图文信息技术

基于印刷量子点的多重组合信息可靠性编解码算法

王育军，曹鹏
（北京印刷学院 高端印刷装备信号与信息处理北京市重点实验室，北京 102600）

摘要：目的 针对印刷量子点的点阵图像用于实现信息记录、信息隐藏和信息防伪时，存在因打印信息污损和图像识读信息误判引起的误码率高这一突出问题，设计一种信息可靠性编解码算法。**方法** 该算法采用二维奇偶校验码+BCH 码+交织编码+帧同步组合方式。**结果** 经实验测试验证，该组合方式得到的印刷量子点图像与汉明码和 RS 编码相比，随机性更高，具有更加突出的纠错能力，信息解码识读速率更快、鲁棒性更好。**结论** 该算法可很好地解决印刷量子点信息的突发性错误和随机性错误，同时也解决了印刷量子点图像在信息防伪领域应用推广的瓶颈问题，扩展信息增值服务功能。

关键词：可靠性编码；半色调网点；信息防伪；信息隐藏；点阵图像
中图分类号：TN911.3 **文献标识码：**A **文章编号：**1001-3563(2021)19-0192-12
DOI：10.19554/j.cnki.1001-3563.2021.19.026

Reliability Encoding and Decoding Algorithm of Multiple Combination Information Based on Printed Quantum Dots

WANG Yu-jun, *CAO Peng*
(Beijing Key Laboratory of Signal and Information Processing for High-end Printing Equipment, Beijing Institute of Graphic Communication, Beijing 102600, China)

ABSTRACT: In order to realize information recording, information hiding and information anti-counterfeiting, a kind of information reliability codec algorithm is designed to solve the prominent problem of high bit error rate caused by the stain of printed information and the misjudgment of image reading information when the dot matrix image of printed quantum dots is used to realize information recording, information hiding and information anti-counterfeiting. The algorithm adopts the combination mode of two-dimensional Parity Check code, BCH code, interleaved code and frame synchronization. The experimental results show that compared with Hamming code and RS code, the image of printed quantum dots obtained by the combined coding method has higher randomness, more prominent error correction ability, faster information decoding and reading speed and better robustness. This algorithm can well solve the sudden error and random error of printed quantum dot information, and also solve the bottleneck problem of the application and promotion of printed quantum dot image in the field of information anti-counterfeiting, and expand the value-added service function of information.

KEY WORDS: reliability coding; halftone dots; information anti-counterfeiting; information hiding; dot matrix image

收稿日期：2020-12-04
基金项目：国家自然科学基金面上项目（61972042）；北京市基金-市教委联合项目（KZ202010015023）；北京印刷学院校级项目（Ef202001）
作者简介：王育军（1996—），男，北京印刷学院硕士生，主攻数字图像处理与现代通信技术的交叉应用。
通信作者：曹鹏（1969—），男，博士，北京印刷学院教授，主要研究方向为 ICT 与印刷技术交叉创新。

半色调技术[1—4]在印刷防伪领域起着至关重要的作用，主要应用于版权标识、身份证件和印刷制品等产品的信息防伪与信息隐藏。半色调加网与信息隐藏技术[5]就是其中一项关键和核心技术。按照加网方式的不同可将半色调信息防伪技术分为调幅加网技术[6]、调频加网技术[7]和混合加网技术[8]，这些技术利用人眼视觉识别的低通滤波性，通过改变半色调网点的大小、形状、布局、遮盖率和调制方式等因素有效解决原始连续调图像再现的问题，但这些技术在进行信息调制时比较复杂，对信息识读与提取比较困难，并且难以克服误码问题。

