-1$

数值 D_{ij} 称为 A 的 DCT 系数, A_{mn} 为空域图像像素值。

1.3 二值水印的嵌入

图 1 中对原始水印降维、编码后进行 SP 二维交织后形成 S 方阵,将 S 方阵中的 0、1 分别用两组不同的八位 0、1 随机数矢量 k_0 和 k_1 代替,然后将随机数 k_0 或 k_1 嵌入到对应的经过二维 DCT 变换后的载体图像 8×8 子块的中频部分。如图 2 “*”所示。

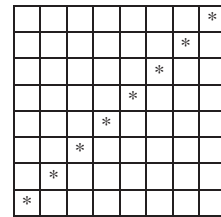


图 2 二维 DCT 中频嵌入

1.4 二值水印的提取

图 1 中对经过剪切攻击后嵌有水印的图像的每个 8×8 子块进行二维 DCT 变换,从每个 8×8 的子块中提取中频的 8 位数值(图 2),将其分别与 k_0 和 k_1 进行比较,与 k_0 接近的判为“0”,与 k_1 接近的判为“1”,然后形成 R 方阵。对 R 方阵进行解交织、解码、升维就可以恢复出水印。

2 RS 纠错码

RS 码属于非二进制 BCH 码,也属于线性分组码中的循环码,与 BCH 码不同的是 RS 码的码字向量的每一个分量为一个符号,每个符号含有 m 个比特。一个码长为 n ,信息位长为 k ,可以纠正任意小于等于 t 个符号差错的 RS 码可以表示为 (n, k, t) 。其中码长 $n = 2^m - 1$ (符号),也可以写成 $n = m \cdot (2^m - 1)$ (比特);校验位长 $r = n - k = 2t$ (符号),也可以写成 $r = m \cdot 2t$ (比特)。设 $\alpha \in GF(q)$ 且是一本原元, α 是生成多项式 $f(x)$ 的根,则最小汉明距离至少为 $2t$ 的 RS 码的生成多项式为

$$g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{2t}) = g_{n-k}x^{n-k} + g_{n-k-1}x^{n-k-1} + \cdots + g_1x + g_0 \quad (4)$$

其生成矩阵为

$$G = \begin{bmatrix} g_{n-k} & g_{n-k-1} & \cdots & g_1 & g_0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & g_{n-k} & \cdots & g_2 & g_1 & g_0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & g_{n-k} & g_{n-k-1} & g_{n-k-2} & g_{n-k-3} & \cdots & g_1 & g_0 & 0 \\ 0 & 0 & \cdots & 0 & g_{n-k} & g_{n-k-2} & g_{n-k-2} & \cdots & g_2 & g_1 & g_0 \end{bmatrix} \quad (5)$$

通过将信息序列与生成矩阵 G 相乘可以得到 RS 编码后的码字,解码部分通常用 Berlekamp Massey 算法实现,具体算法可参见文献[9]。

3 SP 二维交织

3.1 SP 二维交织算法原理

SP 二维交织技术^[2]首先将大小为 $2^n \times 2^n$ 的数组作为交织的对象,将数组四等分为四个象限,然后每个象限又四等分为四个象限,重复这一过程直到最后的象限为 2×2 为止,这些 2×2 的数组构成了最基本的单元。具体构造如下:

先将 2×2 子块内元素按照式(6)的顺序排列成 4 个元素的交织方阵,然后再根据式(7)构造出更高阶的交织方阵。

$$S_4 = \begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix} \quad (6)$$

$$S_{4i} = \begin{bmatrix} 4 \times S_i + 0 & 4 \times S_i + 2 \\ 4 \times S_i + 3 & 4 \times S_i + 1 \end{bmatrix} \quad (7)$$

其中:式(7)中的0、1、2、3都为 2×2 的矩阵。

3.2 与 BCH 编码相结合应用于水印的 SP 二维交织

将 SP 二维交织与 BCH 编码相结合应用于水印系统^[7]可以首先根据式(7)构造出 64 个元素的交织方阵 S_{64} ,如图 3(a)所示。然后将经过 BCH 编码后的 64 位比特序列按照图 3(a)中元素的顺序放入其中。

0	32	8	40	2	34	10	42
48	16	56	24	50	18	58	26
12	44	4	36	14	46	6	38
60	28	52	20	62	30	54	22
3	35	11	43	1	33	9	41
51	19	59	27	49	17	57	25
15	47	7	39	13	45	5	37
63	31	55	23	61	29	53	21

