

一种新的基于比特置乱的超混沌图像加密算法

谢国波,王 添

(广东工业大学 计算机学院, 广东 广州 510006)

摘 要:提出了一种新的基于超混沌和比特替换的图像加密算法. 算法所采用的混沌系统为 Hyperhenon 映射和 Kent 映射,而且在加密过程中引入了与图像本身特性密切相关的参数. 首先是利用 Kent 映射所产生的一组混沌序列来对明文图像位置进行置乱;再通过 Hyperhenon 映射产生的混沌序列,结合该混沌序列的特性来对每个像素进行内部比特置乱和像素扩散,从而使明文图像达到更好地加密效果. 实验仿真结果显示,新的加密算法既能较好地抵抗统计特性分析和差分攻击,又能有效抵抗选择明文(密文)攻击,还具有密钥空间大、加密效果好等优点.

关键词:混沌系统;图像加密;比特;Kent 映射;Hyperhenon 映射

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2016)07-0028-05

A Novel Hyperchaotic Image Encryption Algorithm Based on Bit Scrambling

XIE Guo-bo ,WANG Tian

(Faculty of Computer, Guangdong University of Technology, Guangzhou 510006,China)

Abstract: We propose a new chaotic image encryption algorithm based on hyperchaotic and bit substitution . The algorithm uses Hyperhenon map and Kent map , and makes the encryption process be related closely with the plaintext image's self characteristics. First, A chaotic sequence generated by Kent map is used to make image position global scrambling ;Then ,use Hyperhenon map to generate a chaotic sequence,and by using properties of the chaotic sequence to scramble internal bit of each pixel and pixel diffusion so that plain image information can be well hidden. The simulation results show that the algorithm can better resist statistical characterization, differential attack, and can effectively resist chosen plaintext (ciphertext) attacks, and have big key space, good encryption effect.

Key words: chaotic systems;image encryption;bit;Kent map;Hyperhenon map

1 引言

网络给人们的工作和生活带来了很多便捷,但是网络信息安全问题也是接踵而至. 因而数字图像的加密技术成为了时下信息安全领域的一个热点. 近年来,混沌系统以其对初值敏感性高、无周期性和伪随机性等特点使得它越来越多地被应用于图像加密中,已有许多基于混沌系统的图像加密算法^[1-3]被提出.

目前基于混沌图像加密算法大都采用像素位置置乱和像素值替代的思想,该思想也很好地体现出了置乱和扩散这两个密码设计的基本原则. 仅仅使用一维混沌系统对图像加密不能有效抵抗常见的攻击,而超混沌系统因具有更好的混沌特性以及随机性受到了众多学者们的青睐,在混沌图像加密中被广泛应用. 文献[4]提出一种基于 Logistic 映射和超混沌的图像加密算法,文献[5]提出了一种基于 Lorenz 超混沌系统的彩色图像加密算法. 而文献

收稿日期: 2015-07-06; **修回日期:** 2015-08-29

基金项目: 广东省重大科技专项(2012A080103010);广东省重点实验室建设专项(2011A091000046);粤港关键领域重点突破项目(2012A080107007);广东省科技计划项目(2012B060500071);广东省自然科学基金(2014A030313512)

[6]提出了一类具有“置乱-替代”架构的混沌加密算法,但它们的抵御选择明文(密文)攻击能力较弱,容易被黑客攻击.例如文献[7]中所提出的通过选择一组特殊明文(密文)就可以成功破解这类加密算法.

基于以上这些混沌图像加密算法存在的不足,本文提出了一种基于比特置乱的超混沌图像加密算法.这种新的加密算法不仅有较好的抗统计特性分析能力和抗差分攻击能力,而且具有较大的密钥空间和对初始条件极度敏感等特性.

