基于联合变换的旋转不变光学图像加密

韩振海，刘秋武，刘 艺，王仕璠

(电子科技大学物理电子学院 成都 610054)

【摘要】利用两个彼此独立的编码脉冲相位掩模在联合变换相关器中对需要保护的图像进行编码，实现对原始图像的加密。该方法的特点是解密时加密图像的旋转不会影响解密效果，相位分布是密钥的合法持有者唯一掌握的确定性函数，可以重构，便于实际应用。计算机模拟的结果证明了方法的可行性。

关 键 词 光学图像; 加密; 联合变换; 旋转不变; 编码脉冲信号; 相位掩模板

中图分类号 O438; TN249 文献标识码 A

Optical Image Encryption with Rotating Invariance Based on Joint Transform Correlator

Han Zhenhai，Liu Qiuwu，Liu Yi，Wang Shifan

(School of Physical Electronics, UEST of China Chengdu 610054)

Abstract Two phase mask plate with independent chirp signals are used to encode image in the joint transform correlator,so as to make encrypt the original image.The characteristic of this method is when decoding,the rotation of encrypted image can not affected decoding effect,and moreover,owing to the fact that phase distribution is a decisive function only grasped by owner of secure key and the secure key can be regenerated.It makes the practical use convenient.The results of computer simulation shows the feasibility of this method.

Key words optical image; encryption; joint transform correlator; rotating invariance; chirp; phase mask plate

利用光学信息处理对图像进行保密和安全检查是近年来引起国内外广泛关注并不断发展的一种有效方法。文献[1]提出利用两个随机相位掩模在联合变换相关器中对需要保护的图像进行编码，安全度极高。但是，由于相位掩模具有完全随机性的特点，所以其制备具有很大困难；而且，该随机相位掩模不能重构，一旦遗失或损坏，便无法对加密图像进行解密。这些因素在很大程度上限制了实际应用。

本文在保持一定加密安全度的前提下，利用可重构的编码脉冲信号(chirp)相位掩模对图像在联合变换相关器中进行编码加密。

1 理论分析

由密钥的合法持有者唯一掌握的两个彼此独立的编码脉冲相位掩模$n(x, y)$和$b(x, y)$的分布规律为

$$\begin{cases} n(x,y)=\mathrm{e}^{-\mathrm{i}\pi(x^2+y^2+k_n)} \\ b(x,y)=\mathrm{e}^{-\mathrm{i}\pi(x^2+y^2+k_b)} \end{cases}$$

式中 k_n、k_b 为控制参数。利用函数的傅里叶变换关系

$$\mathrm{e}^{\pm\mathrm{i}\pi(x^2+y^2)} \Leftrightarrow \mathrm{e}^{\pm\mathrm{i}\frac{\pi}{2}}\mathrm{e}^{\mp\mathrm{i}\pi(x^2+h^2)}$$

收稿日期：2003 – 06 – 30

作者简介：韩振海(1971 –)，男，硕士生，现工作单位为甘肃河西学院 主要从事信息光学方面的研究.

可得到这两个编码脉冲相位函数的傅里叶变换谱为

$$N(x,h)=F\{\mathrm{e}^{-\mathrm{i}\pi(x^2+y^2+k_n)}\}=-\mathrm{i}\mathrm{e}^{\mathrm{i}\pi(x^2+h^2+k_n)}$$

$$B(x,h)=F\{\mathrm{e}^{-\mathrm{i}\pi(x^2+y^2+k_b)}\}=-\mathrm{i}\mathrm{e}^{\mathrm{i}\pi(x^2+h^2+k_b)}$$

式中 x、h为频域坐标，$F\{\cdot\}$为Fourier变换，$N(x,h)$、$B(x,h)$分别为$n(x,y)$、$b(x,y)$的Fourier变换谱。编码脉冲相位掩模相应的频谱，仍然为纯相位型函数；而且，不管是编码脉冲相位掩模，还是它们的频谱，均具有二维圆对称的特性。

