文章编号：1001-3806(2010)03-0401-04

基于干涉的二值图像逻辑运算加密技术

邓晓鹏，文 伟
（怀化学院 物理与信息工程系，怀化 418008）

摘要：为了对二值图像的内容进行保密，针对以往二值图像加密技术的缺陷，提出了一种基于干涉的二值图像逻辑运算加密技术。加密时，先选择一幅携带一定信息的二值图像作为加密后图像；然后根据被加密图像、加密后图像和解密密匙的逻辑关系在计算机中求出解密匙；最后利用光的干涉原理对图像进行解密。结果表明，该方法加密方便，解密系统设置简单，不需要精确对准，而且能够实现多重认证，安全性能非常高。

关键词：图像处理；加密；干涉；二值图像；逻辑
中图分类号：O438 **文献标识码**：A **doi**：10.3969/j.issn.1001-3806.2010.03.033

Binary image encryption using logic operations based on interferometer

DENG Xiao-peng, WEN Wei
(Department of Physics and Information Engineering, University of Huaihua, Huaihua 418008, China)

Abstract: For encoding binary images, binary image encryption using logic operations based on interferometer was presented to overcome the shortcomings of the previous binary image encryption. Firstly, a binary image which carries certain information is chosen as encrypted image. Secondly, a key which is used for decrypting image is obtained using logical relationship between them. Finally, the decrypted image is reconstructed with the principle of optical interference. Computer simulation and optical experiment show that encryption is very convenient and decryption system is simple. Also, this method can realize multi-authentication, so safety performance is very high.

Key words: image processing; encryption; interferometer; binary image; logic

引 言

二值图像作为一种特殊的图像类型，在承载信息中占有重要的地位，几乎所有的文字信息都可用二值图像来表示，因此，探索简易、可行和安全的二值图像加密技术具有重要的学术和应用价值。国内外学者在这方面进行了大量的研究[1-9]，提出了很多方法。其中，最经典是双随机相位加密技术[1]。该技术是采用4*f*系统来实现：把两块统计无关的随机相位掩膜(random phase mask, RPM)分别置于4*f*系统的输入平面和傅里叶频谱平面，分别对待加密图像$f(x, y)$的空间信息和频谱信息作随机编码，达到加密目的。但是，对于双随机相位加密技术，由于加密后的图像是复数，不便于储存和直接打印，同时，在解密阶段需要高精度的系统准直，虽然基于联合变换的加密系统在一定程度上解决了上述问题，但是由于存在较强的零级相关峰，能量分散，解密图像质量不高[2]，另外，由于这一类加密技术采用的是线性系统，因此存在一定的安全隐患，其破解方法已有报道[3]。除此之外，就是专门针对二值图像每个像素只有0和1两种可能灰度值的特点，利用光的偏振特性进行二值图像加密[4-5]。由于是利用光的偏振特性实现二值图像加密，因此，在加解密阶段都需要偏振片，系统显的非常复杂，而且要求偏振片的偏振方向及系统的各个元件精确对准。这些缺点这一定程度上影响了该技术的使用价值。

针对二值图像像素值的特点，本文中提出一种基于干涉的二值图像逻辑恢复算法加密技术。该方法是利用光的干涉原理结合逻辑运算实现二值图像加密的。加密时，先选择一幅特定的实数二值图像作为宿主图像，在被加密图像已知的情况下，根据光的干涉原理在计算机中进行逻辑运算反求出解密密匙。解密时，只要利用光的干涉原理便可恢复原图像。在该技术中，由于加密后图像选择是一幅特定的图像，因此不会引起攻击者的注意，并且解密密匙至少为两个，缺少其中的任何一个都不能恢复原图像，可实现多重认证。同时可以选择多个解密密匙实现多种逻辑运算，故该

基金项目：湖南省教育厅科研资助项目(07C506)；怀化学院科研资助项目

作者简介：邓晓鹏(1972-)，男，硕士，副教授，现主要从事光信息处理的研究。
E-mail: dxpzqh@163.com

收稿日期：2009-04-13；收到修改稿日期：2009-05-25

方法的安全性能非常高。另外,由于处理的是二值图像,因此,很容易将它通过示液晶显示器(liquid crystal display,LCD)进行相位调制或通过光学光刻技术制成纯相位掩膜,便于存储和复制。

