

一种基于二元位相加密的大信息量数字全息水印*

陈林森 周小红 邵洁

(教育部现代光学技术重点实验室,苏州大学信息光学工程研究所,苏州 215006)

摘要 研究了一种基于二元位相加密的大信息量数字全息水印方法,对需隐藏的水印信息用二元位相编码,然后再用2台阶位相密钥进行加密,作为水印插入宿主图像中,解码后得到了高质量的水印结果.与平面波照明数字全息水印相比,采用位相密钥数字全息水印有效地提高了水印提取的安全性和相对光学效率,并保持了对大信息量水印的提取质量,解码过程不依赖于原图像.计算和分析了二元位相密钥的空间分布对水印信息提取质量的影响,计算结果验证了理论的正确性.

关键词 二元光学;位相编码;数字全息水印

中图分类号 O436.1;TH74

文献标识码 A

0 引言

在光学编码方法上,Javidi等人^[1,2]提出了双随机位相编码并用于数字水印,算法安全性高,但水印解码时要求严格的对准性,数字水印不能实现硬输出(打印),限制了其实用性.Nobukatsu Takai等人将光全息概念应用到数字水印算法中^[3,4],提出了数字全息水印(digital hologram watermarking),由于最终解码后的图像是强度分布,因此,为了改善傅里叶变换光场的均匀性,在目标物(水印)上调制了随机位相分布,然后将水印的傅里叶变换分布插入到宿主图像中.结果表明,全息水印有较强的鲁棒性和抗攻击性,尤其具有抗剪切的特点,但由于傅里叶变换同时具有振幅和位相信息,水印解码后的光学效率很低,同时,只需作逆傅里叶变换就能够获得隐藏的信息,缺乏数字水印应有的安全性.

对于具有大信息含量的水印,需要提高水印解码时的光学效率,同时降低解码过程中产生的噪声.

基于二元位相恢复的迭代算法,我们提出了具有位相密钥的二元位相数字全息水印方法,采用2/2台阶组合提高了数字水印解码的光学效率,从而有效地保证了大信息量水印的提取质量,解码过程不依赖原宿主图像.分析了不同二元位相密钥的尺寸下对数字水印提取质量的影响.该方法比直接傅里叶变换数字水印方法有更高的光学效率、比平面波照明二元位相数字水印方法更具安全性,计算结果验证了理论的正确性.

1 二元位相加密与全息水印

1.1 全息水印原理和二元位相算法

设 $O(x,y)$ 和 $R(x,y)$ 分别是物光场和参考光场原始分布,经过传播后的波前为 $o(u,v)$ 和 $r(u,v)$,两光波相互干涉后形成的光场为

$$I(x,y) \propto |o(u,v) + r(u,v)|^2 = (|o(u,v)|^2 + |r(u,v)|^2) + o(u,v)r^*(u,v) + o^*(u,v)r(u,v) \quad (1)$$

这里*为复共轭,用原参考光 $r(u,v)$ 照明,可得到原始物光波前再现(第二项),当物光波与参考光波具有夹角时,式(1)中的三个光场分布在空间上是分离的.从加密角度,参考波前 $r(u,v)$ 是一个密钥,如果 $R(x,y)$ 是空间随机位相分布,则 $r(u,v)$ 是其远场衍射光场.一般地, $o(u,v)r^*(u,v)$ 是复振幅分布,既有位相又有振幅,常用计算全息(CGH)的方法(如迂回位相法)整体上计算光场 $o(u,v)r^*(u,v)$ 的干涉条纹分布,但CGH的方法得到结果是一种振幅分布,光学再现效率很低.

本文提出采用二元光学位相恢复算法求出式(1)中第二项或第三项的纯二元位相分布作为数字全息水印,即分别计算出原始物光场和参考光场经过远场传播后光场的二元位相分布,明显的优点是这种二元位相结构具有较高衍射效率^[5]以及具备全息图的鲁棒性.光场的远场传播的过程是傅里叶变换来表达.位相分布的求解是一个迭代过程^[6-10],主要做法是,假设初始相位分布是 $\phi_i(x,y)$,由具有振幅分布 $f(x,y)$ 的像平面开始,然后,对衍射光学元件(频谱面)平面 (u,v) 和像平面 (x,y) 处的光场分别用快速傅里叶变换进行迭代计算,在像平面采用 $f(x,y)$ 对变换后的目标光场的振幅进行替换,保留位相分布.在衍射光学元件平面处,振幅调制被限制在照明光束的常数振幅,并对位相角进行量化.这样,经过数十次迭代运算,获得了一个具有台阶纯位相全息图 $\exp[j\phi(u,v)]$.由于二元位相图在远场的正负一级衍射光占了绝大部分光

