

复数基下的数字媒体表达及信息隐藏

陈伟, 陈亚楠, 刘渊

(江南大学数字媒体学院, 江苏 无锡 214122)

摘要: 随着数字媒体技术的飞速发展及广泛应用, 数字媒体信息安全问题日益引起高度关注。由于数字媒体形式多样, 以往的相关研究工作集中于某一具体媒体形式的安全保护, 如文字、图像、声音、视频。在计算机及网络环境下, 一切对象以数字化的形式出现。将所有数字媒体信息在复数基的形式下进行统一表达, 给出数字媒体与复数之间的相互转换算法, 从而将数字媒体之间的关系变换为复平面上点的几何关系, 并实现了数字媒体的信息隐藏。

关键词: 复数基; 高斯整数; 数字媒体; 信息隐藏

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00106

Digital media representation under complex number base and its application on information hiding

CHEN Wei, CHEN Ya-nan, LIU Yuan

(School of Digital Media, Jiangnan University, Wuxi 214122, China)

Abstract: With the rapid development and wide application of the digital media technology, the information security problem is becoming more and more highly attention. Because of the various kinds of medias, previous research works have focused on a specific digital media from, such as text, image, audio and video. As a fact that all the objects were expressed in digital forms under the environment of computer and network, a unified form for all kinds of digital media under the complex number base system was proposed. The algorithm of the digital media signal and the complex number intercom version were given, so the relationship among the digital media could be converted to the corresponding geometric relationship on the complex plane. In the experiments, the proposed method was applied to the application of the digital media information hiding.

Key words: complex base, gauss integer, digital media, information hiding

1 引言

数字媒体是指以二进制 0-1 序列的形式记录、处理及传播的信息载体, 包括数字化的文字、

图形、图像、声音、视频、动画等多种形式。随着网络基础设施的完善, 一个可以综合各种数字媒体服务的信息高速公路正在向世人开放。从技术角度讲, 数字媒体的内容生产、网络传播及安

收稿日期: 2016-10-16; 修回日期: 2016-11-20。通信作者: 陈伟, wchen_jdsm@163.com

基金项目: 国家自然科学基金资助项目 (No.61602213); 浙江大学 CAD&CG 国家重点实验室开放课题基金资助项目 (No.A1609); 国家科技支撑计划基金资助项目 (No.2015BAH54F00)

Foundation Items: The National Natural Science Foundation of China(No.61602213), The Open Project of the State Key Laboratory of CAD&CG of Zhejiang University(No.A1609), The National Science and Technology Support Program (No.2015BAH54F00)

全保护是该产业的三大支撑,而这 3 个方面又是相互联系与影响的。随着数字媒体技术的飞速发展及广泛应用,数字媒体信息安全问题日益引起高度关注。

在以往的研究工作中,基本上都聚焦于单一类型数字媒体的信息安全保护研究,如数字图像的水印技术^[1-4]与信息隐藏^[5-7]、音频信号的安全保护^[8,9]、位置信息保护^[10,11]等。在各自的领域中提出了多种多样的算法,也取得了一定的成功。本文打破了不同数字媒体在算法适用性上的限制,以一种统一的技术来研究数字媒体的信息隐藏。

为了实现这一目的,本文从数字媒体信号的表达这一基本问题入手。在计算机及网络环境下,文字、声音、图像、视频等表现形式,都是以 0-1 序列码的形式出现,即本质上是一个二进制数字。而如何表示数是数学理论及应用的根本问题之一,记数法是数学研究的永恒课题。实际上,在数学研究领域,除了所熟知的十进制和二进制系统,还存在多种多样的记数法,如位值制系统^[12]、基数系统^[13]、 β -展开系统^[14]。

记数法建立在某个基 B 和有限数字符号集 S 上,在基 B 的选择上,不只限于正整数、负整数及非整数,复数也可作为基。遗憾的是,迄今为止,这方面的研究十分有限^[15,16]。实际上,随着数字媒体技术的发展,一切对象以数字化的形式出现,将数字信息在复数基下进行表达,会有许多特殊的性质及应用^[17,18]。本文将数字媒体信号在复数基下进行统一表达,将数字媒体转换为复平面上的点,运用平面几何关系,实现了数字媒体之间的信息隐藏。