(a) SP 交织后的数组

0	1	4	5	16	17	20	21
2	3	6	7	18	19	22	23
8	9	12	13	24	25	28	29
10	11	14	15	26	27	30	31
32	33	36	37	48	49	52	53
34	35	38	39	50	51	54	55
40	41	44	45	56	57	60	61
42	43	46	47	58	59	62	63

(b) SP 去交织后的数组

图3 SP 交织技术

如图 3(a)所示,假设经过 BCH 编码和 SP 交织后的水印发生了 2×2 突发错误,位于第 1、20、43、62 位。去交织后如图 3(b)所示,突发错误被分散到了四个独立的象限,亦即独立的码字中,随后的译码中这 4 个错误比特能被纠正。因此以比特为单位的 SP 二维交织技术与 BCH 编码相结合运用于数字水印能够有效地抵抗剪切攻击。

然而在普通信道中 RS 码的纠错能力更强,尤其是其抗突发错误要优于 BCH 码。如果将 RS 码与交织结合应用于数字水印系统中,其抗剪切攻击的鲁棒性会更强。

3.3 与 RS 编码相结合应用于水印的 SP 二维交织

假设先对 A、B 两个码字 8 个分量即 32 个比特进行 RS(8, 4)编码,编码后的水印为 64 比特,然后以每个 bit 为单位在 8×8 矩阵中进行 SP 二维交织。图 4(b)和(d)中 A、B 分别为独立码字,数字为每一个码字分量对应的 4 个比特序号。

0	1	4	5	16	17	20	21
2	3	6	7	18	19	22	23
8	9	12	13	24	25	28	29
10	11	14	15	26	27	30	31
32	33	36	37	48	49	52	53
34	35	38	39	50	51	54	55
40	41	44	45	56	57	60	61
42	43	46	47	58	59	62	63

(a) 未交织的数组

A1	0~3	B1	32~35
A2	4~7	B2	36~39
A3	8~11	B3	40~43
A4	12~15	B4	44~47
A5	16~19	B5	48~51
A6	20~23	B6	52~55
A7	24~27	B7	56~59
A8	28~31	B8	60~63

(b) 未交织时 RS 码字错误位置

0	32	8	40	2	34	10	42
48	16	56	24	50	18	58	26
12	44	4	36	14	46	6	38
60	28	52	20	62	30	54	22
3	35	11	43	1	33	9	41
51	19	59	27	49	17	57	25
15	47	7	39	13	45	5	37
63	31	55	23	61	29	53	21

(c) 8×8 SP 交织后的数组

A1	0~3	B1	32~35
A2	4~7	B2	36~39
A3	8~11	B3	40~43
A4	12~15	B4	44~47
A5	16~19	B5	48~51
A6	20~23	B6	52~55
A7	24~27	B7	56~59
A8	28~31	B8	60~63

(d) 8×8 SP 交织后 RS 码字错误位置

图4 SP 交织前后的 RS 码突发错误位置对比

由图 4(a)所示,在交织前,发生突发错误的 8 个比特对应于 RS 码的码字 A 中的 A1~A4 码字分量(图 4(b));而进行 SP 二维交织后(图 4(c)),发生突发错误的 8 个比特对应于 RS 码的码字 A 中的 A2、A4、A5、A7 码字分量以及码字 B 中的 B2、B4、B5、B7 码字分量(图 4(d))。也就是说在加入 SP 二维交

织后,RS 码要纠错的码字反而增加了。因此,以比特为单位的 SP 二维交织并不适合于 RS 纠错码。

为了充分发挥 RS 码的抗突发错误的能力,本文将 SP 二维交织进行了改进,并将其与 RS 码结合应用于水印系统中。改进后的 BSP 交织算法与 SP 交织算法类似,所不同的是 BSP 交织算法是以多比特的码字分量为交织对象。

4 BSP 二维块交织

仍然以 RS(8,4)码为例,先按照式(6)构造出一个低阶的 4×4 SP 二维交织矩阵 S_{16} (图 5(a)),然后以 RS(8,4)码码字分量的长度 4 构成 2×2 的矩阵单位块,矩阵块内的比特排列顺序为图 5(b)所示;然后将每个 2×2 的单位块按照图 5(a) 4×4 SP 交织矩阵内元素的排列顺序排列成新的 BSP 二维交织矩阵。如图 5(c)所示。

0	8	2	10
12	4	14	6
3	11	1	9
15	7	13	5

(a) 4×4 SP 交织

0	1
2	3

(b) 单位块内的比特位置顺序

0	1	32	33	8	9	40	41
2	3	34	35	10	11	42	43
48	49	16	17	56	57	24	25
50	51	18	19	58	59	26	27
12	13	44	45	4	5	36	37
14	15	46	47	6	7	38	39
60	61	28	29	52	53	20	21
62	63	30	31	54	55	22	23