*江苏省“六大人才高峰”基金资助项目

Tel:0512-65112851 Email:lschen@suda.edu.cn

收稿日期:2004-04-05

强^[5],所以, $\exp [j\phi(u, \nu)]$ 在远场的再现光场分布 $f_i(x, y)$ 可表述为

$$f_i(x, y) = FT\{\exp [j\phi(u, \nu)]\} = f_{-1}(x, y) + f_{-1}(x, y) + n(x, y) \quad (2)$$

这里 $FT\{\}$ 表示傅里叶变换算符, $f_{+1}(x, y)$ 、 $f_{-1}(x, y)$ 分别是正、负一级衍射再现像. $n(x, y)$ 是由位相数字化及算法误差带来的噪声, 算法精度越高, 再现像 $f_{+1}(x, y)$ 越接近原始图像 $f(x, y)$. 二元位相全息图衍射效率定义为目标图像区域 Ω 内的光强与整个再现光强之比

$$\eta = \frac{\sum_{(x,y) \in \Omega} f^2(x, y)}{\sum_x \sum_y f^2(x, y)} \quad (3)$$

用来评价二元位相结构的衍射品质. 当位相台阶 $L=2$ 且位相角 $\phi(x, y)$ 取值 0 或 π 时, $f_{+1}(x, y)$ 和 $f_{-1}(x, y)$ 为关于原点对称 (共轭) 的再现光场, 即 $f_{+1}^*(x, y) = f_{-1}(x, y)$; 当 $L=4, 8$ 或更高台阶时, $f_{-1}(x, y) \rightarrow 0$, $f(x, y) \approx f_{+1}(x, y) + n(x, y)$. 这样, 通过迭代傅里叶变换算法分别求得物光和参考光波前的位相分布 $\exp [j\phi_o(u, \nu)]$ 和 $\exp [j\phi_r(u, \nu)]$. 考虑远场衍射和光场传播可逆原理, 则 $O_i(x, y) = FT\{\exp [j\phi_o(u, \nu)]\}$

$R_i(x, y) = FT\{\exp [j\phi_r(u, \nu)]\}$, 下标 i 表示衍射像.

1.2 二元位相水印的嵌入

根据需隐藏的水印信息 $O(x, y)$ 和空间分布 $R(x, y)$, 经过迭代算法分别获得的物光波前和参考光波前的二元位相分布 $\exp [j\phi_o(u, \nu)]$ 和 $\exp [j\phi_r(u, \nu)]$ 后者作为位相密钥, 如果宿主图像是彩色图像, 则先将彩色图像分解成 R, G, B 三个灰度分量, 将 $\exp [j\phi_o(u, \nu) - j\phi_r(u, \nu)]$ 作为加密水印插入其中的一个灰度分量中. 设 $C_o(u, \nu)$ 是彩色图像一个归一化灰度分量, $C(u, \nu)$ 是含有水印信息的灰度图像, 则有

$$C(u, \nu) = C_o(u, \nu) + \alpha \exp [j\phi_o(u, \nu) - j\phi_r(u, \nu)] \quad (4)$$

式中 $\alpha (0 \sim 0.3)$ 表示水印含量. 然后, 再将上述分量与其余量个分量合成为彩色图像, 这样, 水印的隐藏效果很好. 在图像文件读写或硬输出 (打印或二值化) 过程中, 实际输出的图像是式 (4) 的模, 光场 $\exp [j\phi_o(u, \nu) - \phi_r(u, \nu)]$ 通过其实部将位相结构插入到宿主图像中.

