第 58 卷 第 3 期 2009 年 3 月
1000-3290/2009/58(03)/1662-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.58,No.3,March,2009

基于双相位编码的单通道彩色图像加密*

杨晓苹[1)†] 高丽娟[1)] 王晓雷[2)] 翟宏琛[2)] 王明伟[2)]

1)(天津理工大学电子信息与通信工程学院,天津 300191)

2)(南开大学现代光学研究所,教育部光电信息技术科学重点实验室,天津 300071)

(2008 年 5 月 27 日收到;2008 年 8 月 6 日收到修改稿)

提出一种基于双相位编码的单通道彩色图像加密方法. 在该方法中,将彩色图像转换到 *HSI* 空间,*I* 分量即可作为相位编码的原始待加密图像;而采用双随机相位加密技术对 *S* 分量加密后得到的相息图,与 *H* 分量一起构成了对 *I* 分量加密的双相位. 由于双随机相位加密技术有很高的安全性,在不知密钥的情况下解出 *S* 分量几乎是不可能的,由此保证了彩色图像加密的安全性. 模拟实验结果证明了该方法的有效性.

关键词:彩色图像,单通道,双相位编码

PACC:4225F,4230K

1. 引 言

在国际上不断发展的新一代信息安全理论与技术的研究中,基于光学理论与方法的数据加密、隐藏和提取技术成为了一个重要的组成部分[1,2]. 近年来,国内外很多学者都开始从事这方面的研究,并提出了很多新方法,新技术[3—15]. 在这些研究中,大多是采用单色光照明,因此所恢复的图像将会失去彩色信息.

色彩是自然界的基本属性之一,图像的色彩信息在许多场合都是非常有用的,彩色图像信息的加密处理正受到越来越多的重视. 在这类研究中,彩色图像通常被分成 3 个或多个通道[12—15],再采用和灰度图像相同的处理方法,解密时将各个通道组合起来,以恢复原来的彩色图像,这类方法常被称为多通道彩色图像处理. 由于使用了多个通道,则相应的光学实现系统也就需要多个光源和多套光学元件,在增加了实验难度的同时,也增加了系统的成本,使此类方法的实用性受到限制.

本文提出一种基于双相位编码的单通道彩色图像加密方法. 在该方法中,图像首先被从 *RGB* 空间转换到 *HSI*(色调、饱和度、强度)空间,再将其合并到一个通道中,采用双相位编码技术加密. 其中,*I*(强度)分量可作为双相位编码时的原始待加密图像,而编码时所用的密钥,可由 *H*(色调)分量和 *S*(饱和度)分量获得. 因为在 *HSI* 空间中,色调与一个角度相对应,可以将其作为一个相位角来处理,该相位即可作为双相位编码中的相位密钥之一;而采用双随机相位加密技术[7]对 *S* 分量加密后得到的相息图,可作为双相位编码的另一个密钥. 由于仅使用一个通道对彩色图像加密,其相应的光学实现系统仅需一个光源和一套光学元件,不仅使实验难度降低,也减少了系统的成本. 又因为采用双随机相位加密技术得到的 *S* 分量的相息图,在加密的过程中引进了随机相位因子,在不知密钥的情况下解密出 *S* 分量几乎不可能,从而保证了本方法的安全性. 模拟实验结果证明了本文所提出方法的有效性.

2. 色彩空间的转换

本文中,图像的彩色信息被转换成振幅和位相信息,以实现单通道加密. 而彩色图像通常用红、绿、蓝三元组的二维矩阵来表示. 为此,首先需将彩色图像用 *HSI* 表示.

在 *RGB* 和 *HSI* 之间的变换公式有多种形式,所有变换方法的基本思想都是一致的. 一般而言,对

* 国家自然科学基金(批准号:60577017,60777007),光电信息技术科学教育部重点实验室开放项目(批准号:2005-14)资助的课题.

† 通讯联系人. E-mail:yangxiaoping@tsinghua.org.cn

一种从 *RGB* 空间转换到 *HSI* 空间的方法，只要它能保证转换后的色调 H 是一个角度，饱和度 S 和强度 I 相互独立，并且此转换是可逆的即可. 本文选择的转换公式如下.