用这两个编码脉冲相位掩模$n(x,y)$和$b(x,y)$对原始图像$f(x,y)$在联合变换相关器中进行加密。如图1所示，输入图像$f(x,y)$和编码脉冲相位掩模$n(x,y)$重叠后置于输入面上$x=a$处，另一编码脉冲相位掩模$b(x,y)$则置于输入面上$x=-a$处。经Fourier变换后，可在Fourier频域得到它们的频谱，即

$$e(x,h)=F\{n(x-a,y)f(x-a,y)+b(x+a,y)\}=N(x,h)*F(x,h)\,\mathrm{e}^{-\mathrm{i}4\delta xa}+B(x,h)\,\mathrm{e}^{\mathrm{i}2\pi xa}$$

式中 *为卷积运算，$F(x,h)$为$f(x,y)$的Fourier变换谱。其联合变换功率谱(JTPS)为

$$E(x,h)=\left|e(x,h)\right|^2=\left|N(x,h)*F(x,h)\right|^2+1+\left[N(x,h)*F(x,h)\right]^*B(x,h)\,\mathrm{e}^{\mathrm{i}4\pi xa}+\left[N(x,h)*F(x,h)\right]B(x,h)^*\,\mathrm{e}^{-\mathrm{i}4\pi xa}$$

式中 上标*为共轭。可以看出，原始图象信息已被淹没在联合变换功率谱$E(x,h)$中，即使将$E(x,h)$进行Fourier逆变换，也只能得到噪声图像[1]。因此，联合变换功率谱$E(x,h)$可作为原图像的加密图像。

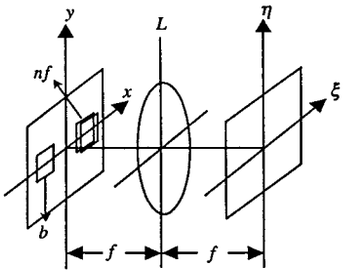

图1 图像加密

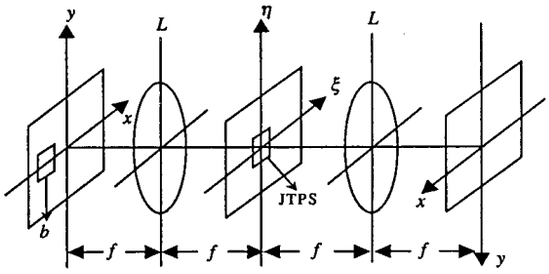

图2 图像解密

分析解密过程。如图2所示，将密钥$b(x,y)$置于输入面内原位置$x=-a$处，经Fourier变换后，与置于频域内$x=0$处的加密图象$E(x,h)$重叠并相乘，得到

$$G(x,h)=E(x,h)B(x,h)\,\mathrm{e}^{\mathrm{i}2\pi xa}=\left|N(x,h)*F(x,h)\right|^2B(x,h)\,\mathrm{e}^{\mathrm{i}2\pi xa}+B(x,h)\,\mathrm{e}^{\mathrm{i}2\pi xa}+$$
$$\left[N(x,h)*F(x,h)\right]^*B(x,h)B(x,h)\,\mathrm{e}^{\mathrm{i}6\pi xa}+\left[N(x,h)*F(x,h)\right]\mathrm{e}^{-\mathrm{i}2\pi xa}$$

再将上式进行一次Fourier逆变换，得

$$g(x,y)=F^{-1}\{E(x,h)B(x,h)\,\mathrm{e}^{\mathrm{i}2\pi xa}\}=$$
$$[n(x,y)f(x,y)]\otimes[n(x,y)f(x,y)]*b(x,y)*d(x+a)+b(x,y)*d(x+a)+$$
$$[n(x,y)f(x,y)]\otimes b(x,y)*b(x,y)*d(x+3a,y)+n(x,y)f(x,y)*d(x-a)$$

式中 $\otimes$为相关运算。可看出，在输出面上$x=a$处会出现$n(x,y)f(x,y)$，由于$f(x,y)$通常为正值函数，因此位相函数$n(x,y)$的存在并不影响原图像$f(x,y)$在诸如CCD等强度探测器上的再现。在输出面上$x=-a$、$x=-3a$处形成的则是与$f(x,y)$无关的噪声。