1.3 水印的提取

水印的提取 (解码) 过程如下: 先将含有水印的彩色图像分解, 对其中一幅含有水印的灰度图像用位相密钥 $\exp [j\phi_r(u, \nu)]$ 照明, 并进行傅里叶变换, 考虑到 α 是一个远小于 1 的数, 解码结果 $W(x, y)$ 为

$$W(x, y) = FT\{C_1(u, \nu) + \alpha \exp [j\phi_o(u, \nu) - j\phi_r(u, \nu)]\} \exp [j\phi_r(u, \nu)] \approx FT\{C_1(u, \nu) \cdot \exp [j\phi_r(u, \nu)] + (\alpha/2) \exp [j\phi_o(u, \nu)] + (\alpha/2) \cdot \exp [-j\phi_o(u, \nu) + 2j\phi_r(u, \nu)]\} = FT\{C_1(u, \nu)\} \otimes R_i(x, y) + (\alpha/2) O_i(x, y) + (\alpha/2) FT \cdot \{\exp [2j\phi_r(u, \nu)]\} \otimes O_i^*(x, y) \quad (5)$$

式 (5) 是一个复振幅光场, \otimes 表示卷积, 第一项为宿主图像灰度分量傅里叶变换与密钥空间分布 $R(x, y)$ 的卷积, 位于再现光场的中央区域, 具有很强的光强; 第二项是需要提取的水印信息 (物光) $O_i(x, y)$; 第三项为物光共轭像 $O_i^*(x, y)$ 卷积了一个因子 $FT\{\exp [2j\phi_r(u, \nu)]\}$, 从式 (5) 可知, 位相角 $\phi_r(u, \nu)$ 和 $\phi_o(u, \nu)$ 的取值对水印信息提取质量将产生影响.

让 $FT\{\exp [2j\phi_r(u, \nu)]\} = \delta(x, y)$ 的条件有两个, 第一, $\phi_r(u, \nu)$ 为常数 (平面波照明), 这种水印方法没有加密效果, 第二, $\phi_r(u, \nu)$ 取两台阶且为 $\{0, \pi\}$ 分布, 则 $\exp [2j\phi_r(u, \nu)] = 1$, 光场 $W(x, y)$ 中形成两个相互共轭的水印, 显然, 两台阶 $\phi_r(u, \nu)$ 具有加密功能. 当 $\phi_o(u, \nu)$ 也为 $\{0, \pi\}$ 时, $\exp [j\phi_o(u, \nu)]$ 产生正负一级衍射光, 根据式 (2), $O_i(x, y)$ 的 $+1$ 衍射光与 $O_i^*(x, y)$ 的 -1 衍射光将相干叠加, 式 (5) 简化成

$$W(x, y) = FT\{C_1(u, \nu)\} \otimes R_i(x, y) + (\alpha/2) \cdot O_i(x, y) + (\alpha/2) O_i^*(x, y) = FT\{C_1(u, \nu)\} \otimes R_i(x, y) + n(x, y) + 2(\alpha/2) O_{-1}(x, y) + 2(\alpha/2) \cdot O_{-1}(x, y) \quad (6)$$

这样, 设 L_o, L_r 分别为 $\exp [j\phi_o(u, \nu)]$ 和 $\exp [j\phi_r(u, \nu)]$ 的台阶数, 对 $L_o/L_r = (2/2)$ 台阶组合位相结构, 目标水印图像区域 Ω 的提取的水印光强为 $w^2(x, y) = 4[(\alpha/2) O_{-1}(x, y)]^2$.

而对多台阶组合位相结构, -1 级衍射光效率很低, 不能形成 $(2/2)$ 台阶一样的相干叠加. 从而, L_o/L_r 为 $(2/2)$ 台阶组合的二元位相水印提取的光强最高, 有利于大信息量水印的提取. 无位相密钥情况下对含有水印的图像 $|C(u, \nu)|$ 进行傅里叶变换解码, 得到的光场分布

$$W(x, y) \approx FT\{C_1(u, \nu)\} + (\alpha/2) O_i(x, y) \otimes R_i^*(x, y) + (\alpha/2) O_i^*(x, y) \otimes R_i(x, y) \quad (7)$$

需要解码的信息是式 (7) 中的第二、三项, 均是密钥空间分布与水印信息的卷积, 为模糊像, 这表明没有位相密钥就不能解出水印信息.

2 大信息量水印提取结果与质量评价

图 1 给出了进行 20 迭代傅里叶变换运算后的 $2/2$ 台阶组合的二元位相全息水印的编码、解码过

程. 图 1(a) 是大信息量水印图像 $O(x, y)$, 512×512 像素, 约有 500 多个字符. 图 1(b) 是经过迭代运算后的两阶段二元位相分布 $\exp[j\phi_0(u, \nu)]$, 图 1(c) 为条形 (9×99) 随机空间分布 $R(x, y)$, 其两

阶二元位相结构 $\exp[j\phi_r(u, \nu)]$ 参见图 1(d) 并作为位相密钥, 加密后的水印为图 1(e), 用彩色图像 (测试图像用 lena. bmp, 512×512 像素, $\alpha = 0.10$) 的 b 分量作为宿主图像. 从图 1(f) 可以看出, 图像