2.1. *RGB* 到 *HSI* 的彩色模型转换

给定一幅 *RGB* 彩色格式的图像，每一个 $[0,1]$ 范围内的 *RGB* 像素值和 H 分量可用下面的公式得到[16]：

$$H = \begin{cases} \theta, & B \leqslant G, \\ 360 - \theta, & B > G, \end{cases} \tag{1}$$

其中

$$\theta = \arccos\left\{ \frac{\frac{1}{2}[(R-G)+(R-B)]}{[(R-G)^2+(R-G)(G-B)]^{1/2}} \right\}. \tag{2}$$

色饱和度分量由下式给出：

$$S = 1 - \frac{3}{(R+G+B)}[\min(R,G,B)]. \tag{3}$$

强度分量为

$$I = \frac{1}{3}(R+G+B). \tag{4}$$

2.2. *HSI* 到 *RGB* 的彩色模型转换

设 H,S,I 归一化在 $[0,1]$ 范围内，与之对应的 R,G,B 的值也在 $[0,1]$ 之间，则由 *HSI* 转换为 *RGB* 的公式与颜色点落在色环的哪个扇区有关. 将 H 乘以 360°，则色调值返回到 $[0,360°]$ 的范围.

当 H 在 $[0,120°]$ 之间时，

$$\begin{aligned} R &= I\left[1 + \frac{S\times\cos(H)}{\cos(60°-H)}\right], \\ B &= I(1-S), \\ G &= 3I - R - B. \end{aligned} \tag{5}$$

当 H 在 $[120°,240°]$ 之间时，

$$\begin{aligned} G &= I\left[1 + \frac{S\times\cos(H-120°)}{\cos(180°-H)}\right] \\ R &= I(1-S), \\ B &= 3I - R - G. \end{aligned} \tag{6}$$

当 H 在 $[240°,360°]$ 之间时，

$$\begin{aligned} B &= I\left[1 + \frac{S\times\cos(H-240°)}{\cos(300°-H)}\right], \\ G &= I(1-S), \\ R &= 3I - G - B. \end{aligned} \tag{7}$$

3. 彩色图像的单通道加密

3.1. 密钥——S 分量的加密

设转换后得到的彩色图像的 S 分量的复振幅用 $s(x,y)$ 表示，以它作为一个图像，采用基于相息图迭代的双随机相位法[7]，将其加密为一个仅位相分布的相息图，此相息图即可作为原彩色图像相位编码时的密钥. 将 $s(x,y)$ 加密为 $g(x,y)$ 的过程可表示为

$$g(x,y) = \mathrm{FT}^{-1}\{\mathrm{FT}\{s(x,y)\exp[\mathrm{i}2\pi p(x,y)]\} \times \exp[\mathrm{i}2\pi b(u,v)]\} \tag{8}$$

其中，FT 为傅里叶变换，FT^{-1} 为傅里叶逆变换，(x,y) 表示二维空间坐标，(u,v) 为二维频域坐标，$p(x,y)$ 和 $b(u,v)$ 分别代表两个在 $[0,1]$ 之间均匀分布的二维随机阵列. $g(x,y)$ 即为 S 分量的相息图，$g(x,y)$ 的相位分布及 $b(u,v)$ 的相位分布可通过迭代算法求出[7]. $b(u,v)$ 一经确定，即可用 $B(u,v)=\exp[\mathrm{i}2\pi b(u,v)]$ 作为从相息图 $g(x,y)$ 本身来恢复 $s(x,y)$ 的密钥. 由于 $p(x,y)$ 是随机噪声，因而 $b(u,v)$ 也是随机的，只不过这一随机相位的分布会与 $p(x,y)$ 和原图像 $s(x,y)$ 紧密相关. 所以，用 $B(u,v)$ 作为密钥，有很高的安全性.

对 $g(x,y)$ 解密，则可得到解密后的 S 分量 $S'(x,y)$，该运算即为加密过程的逆运算

$$S'(x,y) = \mathrm{FT}^{-1}\{\mathrm{FT}\{g(x,y)\}\exp[-\mathrm{i}2\pi b(u,v)]\} \times \exp[-\mathrm{i}2\pi p(x,y)]. \tag{9}$$

3.2. 基于双相位的单通道彩色图像加密

设彩色图像在 *HSI* 空间中的 I 分量用 $I(x,y)$ 表示，其复振幅可用 $\sqrt{I(x,y)}$ 表示，归一化的 H 分量用 $H(x,y)$ 表示. 采用双相位编码技术对其加密