2 算法原理

2.1 Hyperhenon 与 Kent 混沌系统简介

Hyperhenon 映射是一个超混沌系统,超混沌系统经常用于混沌加密算法中,因为超混沌系统具有两个或两个以上正的 Lyapunov 指数,相比于普通的混沌系统具有更好的动力学特性及更好的随机性. Hyperhenon 映射的定义为

$$\begin{cases} X_{k+1} = c - Y_{k+1}^2 - d \cdot Z_{k+1} \\ Y_{k+1} = X_k \\ Z_{k+1} = Y_k \end{cases} \quad k = 0, 1, 2, \dots \quad (1)$$

当 $c = 1.76, d = 0.1$, 且初始值 x_0 在 $(0, 1)$ 中取值时,系统将进入混沌状态,将式(1)进行迭代可产生一组超混沌序列.

Kent 映射是一种具有良好性能的混沌系统,因此本文利用它来产生混沌序列,它的映射关系如下:

$$F(x) = \begin{cases} x/a, x \in (0, a] \\ (1-x)/(1-a), x \in (a, 1] \end{cases} \quad (2)$$

式中 a 作为该混沌系统的一个控制参数,当 $x \in (0, 1), a \in (0, 1)$ 时,式(2)具有一个正的 Lyapunov 指数,使得 Kent 映射处于混沌状态,由混沌特性可知,初始条件 x_0 在 Kent 映射中产生的序列是一种非周期且收敛的伪随机序列.同时, Kent 映射对初始条件极其敏感,初始值哪怕产生非常小的变化,结果也将产生两个完全不同的伪随机序列.

2.2 加密和解密原理

2.2.1 图像像素位置的置乱

用 A 来表示一个大小为 $m \times n$ 的灰度图像, t 作为混沌系统产生混沌序列的迭代次数,将 avg 作为像素平均值以及 sum 用作图像所有像素值的总和,加密步骤如下所示.

(1) 先按照行优先的顺序把明文图像 A 转换为长度为 $m \times n$ 的一维序列 $L = \{l_1, l_2, l_3, \dots, l_{m \times n}\}$, 取值范围在 $[0, 255]$ 之间.

(2) 将明文图像的所有像素值相加得到像素值总和为 sum , 继续用 sum 除以图像像素点的个数 $m \times n$, 由式(3)可得明文图像的平均像素值 avg , 式(4)、(5)可得出 Kent 映射的控制参数 a 以及迭代次数 t .

$$\text{avg} = \text{sum} / m \times n \quad (3)$$

$$a = \frac{\text{mod}(\text{sum} \times 100, m \times n)}{m \times n} \quad (4)$$

$$t = m + n + \text{mod}(\text{avg} \times 10^8, m + n) \quad (5)$$

(3) 设置 Kent 映射的初始值为 x_0 , 将 x_0 和以上步骤中所得的 a 代入式(2), 将 Kent 映射迭代 t 次用来除去暂态效应所带来的影响, 以第 t 次为起点继续迭代 Kent 映射 $m \times n$ 次, 从而产生一组长度为 $m \times n$ 的混沌序列 $K = \{k_1, k_2, \dots, k_{m \times n}\}$. 然后对混沌序列 K 按照从大到小进行排序, 进而得到一组用于标记排序后的序列中各元素在排序前序列 K 中所处位置序号的位置序列 $K' = \{k'_1, k'_2, \dots, k'_{m \times n}\}$, 用序列 K' 来对序列 L 进行全局性位置置乱, 最终就得到了一组置乱图像序列 $L' = \{l'_1, l'_2, \dots, l'_{m \times n}\}$.

2.2.2 图像像素的比特置乱和扩散

由于超混沌具有更好地混沌特性, 此阶段将采用 Hyperhenon 超混沌系统来产生一个混沌序列, 再将 L' 中所有的序列值转化为八位二进制形式进行表示, 结合混沌序列自身的特性来对图像像素进行比特置乱和扩散操作, 从而得到最终加密密文.

(1) 设置初始值 X_0 为 x_1, Y_0 为 y_1 , 将其代入 Hyperhenon 超混沌映射进行迭代 800 次以后, 继续迭代 $m \times n$ 次, 得到一个长度为 $m \times n$ 的混沌序列 $P = \{p_1, p_2, \dots, p_{m \times n}\}$.