1 加解密原理

根据光的干涉理论,当两束相干光在空间相遇时,将会产生干涉现象。设两束光波的表达式分别为:$E_1 = E_0\exp(i\theta_1)$ 和 $E_2 = E_0\exp(i\theta_2)$,则合成光振幅分布为:

$$E = E_1 + E_2 = E_0[\exp(i\theta_1) + \exp(i\theta_2)] \quad (1)$$

合成光强分布为:

$$I = \langle E^2\rangle = \langle (E_1 + E_2)(E_1 + E_2)^*\rangle = \langle {E_1}^2\rangle + \langle {E_2}^2\rangle + 2\langle E_1E_2\rangle = 2{E_0}^2(1 + \cos\Delta\theta) \quad (2)$$

式中,$\Delta\theta$ 为相位差,来自于两光波的初相位差和不同的传播路径而引起的相位差。从(2)式可以看出,当 $\Delta\theta$ 等于 π 的偶数倍时,光强达到最大值;而当 $\Delta\theta$ 等于 π 的奇数倍时,光强达到最小值 0。

现假设 E_1 和 E_2 分别代表两幅只有 0 和 π 两个相位值的二值纯相位图像的光振幅分布,则当两幅图像上对应像素点的相位分布相同时,该像素点的光强达到最大,而当两幅图像上对应像素点的相位分布不相同时,该像素点的光强达到最小值 0,如图 1 所示。如果选择合适的纯二值相位图像,通过干涉便可得到想要的二值图像。

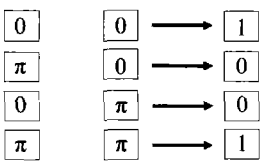

Fig. 1 Result of interfering between two pixels

利用上述干涉原理,可以对二值图像进行加解密。假设 $f(x,y)$,$r(x,y)$ 和 $e(x,y)$ 分别表示被加密的二值图像、随机二值图像和加密后的二值图像。加密时,先对被加密图像和随机二值图像进行相位调制,使它们转化为纯二值相位图像:

$$\begin{cases} f_p(x,y) = \exp[i\pi f(x,y)] \\ r_p(x,y) = \exp[i\pi r(x,y)] \end{cases} \quad (3)$$

式中,下标 p 表示二值图像经相位调制后的相位。然后两者相乘:

$$e_p(x,y) = f_p(x,y)r_p(x,y) = \exp\{i\pi[f(x,y) + r(x,y)]\} = \exp[i\pi e(x,y)] \quad (4)$$

由于(4)式结果为纯相位图像,不便保存和复制,可以通过光学光刻技术制成纯相位掩膜或就采用 $e(x,y)$ 作为加密后图像。解密时,对于前者,只要用表示加密密匙和加密后图像的相位掩膜进行相乘;对于后者,先通过 LCD 进行相位调制,再进行相乘,即:

$$f_p(x,y) = e_p(x,y)r_p(x,y) = \exp\{i\pi[f(x,y) + 2r(x,y)]\} = \exp[i\pi f(x,y)] \quad (5)$$

由于 $f_p(x,y)$ 是一个纯二值相位图像,无法利用探测器 CCD 进行探测,因此,必须对它进行相幅转换,可以利用二值相位图像只有 0 和 π 两个相位值的特点,根据干涉原理来恢复原图像:

$$f' = |R(x,y) + R(x,y)f_p(x,y)|^2 = |R(x,y)|^2|1 + \exp[i\pi f(x,y)]|^2 = |R(x,y)|^2\begin{cases} 4, (f(x,y) = 0) \\ 0, (f(x,y) = 1) \end{cases} \quad (6)$$

式中,$R(x,y)$ 是一束任意相干参考光。由上述结果可以看出,解密后的图像 $f'(x,y)$ 仍为二值图像,只不过是原图像 $f(x,y)$ 的负像。

在上述加密方法中,加密后的图像是由加密密匙决定的,由于加密密匙是一幅随机二值图像,根据它的加密原理可知加密后的图像也是一幅随机噪声图像。由于在一般加密过程中加密后的图像往往是以噪声的形式出现的,因此易受到未授权者的有意攻击,为了避免这种情况,先选择任意一幅携带一定信息的二值图像作为加密后的图像 $e(x,y)$,然后根据上述解密原理求出解密密匙 $d(x,y)$。既已知 $e(x,y)$ 和 $f(x,y)$,根据下式求 $d(x,y)$:

$$e_p(x,y)d_p(x,y) = \exp\{i\pi[e(x,y) + d(x,y)]\} = \exp[i\pi f(x,y)] \quad (7)$$

