

基于 RGB 图像传输的双随机相位加密隐藏技术

孙敏, 苏显渝

(四川大学 光电科学技术系, 成都 610004)

摘 要:提出了一种通过彩色宿主图像隐藏双随机相位编码信息的方法. 将需隐藏的原始信息, 经双随机相位编码, 压缩后按一定的编码规则隐藏在宿主图像(RGB 图像)的低位. 在提取隐藏图像过程中直接对携带隐藏信息的融合图像进行处理, 不需要利用原始 RGB 宿主图像, 且重构图像的质量较好, 不受原始宿主图像的影响. 在此基础上对因原始隐藏信息在编码、存储、传输过程中对融合图像和重构图像的影响做了分析, 并在 MATLAB 环境中对分析结果做了模拟验证. 结果表明, 该方法可以得到非常好的重构图像.

关键词:图像隐藏; 双随机相位编码; BMP 图像; 图像质量

中图分类号: TN911.7

文献标识码: A

文章编号: 1004-4213(2008)02-0320-5

0 引言

近年来利用傅里叶光学信息处理对图像进行加密发展较为迅速. 其中 B. Javidi 于 1994 年提出的双随机相位编码方法由于具有极高的保密性, 且完全可以用光学方法实现, 因而受到人们越来越多的关注^[1-9]. 双随机相位编码方法就是在空域和频域对隐藏图像进行随机相位调制, 使之成为振幅和相位随机分布的复数波. 这种经编码后的波场光强分布为看似杂乱无章的随机灰度图, 从其灰度分布很难得到与隐藏信息内容有关的任何规律. 在实际应用中往往采用灰度迭加方法按适当的权重把编码后的信息隐藏在宿主图像中, 使生成的融合图像与原始宿主图像无人眼能观察到的明显差异^[2].

目前在提取隐藏图像时主要采用两种方式: 一种是从融合图像中去除原始宿主图像, 然后再进行解码运算. 但这样宿主图像必须伴随融合图像一起传递, 在图像数量较大时(例如视频信号)显得极不方便, 并且假如这两幅看似完全相同的图像被同时截获, 容易引起注意, 从而丧失了图像隐藏的意义; 另一种方式是直接对融合图像进行解码运算. 但这样宿主图像将会以噪音的形式迭加在重构图像上, 严重影响重构图像的质量. 现实生活中, 传输的图像大多为彩色图像. 因此, 把要隐藏的信息隐藏于彩色图像中, 更具有实用性.

本文提出一种通过彩色宿主图像隐藏双随机相位编码信息的方法, 将编码信息的实部和虚部同时迭加在一幅任意选取且足够大的彩色图像中, 在提取隐藏图像时直接对融合图像进行处理, 不需要利用原始宿主图像, 重构图像也不受宿主图像的影响,

并在此基础上对影响融合图像和重构图像的各种因素进行了分析讨论.

1 双随机相位编码、解码方法

假设 $f(x, y)$ 为隐藏图像, 像素数目大小为 $M \times N$. (x, y) 和 (v, w) 分别为空间域和频率域的坐标函数, $\Psi(x, y)$ 表示双随机相位编码后的图像. $p(x, y)$ 和 $b(v, w)$ 为在 $[0, 1]$ 之间分布的两个独立的随机序列. 则编码图像可以表示为

$$\Psi(x, y) = \text{FT}^{-1} \{ \text{FT} \{ f(x, y) \exp \cdot [j2\pi p(x, y)] \} \exp [j2\pi b(v, w)] \} \quad (1)$$

式中 FT, FT^{-1} 分别表示傅里叶变换及逆变换.

解密过程可表示为

$$f(x, y) = \text{FT}^{-1} \{ \text{FT} [\Psi(x, y)] \exp \cdot [-j2\pi b(v, w)] \} \exp [-j2\pi p(x, y)] \quad (2)$$

显然, 若不知 $p(x, y)$ 和 $b(v, w)$, 则基本上不可能由 $\Psi(x, y)$ 得到 $f(x, y)$, 因此 $p(x, y)$ 和 $b(v, w)$ 被称作双随机位相编码过程的密钥.