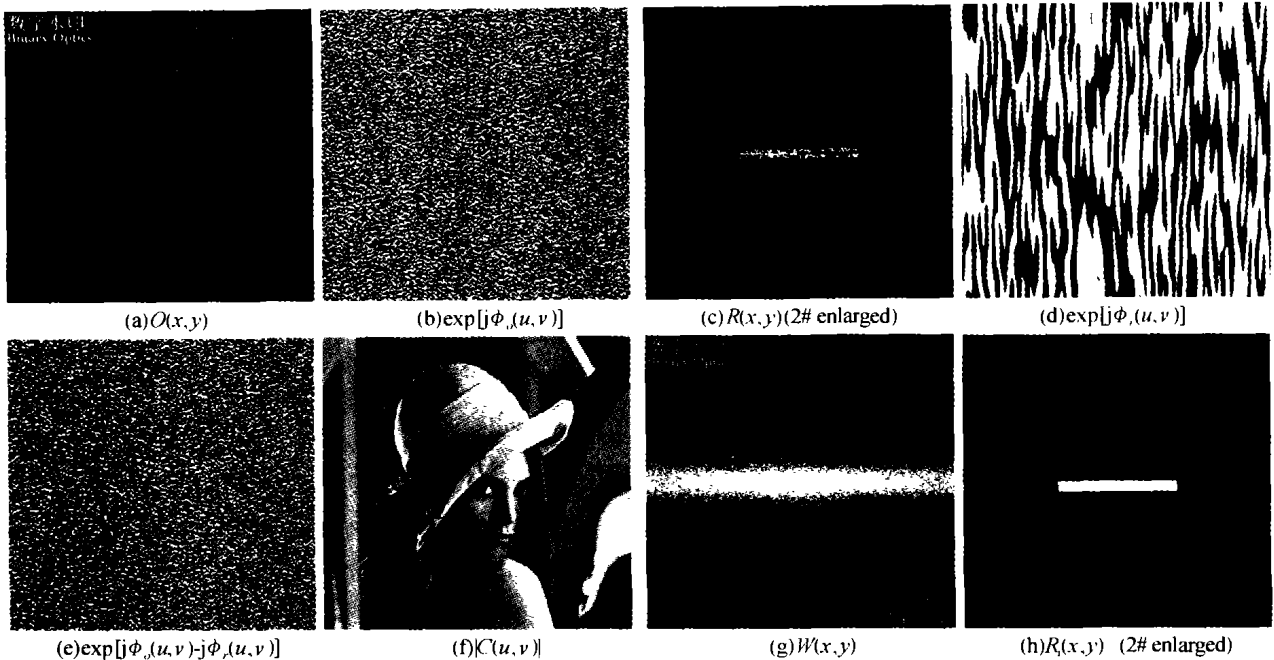


图 1 有密钥二元位相结构的全息水印编码与解码

Fig. 1 Encrypting and decrypting of hologram watermarking by using binary phase structures with phase key

$I[C(u, \nu)]$ 水印隐藏效果很好, 整个解码过程不依赖于原始图像. 解码后得到的水印信息, 用相关系数 C_R 和相对光学效率 Q 来评价水印提取质量. C_R 用于判断从宿主图像解码后在目标区域 Ω 内, 水印 $w(x, y)$ 与由二元位相结构 (插入宿主图像前) 再现像 $O_{i+1}(x, y)$ 之间的相关性, 由此确定是否能够解码以及解码后的水印相似性

可以看出, $R(x, y)$ 的结构设计使得 $\exp[j\phi_r(u, \nu)]$ 的正、负一级再现像相互补, 总的再现像成为一个叠加了噪声的均匀光场, 这样, 不可能从解码光场 $R_r(x, y)$ 中获得有关 $R(x, y)$ 的空间分布信息, 即在 $R(x, y)$ 的结构设计下, 两阶段位相结构使变换具有不可逆性. 由于 $R(x, y)$ 是条形设计, 解码后中央光场与水印光场在空间上是分离的, 减小了中央区域中边缘噪声对水印的影响. 图 1 的结果证明了理论的正确性. 表 1 给出了 $\alpha = 0.10$, $X = 9$ 像素下, 用不同 Y 尺寸的 $R(x, y)$ 制成的位相密钥对图 1(f) 的大信息量水印进行提取结果的相关系数 C_R , 水印提取质量基本不随 Y 尺寸而变化, 这样, 在 X 不变时, 我们就可以通过在 Y 方向上增加随机分布 $R(x, y)$ 的空间尺寸来提高位相密钥的安全性. $R(x, y)$ 的有限空间尺寸使其变换后位相分布在一定的区域内变化平缓, 解码时容许位相密钥与水印宿主图像之间有一定的位移量. 表 1 中看到, 随著 X 方向上的尺寸增大, 解码后的 C_R 逐渐下降, 表明靠近中央光场的水印提取质量下降.