2 预备知识

2.1 位值制记数法

人们最熟悉的表示数的系统是十进制和二进制。在十进制位置记数法中,只要采用 0,1,2,...,9 这 10 个数字符号就可以把所有的非负整数通过有限形式表示出来。采用二进制时,用 0、1 这 2 个数字符号表示。这时 10 与 2 分别称为十进制和二进制系统的基。大于 1 的任何正整数 a 均可作为表示非负整数的基。实际上,对任意非负整数 p ,

总可以找到 $r_0 \in \{0,1,\dots,a-1\}$ 及非负整数 p_1 , 使

$$p = p_1 a + r_0 \quad (1)$$

具有这种性质的最小的数字符号集合 $\{0,1,\dots,a-1\}$ 称为模 a 的完全剩余类。进一步地,存在非负整数 p_2 和 $r_1 \in \{0,1,\dots,a-1\}$, 使

$$p_1 = p_2 a + r_1 \quad (2)$$

如此进行下去,经过有限步,有 r_k 和 $r_{k-1} \in \{0,1,\dots,a-1\}$, 使

$$p_{k-1} = r_k a + r_{k-1} \quad (3)$$

依次回代得到

$$p = r_k a^k + r_{k-1} a^{k-1} + \dots + r_1 a + r_0 \quad (4)$$

或记为

$$p = (r_k r_{k-1} \dots r_1 r_0)_a \quad (5)$$

这便是 a 进制系统。

在正整数基 $a > 1$ 下,表示负整数需要采用负号。但是,如果选取负整数 $a < -1$ 作为基,容易验证,只要用 $|a|$ 个数字符号 $0,1,2,\dots,|a|-1$ 就可以把所有整数(包括负整数)表示出来,此不累述。

2.2 复数基

把基的概念推广到复数中去,数字符号采用 0 和自然数。设 x, y 为实整数,则 $Z = x + iy$ 称为高斯整数。假设选定的复数基为 b (其中,应包含虚数单位 $i = \sqrt{-1}$),那么高斯整数可表达为 $Z = \sum_{j=0}^k r_j b^j$, 称 Z 在复数基 b 下是可表示的。高斯早年已从数学理论上证明,如果 ξ 和 η 互为素数,那么数字符号集 $S = \{0,1,\dots,\xi^2 + \eta^2 - 1\}$ 构成模 b 的完全剩余类。根据数字计算机的特点,自然规定 $S = \{0,1\}$, 于是可选择的复数基有 $b = \xi + i\eta (\xi, \eta = \pm 1)$, 表 1 以 $b = -1 + i$ 为例,列出前面若干正整数在十进制、二进制及复数基系统下的表示。

2.3 0-1 码到复平面的映射

如前所述,当选定复数基 b 及数字符号集 S 后,就可以研究高斯整数(复平面上的点)的表示问题。下面借助图像来直观地解释 0-1 序列码到复平面上点的映射。

表1 以 $b=-1+i$ 为基的整数

十进制	二进制	$b=-1+i$
0	0	0
1	1	1
2	10	$-1+i$
3	11	i
4	100	$-2i$
5	101	$1-2i$
6	110	$-1-i$
...	...	...

把复平面分割成边长为单位 1 的正方形方块, 每个方块

$$\{(x, y) | k \leq x \leq k+1, l \leq y \leq l+1\} \quad (6)$$

对应一个高斯整数 $k+il$, 把在基 $b=\xi+i\eta$ ($\xi, \eta=\pm 1$) 下表达出来的高斯整数对应的方块涂上颜色。为了区分不同的高斯整数, 本文按照表达复数的 0-1 码长度从小到大的次序进行排列, 记长度为 L , 下面以 $b=-1+i$ 为例进行说明。