2 图像隐藏原理及改进方法

已编码信息 $\Psi(x, y)$ 通常为复振幅函数 ($\Psi = \Psi_R + j\Psi_I$), 可以将 $\Psi(x, y)$ 的实部和虚部分别隐藏在两幅宿主图像中, 即

$$T'_1(x, y) = T_1(x, y) + \alpha\Psi_R(x, y) \text{ 和}$$

$$T'_2(x, y) = T_2(x, y) + \alpha\Psi_I(x, y). \text{ 式中,}$$

$T_1(x, y)$ 、 $T_2(x, y)$ 为原始宿主图像, α 为迭加重. 若用算符“ \mathcal{R} ”表示式(2)中的解码运算, 如前所述, 通常从融合图像中重新提取隐藏图像的方法有两种

$$f' = \mathcal{R} [(T'_1 - T_2) + j(T'_2 - T_2)] = \alpha \mathcal{R} \Psi = \alpha f \quad (3)$$

$$f' = \text{Re} [\mathcal{R}(T'_1 + jT'_2)] = \alpha f + \text{Re} [\mathcal{R}(T_1 + jT_2)] \quad (4)$$

由于隐藏图像 f 一般为实图像,因此式(4)中仅取解码运算的实部,结果可见重构图像 f' 上迭加了噪音项,并且噪音的分布特性与宿主图像有关.研究表明,宿主图像的平均灰度值越大则重构图像的信噪比越低^[7].运用式(3)提取隐藏图像的效果较好,但必须传递原始宿主图像,即使融合图像和宿主图像经不同的渠道传递,若解码时所用的宿主图像与用来生成融合图像时的宿主图像相比在灰度值上有轻微变化(这在实际情况中是难免的),将会引入新的噪音.假设隐藏编码信息实部和虚部的两幅宿主图像分别微变 $\Delta\Psi_R$ 和 $\Delta\Psi_I$,按式(3)做解码运算且仅取实部则有

$$f' = \text{Re} \{ \mathcal{R}[T'_1 - T_1] + j[T'_2 - T_2] \} = \alpha f + \text{Re} [\mathcal{R}(\Delta\Psi_R + \Delta\Psi_I)] \quad (5)$$

可见重构图像上仍将迭加噪音,此时噪音与宿主图像的微变有关^[7].

以上的隐藏方法,都要调整迭加权重.权重小时,重构图像质量较差,权重大时,宿主图像将严重变形.为了解决这个问题,通过对 RGB 图像进行分析,把相位编码信息隐藏在 RGB 图像中,不需要调整权重,只需要再做一次简单的编码即可.为了追求被隐藏的敏感信息的最大容量,选择 24 位 BMP 真彩色图像作为载体.根据计算机视觉理论,人眼感受颜色是通过 3 种可见光对视网膜的锥状细胞的刺激来实行的,这些光在波长为 630 nm(红色)、530 nm

(绿色)、450 nm(蓝色)时的刺激达到高峰.在这种以红(R)、绿(G)、蓝(B)为基色的颜色模型中,亮度信号 Y 和 3 种基色的关系为: $Y = 0.30R + 0.59G + 0.11B$. 可见人眼视网膜锥状细胞对绿色最敏感,对蓝色最不敏感.在 24 位真彩色的 BMP 位图中,每个象素的 RGB 颜色值由 3 个字节表示,其中每个字节表示一种基色的值(0~255).当改变绿色分量字节最低位的值时,人眼感受不到这种细微的变化.而由亮度公式可知,红色分量字节改变最低 2 位、蓝色分量字节改变最低 3 位,人眼的视锥细胞仍不能明显觉察到图像的变化.于是在 24 位真彩色的 BMP 位图中,每个像素的 3 个字节中最多可以利用 6 个比特来存储敏感信息并不影响图像的视觉效果^[10].选择图像红色分量二进制编码的最低两位,绿色分量中的最低一位,蓝色分量中的最低三位来实现双随机相位信息的隐藏.例如一个值为 168 的像素点,首先乘一个压缩系数 1/4(根据具体情况选择压缩系数)得到 42,用六位二进制编码表示为 101 010,再经过编码处理分成 101、0、10 三位分别迭加到去除冗余值的 BMP 宿主图像中,即可实现隐藏.信息加密、编码和解密过程流程图如图 1.图中 1(a)是加密过程流程图,待隐藏的原始信息,经双随机相位编码、压缩后按一定的编码方法隐藏在宿主图像的低位.详细的编码隐藏方法如图 1(b).图 1(c)是解密过程框图.