基于半色调网点的点阵图像空间位置信息的数据记录与信息隐藏方法，具有良好的抗复制、信息隐藏效果好、数据记录容量大等显著优势，已成为印刷信息防伪领域的研究热点。Fu 等[9]针对半色调图像，提出一种高容量的数据隐藏智能对切换（DHSPT）技术，该技术通过半色调图像的伪随机位置对数据进行隐藏，可以隐藏大量的数据且视觉质量很好。Kim 等[10]提出了一种将（15,11）汉明编码与误差扩散相结合的半色调信息隐藏技术，这种技术可以在保证视觉质量的情况下具有较高的数据嵌入能力，且具有一定的纠错能力。MA 等[11]将原始图像分为用来承载待隐藏数据的主图像和防止图像质量下降的从图像，通过汉明编码将待隐藏的信息嵌入主图像中，这种方法嵌入的效率较高且能保证视觉质量。Jana 等和 Cao 等[12—14]将（7,4）汉明编码应用到信息隐藏，实现很好的纠错能力，并且都得到了很好的防伪效果。Lien 等[15]通过汉明编码将数据隐藏在半色调图像的像素块中，这种方法不仅能提高半色调图像的视觉质量，而且可以从局部篡改图像中恢复原始数据信息。葛乃馨[16]研究了基于网点形状的半色调信息隐藏算法以及基于抗打印-扫描半色调水印的防伪方案，分析防伪信息在半色调图像中的隐藏性能，并且利用网点模板筛选出隐藏信息网点位置来提取信息。刘丽和杨文杰等[17]综述了信息技术在印刷包装防伪上的应用研究进展，介绍基于图像处理技术的印刷包装防伪应用，拓展信息技术在印刷包装防伪上的应用领域。陈方方[18]将水印信息以 FM 网点的形式按灰度相当、纹理近似的原则调制 AM 网点图像，达到了水印信息植入和抗复制目的，并且通过构建缩微文字点阵字库模版，基于灰度和形态双重匹配原则，将缩微文字以微结构纹理形式植入载体图像，在完美再现半色调图像的同时，实现了以缩微文字为纹理的印刷防伪目的。朱建乐[19]研究了一种基于 BCH 码+奇偶校验码的印刷量子点信息防伪与信息隐藏算法，得到的图像是基于 3×3 单位像素的印刷量子点图像，实现了一定的信息防伪的功能。

文中提出了一种基于印刷量子点的多重组合信息可靠性编解码算法。印刷量子点是一种在打印信息防伪领域中的最小成像单元——1×1~2×2 单位像素的半色调网点。文中研究的印刷量子点为单个像素（成像单元为 1×1）且不可再分的最小成像单元，通过将二维奇偶校验、BCH 编码、交织编码和帧同步编码进行组合，实现用印刷量子点记录信息数据，并且可以截取局部印刷量子点点阵掩膜图像（印刷量子点图像）进行信息解码识读。该印刷量子点图像的加网方式可以采用二次 FM 和 FM-AM 混合加网的方式实现。分析了 BCH 码、汉明码和 RS 码的性能，借助 Matlab 工具进行仿真验证。

1　编解码方案设计

1.1　编码方案设计

1.1.1　BCH 编码原理

BCH（Bose-Chaudhuri-Hocquenghem）码[20]是一类重要的循环码，能够纠正多个随机错误，而且也适用于纠正突发错误。这类码由 Hocquenghem 于 1959 年首次提出[21]，Bose 和 Chaudhuri 在 1960 年也独立提出了这种码[22]。BCH 码可以用有限域 GF(q^m)（$m\geqslant 3$ 为任意正整数）中生成多项式 $g(x)$的根来表示：

$$g(x)=LCM[m_1(x),m_3(x),\cdots,m_{2t-1}(x)] \tag{1}$$

式中：t 为纠错的数量；$m_i(x)$ 为素多项式（i=1,3,…,2t−1）；LCM 为取最小公倍数。

根据生产多项式以及循环码的循环移位特性可以构造 BCH 码的生成矩阵 $\boldsymbol{G}$。若设 $C(x)=q(x)g(x)$是 BCH 码的任一码字，则 $\alpha,\alpha^3,\cdots,\alpha^{2t-1}$ 为码多项式 $C(x)$的根，即若多项式为：

$$C(x)=c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\cdots+c_1x+c_0 \tag{2}$$

则有：

$$C(\alpha^i)=c_{n-1}(\alpha^i)^{n-1}+c_{n-2}(\alpha^i)^{n-2}+\cdots+c_1(\alpha^i)+c_0=0 \tag{3}$$

其中，$i=1,3,\cdots,2t-1$。根据 $CH^{\mathrm{T}}=0$ 可知 BCH 码的校验矩阵 $\boldsymbol{H}$ 为：

$$\boldsymbol{H}=\begin{bmatrix}\alpha^{n-1} & \alpha^{n-2} & \cdots & \alpha & 1\\ (\alpha^3)^{n-1} & (\alpha^3)^{n-2} & \cdots & \alpha^3 & 1\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ (\alpha^{2t-1})^{n-1} & (\alpha^{2t-1})^{n-2} & \cdots & \alpha^{2t-1} & 1\end{bmatrix} \tag{4}$$