(2) 将置乱图像序列 $L' = \{l'_1, l'_2, \dots, l'_{m \times n}\}$ 中所有序列值转化为 8 位二进制数, 通过比较 P 中相邻两数的大小来对像素进行比特位置置乱. 如果 $p_i > p_{i+1}$, 则将 l'_i 中的第 1、2、3、4 位依次与第 5、6、7、8 位相互交换; 如果 $p_i < p_{i+1}$, 则将 l'_i 中的第 1、3、5、7 位于第 2、4、6、8 位依次相互交换, 特别地, 当 $i = m \times n$ 时, 则比较 $p_{m \times n}$ 和 p_1 的大小. 以 $l'_1 = 10110110$ 为例, 交换过程如图 1 所示.

(3) 将经过比特置乱后所有 l'_i 转成十进制数, 得到中间密文序列 $C' = \{c'_1, c'_2, \dots, c'_{m \times n}\}$, 如此, 就保证了所有的像素实现了自我信息隐藏. 把混沌序列 P 中的序列值代入式(6)变成取值范围在 $[0, 255]$ 之间的序列 $Q = \{q_1, q_2, \dots, q_{m \times n}\}$.

$$q_i = \text{mod}(p_i \times 10^8, 256),$$

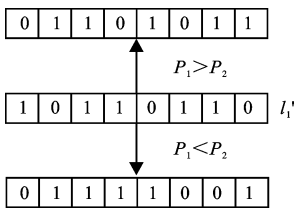


图 1 比特交换原理图

$$1 \leq i \leq m \times n \tag{6}$$

(4) 对每个中间密文 c_i' 进行式(7)操作,可令 c_0 为 $[0,255]$ 中的任意数,因此 c_0 也可作为一个密钥.这一步使得中间密文前后紧密相关,以达到像素扩散作用,得到最终密文 $C = \{c_1, c_2, \dots, c_{m \times n}\}$.

$$c_i = \text{mod}(q_i + c_i', 256) \oplus c_{i-1},$$
$$1 \leq i < m \times n \tag{7}$$

2.2.3 解密算法

解密过程是加密过程的逆过程.首先,将加密密文中的各值按式(8)进行计算可得 c_i' :

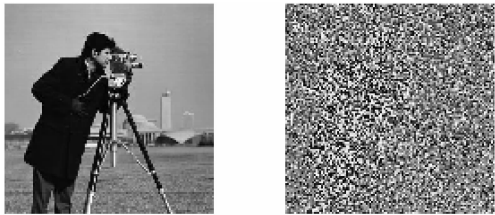
$$c_i' = \text{mod}(c_i \oplus c_{i-1} + 256 - q_i, 256) \tag{8}$$

然后,将 c_i' 转化为二进制数,利用 P 将其二进制数顺序调换原有顺序,且转化为为十进制可得置乱图像序列 L ;最后,最后将 L 进行反置乱即可得到明文序列 L .

3 实验仿真及分析

3.1 算法仿真

该实验仿真所使用的是大小为 256×256 的 Cameraman 灰度图像作为明文图像,其中加密系统的初始密钥包括 Hyperhenon 混沌系统中用到的 $x_1 = 0.526\ 647\ 484\ 9, y_1 = 0.645\ 276\ 523\ 2$ 和 Kent 混沌系统中的 $x_0 = 0.456\ 159\ 265\ 0$,在加密过程用到的参数可设置 $c_0 = 250$,而 Kent 混沌系统的控制参数 S 是由图像自身的特性所决定.通过实验得到的加密后图像如图 2(b)所示,可见加密效果良好.