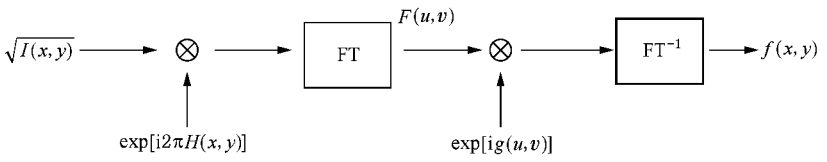

图 1　双相位加密算法框图

的算法框图如图 1 所示. 其中,$g(u,v)$即为 S 分量的相息图. 该算法可用下式表示:

$$f(x,y) = \mathrm{FT}^{-1}\{\mathrm{FT}\{\sqrt{I(x,y)}\exp[\mathrm{i}2\pi H(x,y)]\} \times \exp[\mathrm{i}g(u,v)]\}. \quad (10)$$

以上算法可由图 2 所示的光学系统实现. 从图中可见,将待加密的彩色图像的 I 分量的振幅和一个相位板紧靠在一起,该相位板的相位分布即为 $\exp[\mathrm{i}2\pi H(x,y)]$(可采用 SLM 来得到),将它们置于光学系统的输入平面,用平行相干光照明,则在傅里叶谱平面,得到 $\sqrt{I(x,y)}\exp[\mathrm{i}2\pi H(x,y)]$ 的傅氏谱,将其和对 S 分量加密得到的相位因子 $\exp[\mathrm{i}g(u,v)]$相乘,再经逆傅氏变换,即可在输出平面上得到加密后的图像 $f(x,y)$.

由 $f(x,y)$得到 $I(x,y)$的解密图像 $I'(x,y)$的运算是加密系统的逆运算,可表示为

$$\sqrt{I'(x,y)} = \mathrm{FT}^{-1}\{\mathrm{FT}\{f(x,y)\}\exp[-\mathrm{i}g(u,v)]\} \times \exp[\mathrm{i}2\pi H(x,y)]. \quad (11)$$

利用(5)—(7)式,将 $I'(x,y)$,$H(x,y)$和由 $g(u,v)$解密得到的 S 分量 $S'(x,y)$转换成 RGB 分量,并将其合成,即可得到原彩色图像.

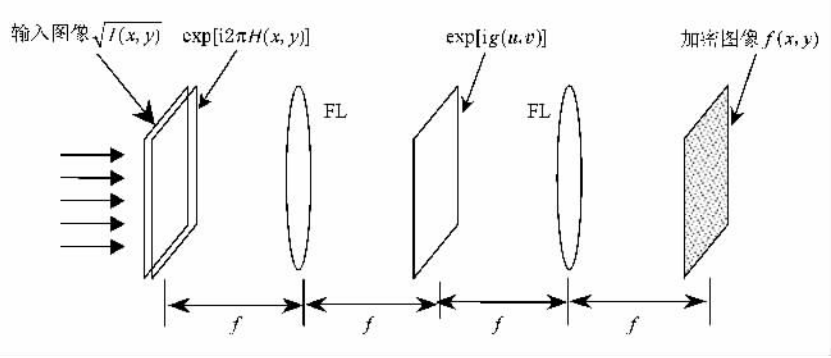

图 2 双相位加密系统示意图

图 3 待加密图像的色彩空间转换 (a) 原始待加密彩色 RGB 图像;(b) 与(a)对应的 H 空间图像;(c) 与(a)对应的 S 空间图像;(d) 与(a)对应的 I 空间图像

4. 模拟实验结果

我们对以上算法进行了计算机模拟实验. 图 3 为待加密图像的色彩空间转换实验，其中图 3(a)为一幅待加密的 128 × 128 像素的 *RGB* 空间彩色图像，图 3(b)，(c)，(d)分别为由转换公式(1)—(4)得到的该图像的 *HSI* 空间图像.

图 4 为对图 3(c)的 *S* 分量加密的结果. 其中图 4(a)为加密后得到的相息图，图 4(b)为解密后的 *S* 分量图像.

图 5 为采用双相位加密技术对图 3 的彩色图像加密得到的结果. 其中，图 5(a)为由图 3(b)，(d)的 *I* 分量和 *H* 分量得到的图像 $\sqrt{I(x,y)}\exp[i2\pi H(x,y)]$(显示时取实部)，图 5(b)为对 $\sqrt{I(x,y)}\exp[i2\pi H(x,y)]$ 加密得到的图像 $f(x,y)$，使用的密钥即为图 4(a)所示的相息图，图 5(c)为对 $f(x,y)$ 解密后得到的图像 $I'(x,y)$，图 5(d)为解密后得到的 *RGB* 图像. 由图可见，解密后合成的 *RGB* 图像，与原始待加密的 *RGB* 图像在视觉上几乎没有什么区别.

