# 基于三维成像技术的安全二维码

刘轶群,魏悦川,张敏情,周潭平,杨晓元

(武警工程大学 密码工程学院 网络与信息安全武警部队重点实验室,陕西 西安 710086)

**摘 要:** 扫码移动支付存在的安全漏洞已成为电子支付安全迫切需要解决的问题。提出了一种基于三维成像技术的安全二维码系统。首先,利用集成成像技术生成三维数字水印,作为商家标识;其次,对标识进行基于身份的数字签名;再次,在菲涅耳域,利用安全二维码系统把携带有签名信息的三维数字水印,经过压缩编码后隐藏到二维码中。最后,用户扫码识别并提取出隐秘数据,同时验证签名信息,如果验证通过,计算重构并显示出三维数字水印图像,经用户鉴别后确认是否支付,完成双向认证过程。实验结果表明,采用基于身份的数字签名技术可以有效地防止三维数字水印被篡改、伪造、无正当理由式否认等情况。所提方法不仅增强了扫码移动支付的安全性,而且提高了系统的实时性和便捷性。多个系统参数组合作为密钥,有效地增加了密钥维度,拓宽了密钥空间,增加了攻击的难度,提高了系统安全性与稳健性。双向认证可信的扫码支付既确保了用户个人资金的安全,也维护了商家的信誉和财产安全。

**关键词:** 安全二维码; 三维认证; 集成成像技术; 三维光学信息隐藏; 双向认证

**中图分类号:** O438 **文献标志码:** A **DOI:** 10.3788/IRLA201948.0503003

# Secure quick response code based on the technology of three-dimensional imaging

Liu Yiqun, Wei Yuechuan, Zhang Minqing, Zhou Tanping, Yang Xiaoyuan

(Key Laboratory of CAPF Network & Information Security, Cryptology Engineering College, Engineering University of the Armed Police Force, Xi′an 710086, China)

**Abstract:** The security of electronic payment has become an urgent problem. A secure Quick Response (QR) code system was proposed based on the technology of three-dimensional (3D) imaging and 3D authentication information. Firstly, the integral imaging technology was used to generate 3D digital watermark as the logo of the merchant. Secondly, identity based digital signature was carried out. Then, in the Fresnel domain, the 3D digital watermark with signature information was carried by using a secure QR code system, which was then compressed and hidden in the QR code. Finally, the users scan QR code to identify and extract the hidden data. If the signature information of verification was confirmed by users, the algorithm of reconstruction was executed, and the 3D digital watermark images were displayed. The payments were confirmed after the users were authenticated. The process of interactive authentication

**收稿日期:** 2018-12-12; **修订日期:** 2019-01-16

**基金项目:** 国家自然科学基金(61379152,61572521);陕西省自然科学基金(2016JQ6030,2015JM6353)

**作者简介:** 刘轶群(1979-),男,博士,主要从事光学信息安全、三维成像与显示方面的研究。Email:wjliuyiqun@126.com

was completed. According to the results of experiments, the schemes can effectively prevent the 3D digital watermark from being tamper-bent, falsified, and unjustified. The proposed method not only enhances the security of scanning mobile payment, but also improves the real-time and convenience of the system. When multiple parameters of the proposed system are combined as keys, the dimensions of keys are effectively increased. The key space is broadened. The difficulty of illegal attack is enhanced, and the safety and stability of the system are improved too. It can protect the security of personal fund, and also maintain the reputation and property security of enterprises.