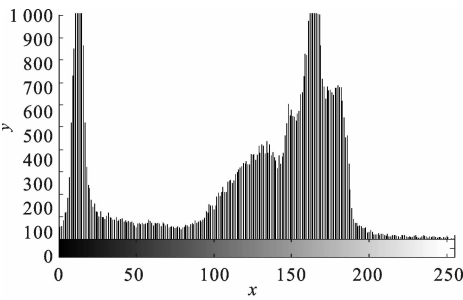
(a) 明文图像 (b) 加密图像

图 2 加密解密图

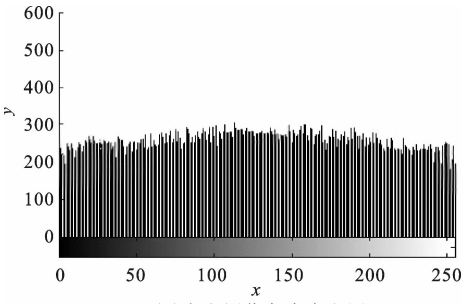
3.2 算法统计特性分析

本文主要从两个方面对该加密算法进行统计特

性分析,一方面是从加密前和加密后的灰度直方图来观察分析.如图 3 所示,加密前图像的灰度直方图呈不均匀分布,可看出图像像素值的分布特点.然而,加密后的密文图像灰度直方图分布很均匀,由此就很好地隐藏了明文图像信息.



(a) 明文图像灰度直方图



(b) 密文图像灰度直方图

图 3 灰度直方图

另一方面,再从加密前后图像的相邻像素相关性来进行分析.从明文图像中可任意选取相邻像素(水平、垂直以及对角的),可通过式(9)~(12)计算出图像像素之间的相关性:

$$\bar{x} = \frac{1}{N} \sum_{i=1}^N x_i \tag{9}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - \bar{x}) \tag{10}$$

$$\text{Conv}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - \bar{x})(y_i - \bar{y}) \tag{11}$$

$$\gamma_{xy} = \frac{\text{Conv}(x, y)}{\sqrt{D(x)} \sqrt{D(y)}} \tag{12}$$

式中, x 和 y 表示的是明文图像中两个相邻像素灰度值,而式中的 γ_{xy} 表示的是相邻像素的相关系数.实验仿真过程中,可从明文和密文图像中分别随机抽取垂直方向 400 组相邻点,并以此来描绘出这组像素值的关系图,图 4(a)表示的是明文图像垂直方向相邻点的像素值关系,图 4(b)则表示出了密文图像垂直方向相邻点的像素值关系.因此,加密前明文图像的相邻点之间是密切相关的,但是加密后密文图像的相邻点之间是没有任何关系的.

从明文图像的水平、垂直和对角线方向来选取

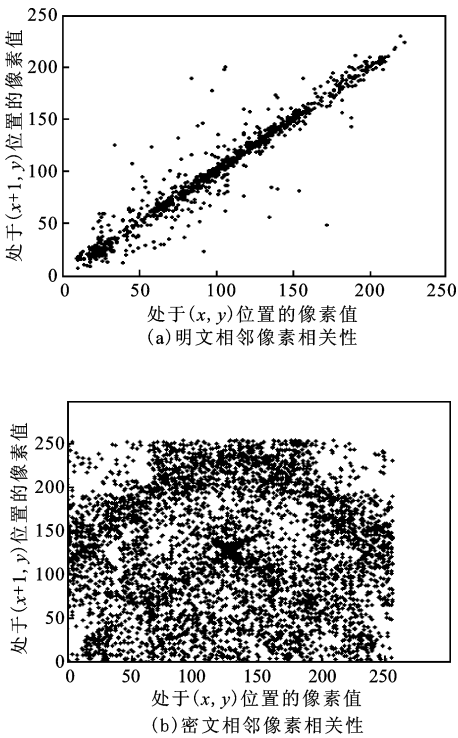


图 4 相邻像素相关性图

所有点,以此算出各自的相关系数,并与文献[8-10]所得的结果对比分析,如表 1 可见,明文图像的相关系数都非常接近 1,因此说明明文图像的相邻像素具有很高的相关度.然而,加密后的密文图像的相邻像素相关系数趋近于 0,从而说明密文图像的相邻元素基本上没有任何关系了,也就表明该算法已达到很好的加密效果.所以,密文图像已具有很好的抗统计分析攻击能力.