需要特别指出的是，由于编码脉冲相位掩模$b(x,y)$的频谱$B(x,h)$具有二维圆对称的特性，所以解密时加密功率谱$E(x,h)$在频谱面内绕光轴不论发生怎样的旋转，它和圆对称频谱$B(x,h)$叠加的效果都是相同的。本文正是利用这一特性来实现旋转不变的光学图像解密。

解密图像$f'(x,y)$的质量可用其与原图像$f(x,y)$的相关程度来衡量，定义为

$$f'(x,y)\otimes f(x,y)=\iint_{-\infty}^{+\infty}f'(a,b)f(a-x,b-y)\mathrm{d}a\mathrm{d}b$$

2 模拟结果

本文采用如图3所示的128×128像素的“saturn”图像作为原始待加密图像，两相位掩模的控制参数分别取$k_n=1.32$、$k_b=1.32$。利用上面提出的编码脉冲相位掩模对原图像加密后的结果如图4所示，可看出，加密

后的图像已呈噪声分布。

图3　原始图像

图4　加密图像

图5　正确相位解密后的图像

解密时，先采用加密时的合法密钥$b(x, y)$，得到图5所示的结果，可以正确地解密出原始图象。为检验该方法抗盲解密的能力，本文仅改变相位掩模$b(x, y)$的控制参数k_b，改变量Δk_b依次为0.001, 0.002, 0.003, …, 0.010，以考察解密后的图像与原图像的差异。关于解密后图像与原图像的差异，可以用二者的均方差来衡量[2]，本文认为比较二者的相关程度更为合理。具体做法是将解密图像和原始图像模拟输入联合变换相关器(JTC)[3]，计算并提取二者的互相关峰值。图6所示是$\Delta k_b = 0.001$时的解密图像，无法从中识别出原图像信息；图7所示是不同Δk_b下的相关峰值曲线。

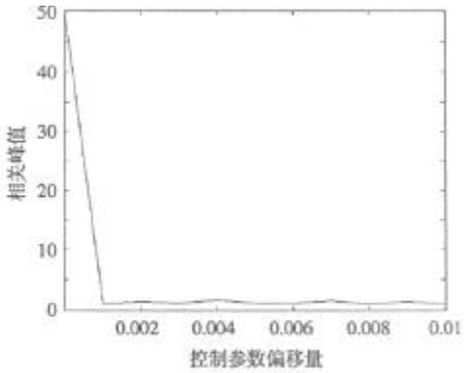

图6　$\Delta k_b = 0.001$时的解密图像　　图7 不同Δk_b下的相关峰值　　图8 加密功率谱旋转90°后的解密图像

以上结果表明该编码脉冲相位用于图像加密具有较强的抗盲解密的能力。

下面再考察加密图像的旋转对解密效果的影响。具体方法是先将加密功率谱在频谱面内绕光轴旋转任意角度，不失一般性将其旋转90°后再在解密光学系统中进行解密。图8所示是加密功率谱旋转90°后解密得到的与原图像相同但也旋转了90°的图像，可以看出，采用编码脉冲相位作为密钥可实现加密图像的旋转不变，该性质使图像解密对方向性不敏感，解密时不再受加密图像取向的限制，给实际应用带来了便利。

3　结　论

通过模拟计算，利用编码脉冲相位对图像在联合变换相关器中进行加解密是完全可行的，该方法的优点是相位密钥可以重构，便于密钥的保存和传输；解密时不再受加密图像取向的限制。

参　考　文　献

[1] Nomura T, Javidi B. Optical encryption using a joint transform correlator architecture[J]. Opt Eng, 2000, 39(8): 2 031-2 035

[2] Tian X, matoba O, Shimura T, *et al.* Secure optical storage that uses fully phase encrytion[J]. Appl Opt, 2000, 39(35): 6 689-6 694

[3] Weaver C S, Goodman J W. A technique for optically convolving two function[J]. Appl Opt, 1966, 5: 1 248-1 249

编　辑　孙晓丹