**Key words:** secure QR code; 3D authentication; integral imaging technology; 3D optical information hiding; interactive authentication

## 0 引 言

在现代社会生活中，人们常常扫描二维码进行便捷的移动支付，然而，这种支付方式存在着被篡改、被伪造与木马病毒诱导链接等安全漏洞,不仅造成了用户财产损失，也对用户鉴别标识的真假提出了较高要求。

二维码是用某种特定的几何图形，按一定规律在平面上分布黑白相间的图形来记录数据符号信息。虽然二维码能有效地存储信息,但是它无法确保信息来源的真实可靠，常常导致数据很容易被篡改与伪造。在多媒体网络环境中,发挥信息安全技术、密码编码方法和数字版权保护手段等优势，可以确定数字多媒体本文的作者、版权归属与权利信息等,保护合法登记的权益人的利益与声誉[1-4]。Huang Hsiang-Cheh 等提出了一种基于直方图平移的可逆信息隐藏的 QR 安全保护技术[5],但是嵌入隐秘数据量太多，降低了 QR 图像质量和识别准确率。由于 QR 码的冗余数据少,密文信息容量较明文信息增加较多,系统抗攻击性能较弱,导致方法的实用性不够强。基于干涉原理的多图像加密系统,实现对 QR 码的保护[6]。然而,隐秘数据的恢复质量较低,方法的实用性方面还存在着不足。利用全息技术可以产生的三维全息彩色图像作为防伪认证凭据，防止对机密文档和认证信息的非法复制。基于全息术的图像加密与信息隐藏技术,全息技术需要相干光源,在生成动态三维图像的过程中，它还会受到空间光调制器(Space Light Modulation,SLM)和计算机处理速度等因素的影响。存在着信息存储效率低、全息图像数据量太大、设备成本较高、图像分辨率较低、成像尺寸偏小、动态实时性差、对环境条件要求限制多、抵抗相位索引恢复攻击能力弱、对光学仪器精密程度要求高、制作耗时长、现地组建流程繁琐[7]等现实问题。显然,全息技术用于实时性移动支付还有一些技术难点需要解决。

在信息安全和多媒体信息隐藏研究领域，采用信息光学理论与技术,融合光的相干干涉成像、非相干干涉成像、衍射、计算全息等计算过程,对光波的波长、振幅、相位、偏振态、空间频率、光学透镜的焦距、光学图像的光强、相位,以及光学元器件的特性参数等进行多维编码，能够有效地实现数据加密和信息隐藏[8-12]。集成成像技术是一种裸视 3D 显示技术,其成像与显示分为两个阶段:一、集成成像系统的记录阶段;二、集成成像系统的 3D 显示阶段[13-17]。Hwang Dong-Choon 等[18]指出集成成像技术可用于数字水印,在攻击可控的情况下,所提出的水印生成与提取系统具有实用价值。Li Xiaowei 等[19-20]采用一种无透镜集成成像技术进行图像加密。上述研究成果表明集成成像技术适用于光学图像加密和光学信息隐藏,但是从现有文献来看,还缺少把集成成像技术运用于 QR 码安全保护的研究工作。为提高移动支付的安全性、实时性、微型化和便捷性,特别是运用集成成像三维新媒体进行光学图像加密和光学信息隐藏方面的研究工作还做得不够,非常值得继续深入地开展研究。

文中提出并设计了一种基于三维成像技术的安全二维码系统。半实物仿真实验结果表明,采用基于身份的数字签名技术可以有效地防止三维数字水印

被篡改、伪造、无正当理由式否认等情况。新方法具有双向认证,实时性高;光学图像信息隐藏技术嵌入率高;认证的信息可以兼容二维或三维图像;采用数字签名技术对三维图像进行签名与验证; 用户体验感和交互性好等优点。

## 1 主要原理

基于三维成像技术的安全二维码系统的实现流程如图 1 所示。首先,利用基于智能深度反转模型的计算集成成像技术生成三维图像 (三维数字水印),作为商家标识;其次,对标识进行数字签名;再次,携带有签名信息的三维数字水印, 经过霍夫曼压缩编码后,在菲涅耳域采用三维数字水印的嵌入算法,有效地把三维隐秘数据隐藏到二维码中;最后,用户扫码识别并提取出三维数字水印, 验证公告板中信息和签名信息正确后, 利用集成成像显示技术重构显示出三维数字水印,用户认证成功,确认支付操作,完成双向认证过程。否则,退出访问。文中的二维码中除了包含基本信息以外, 还包含商户的 ID 信息,作为公钥。