表 1 密文图像像素相关系数

方向	原始图像	加密图像	文献[8]	文献[9]	文献[10]
水平	0.965 04	0.001 45	0.032 22	-0.043 27	0.015 42
垂直	0.972 74	-0.002 13	-0.013 74	0.002 61	0.032 56
对角	0.984 38	0.007 53	-0.008 71	0.006 53	0.007 62

3.3 抗选择明文(密文)攻击分析

选择明文(密文)攻击指的是:首先,攻击者选择一组特定的明文(密文),使用此加密算法来得到对应的加密密文(明文);然后,根据该加密密文所呈现出来的特征逐步推算出中间密文,最后根据中间密文来得出明文图像,由此来破解加密算法.近年,学者们采用的方法通常是先选择一个与密文图像大小相同的而且像素值全部为 0 的特殊图像来得出中间密文,再选取一个唯一标示其中像素点位置的图像,以此来对该像素点进行追踪,

从而破解出该像素点在明文图像中所在的位置,最后成功破解出明文图像.这种破解方案已成功破解一些加密算法.

但是,这种破解方法用于本文所提出的加密算法却是行不通的.一方面,由于该加密算法在对明文图像进行全局置乱时,所采用的混沌系统迭代次数 K 以及参数 S 均与明文图像的像素值总和 sum 和平均值 avg 密切联系在了一起,因此当明文像素值全为 0 时,那么 $a=0$,直接会导致无法产生混沌序列,也就不可能成功获得中间密文;另一方面,即使攻击者使用的特殊明文为非全 0 的已知明文攻击,从本文加密算法的加密步骤中可得,它在进行像素比特置乱和扩散时融合进了一组混沌序列 P ,如果不能准确得到密钥 x_1 ,那么将很难破解该加密密文,这正是该算法的特殊性所在.综上所述,本文的图像加密算法能够很好抵抗选择明文(密文)攻击.

3.4 抗差分攻击性能分析

主要进行以下两个方面的分析:首先,对明文敏感性分析;其次,对密钥敏感性分析.

3.4.1 明文敏感性分析

明文敏感性是指:即使明文图像只是发生微小的变化也会引起密文图像的巨大改变.例如,将把明文图像中的某个像素点的像素值进行减 1 或者加 1,会导致最终完全不同的密文图像.密文对明文的敏感性越强,表明加密算法的抗差分攻击性能越好,因为攻击者就是对明文作出微小的改变来观察密文的变化,进而推导出加密过程来破解加密算法.基于对这点的考虑,本文的算法在加密过程中巧妙的融合了明文图像的像素值总和 sum 和像素平均值 avg 等这些图像自身的特性,使得明文特性与加密过程紧密相关,且在式(4)中对像素值总和进行了放大 100 倍,因此只要像素值哪怕只改变 1 就相当于改变了 100.所以,明文图像产生的微小变化将会导致整个加密过程发生巨大的变化.

在明文敏感性分析中,通常采用像素值变化率(NPCR)和归一化平均变化强度(UACI)来对密钥与明文雪崩效应进行分析和描述.用 Q_1 和 Q_2 来代表两幅加密图像, Q_1 代表明文图像的加密密文, Q_2 为微小改变明文图像中某个像素点的像素值后进行加密后的密文,设位于 (i, j) 位置的像素值依次为 $Q_1(i, j)$ 和 $Q_2(i, j)$.定义一个二维矩阵 P ,它与 Q_1 大小相同,当 $Q_1(i, j) = Q_2(i, j)$ 时,令 $P(i, j) = 0$,否则 $P(i, j) = 1$. Y_{NPCR} 和 Y_{UACI} 定义如下:

$$Y_{NPCR} = \frac{\sum_i \sum_j P(i,j)}{M \times N} \times 100\% \tag{13}$$

$$Y_{UACI} = \frac{1}{M \times N} \left[\sum_i \sum_j \frac{|Q_1(i,j) - Q_2(i,j)|}{256} \right] \times 100\% \tag{14}$$

从明文图像中任取 5 个像素点对其进行微小改变,分别进行五组实验,来观察其 NPCR 和 UACI 值的大小并与文献[8] 中的算法进行对比,可得结果如表 2 所示.

表 2 NPCR 和 UACI 值

组号	本文算法		文献[8]算法	
	NPCR	UACI	NPCR	UACI
1	0.996 724	0.337 121	0.745 541	0.253 423
2	0.999 845	0.329 541	0.884 724	0.265 361
3	0.997 987	0.332 435	0.842 628	0.197 387
4	0.999 243	0.340 223	0.696 753	0.318 564
5	0.998 924	0.331 467	0.856 457	0.248 761

所以,明文图像的微小变化将会使密文图像产生显著变化,可见本文加密算法能够有效地抵抗差分攻击.