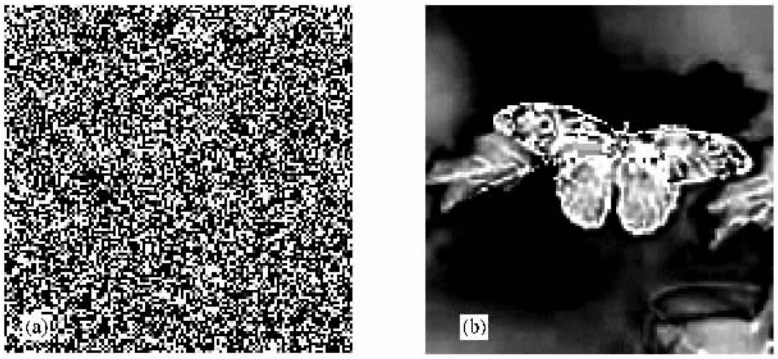

图 4　*S* 分量加密的结果　(a) 与图 3(c)对应的 *S* 分量的相息图；(b) 对相息图解密后得到的 *S* 分量图像

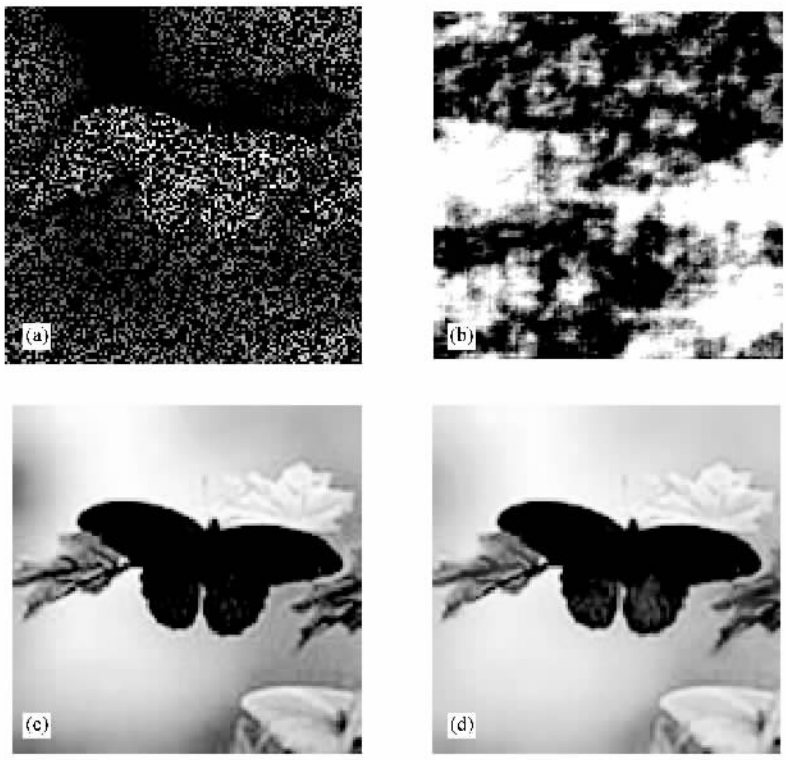

图 5　彩色图像的单通道加密实验　(a) $\sqrt{I(x,y)}\exp[i2\pi H(x,y)]$ 振幅的实部；(b) 对(a)加密得到的结果；(c) 对(b)解密得到的结果 $I'(x,y)$；(d) 解密后合成的 *RGB* 图像

5. 结 论

本文提出一种基于相位编码的单通道彩色图像加密方法. 在该方法中,将彩色图像转换到 *HSI* 空间,并将其合并到一个通道,实现了对彩色图像的单通道加密. 其中,*I* 分量即可作为相位编码的原始待加密图像. 而采用双随机相位加密技术对 *S* 分量加密后得到的相息图,与 *H* 分量一起构成了对 *I* 分量加密的双相位. 因为双随机相位加密技术有很高的安全性,在不知密钥的情况下解出 *S* 分量几乎不可能,由此也保证了本文提出的彩色图像加密的安全性. 由于仅使用一个通道对彩色图像加密,其相应的光学实现系统也就只需要一个光源和一套光学元件,不仅使实验难度降低,也减少了系统的成本. 模拟实验结果表明了该方法的有效性.