长度为 1, 除 0 之外, 有 1 个数

$$(1)_b = 1 \quad (7)$$

把这 2 个数 (包括 0) 画在复平面上, 如图 1(a) 所示。

长度为 2, 有 2 个数

$$(10)_b = -1+i, (11)_b = i \quad (8)$$

把这 2 个数补画到之前的复平面上, 如图 1(b) 所示。

长度为 3, 有 4 个数

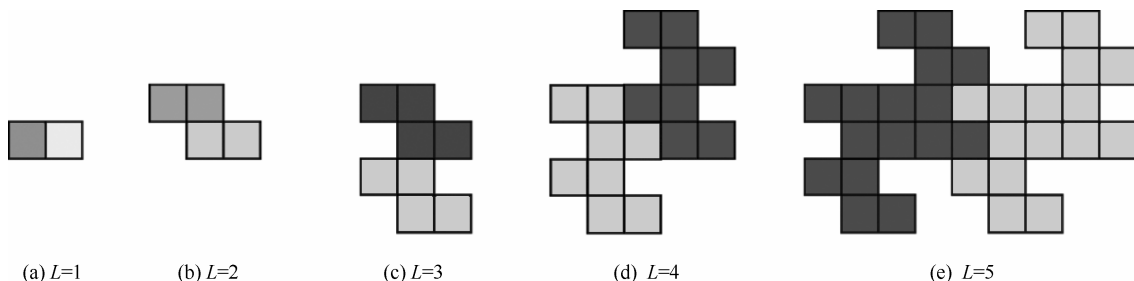


图1 不同长度的复数

$$\begin{cases} (100)_b = -2i \\ (101)_b = 1-2i \\ (110)_b = -1-i \\ (111)_b = -i \end{cases} \quad (9)$$

同样, 这 4 个新增加的复数如图 1(c) 所示。

继而在长度为 4 及长度为 5 时, 分别对应 8 个及 16 个复数, 如图 1(d) 和图 1(e) 所示。

一般地, 长度为 $L=k+1$, 有 2^k 个复数 (最高位保持为 1)。于是把这 2^k 个方块涂上同一种颜色画在复平面上。如此迭代下去, 生成的图形序列如图 2 所示。