(c) 8×8 BSP 交织后的数组

A1	0~3	B1	32~35
A2	4~7	B2	36~39
A3	8~11	B3	40~43
A4	12~15	B4	44~47
A5	16~19	B5	48~51
A6	20~23	B6	52~55
A7	24~27	B7	56~59
A8	28~31	B8	60~63

(d) 8×8 SP 交织后 RS 码字错误位置

图5 BSP 交织前后的 RS 码突发错误位置对比

由图 4(a)所示,在交织前发生突发错误的 8 个比特对应于 RS 码的码字 A 中的 A1~A4 码字分量(图 4(b));而进行 BSP 二维交织后(图 5(c)),发生突发错误的 8 个比特对应于 RS 码的码字 A 中的 A1、A5 码字分量以及码字 B 中的 B1、B5 码字分量(图 5(d))。也就是说在加入 BSP 二维交织后,A 码组中的 4 个错误码字分量被均匀分配到了 A 和 B 码字中。因此在数字水印系统中,以码字分量为单位的 BSP 交织能与 RS 纠错码很好地结合提升其纠突发错误的能力。本文将 BSP 交织与 RS 纠错码相结合应用于水印系统,提升其抗剪切攻击的鲁棒性。

5 性能评估与仿真结果分析

5.1 水印的性能评估^[10]

本算法用归一化相关系数(NC)来计算原始水印与提取水印图像之间的相似程度,公式为

$$NC(W, W') = \frac{\sum_{i=1}^{M_1} \sum_{j=1}^{M_2} [W(i, j) W'(i, j)]}{\sqrt{\sum_{i=1}^{M_1} \sum_{j=1}^{M_2} [W(i, j)^2]} \times \sqrt{\sum_{i=1}^{M_1} \sum_{j=1}^{M_2} [W'(i, j)^2]}} \quad (8)$$

其中:W 表示原始水印图像;W'表示提取的水印图像。大小为 $M_1 \times M_2$,计算的数值越大表示相似程度越高。

5.2 仿真实验

在仿真实验中,选用 512×512 的 Lena 灰度图像作为载体,选用 40×32 的二值图像作为水印,水印的嵌入强度为 $\alpha =$

15,具体嵌入提取过程如图1所示。将提取后的水印与原始水印进行NC相似度比较。其中编译码部分分别采用BCH(15,5)和RS(15,5)进行对比,BCH码采用SP二维交织,而RS码采用SP二维交织以及BSP二维块交织。

图6为512×512的原始载体图像和40×32二值水印。



图6 原始载体图像和二值水印

图7为嵌有水印的载体图像经过1/4面积剪切攻击后提取恢复出来的图像水印。

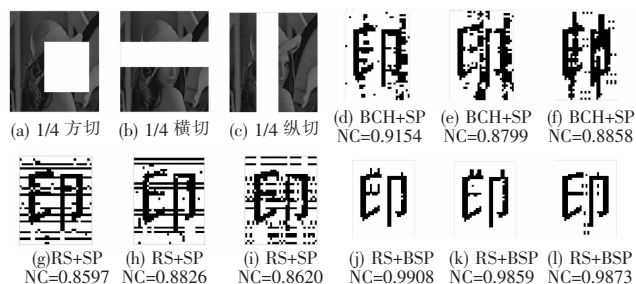


图7 1/4面积剪切攻击后提取出的水印

图7(a)为对嵌有水印载体的图像的任意位置选取面积为其1/4的方块进行剪切;(d)(g)和(j)分别为对水印进行BCH(15,5)编码加SP交织、RS(15,5)编码加SP交织和RS(15,5)编码加BSP交织后从方块剪切后的载体图像中恢复出来的水印。

图7(b)(c)为对嵌有水印载体图像的任意位置进行横向以及纵向切割,所切割条状的宽度为载体图像边长的1/4;(e)(h)和(k)以及(f)(i)和(l)分别为对横向以及纵向切割后恢复出来的水印,其中对水印同样进行BCH(15,5)编码加SP交织、RS(15,5)编码加SP交织和RS(15,5)编码加BSP交织进行对比。

由图7(d)(g)(j);(e)(h)(k);(f)(i)(l)的视觉效果以及NC相似度对比可知对RS编码直接进行SP交织并不合适,而RS编码与改进后的BSP交织相结合应用于水印其抗剪切攻击的鲁棒性要优于BCH码加SP交织。