为进一步增加该加密系统的安全性,还可以先行对 *H* 分量也使用双随机相位加密技术,将其加密为相息图,并在系统的输入面上,以此相息图来替代 *H* 分量作为双相位编码的密钥之一. 同样,在不知密钥的情况下,几乎无法解出 *H* 分量,从而使整个系统的密钥个数增加,安全性能加强.

[1] Rosen J, Javidi B 2001 *Appl. Opt.* **40** 3346

[2] Yamamoto H, Hayasaki Y, Nishida N 2003 *Opt. Lett.* **28** 1564

[3] Unnikrishnan G, Singh K 2001 *Opt. Commun.* **193** 51

[4] Liu S T, Yu L, Zhu B H 2001 *Opt. Commun.* **187** 57

[5] Yang X P, Zhai H C 2005 *Acta. Phys. Sin.* **54** 1578 (in Chinese) [杨晓苹、翟宏琛 2005 物理学报 **54** 1578]

[6] Yang X P, Zhai H C, Liu F M 2003 *Journal of Optoelectronics·Laser.* **14** 1187 (in Chinese) [杨晓苹、翟宏琛、刘福民 2003 光电子激光 **14** 1187]

[7] Liu F M, Zhai H C, Yang X P 2003 *Acta. Phys. Sin.* **52** 2462 (in Chinese) [刘福民、翟宏琛、杨晓苹 2003 物理学报 **52** 2462]

[8] Apolinar J M R, Ramon R V 2004 *Opt. Commun.* **236** 295

[9] Kishk S, Javidi B 2003 *Opt. Lett.* **28** 167

[10] Yang X P, Zhai H C, Wang M W 2008 *Journal of Optoelectronics·Laser.* **19** 111 (in Chinese) [杨晓苹、翟宏琛、王明伟 2008 光电子·激光 **19** 111]

[11] Yang X P, Zhai H C, Wang M W 2008 *Acta. Phys. Sin.* **57** 847 (in Chinese) [杨晓苹、翟宏琛、王明伟 2008 物理学报 **57** 847]

[12] Chen L F, Zhao D M 2007 *Opt. Exp.* **15** 16080

[13] Jin W M, Ma L H, Yan C J 2006 *Opt. Commun.* **259** 513

[14] Chen L F, Zhao D M 2006 *Opt. Exp.* **14** 8552

[15] Yamaguchi I, Matsumura T, Kato J 2002 *Opt. Lett.* **27** 1108

[16] Gonzalez R C, Woods R E 2007 *Digital Image Processing*, Second Edition (Beijing: Publishing House of Electronics Industry) (in Chinese) p235 [R C 冈萨雷斯、R E 伍德著,阮秋琦、阮宇智译 2007 数字图像处理(第二版)(北京:电子工业出版社) 第 235 页]

Single-channel encryption of color image based on double-phase encoding*

Yang Xiao-Ping[1)†] Gao Li-Juan[1)] Wang Xiao-Lai[2)] Zhai Hong-Chen[2)] Wang Ming-Wei[2)]

1)(*School of Electronics Information and Communications Engineering, Tianjin University of Technology, Tianjin* 300191, *China*)

2)(*Institute of Modern Optics, Nankai University, Key Laboratory of Opto-electronic Information Science & Technology, MEC, Tianjin* 300071, *China*)

(Received 27 May 2008; revised manuscript received 6 August 2008)

Abstract

In this paper, a new method of encrypting a color image in one channel based on double-phase encoding is presented. In this method, the colors of a color image are converted from *RGB* to *HSI*, so the *I* component can be used as the original image which could be encoded with double-phase. The kinoform of *S* is obtained by using double-random phase encryption and the *H* component can be used as the two phases. It is difficult to recover the *S* component if the phase keys are not available, because double-random phase encoding is robust to blind retrieval trials, so the security of the method proposed is guaranteed. Computer simulations are presented to illustrate the efficiency of this method.

Keywords: color image, single-channel, double-phase encoding

PACC: 4225F, 4230K

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60577017, 60777007) and the Opening Subject Key Laboratory of Opto-electronic Information Science & Technology, MEC (Grant No. 2005-14).

† E-mail: yangxiaoping@tsinghua.org.cn