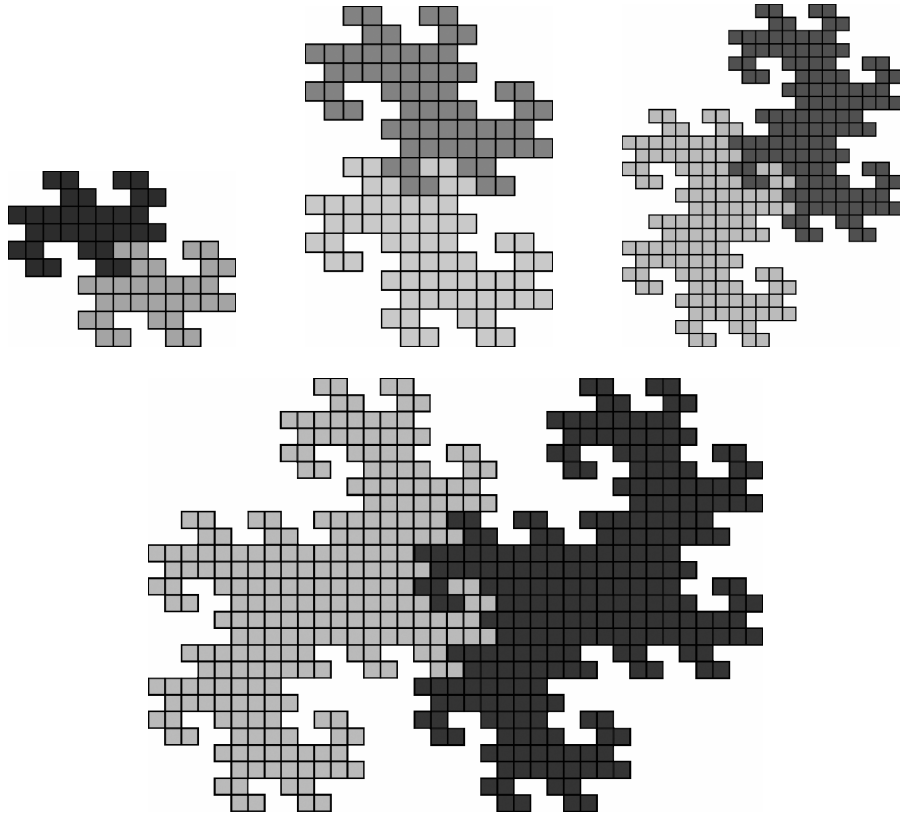
2.4 高精度计算

在 2.3 节中, 从数学理论上阐述了复数基下的数的表示问题, 图 1 及图 2 能够从直观上理解相应的原理。实际上, 在应用时所涉及的数字会非常大 (如构成一段声音的 0-1 序列所对应的数字), 在将该数字在复数基下转换成一个高斯整数, 以及在复数域下进行相关的操作时, 必然遇到大整数运算 (见实验部分)。在数值计算领域, 这类问题属于高精度计算算法。

由于计算机硬件所限, 数的表示范围及精度有限。例如, C/C++ 中的 `int` 类型表示的范围是 $-2^{EXP31} \sim 2^{EXP31}-1$, 而实际应用中会遇到基本数据类型无法表示的大整数。本文仅涉及大整数的加法和减法计算, 主要包括 2 部分内容: 一方面是存储问题, 需要用字符数组来存储一个长整数, 每个数组元素对应一位 (从低位到高位); 另一方面是计算问题, 原理很简单, 就是模拟小学生列竖式逐位做加法或减法。

3 复数基下的数字信息表达

本节讨论数字媒体信息与高斯整数之间的相互转换算法。即 0-1 序列码在复数基 $b=\xi+i\eta$ ($\xi, \eta=\pm 1$)

图 2 高斯整数在复数基 $b = -1 + i$ 下的图形序列

下的表达以及相反的过程。

3.1 高斯整数转换为数字媒体 0-1 序列

设复平面上的一个高斯整数为 $P_0 + iQ_0$, 假设它对应的 0-1 序列为 $e_N e_{N-1} \cdots e_2 e_1 e_0, e_j \in \{0, 1\}$ 。本文的目标是确定 $e_j, j = 0, 1, \dots, N$, 使 $P_0 + iQ_0 = e_N b^N + e_{N-1} b^{N-1} + \cdots + e_1 b^1 + e_0 b^0$ 。

为了构造迭代算法, 记

$$\begin{aligned} P_0 + iQ_0 &= (\zeta + i\eta)(P_1 + iQ_1) + e_0 \\ &= \zeta P_1 - \eta Q_1 + (\eta P_1 + \zeta Q_1)i + e_0 \end{aligned} \quad (10)$$

那么

$$P_0 = \zeta P_1 - \eta Q_1 + e_0, Q_0 = \eta P_1 + \zeta Q_1 \quad (11)$$

由此得到迭代关系

$$\begin{bmatrix} P_{k+1} \\ Q_{k+1} \end{bmatrix} = \begin{bmatrix} \zeta & \eta & -\zeta \\ -\eta & \zeta & \eta \end{bmatrix} \begin{bmatrix} \frac{P_k}{2} \\ \frac{Q_k}{2} \\ \frac{e_k}{2} \end{bmatrix} \quad (12)$$

在迭代过程中需要始终保证 P_k, Q_k 为整数, 令 $e_k = \lfloor \text{mod}(P_k - Q_k, 2) \rfloor$ 。也就是说, 当 P_k, Q_k 的奇偶性相同时, $e_k = 0$, 否则 $e_k = 1$ 。当 P_k, Q_k 同时为零时, 迭代终止。将迭代过程中得到的 e_k 依次排列得到最终的结果 $e_N e_{N-1} \cdots e_2 e_1 e_0$, 即给定的高斯整数 $P_0 + iQ_0$ 在复数基 $b = \zeta + i\eta$ 下的 0-1 序列表达。

3.2 数字媒体 0-1 序列转换为高斯整数

相反地, 如果给定某个数字媒体信号, 其 0-1 序列码为 $e_N e_{N-1} \cdots e_2 e_1 e_0$, 计算它在复数基 $b = \zeta + i\eta$ 下对应的高斯整数。为了构造该算法, 首先令 $(\zeta + i\eta)^k = r_k + is_k$, 显然, 当 $k = 0$ 时, 有 $r_0 = 1, s_0 = 0$ 。