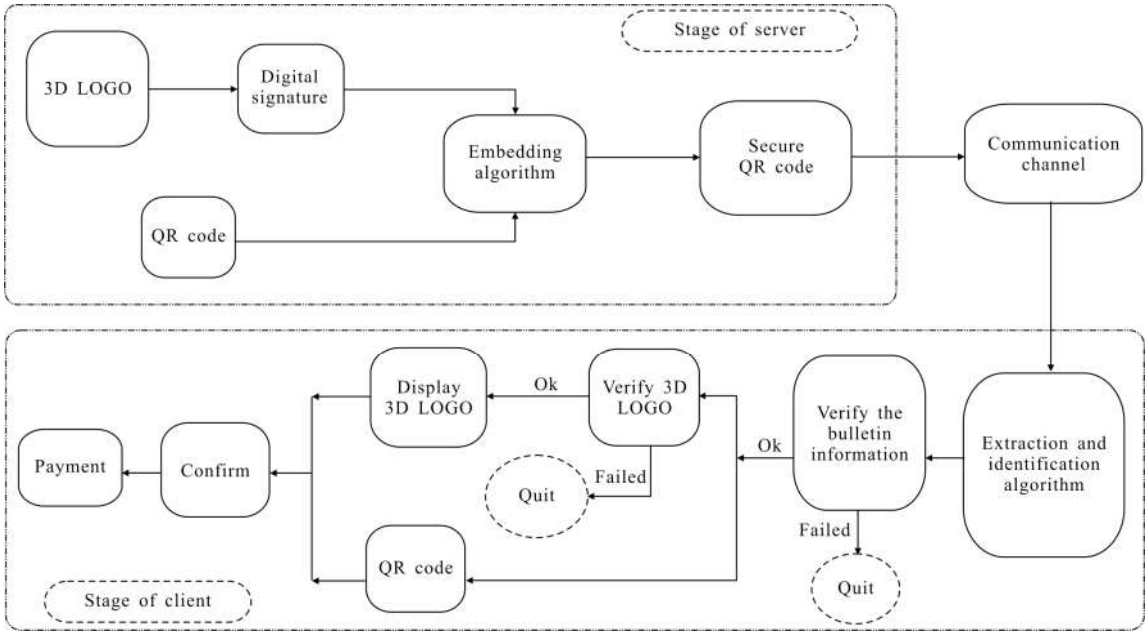


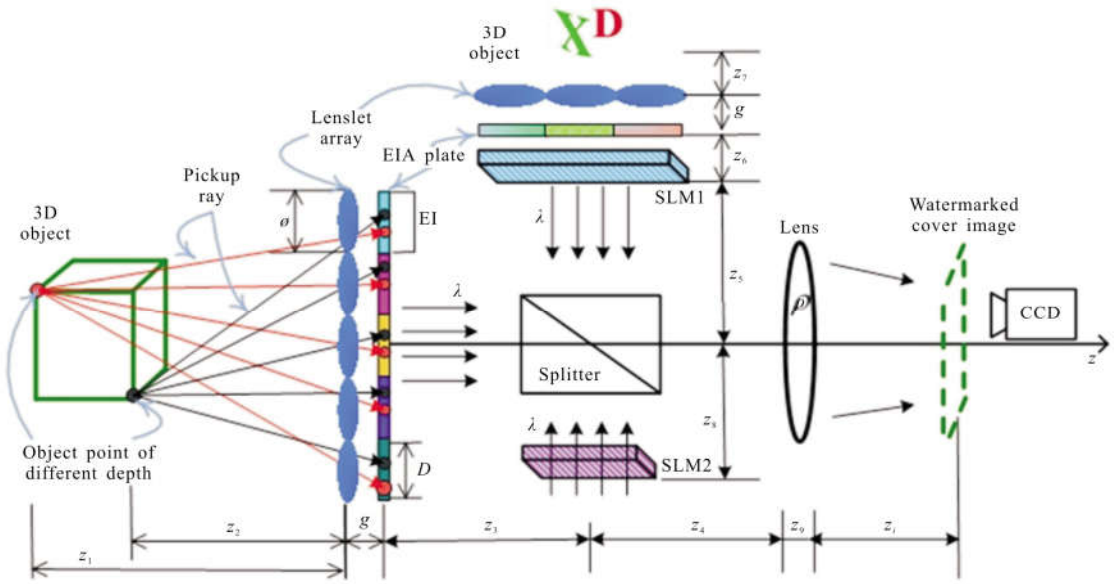

图 1 安全二维码的流程图

Fig.1 Flow diagram of secure QR code

### 1.1 系统组成与实现过程

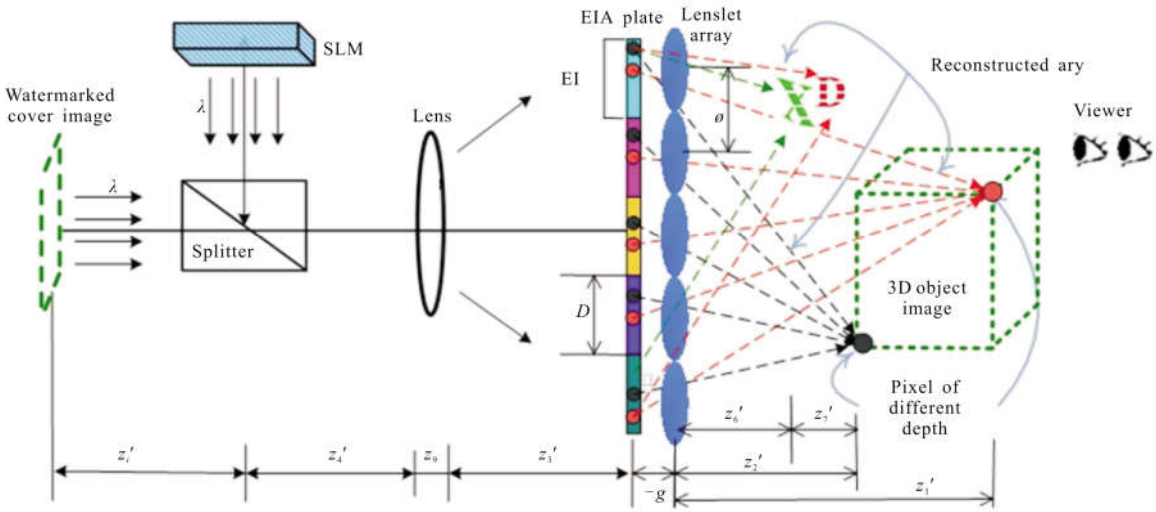
基于三维成像技术的安全二维码, 由三维数字水印记录与嵌入子系统、三维数字水印提取与显示子系统两部分组成[13-14],如图 2 所示。假设图 2(a)所示的三维数字水印记录与嵌入子系统由微透镜阵列、分光器、随机相位掩模板、成像透镜、CCD 相机等组成。$Z_i, i=1,2,\cdots, i\in Z^+$表示不同平面之间距离,$g$ 表示针孔阵列到微单元图像平面的距离,$D$ 表示微单元图像的尺寸,$\phi$ 表示微透镜中心之间间距,成像透镜 $\rho$ 的焦距为 $f$,其透过率频谱函数为 $T(s,t;f)$。系统产生的含三维隐秘数据的 QR 码被 CCD 相机记录存储。在此嵌入过程中,集成成像的 EIA 图像具有类全息特性,获得一部分的 EIA 图像,可以恢复显示出三维物体的图像,而与全息图相比,图像大小明显减少,存储容量也降低了。采用霍夫曼编码对 EIA 图像数据进行压缩编码,再嵌入 QR 码中,从而整体减少了隐秘数据的嵌入量, 却不会明显降低三维图像质量。