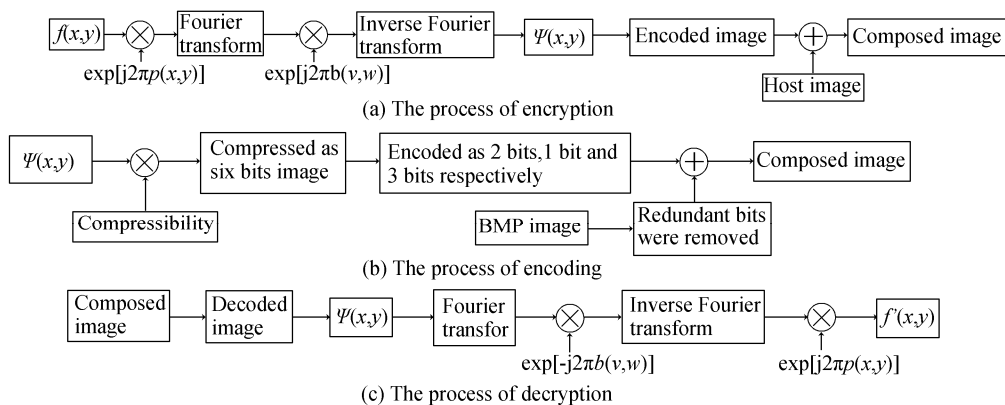


图 1 加密、编码、解密过程

Fig. 1 The process of encryption, encoding and decryption

3 影响成像质量的因素分析

由于宿主图像在编码、存储和传输过程中会受到一系列的影响或者攻击,故讨论由 BMP 位图隐藏双随机相位编码信息可能产生的失真问题,具有重要的实际意义.

1) 无论是光学方法或数值方法进行双随机相位编码,得到的已编码信息为一复数矩阵.不论是该矩阵的实部还是虚部,都含有值为小数或者负数的元

素.而隐藏在 BMP 位图中时,编码信息灰度值范围在 0~63 的整数值之间,要求所有像素点的值都为非负数.在存储时,负数部分的元素会被截断为 0,小数部分被截断为整数.因此,存储信息的像素值实际上是最接近于编码信息值的非负整数.这样实际记录的已编码图像信息与“真实值”之间就会有一定的偏差.为了解决这个问题,通常在双随机编码信息真实值上叠加一个偏移量,保证要存储的编码信息矩阵元素都为正数,然后再做压缩,使编码信息灰度

值范围在 0~63 之间,从而减小因数据截断引起的信息误差.

2)由于一般选用图像的灰度级在 0~255 之间,而 BMP 图像通常只选用六位作隐藏位,所以隐藏的灰度级在 0~63 之间.这就要求对原始灰度图像做一定的压缩处理,也就是使灰度值范围变小.例如一个值为 201 的像素点,首先乘上一个压缩系数 1/4 (根据具体情况选择)得到 50.25,截断小数部分得到 50.在解密时,为了达到原始图像的灰度级,又要扩大已编码图像,若乘以 4 得到 200,从而在数值上产生偏差.

3)在传输过程中,融合图像表面的像素可能会丢失,主要包括图像缺损、图像表面的划痕和图像褪色等.这样从宿主图像提取出的双随机相位编码图像也会在相应位置上产生图像缺损.在解密时,可用到的信息就会减少,势必对解密图像会产生影响.定义信噪比 SNR 来分析重构图像质量

$$\text{SNR} = \lg \left\{ \frac{2^{2n} - 1}{\left[\frac{1}{M \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (P_{i,j} - Q_{i,j})^2 \right]^{1/2}} \right\}$$

式中 $P_{i,j}$, $Q_{i,j}$ 分别表示两幅 $M \times N$ 的原始隐藏图像和重构图像,下标 i, j 分别表示两幅图像的行和列. SNR 表示重构图像的信噪比.