由于加密后的图像和解密图像均为携带一定信息的二值图像,根据上述解密原理求出的解密密匙 $d(x,y)$ 不具备随机性,安全性能不高,可以把 $d(x,y)$ 分成 $d_1(x,y)$,$d_2(x,y)\cdots d_i(x,y)$,其中 $d_1(x,y)$,$d_2(x,y)\cdots d_{i-1}(x,y)$ 为任意已知的随机二值图像,这样既可以避免上述问题,又可增加密匙个数,实现多重认证。下面以两个密匙为例,根据(7)式求解 $d_2(x,y)$。为了简单起见,令参考光光强 $|R(x,y)|^2 = 1$。

Table 1 Truth value table based on the principle of interferometer

$e(x,y)$	$d_1(x,y)$	$d_2(x,y)$	$f(x,y)$	$f'(x,y)$
0	0	0	0	4
0	0	1	1	0
0	1	0	1	0
1	0	0	1	0
1	1	0	0	4
1	0	1	0	4
0	1	1	0	4
1	1	1	1	0

从表 1 可以看出,解密过程实际上就是已知 $e(x,y)$,$d_1(x,y)$ 和 $d_2(x,y)$,根据下面逻辑表达式求被加密图像 $f(x,y)$ 的过程:

$$f = ed_1d_2 + \bar{e}d_1\,\bar{d_2} + e\,\bar{d_1}\,\bar{d_2} + \bar{e}\,\bar{d_1}d_2 \qquad (8)$$

由于加密后的图像 $e(x,y)$ 为预先指定的一幅携带一定信息的二值图像，虽然 $d_1(x,y)$ 可以是任意的随机二值图像，但是 $d_2(x,y)$ 不能为任意的随机二值图像，否则不能恢复 $f'(x,y)$。因此必须根据上述逻辑关系反求出 $d_2(x,y)$。根据表 1 可得出 $d_2(x,y)$ 的逻辑表达式：

$$d_2 = ed_1f + \bar{e}d_1\bar{f} + e\,\bar{d_1}\bar{f} + \bar{e}\,\bar{d_1}f \qquad (9)$$

当只采用一个密匙进行加解密图像时，上述逻辑关系简化为逻辑异或运算，如果增加密匙个数还可实现更复杂的逻辑运算。从上述加解密原理可以看出，加密过程实际上就是已知 $e(x,y)$ 和 $f(x,y)$ 利用(9)式的逻辑关系反求出解密密匙的过程。上述过程很容易在计算机中完成。具体步骤如下：首先选择一幅特定的二值图像作为加密后的图像 $e(x,y)$；然后生成一幅随机二值图像作为解密密匙 $d_1(x,y)$；最后根据(9)式的逻辑关系求出解密密匙 $d_2(x,y)$。

相对于加密过程，解密要简单得多，利用图 2 中所示的光学系统根据干涉原理便可进行解密。具体过程

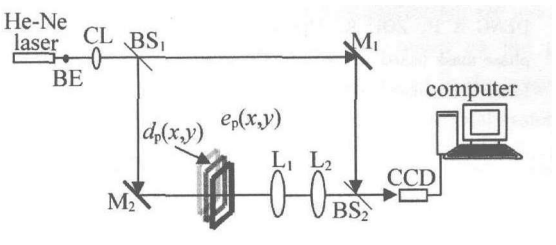

Fig. 2　Setup for decryption

如下：将分别通过相位调制的 $e(x,y)$ 和解密密匙 $d(x,y)$ 重叠放置在傅里叶变换透镜 L_1 前的焦面上。由 He-Ne 激光器发出的激光经扩束器(beam expender，BE)和准直透镜(collimating lens，CL)获得准直相干光，再由分光镜(beam splitters，BS) BS_1 分成两路，一路经过平面反射镜 M_1 作为参考光 $R(x,y)$，另外一路经过平面反射镜 M_2 照射到 $e_p(x,y)d_p(x,y)$ 上，经 L_1 和 L_2 组成的 $4f$ 系统成像在透镜 L_2 后的后焦面上与参考光产生干涉，用 CCD 接收它们的干涉图像，也就是解密后的图像。