同样地, 为了构造迭代算法, 令

$$\begin{aligned} (\zeta + i\eta)^k &= (\zeta + i\eta)(r_{k-1} + is_{k-1}) \\ &= \zeta r_{k-1} - \eta s_{k-1} + i(\eta r_{k-1} + \zeta s_{k-1}) \end{aligned} \quad (13)$$

那么

$$r_k = \zeta r_{k-1} - \eta s_{k-1}, s_k = \eta r_{k-1} + \zeta s_{k-1} \quad (14)$$

由此得到迭代关系

$$\begin{bmatrix} r_{k+1} \\ s_{k+1} \end{bmatrix} = \begin{bmatrix} \zeta & -\eta \\ \eta & \zeta \end{bmatrix} \begin{bmatrix} r_k \\ s_k \end{bmatrix} \quad (15)$$

由于已知

$$\begin{aligned} P_0 + iQ_0 &= e_N b^N + e_{N-1} b^{N-1} + \cdots + e_1 b^1 + e_0 b^0 \\ &= e_N (r_N + is_N) + e_{N-1} (r_{N-1} + is_{N-1}) + \cdots + \\ &\quad e_1 (r_1 + is_1) + e_0 \\ &= \sum_{j=0}^N e_j r_j + i \sum_{j=0}^N e_j s_j \end{aligned} \quad (16)$$

从而

$$P_0 = \sum_{j=0}^N e_j r_j, Q_0 = \sum_{j=0}^N e_j s_j \quad (17)$$

因此, 该数字媒体信号在复数基 $b = \zeta + i\eta$ 下对应的高斯整数为 $P_0 + iQ_0$ 。

3.3 复数基下数字媒体信息隐藏

如前文所述, 本文构造了数字媒体信号 (0-1 序列码) 与高斯整数之间的相互转换算法。根据这一理论, 本文将应用到数字媒体信号的信息隐藏中。定义函数 $G(x): x \rightarrow N$ 为数字媒体 (文字、声音、图像、视频等) 编码到 0-1 序列的映射, 其逆映射为 $G^{-1}(N): N \rightarrow x$; 函数 $F_b(N): N \rightarrow Z$ 为 0-1 序列到复平面上高斯整数的映射, 其逆映射为 $F_b^{-1}(Z): Z \rightarrow N$ 。那么, 复合函数 $T(x) = F_b(G(x)): x \rightarrow Z$ 为数字媒体到高斯整数的变换。如图 3 所示。

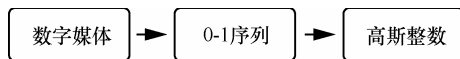


图3 从数字媒体到高斯整数

针对不同的数字媒体, 通过本文算法得到复平面上的各自对应点。那么, 原来这些数字媒体之间的关系就转换为复平面上点与点之间的几何关系。这样一来, 传统的平面几何学中的若干理论可应用于数字媒体信息隐藏中。图4是一张示意图, 一段声音信号经计算得到高斯整数 Z_1 , 一张卡通画经计算得到高斯整数 Z_2 。假设该段声音是需要保密的 (不能公开), 而卡通画是可以公开的, 那么, 在复数基的意义下, 声音 (Z_1) 减去卡通画 (Z_2) 得到差向量 $Z' = Z_1 - Z_2$, 从而可以实现声音与卡通画之间的相互转换。即通过公开的卡通图像中恢复声音 $Z_1 = Z_2 + Z'$ 。