4)在实际应用中,如果传输所用带宽有限,在对成像质量要求不是很高的情况下,可以选取隐藏图像的实部或者虚部进行传输,解密时,由于缺少了相位信息,将对重构图像产生影响.

4 数值模拟结果与分析

为了简单起见,分别选择一幅 256×128 像素的 BMP 彩色图像作为宿主图像和 128×128 像素的 BMP 灰度图像作为隐藏信息.灰度级均为 0~255.

现模拟同时隐藏了信息的实部和虚部的结果.图 2(a)为要隐藏的原始信息,图 2(b)为图 2(a)经过双随机相位加密后的随机相位编码图像.在视觉上呈现杂乱无章的灰度分布.为了传输该图像,选择图

3(a)为原始宿主图像,是一幅 256×128 像素的 24 位 BMP 位图.图 3(b)为加入隐藏信息图 2(b)的融合图像.两幅图片在视觉上无任何差别,达到了很好的隐藏效果.图 4(a)为图 3(b)得到的重构灰度图像,和原始隐藏信息相比几乎没有视觉上的差异.如果采用灰度迭加方法按适当的权重把编码后的信息隐藏在宿主图像中^[2],则重构图像的质量较差.图 4(b)为迭加权重为 1 时的重构灰度图像,图 4(c)为迭加权重为 0.1 时得到的重构图像.由此可见,采用本文提出的将需隐藏的原始信息,经双随机相位编码,压缩后按一定的编码规则隐藏在宿主图像低位的方法,不但在视觉上达到了很好的隐藏效果,而且重构图像质量较好,不受宿主图像影响.