3.4.2 密钥敏感性分析

密钥敏感性是指:即使密钥发生非常微小的变化也会导致图像发生巨大的变化.对明文图像进行解密时,即使解密密钥发生微小变化,也无法加密得到原来的明文图像.实验仿真中,正确解密得到的解密图像正确无误,即使是对某个密钥进行 10^{-10} 的改变也无法成功解密出明文图像,可见本文的算法具有较强的密钥敏感性.

3.5 密钥空间分析

在本文的图像加密算法中,初始密钥主要有 x_0 和 x_1, y_1 , 它们的取值范围均为 $(0, 1)$. 所以,如果每个初始密钥采用的数据类型都是双精度数据,那么每个初始密钥都可以保留 15 或 16 位有效数字,可得密钥空间至少为 10^{45} . 再加上算法中还有混沌序列迭代次数 t 和 Kent 混沌系统的控制参数 a , 以及对 Hyperhenon 混沌系统的迭代次数等,若是将这些参数都算作密钥,该加密系统将会得到更大的加密空间. 所以分析表明,该加密系统的密钥空间足够大,从而可以更好地保证其安全性,且可以很好地抵抗穷举攻击.

4 结束语

基于一些在安全性上存在不足的混沌图像加密算法,本文提出了一种全新的加密算法. 该算法

主要有两大特点:首先,在加密过程中使用明文图像的相关特性来生成所需混沌系统的控制参数,从而使密钥序列与明文图像紧密联系,当明文图像的发生微小改变时,密钥序列也随之发生巨大变化;其次,该算法加密过程对每个像素点进行了内部比特置乱之后再行像素扩散操作,使得密文得到很好的扩散作用,增强了加密算法的抗差分攻击能力. 通过实验仿真表明,该加密算法加解密速度快且简单易行,不仅具有密钥空间大,对初始密钥和明文图像非常敏感等特性,而且能有效抵抗各种攻击. 因此,该加密方案有较高的安全性且具有良好的应用前景.

参考文献:

[1] Guan Z H, Huan W J. Chaos based image encryption algorithm[J]. Physics Letters A, 2005, 364(1/3): 153-157.

[2] Wang X Y, Lei Y. A novel chaotic image encryption algorithm based on water wave drop diffusion models[J]. Optics Communications, 2012, 285(20): 4033-4042.

[3] 周蕊, 于晓明, 焦占亚. 一种基于混沌序列的数字图像加密算法[J]. 微电子学与计算机, 2010, 27(12): 62-64.

[4] 李玲, 王伟男, 李津杰, 等. 基于 Logistic 映射和超混沌自适应图像加密算法[J]. 微电子学与计算机, 2012, 29(1): 42-46.

[5] 郑继明, 高文正. 彩色图像的混沌加密算法[J]. 计算机工程与设计, 2011, 32(9): 2934-2937.

[6] Zhu Z L, Zhang W, Kwok-Wo W. A chaos-based symmetric image encryption scheme using a bit-level permutation[J]. Information Sciences, 2011, 181(6): 1171-1186.

[7] Zhu C X, Liao C L, Deng X H. Breaking and improving an image encryption scheme based on total shuffling scheme[J]. Nonlinear Dynamics, 2013, 71(1/2): 25-34.

[8] Teng L, Wang X Y. A bit-level image encryption algorithm based on water wave motion and water drop diffusion models[J]. Optics Communications, 2012, 285(20): 4048-4054.

[9] Liao X F, Lai S Y, Zhou Q. A novel image encryption algorithm based on self-adaptive wave transmission [J]. Signal Processing, 2010, 90(9): 2714-2722.

[10] Kanso A, Ghebleh M. A novel image encryption algorithm based on a 3D chaotic map[J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(4): 2943-2959.