在图 2(b)所示的三维数字水印提取与显示子系统中, 合法授权用户接收到通信链路传递过来的含水印的加密载体图像, 然后减去随机相位掩模板在上述嵌入过程中的贡献, 利用离散菲涅耳衍射的逆变换提取出水印, 使用集成成像的计算重构算法显示出三维数字水印对应的三维物体图像。从三维数




(a) 三维数字水印记录与嵌入子系统

(a) Principle of pickup and embedding subsystem of 3D digital watermarking




(b) 三维数字水印提取与显示子系统

(b) Principle of extraction and display subsystem of 3D digital watermarking

图 2 三维数字水印系统原理示意图

Fig.2 Schematic diagrams of principle of 3D digital watermarking system

字水印的提取过程来看，三维数字水印算法在提取水印时不需要原始载体图像,因此属于盲水印算法。在提取出三维数字水印微单元图像的基础上，利用集成成像的计算重构算法还原显示出三维数字水印的图像。

### 1.2 公告板

公告板的作用在于防止不法分子，利用自己的二维码替换商户的合法二维码,从而获利。公告板包含每个商家的一个公钥(ID)、序号、商店名称等信息。在用户跳转到对应的网页前,用户和商家会做公

告板的信息核对工作。首先,客户端主动识别出二维码中商家的 ID 信息。其次,客户端自动跳转到公告板,并查询显示商家 ID 对应的其他信息。最后,用户和商家核对公告板中的序号等其他信息是否与商家本身的版权信息相同。假如相同,则确认该二维码是商家生成的;否则二维码可能是被替换过的。需要注意,其中的序号信息对于每个商家都是不一样的。序号信息也可使用唯一表示商家身份的手机号码进行区分。

### 1.3 数字签名

数字签名是为了防止三维图像(三维数字水印)在网络传输中被非法用户篡改,非法伪造,以及商家以某种理由进行否认等情况的出现。考虑到公钥密码算法处理效率低,会造成签名与验证过程比较耗时,为解决这个问题,采用单向散列函数(哈希函数)求出三维图像的散列值(哈希值),然后对散列值(哈希值)进行签名与验证。具体步骤如下:(1) 商家申请生成公私钥对,其中公钥为标识商家的身份信息,将身份信息发布到公告板。(2) 商家用单向散列函数计算三维图像的散列值。(3) 商家用自己的私钥对散列值进行加密。用私钥加密散列值所得到的密文就是商家对这条散列值的签名,因为只有商家才持有自己的私钥,因此,除了商家以外,其他人无法生成相同的签名(密文)。(4) 商家将三维图像和签名发送给用户。(5) 用户查询公告板,使用商家的公钥(也就是商家的 ID)对签名信息进行认证。如果签名用商家的私钥进行加密,生成密文(签名),那么用商家的公钥能够正确解密,解密结果为三维图像的散列值。如果提取出的签名不是用商家的私钥进行加密而得到的密文,那么就无法使用用户的公钥正确解密。(6) 用户将签名解密后得到的散列值与商家直接发送的三维图像的散列值进行比对。如果两者一致,则签名验证成功;否则,验证失败。

## 2 半实物仿真实验结果分析

文中使用 MATLAB 软件进行了计算光学实现与数值验证,减少了实际光学信息隐藏系统的复杂性,避免光学成像器件之间存在的匹配问题,降低了实验成本,提高了系统的有效性。然而,XD 图像的立体显示,选用手机与透镜阵列实物测试方式进行观测与分析。XD 微单元图像作为水印图像,大小为 64 pixel×64 pixel,图像格式类型为 PNG。实验环境与仪器设备参数包括:微透镜阵列由 60×60 个直径为 0.983 6 mm 微透镜组成,计算机 CPU 型号为 Intel i7-2630M,手机型号为 Huawei P7,手机操作系统版本为 Android 4.4,应用程序开发软件为 MATLAB2010,Eclipse for Android Developer。