$$C_R = \frac{\sum_{(x,y) \in \Omega} (A(x,y)B(x,y)) / \sqrt{\sum_{(x,y) \in \Omega} A^2(x,y) \sum_{(x,y) \in \Omega} B^2(x,y)}} \quad (8)$$

这里 $A = w(x, y) - \bar{w}(x, y)$; $B = O_{i+1}(x, y) - \bar{O}_{i+1}(x, y)$ 由式 (2) 和 (6), 水印提取的相对光学效率 Q 定义为, 含水印的宿主图像解码后在目标水印内的光强与二元位相结构 (插入宿主图像前) 在整个再现光场内的光强之比

$$Q = (2/\alpha) \sum_{(x,y) \in \Omega} w^2(x,y) / \sum_x \sum_y O_i^2(x,y) \quad (9)$$

式中乘以一个与水印含量相关比例系数 $(2/\alpha)^2$ 是为了方便与插入宿主图像前的二元位相结构衍射效率的比较. 图 1(g) 的相关系数 $C_R = 0.9906$, 图 1(h) 是 $\exp[j\phi_r(u, \nu)]$ 的远场衍射再现像 $R_r(x, y)$,

表 1 位相密钥的不同空间分布 $R(x, y)$ 的水印提取质量

Size of $R(x, y)$	9 × 9	9 × 39	9 × 69	9 × 99	9 × 129	9 × 159	9 × 189	9 × 249
C_R	0.9900	0.9903	0.9901	0.9906	0.9902	0.9904	0.9901	0.9902
Size of $R(x, y)$	5 × 99	7 × 99	9 × 99	11 × 99	13 × 99	15 × 99	17 × 99	19 × 99
C_R	0.9940	0.9921	0.9906	0.9880	0.9871	0.9855	0.9834	0.9814

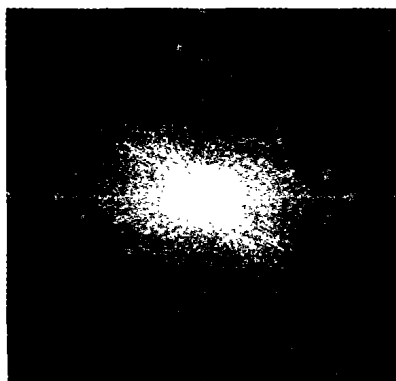
表 2 给出了平面波照明下的二元位相数字全息水印、直接傅里叶变换数字全息水印和具有位相密钥的二元位相数字全息水印的相关系数 C_R 和相对光学效率 Q 。在 $\alpha = 0.10$ 下,平面波照明的二元位相水印解码后的相关系数为 $C_R = 0.998$,表明解码过程对水印提取质量的影响很小,解码结果参见图 2(a);采用图 1(d)所示的位相密钥 ($R(x,y)$) 的尺寸为 9×99 其解码的相关系数 $C_R = 0.9906$,字符的解码质量很好,表明加密后的数字水印的解码质量基本不下降,相关系数略有下降的原因是位相密钥在解码过程中有相干噪声叠加在水印光场上。

表 2 $\alpha = 0.10$ 时不同编码方法下的水印提取质量

	binary phase with plane wavefront	direct FT with plane wavefront	binary phase with key
C_R	0.998	0.963	0.991
Q	1.55	0.103	1.59
η	0.356	0.356	0.356



(a) $W(x,y)$ with binary phase



(b) $W(x,y)$ with direct FT

图 2 数字全息水印的解码

Fig. 2 Decrypted results of hologram watermarking

从表 2 中看出,理论上,水印的相对光学效率 Q 应低于两阶段二元位相结构 $\exp [j\phi_0(u,v)]$ 衍射效率 η 的 4 倍,但实际相对光学效率 Q 高于理论值,表明解码过程中在水印图像上叠加了噪声;作为对比,对用随机位相分布调制后的图像直接傅里叶变换作为水印,不仅解码的相对光学效率很低,同时解码质量还受宿主图像结构的影响,许多字符被掩在噪声之中,导致解码质量下降,参见图 2(b)。由