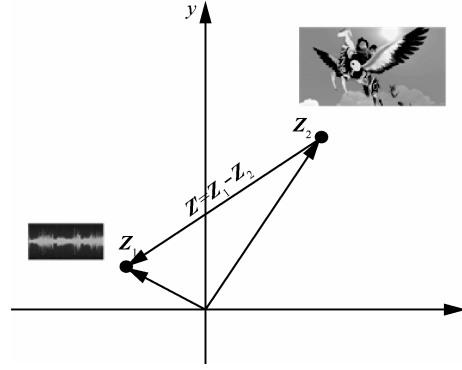


图4 数字媒体的复数基表达及其几何关系

4 实验

下面以数字图像为例, 通过本文算法实现图像的信息隐藏。在以下所有实验中, 取复数基 $b = -1 + i$ 。

实验1 2幅图像之间的信息转换

假设有一幅需要保密的图像, 如图5(a)所示, 为了实现对保密图像的隐藏, 任意选择一幅不相关的公开图像, 如图5(b)所示, 尺寸、颜色、内容等均无特殊要求。通过本文算法, 首先将这2幅图像分别在复数基下转换为复数, 如图6所示, 记为 Z_1, Z_2 。表2中列出了保密图像和公开图像的基本指标, 这些结果均在高精度长整数算法下实现, 计算精确, 无误差。将差向量 $Z' = Z_1 - Z_2$ 作为密钥, 可精确恢复出保密图像, 如图5(c)所示。



(a) 保密图像 motorcycle



(b) 公开图像 Lena



(c) 恢复图像 (精确恢复)

图5 保密图像与公开图像的信息转换

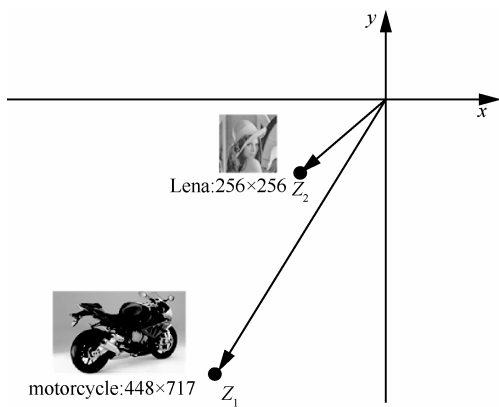


图 6 保密图像与公开图像在复数基下的表达

表 2 保密图像与公开图像

基本指标	保密图像 motorcycle	公开图像 Lena
尺寸	418×717	256×256
0-1 码长度	2 397 648	524 288
复数基下高斯整数数量级	$10^{386\ 783}$	$10^{78\ 914}$

实验 2 根据不相关图像恢复多张保密图像

现有 2 张需要保密的图像，如图 7 中 A、B 所示。在复数基下，分别对应复平面上的 Z_0 、 Z_1 。根据复平面上点的几何关系，可以生成复数 Z_2 、 Z_3 ，其几何关系如图 7 所示。根据本文算法，可重构出 Z_2 、 Z_3 对应的 0-1 码序列，再将其转换为相同尺寸的图像，如图 7 中 C、D 所示。这 2 幅看上去毫无意义的图像可以作为公开图像，而保密图像 A、B 的信息隐藏其中。重构公式分别为

$$Z_1' = Z_2 - \frac{Z_3 - Z_2}{-i} \quad (18)$$

$$Z_0' = Z_1' - \frac{Z_2 - Z_1'}{i} \quad (19)$$

实验结果显示，可精确重构出保密图像 A、B。

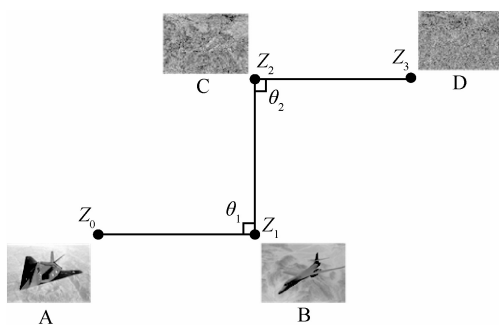


图 7 根据不相关图像恢复多张保密图像

5 结束语

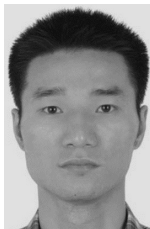
本文从数字媒体的表达这一基本问题入手，给出了不同类型的数字媒体在复数基下的统一表达方法。通过本文算法，将数字媒体信号映射到复平面上的点，再借助于经典的平面几何学关系，实现了一种数字媒体的信息隐藏算法。在算法的具体实现中，由于只涉及长整数的加法与减法运算，数值稳定，能够实现数字媒体的精确重构。结果表明，基于复数基的数字媒体信息处理方法具有较大的研究价值与应用潜力。