使用 MATLAB 编写主程序,然后用 MATLAB Builder for Java 将其打包成 jar 包供 APP 程序调用,实现加解密、嵌入与提取、三维显示等功能。主要实验步骤与结果如下:

(1) 生成测试所需的 QR 码,打开安全二维码扫描软件,如图 3 所示。


(a) 测试生成的 QR 码 (b) 软件主界面

(a) QR code generated for test (b) Main interface of software

图 3 测试准备

Fig.3 Preparatory work of experiment

(2) 对已加入验证信息的二维码进行扫描。

(3) 扫描出验证结果,把微透镜阵列紧贴手机屏幕,从不同的视点观看立体显示效果,如图 4 所示。图像分辨率低是因为显示 3D 图像必须通过微透镜阵列来观看,观看特性参数与微透镜阵列的工艺水平等都会影响 3D 图像的显示质量,而且 3D 图像的一部分重构面超出图像深度范围,因此,图像色彩存在一定的失真,图像分辨率低,变得有些模糊。但是重构显示的三维物体的分辨率、深度和视场范围都符合人类视觉模型的要求,满足集成成像系统的图像质量主观评价标准。集成成像系统的参数是否考虑作为密钥空间的维度,由密文发送方选择确定。

EIAs 图像具有类全息图像的特性,使得微单元图像作为三维水印具有更强的抗攻击性能。系统的多维密钥参数增强了安全性和稳健性[14,18]。

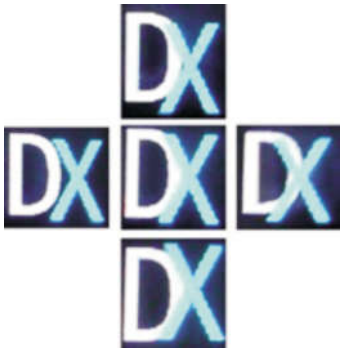


图 4 不同视角显示三维数字水印

Fig.4 Display 3D digital watermarking from different viewing angles

(4) 确认安全,登陆网站,如图 5、6 所示。


图 5 安全登陆网站

Fig.5 Login the website securely


图 6 验证成功后连接的网页

Fig.6 Link the webpage after successful verification

(5) 当扫描未知二维码,由于不含验证信息,给出验证无法通过的提示,自动退出。

## 3 结 论

文中提出了一种基于三维成像技术的安全二维码系统,设计了光学隐秘图像信息隐藏算法,实现了对二维码的安全保护,增强了扫码移动支付方式的安全性。发挥光学的并行性优势,提高了处理与实现的实时性和便捷性,增强了系统的安全性与稳健性。双向认证可信的扫码支付确保了商家与消费者的资金安全。

虽然提出与设计的系统验证了方法的可行性与合理性,但是安全性分析与验证工作仍然不够充分,还需要增加三维数字水印样本的数量与图像大小提高系统的普适性,从而将研究成果转换为实用型产品,服务社会与用户。

**参考文献:**

[1] Langelaar G, Setyawan I, Lagendijk R. Watermarking digital image and video data [J]. ***IEEE Signal Processing Magazine***, 2000, 17(5): 20-46.

[2] 沈昌祥, 张焕国, 冯登国, 等. 信息安全综述 [J]. 中国科学 E 辑: 信息科学, 2007, 37(2): 129-150.

[3] Song Chunlin, Sudirman Sud, Merabti Madjid. A robust region-adaptive dual image watermarking technique [J]. ***Journal of Visual Communication and Image Representation***, 2012, 23(3): 549-568.

[4] Nezhadarya Ehsan, Ward Rabab K. Multiscale derivative transform and its application to image watermarking [J]. ***Digital Signal Processing***, 2014, 33(6): 148-155.

[5] Huang Hsiangcheh, Chang Fengcheng, Fang Waichi. Reversible data hiding with histogram-based difference expansion for QR code applications [J]. ***IEEE Transactions on Consumer Electronics***, 2011, 57(2): 779-787.