下面分析多个密匙的情况下，单个密匙对解密图像的影响。以 3 个密匙为例，具体分析如表 2 所示。表中“×”表示在缺少密匙情况下错误的解密，$f_1(x,y)$ 表示在缺少 $d_1(x,y)$ 的情况下的解密图像，$f_{12}(x,y)$ 表示在缺少 $d_1(x,y)$ 和 $d_2(x,y)$ 的情况下的解密图像。从表 2 可以看出，对于多个密匙，在缺少密匙的情况下，虽然都能解出原图像 50% 的像素，但是由于密匙的随机性，解密后的图像仍然为一幅噪声图像，因此，每个密匙在解密时缺一不可。另外，如果想利用穷举

Table 2　Contrast table of decrypted image

$e(x,y)$	$d_1(x,y)$	$d_2(x,y)$	$d_3(x,y)$	$f(x,y)$	$f_1(x,y)$	$f_{12}(x,y)$
0	0	0	0	0	0	0
0	0	0	1	1	1	0
0	0	1	0	1	1	0(×)
0	1	0	0	1	0(×)	0(×)
1	0	0	0	1	1	1
1	1	0	0	0	1(×)	1(×)
1	0	1	0	0	0	1(×)
0	1	1	0	0	1(×)	0
0	1	0	1	0	1(×)	1(×)
0	0	1	1	0	0	1(×)
1	0	0	1	0	0	0
1	1	1	0	1	0(×)	1
0	1	1	1	1	0(×)	1
1	0	1	1	1	1	0(×)
1	1	0	1	1	0(×)	0(×)
1	1	1	1	0	1(×)	0

法破解原图像，如果图像大小为 $m \times n$，破解次数将达到 $2^{m\times n}$，当 m 和 n 比较大时，$2^{m\times n}$ 是个非常巨大的数字，因此，利用穷举法破解原图像是相当困难的。这些特性既可实现多重认证，又大大增强了安全性能。

2　计算机仿真和光学实验

为了验证该方法的可行性，作者进行了仿真和光学实验。模拟时，原图像为一幅黑体“上”字图，如图 3a 所示；加密后图像选择的是一幅大写“E”字图，如图 3b 所示；图 3c、图 3d 是解密密匙，其中 $d_1(x,y)$ 为任意选择的一幅随机二值图像，$d_2(x,y)$ 是利用(9)式求出的；图 3e 为正确密匙情况下的解密图像；图 3f 为缺少 $d_1(x,y)$ 情况下的解密图像；图 3g 为缺少 $d_2(x,y)$ 情况下的解密图像；图 3h 为盲解密图像。

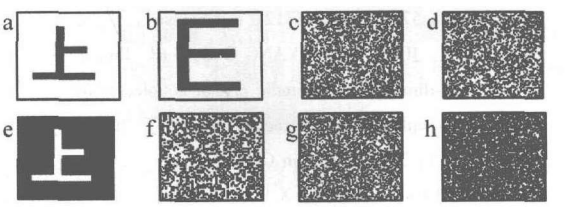

Fig. 3　Simulation result

a—the original image f　b—encrypted image E　c—decryption key d_1　d—decryption key d_2　e—decrypted image f'　f—decrypted image without d_1　g—decrypted image without d_2　h—blind decrypted image

光学解密光路如图 4a 所示。空间光调制器(spatial light modulator，SLM)是由美国 BNS 公司生产的反射式面阵纯相位空间调制器，通过它对 $e(x,y)d(x,y)$ 进行 Pixel-by-Pixel 的相位调制。L_1 和 L_2 均为焦距 70mm 的傅里叶变换透镜。CCD 像素为 2023 × 1520，尺寸为 10.0mm × 7.48mm。照明相干光源为 He-Ne 激光器。由 He-Ne 激光器发出的激光经扩束器 BE 和准直透镜 CL 获得准直相干光，再由分光镜 BS_1 分成