参考文献：

- [1] TAZ K T, ZHANG X P, DIMITRIOS A. Color image watermarking using multidimensional fourier transforms[J]. IEEE Transactions on Information Forensics and Security, 2008, 3(1): 16-28.
- [2] URVOY M, GOUDIA D, AUTRUSSEAU F. Perceptual DFT watermarking with improved detection and robustness to geometrical distortions[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(7): 1108-1119.
- [3] 霍耀冉, 和红杰, 陈帆. 基于邻域比较的 JPEG 脆弱水印算法及性能分析[J]. 软件学报, 2012, 23(9): 2510-2521.
- [4] 朱新山, 陈砚鸣, 董宏辉, 等. 基于双域信息融合的鲁棒二值文本图像水印[J]. 计算机学报, 2014, 37(6): 1352-1364.
- [5] HU X, ZHANG W, HU X, et al. Fast estimation of optimal marked-signal distribution for reversible data hiding[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(5): 779-788.
- [6] 徐甲甲, 张卫明, 蒋瑞祺, 等. 最优结构相似约束下的可逆信息隐藏算法研究[J]. 网络与信息安全学报, 2016, 2(2): 55-61.
- [7] LIN S J, CHUNG W H. The scalar scheme for reversible information-embedding in gray-scale signals: capacity evaluation and code constructions[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(4): 1155-1167.
- [8] NATGUNANATHAN I, YONG X, YUE R, et al. Robust patchwork-based embedding and decoding scheme for digital audio watermarking[J]. IEEE Transactions on Audio, Speech and Language Processing, 2012, 20 (8): 2232-2239.

- [9] ARASHDEEP K, MALAY K D, SONI K M, et al. Hiding biometric features in audio signals using Gram-Schmidt orthogonalisation[J]. International Journal of Electronic Security and Digital Forensics, 2016, 8(1): 63-81.
- [10] 许志凯, 张宏莉, 史建焘, 等. 面向移动社交网络的位置隐私保护方法[J]. 网络与信息安全学报, 2015, 1(12): 50-57.
- XU Z K, ZHANG H L, SHI J T, TIAN Z H. Location privacy protection for mobile social network[J]. Chinese Journal of Network and Information Security, 2015, 1(12): 50-57.
- [11] HENGARTNER U. Hiding location information from location-based services[C]//The International Conference on Mobile Data Management, Mannheim. 2007: 268-272.
- [12] 吴文俊. 王者之路—机器证明机器应用[M]. 长沙: 湖南科学技术出版社, 1999.
- WU W J. Theorem proving by machine and application[M]. Changsha: Hunan Science Technology Press, 1999.
- [13] BERGMAN G. A number system with an irrational base[J]. Math Magazine, 1957, 31(2): 98-110.
- [14] PARRY W. On the β -expansions of real numbers[J]. Acta Math Acad Sci Hungar, 1960, 11: 401-416.
- [15] KUNTH D E. The art of computer programming, vol.2: semi-numerical algorithms[M]. Addison-Wesley, 1969.
- [16] KATAI I, SZABO J. Canonical number system for complex integers[J]. Acta Sci Math, 1975, 37(3):255-260.
- [17] 孙伟, 杨志华, 齐东旭. 图像的复数表示及其在图像秘密分存中的应用[J]. 中国图象图形学报, 2004, 9(11): 1331-1335.
- SUN W, YANG Z H, QI D X. The conversion method from image to complex number and its application in image secret sharing[J]. Journal of Image and Graphics, 2004, 9(11): 1331-1335.
- [18] 朱喜玲, 陈伟, 宋瑞霞, 等. 复数基下的图像伪装算法[J]. 中国图象图形学报, 2015, 20(5): 618-624.
- ZHU X L, CHEN W, SONG R X, QI D X. Image disguise algorithm based on complex number base[J]. Journal of Image and Graphics, 2015, 20(5): 618-624.

作者简介:



陈伟 (1986 -), 男, 江苏宝应人, 博士, 江南大学讲师, 主要研究方向为图像处理。



陈亚楠 (1994 -), 女, 江苏宿迁人, 江南大学本科生, 主要研究方向为图像处理。



刘渊 (1967-), 男, 江苏无锡人, 硕士, 江南大学教授, 主要研究方向为网络安全。