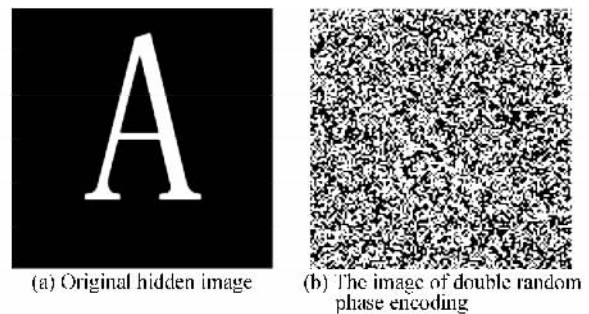


图 2 原始隐藏图像和双随机相位编码后图像

Fig. 2 Original hidden image and the image of double random phase encoding

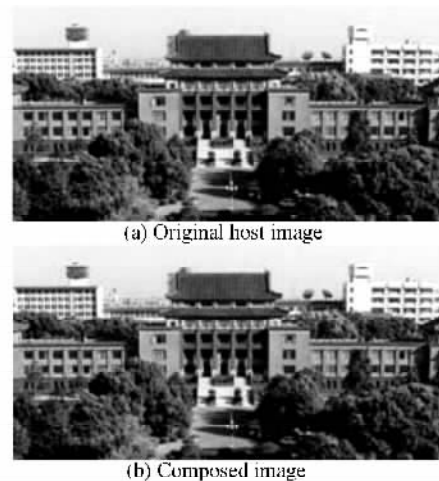


图 3 原始宿主图像和加密融合图像

Fig. 3 Original host image and composed image



图 4 采用 BMP 隐藏双随机相位编码所得重构图像与普通迭加隐藏方法所得重构图像的比较

Fig. 4 The comparison of recovered image from BMP composed image and

the recovered image from plusses for different 1 and 0.1

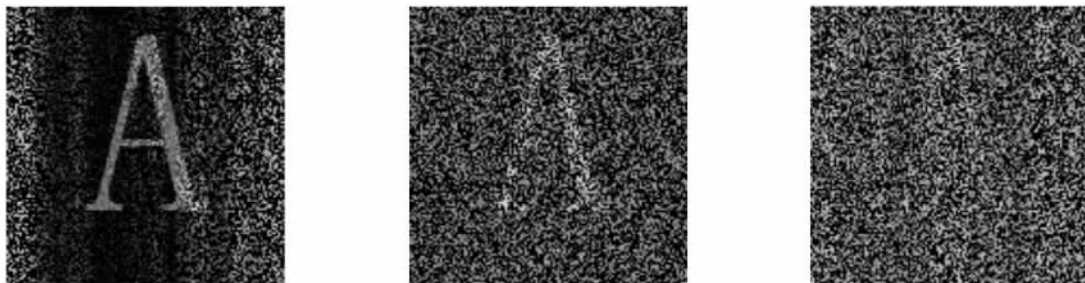
在传输过程中,如果融合图像受到不同程度的影响,将会得到不同效果的重构图像.图5中的(a)~(c)分别为融合图像在传输过程中,图像的1/4、1/2、3/4被遮挡住的融合图像.图6(a)~(c)分别为应用图5(a)~(c)融合图像进行解密所得到的重构图像.



(a)1/4 of the composed image pixels are occluded (b) 1/2 of the composed image pixels are occluded (c) 3/4 of the composed image pixels are occluded

图5 融合图像部分像素值丢失

Fig.5 Part of the composed image pixels are occluded



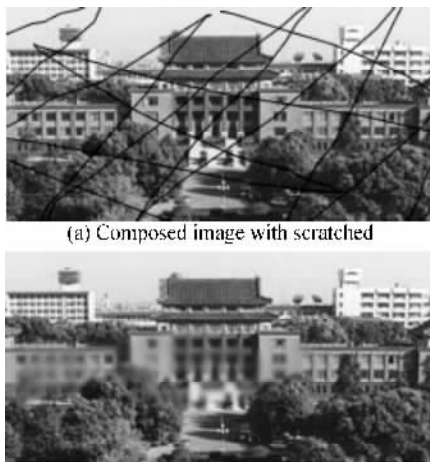
(a) 1/4

(b) 1/2

(c) 3/4

图6 部分融合图像像素丢失时所得重构图像

Fig.6 Recovered image with part of the composed image occlusion



(a) Composed image with scratched

(b) Composed image with fading distortion

图7 划痕和褪色的融合图像

Fig.7 Scratched and fading distortion images



(a) From scratched image

(b) From fading distortion image

图8 从划痕和褪色图像中所获得重构图像

Fig.8 Recovered image from scratched image and fading distortion image

图7中(a)、(b)分别为有划痕和褪色后的融合图像.图8(a)、(b)为对应图7(a)、(b)图像所得到的重构图像.图(9)为融合图像缺损与信噪比 SNR 的关系.实验结果表明,传输过程中图像的局部缺省与退化对解密所得到的重构图像的影响是有限的.

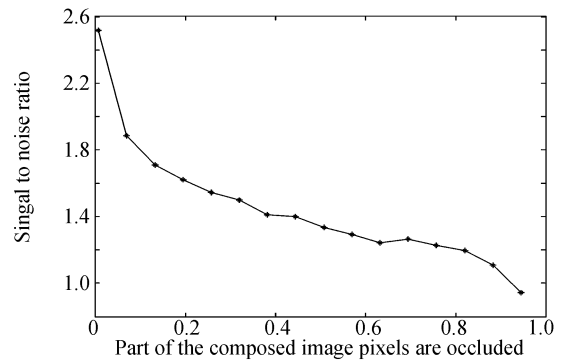


图9 融合图像丢失百分比与 SNR 的关系

Fig.9 The SNR for the recovered image when part of the composed image is are occluded

5 结论

利用 RGB 图像隐藏双随机相位编码信息,不但更符合实际传输的需要,而且隐藏本身就是对图像多加了一重保密措施.本文对由 RGB 图像隐藏的信息的可行性进行了分析,提出了一种通过彩色宿主图像隐藏双随机相位编码信息的方法,将需隐藏的原始信息,经双随机相位编码,压缩后按一定的编码规则隐藏在宿主图像(BMP 图像)的低位.密钥包括双随机相位模板、压缩和编码规则.在信息接收端,根据密钥进行逆变换,可恢复被隐藏的原始信息.对影响成像质量的因素进行了分析,并给出了相应的模拟实验.结果表明所采用的方法隐蔽性强,重建图

像质量较好,传输过程中图像的局部缺省与退化对解密所得到的重构图像的影响是有限的.