于二元位相密钥的空间分布与宿主图像傅里叶变换的卷积作用,相对于平面波照明二元位相方法以及直接傅里叶变换方法,采用二元位相加密方法的解码光场中水印信息的相对强度要高得多。

随着水印信息量的减少,相应的水印含量 α 也可以降低,如果仅将图 1(a)中的左上角的大字母作为水印,在保证解码的相关系数 $C_R = 0.9906$ 时,水印含量 α 可降到 0.03,由于小信息量的二元位相编码的冗余度增加,水印的抗剪切、抗打印输出的性能也随著增高。因此,在二元位相加密的水印信息量与抗攻击性上应有所兼顾。

3 结论

我们提出的基于 $2/2$ 台阶的二元位相加密的数字全息水印方法,对大信息量水印具有很好的隐藏与解码质量,有效地提高了数字全息水印的安全性。因此,该方法可作为信息加密传递的重要手段和一种性能优越的数字全息水印方法。

参考文献

- 1 Bahram Javidi, Guanshen Zhang, Jian Li. Experimental demonstration of the random phase encoding technique for image encryption and security verification. *Opt Eng*, 1996, **35** (9): 2506 ~ 2512
- 2 Sherif Kishk, Bahram Javidi. Watermarking of three-dimensional objects by digital holography. *Opt Lett*, 2003, **28** (3): 167 ~ 169
- 3 Nobukatsu Takai, Yuto Mifune. Digital watermarking by a holographic technique. *Appl Opt*, 2002, **41** (5): 865 ~ 873
- 4 Ferri L C, Mayerhofer A, Frank M. Biometric authentication for ID cards with hologram watermarks. *Proc of SPIE*, 2002, **4675**: 629 ~ 640
- 5 Herzig H P, Ed. Micro: optics elements, systems and applications. Taylor & Francis Ltd., 1997
- 6 Gerchberg R W, Saxton W O. A practical algorithm for the determination of phase from image and diffraction plane pictures. *Optik*, 1972, **35**: 237 ~ 246
- 7 Johansson M, Bengtsson J. Robust design method for highly efficient beam-shaping diffractive optical elements using an iterative-Fourier-transform algorithm with soft operations. *J of Modern Optics*, 2000, **47** (8): 1385 ~ 1397
- 8 Philip Birch, Rupert Young, Maria Farsari, et al. A comparison of the iterative Fourier transform method and evolutionary algorithms for the design of diffractive optical elements. *Optics and Lasers in engineering*, 2000, **33**: 439 ~ 448
- 9 Wyrowski F, Bryngdahl O. Iterative Fourier transform algorithm applied to computer holography. *J Opt Soc Am A*, 1988, **5** (7): 1058 ~ 1065
- 10 Liu Fumin, Zhai Honchen, Yang Xiaoping, et al. Amplitude fitting to binary images reconstructed by kinoforms. *Acta Optica Sinica*, 2003, **23** (6): 666 ~ 670

A Digital Hologram Watermarking with Large Information Contents Based on Binary Phase Encryption Method

Chen Linsen, Zhou Xiaohong, Shao Jie

Key laboratory of modern optical technology, Institute of information optical Engineering, Soochow University, Suzhou 215006

Received date: 2004-04-05

Abstract A digital hologram watermarking with a phase encryption feature is proposed based on a binary optical phase retrieval algorithm. The watermark has been encoded with the binary optical phase algorithm and encrypted with a binary phase key. Comparing to the digital hologram watermarking with binary phase structure under the plane illumination, the security of the proposed method is greatly improved by using a binary phase key while the quality of decrypted watermark with large information contents is almost maintained unchanged. The decrypting processing is independent of original host image. The quality of decrypting watermark under the different sizes of encryption keys has been discussed. The simulation results prove the theoretical analysis.

Keywords Binary optics; Phase encoding; Digital hologram watermarking



Chen Linsen was born in January of 1961. He received BS degree in 1982 and Master degree in 1986 from Soochow University. Now he is a professor in the Institute of Information Optical Engineering of Soochow University. His research activities are involved in the fields of digital photolithographic system, optical information processing, binary optics and holography. He won the National Science and Technology Award in 2002 for his successful work in digital laser photolithographic system.