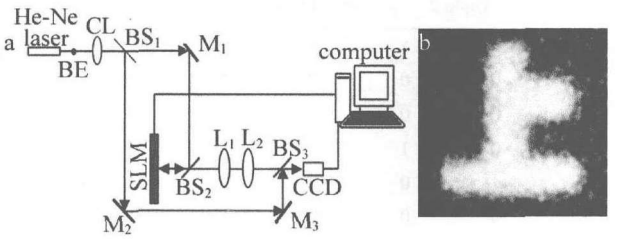

Fig. 4 Setup and result of optical experiment

a—setup of optical experiment b—result of optical experiment

两路，一路经过平面反射镜 M_2 和 M_3 作为参考光；另外一路经 M_1 和 BS_2 照射到 SLM 上，由于 SLM 上显示的是的 $d(x,y)e(x,y)$，所以经 SLM 反射调制后的光为 $e_p(x,y)d_p(x,y)$，最后经 L_1 和 L_2 组成的 $4f$ 系统成像到 CCD 上，与参考光干涉获得解密图像如图 4b 所示。

3 结 论

从以上理论分析和实验结果表明，基于干涉的二值图像逻辑恢复算法加密技术是可性的。与以往方法相比，加密过程非常方便，完全可以在计算机中完成；解密原理和系统设置简单，不需要系统精确对准，容易实现。由于采用的是一幅特定图像作为加密后的图像，再加上多重密匙认证，安全性能非常高。

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] TAKANORI N, BAHRAM J. Optical encryption using a joint transform correlator architecture[J]. Opt Engng, 2000, 39(8): 2031-2035.

[3] CARNICER A, MONTES-USATEGUI M, ARCOS S, *et al*. Ulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys[J]. Opt Lett, 2005, 30(13): 1644-1646.

[4] MOGENSEN P C, lUCKSTAD J. A phase-based optical encryption system with polarization encoding[J]. Opt Commun, 2000, 173(1): 177-183.

[5] HAN J W, PARK C S, RYU D H, *et al*. Optical image encryption based on XOR operations[J]. Opt Engng, 1999, 38(1): 47-54.

[6] LI R, LI P. Research on the image security in double random phase real-value encryption[J]. Acta Photonica Sinica, 2005, 34(6): 952-955(in Chinese).

[7] LI R, LI P. Real-value encryption for optical security system based on holography[J]. Acta Photonica Sinica, 2008, 37(5): 957-959(in Chinese).

[8] DENG X P, ZOU K. Optical image encryption using one random phase mask based on spotlight illumination in the Fresnel domain[J]. Laser Technology, 2006, 30(4): 442-444(in Chinese).

[9] DENG X P, ZOU K. Optical image encryption using one random phase mask based on spotlight illumination in the Fresnel domain[J]. Laser Technology, 2006, 30(3): 327-328(in Chinese).

(上接第 400 页)

[4] DU G Q, LIU N H. Optical transmission spectra of one dimensional photonic crystals with a mirror symmetry[J]. Acta Physica Sinica, 2004, 53(4): 1095-1097 (in Chinese).

[5] CHEN X F, JIANG M P, SHEN X M, *et al*. The defect modes in one-dimensional photonic crystal with multiple defects[J]. Acta Physica Sinica, 2008, 57(9): 5709-5712 (in Chinese).

[6] DONG H X, JIANG H T, YANG C Q, *et al*. Properties of impurity band in one-dimensional photonic crystal coupled-resonator containing defect layers with negative refractive index[J]. Acta Physica Sinica, 2006, 55(6): 2777-2780 (in Chinese).

[7] JIN Y, HUANG ZY, CHEN X F, *et al*. Study on polarization properties of the photonic crystal defect mode[J]. Laser Technology, 2007, 31(3): 277-280 (in Chinese).

[8] JIANG M P, JIANG X F, SHEN X M, *et al*. Study on the polarization property of 1-D photonic crystals[J]. Chinese Journal of Quantum Electronics, 2005, 22(4): 612-616 (in Chinese).

[9] BAYINDIR M, TEMELKURAN B, OZBAY E. Tight-binding description of the coupled defect modes in three-dimensional photonic crystals [J]. Phys Rev Lett, 2000, 84(10): 2140-2143.

[10] BAYINDIR M, TANRISEVEN S, OZBAY E. Propagation of light through localized coupled-cavity modes in 1-D photonic band-gap structures [J]. Appl Phys, 2001, A72(1): 117-119.

[11] XIE Y M, LIU Zh D. Local defect modes in photonic crystal with a number of structral defects[J]. Laser Journal, 2005, 26(6): 34-36 (in Chinese).

[12] VILLENEUVE P R, FAN S, JOANNOPOULOS J D. Microcavities in photonic crystals: mode symmetry, tenability, and coupling efficiency [J]. Phys Rev, 1996, B54(11): 7837-7842.