参考文献

- [1] REFREGIER P, JAVIDI B. Optical image encryption based on input plane and fourier plane random encoding[J]. *Opt Lett*, 1995, **20**(7):767-769.
- [2] KISHK S, JAVIDI B. Information hiding technique with double phase encoding[J]. *Appl Opt*, 2002, **41**(26):5462-5470.
- [3] WANG B, SUN C C, SU W C, *et al.* Shift-tolerance property of an optical double-random phase-encoding encryption system[J]. *Appl Opt*, 2000, **39**(26):4788-479.
- [4] LI Rong, LI Ping. Optical image security based on random phase real-value encryption[J]. *Acta Photonica Sinica*, 2004, **33**(5):605-608.
李榕, 李萍. 基于随机相位实值编码的光学图像加密[J]. 光子学报, 2004, **33**(5):605-608.
- [5] LI Rong, LI Ping. Research on the image security in double random phase real-value encryption[J]. *Acta Photonica Sinica*, 2005, **34**(6):952-955.
李榕, 李萍. 双随机相位图像加密的实值编码研究[J]. 光子学报, 2005, **34**(6):952-955.
- [6] LU Hong-qiang, ZHAO Jian-lin. Iterative double random phase encryption based on pixel scrambling technology[J]. *Acta Photonica Sinica*, 2005, **34**(6):952-955.
陆红强, 赵建林. 基于像素置乱技术的多重双随机相位加密法[J]. 光子学报, 2005, **34**(6):1069-1073.
- [7] ZHOU xin, CHENG Jian-guo. Study on the quality of the composed and reconstructed images in the process of transmitting double random phase encode data[J]. *Optical Technique*, 2004, **30**(5):580-586.
周昕, 陈建国. 双随机相位编码信息隐蔽传递过程中的融合和重构图像质量的研究[J]. 光学技术, 2004, **30**(5):580-586.
- [8] ZHANG Peng, PENG Xiang, NIU Han-ben. A 32D digital watermarking system based on virtual-optics and random mask encoding[J]. *Acta Photonica Sinica*, 2005, **34**(8):1220-1223.
张鹏, 彭翔, 牛憨笨. 一种结合随机模板编码的虚拟光学三维数字水印系统[J]. 光子学报, 2005, **34**(8):1220-1223.
- [9] ZHANG Jing-juan, SITU Guo-hai, ZHANG Yan. Progress of optical security systems based on random phase encoding technology[J]. *Journal of the Graduate School of the Chinese Academy of Sciences*, 2003, **20**(3):265-272.
张静娟, 司徒国海, 张艳. 基于随机相位编码技术的光学安全系统的研究进展[J]. 中国科学院研究生院学报, 2003, **20**(3):265-272.
- [10] LIN Jie, XIAO Peng. Image hiding technique in internet transmission for sensitive information[J]. *Computer Engineering*, 2001, **27**(5):53-55.
凌捷, 肖鹏. 网络敏感信息传输中的图像隐藏技术[J]. 计算机工程, 2001, **27**(5):53-55.

Technology of Double Random Phase Encode Data Hidden in RGB Images

SUN Min, SU Xian-yu

(*Opto-Electronics Department, Sichuan University, Chengdu 610064, China*)

Received date: 2006-10-17

Abstract: A method of hiding original image encoded by double random phase data in the low lever of color host image was proposed. When need to decode, operation can be applied on the composed image directly and original host image will not be needed. The quality of the recovered image will be quite good and will not be influenced by the host image. The factors influencing the quality of the composed image and reconstructed image, which are caused by the process of encoding, accumulating and transmission, are discussed, and experiments were done in MATLAB. The result demonstrates that recovered images of high quality can be obtained in this way.

Key words: Image hiding; Double random phase encoding; BMP image; Image quality



SUN Min was born in 1981. He received his B. S. degree from Sichuan University in 2005. Now he is studying for his M. S. degree in Sichuan University. His major research interests focus on information hiding technique with double random phase encoding.