图8为对嵌有水印的载体图像的任意位置剪切不同面积后水印的抗攻击性能曲线。

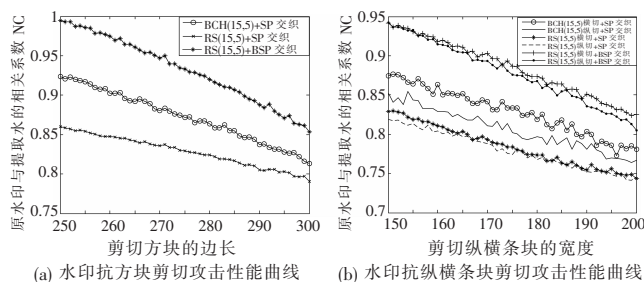


图8 水印抗剪切攻击性能曲线

图8(a)为对载体图像进行方块剪切时水印的抗攻击性能曲线,横坐标为剪切方块的边长,纵坐标为提取水印与原始水印的NC相似度,图中的每个点表示在载体图像中随机取100个位置进行相同面积的方块剪切;然后取NC相似度的平均值,三条曲线由上至下分别表示对水印部分进行RS编码加

BSP交织、BCH码加SP交织以及RS码加SP交织。

图8(b)为在嵌有水印载体图像的任意纵横位置选取不同面积的纵横条块进行剪切后的水印抗攻击性能曲线,横坐标为剪切条块的宽度,纵坐标为水印NC相似度,每个点表示随机取100个纵(或横)位置进行相同面积的条块剪切,取NC平均值,上面两条曲线表示对水印进行RS编码加BSP交织后进行横向条块切割和纵向条块切割,中间两条曲线表示对水印进行BCH编码加SP交织后进行横向条块切割和纵向条块切割,下面两条曲线表示对水印进行RS编码加SP交织后横向和纵向切割。

由图8(a)(b)可知随着剪切面积的增大,NC相似度呈递减趋势,在相同剪切面积下,直接对RS码进行SP交织其抗突发错误的能力还要低于BCH码加SP交织,而对水印进行RS编码加BSP交织后的NC相似度始终要高于BCH码加SP交织以及RS码加SP交织。也就是说在提升水印系统的抗剪切攻击的鲁棒性方面,只有RS码与BSP交织结合才能充分发挥RS码的抗突发错误的性能,并且其性能要优于BCH码加SP交织。

6 结束语

本文提出的一种改进后的BSP二维块交织能够与RS纠错码很好地相结合提升二维空间抗突发错误攻击的鲁棒性。仿真表明,在水印编码交织预处理部分,在相同码率的情况下,RS码直接加SP二维交织后其抗突发错误的能力反而不如BCH加SP交织,而采用RS码加改进的BSP二维交织后水印的抗剪切攻击的鲁棒性却要明显优于BCH码加SP交织。改进后的BSP二维交织能与RS码很好地结合明显提升水印抗剪切攻击的鲁棒性。

参考文献:

- [1] BLAUM M, BRUCK J, VARDY A. Interleaving schemes for multidimensional cluster errors[J]. IEEE Trans on Information Theory, 1998, 44(2): 730-743.
- [2] SHI Y Q, ZHANG Xi-min. A new two-dimensional interleaving technique using successive packing[J]. IEEE Trans on Circuits and Systems I: Fundamental Theory and Applications, 2002, 49(6): 779-789.
- [3] SHI Y Q, ZHANG Xi-min, NI Zhi-cheng, et al. Interleaving for combating bursts of errors[J]. IEEE Circuits and Systems Magazine, 2004, 4(1): 29-42.
- [4] 潘哲朗, 钟金钢. 一种基于纠错编码和交织的盲水印算法[J]. 计算机应用研究, 2005, 22(9): 180-182.
- [5] 刘九芬, 王振武, 黄达人. 抗几何攻击的小波变换域图像水印算法[J]. 浙江大学学报: 工学版, 2003, 37(4): 386-392.
- [6] 王振武, 刘九芬, 黄达人. 一种有意义的图像水印算法[J]. 中山大学学报: 自然科学版, 2003, 42(1): 1-4.
- [7] 潘哲朗, 许红山. SP二维交织算法在水印中的应用[J]. 广州大学学报: 自然科学版, 2005, 4(3): 220-222.
- [8] 王丽娜, 郭迟, 李鹏. 信息隐藏技术实验教程[M]. 武汉: 武汉大学出版社, 2004.
- [9] 王新梅, 肖国镇. 纠错码原理与方法[M]. 西安: 西安电子科技大学出版社, 2001.
- [10] 杨榆. 信息隐藏与数字水印实验教程[M]. 北京: 国防工业出版社, 2010.