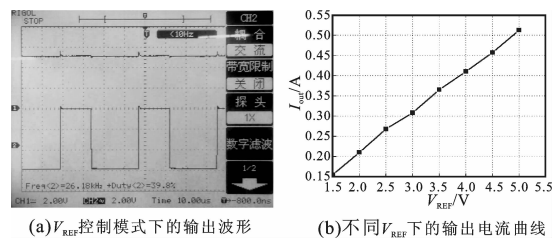


图 15 V_{REF} 控制模式下的输出波形与不同 V_{REF} 下的输出电流曲线

动管的导通电阻为两者饱和压降之和除以负载电流;如图 16 所示为不同电源电压下的驱动 MOS 管导通电阻的变化曲线,从图中可以看出,在电源电压分别为 5 V,4 V,3 V 时,驱动管的导通电阻分别约为 0.65 Ω ,0.8 Ω ,1 Ω . 随着负载电流升高,导通电阻值有所增大,主要原因是负载电流增大,引起芯片发热结温升高,导致导通电阻升高.

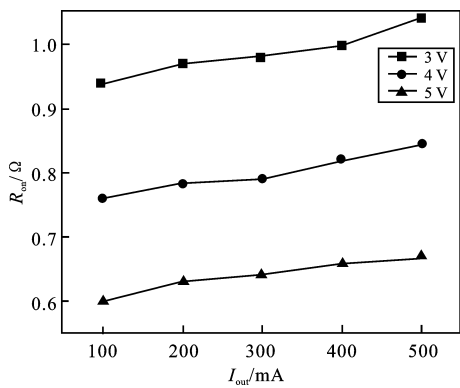


图 16 不同电源电压下的导通电阻变化曲线

5 结束语

本文基于 CSMC 0.5 μm HV CMOS 工艺,实现了一款具有优良动态性能和全面失效保护功能的全集成全桥直流马达驱动芯片. 芯片在 2.5 ~ 5.5 V 工作电压范围内,可以提供最高为 1 A 的驱动电

流;集成了过流、欠压和过温保护电路;提供了待机、正转、反转和制动四种基本驱动模式以及 PWM 调速和模拟电压调速两种调速模式;PWM 调速模式下输出电流与 V_{REF} 的呈线性关系;在电源电压分别为 5 V,4 V,3 V 时,驱动管的导通电阻分别约为 0.65 Ω ,0.8 Ω ,1 Ω . 本文设计的马达驱动芯片可以应用在机器人、仪器仪表和智能家居等领域.

参考文献:

[1] Matsumoto H, Neba Y, Asahara H. Variable-form carrier-based PWM for boost-voltage motor driver with a charge-pump circuit[J]. IEEE Transactions on Industrial Electronics, 2015, 62(8):4728-4738.

[2] Xu Y, Pan H B, He S Z, et al. Monolithic H-bridge brushless DC vibration motor driver with a highly sensitive hall sensor in 0.18 μm complementary metal-oxide semiconductor technology[J]. IET Circuits, Devices & Systems, 2012, 7(4): 204-210.

[3] Gupta V. Working and analysis of the H-bridge motor driver circuit designed for wheeled mobile robots [C]//2010 2nd International Conference on Advanced Computer Control (ICACC). China, Shenyang, 2010: 441-444.

[4] Tham K M, Nagaraj K. A low supply voltage high PSRR voltage reference in CMOS process[J]. IEEE Journal of Solid-State Circuits, 1995, 30(5):586-590.

[5] Ziegler S, Woodward R C, Iu H H C, et al. Current sensing techniques: a review[J]. IEEE Sensors Journal, 2009, 9(4): 354-376.

作者简介:

郭振宗 男,(1982-),硕士.研究方向为模拟集成电路设计.

何进 男,(1975-),副教授,博士生导师.研究方向为模拟、射频、毫米波集成电路设计与系统.

罗将(通讯作者) 男,(1990-),硕士.研究方向为射频、毫米波集成电路设计. E-mail:luojiang@whu.edu.cn.

(上接第 32 页)

作者简介:

谢国波 男,(1977-),博士,教授.研究方向为嵌入式系统.

E-mail:guoboxie@163.com

王添 男,(1990-),硕士研究生.研究方向为嵌入式系统、混沌保密通讯.