[6] Wang Hongjuan, Wang Zhipeng, Zhang Yingying, et al. Using QR codes in multi-image optical interference encryption system to reconstruct high quality original information [J]. ***Acta Optica Sinica***, 2014, 34 (9): 0907001. (in Chinese)
王红娟, 王志鹏, 张颖颖, 等. 利用 QR 码在光学干涉多图像加密系统中实现信息高质量恢复 [J]. 光学学报, 2014, 34(9): 0907001.

[7] Kim Soogil. Analysis of effect of phase error sources of

polarization components in incoherent triangular holography [J]. ***Journal of the Optical Society of Korea***, 2012, 16(3): 256-262.

[8] Muniraj Inbarasan, Kim Byoungho, Lee Byung-Guen. Encryption and volumetric 3D object reconstruction using multispectral computational integral imaging [J]. ***Applied Optics***, 2014, 53(27): 25-32.

[9] Piao Yongri, Shin Donghak, Kim Eunsoo. Robust image encryption by combined use of integral imaging and pixel scrambling techniques [J]. ***Optics and Lasers in Engineering***, 2009, 47(11): 1273-1281.

[10] Kishk S, Javidi B. Watermarking of three-dimensional objects by digital holography [J]. ***Optics Letters***, 2003, 28(3): 167-169.

[11] Peng X, Cui Z, Tan T. Information encryption with virtual-optics imaging system [J]. ***Optics Communications***, 2002, 212(4-6): 235-245.

[12] Kim K T, Kim J J, Kim E S. Information hiding technique using optical correlators [C]//SPIE. 2001: 565-574.

[13] Zhang Jianlei, Wang Xiaorui, Liu Yiqun, et al. Wide-viewing integral imaging display with programmable directional backlight [J]. ***Optik-International Journal for Light and Electron Optics***, 2016, 127(20): 9244-9249.

[14] Liu Yiqun, Zhang Jianqi, Yang Xiaoyuan, et al. An encryption method of the three-dimensional optical image[J]. ***Journal of Sichun University(Engineering Science Edition)***, 2016, 48(1): 126-131. (in Chinese)
刘轶群, 张建奇, 杨晓元, 等. 一种 3 维光学图像加密方法[J]. 四川大学学报(工程科学版), 2016, 48(1): 126-131.

[15] Liu Yiqun, Wang Xiaorui, Zhang Jianqi, et al. An improved security 3D watermarking method using computational integral imaging cryptosystem [J]. ***International Journal of Technology and Human Interaction***, 2016, 12(2): 1-21.

[16] Wang Xiaorui, Guo Qiang. Enhancing computational integral imaging performance using an interpolation method based on non-zero-pixel derivation[J]. ***Appl Opt***, 2010, 49(20): 3997-4003.

[17] Wang Xiaorui, Bu Qingfeng, Zhang Dongyang. Method for quantifying the effects of aliasing on the viewing resolution of integral images [J]. ***Opt Lett***, 2009, 34(21): 3382-3384.

[18] Hwang Dongchoon, Shin Donghak, Kim Eunsoo. A novel three-dimensional digital watermarking scheme basing on integral imaging [J]. ***Optics Communications***, 2007, 277(1): 40-49.

[19] Li Xiaowei, Wang Qionghua, Kim Seoktae, et al. Encrypting 2D/3D image using improved lensless integral imaging in Fresnel domain [J]. ***Optics Communications***, 2016, 381: 260-270.

[20] Zhao Min, Xiong Zhaolong, Xing Yan, et al. Real-time integral imaging pickup system based on binocular stereo camera [J]. ***Infrared and Laser Engineering***, 2017, 46(11): 1103007. (in Chinese)
赵敏, 熊召龙, 邢妍, 等. 采用双目立体相机的实时集成成像拍摄系统[J]. 红外与激光工程, 2017, 46(11): 1103007.