对于定义在 GF(2^3)上的二元本原 BCH 码，m=3，α 为 GF(2^3)上的本原元，GF(2^3)上的本原多项式为 $p(x)=x^3+x+1$。校验元的数量为 mt=3，得到纠错能力 t=1 的(7,4,1)BCH 码，其生成多项式为 $g(x)=x^3+x+1$，根据表 1 中 GF(2^3)的元素列表的形式，可以将(7,4,1)BCH 码的校验矩阵 $\boldsymbol{H}$ 写为：

表 1　GF(2^3)的元素
Tab.1 List of elements for GF(2^3)

幂次 α^k	α 的多项式	多项式系数	十进制表示	最小多项式
α^0	1	001	1	$x+1$
α^1	α	010	2	x^3+x+1
α^2	α^2	100	4	x^3+x+1
α^3	$\alpha+1$	011	3	x^3+x^2+1
α^4	$\alpha^2+\alpha$	110	6	x^3+x+1
α^5	$\alpha^2+\alpha+1$	111	7	x^3+x^2+1
α^6	α^2+1	101	5	x^3+x^2+1

$$\boldsymbol{H}=[\alpha^6,\alpha^5,\alpha^4,\alpha^3,\alpha^2,\alpha,1]=\begin{bmatrix}1&1&1&0&1&0&0\\0&1&1&1&0&1&0\\1&1&0&1&0&0&1\end{bmatrix} \tag{5}$$

1.1.2　方案设计

印刷量子点生成图像在打印或光学图像采集过程中存在量子点污损和误判问题，为了解决由于污损和误判而导致的高误码率问题，需要对印刷量子点图像的生成过程进行可靠性编码研究。这种可靠性编码方案包括如下所述。

1）对待隐藏的明文信息进行预处理，使之成为规范化的二进制数据信息。

2）为保证信息安全，需要对预处理后的二进制数据进行 DES 加密[23]，生成十六进制的密文信息，再将其转换为二进制数据码流。

3）对加密后的一维数据进行串并变换，使之变成二维数据，再对二维数据进行二维奇偶校验编码[24]，得到校验数据信息，实现内层检错的功能。

4）对二维奇偶校验编码后的数据进行 BCH 编码，得到印刷量子点阵本原图像，实现外层纠错的功能。

5）采用帧同步位作为空间矢量特征来记录印刷量子点位置信息，可采用巴克码进行帧同步位信息的记录。

6）为保证与商标等载体图像尺寸匹配，需要对得到的印刷量子点阵本原图像进行周期性复制拼接，得到复制拼接后的印刷量子点阵本原图像

7）利用交织编码的迭代处理[25]进行伪随机信息置乱，解决图像连串成片的误码问题。

8）将置乱后的印刷量子点点阵本原图像进行数据可视化处理，得到码云原图（印刷量子点图像）。

具体编码设计方案见图 1。

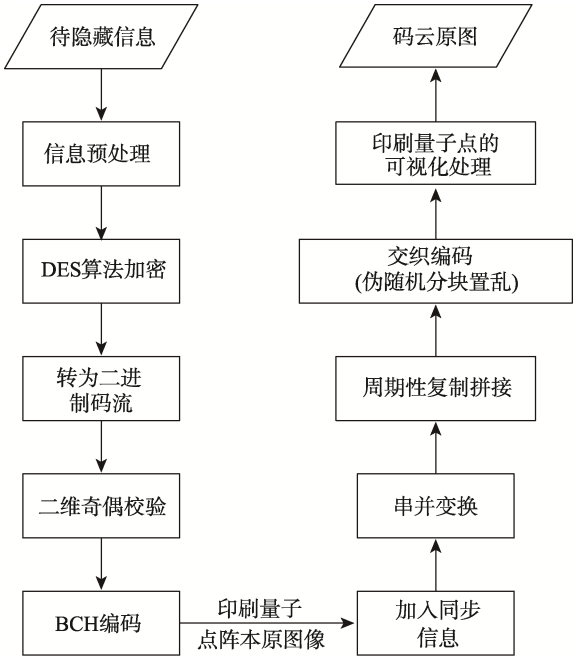


图 1　编码方案设计
Fig.1 Coding scheme design

1.2　解码方案设计

1.2.1　BCH 解码原理

对于能够纠正 t 个错误的(n,k,d)BCH 码，根据错误位置多项式 $\sigma(x)$ 的定义式：

$$\sigma(x)=\sum_{i=1}^{t}(1-x_i x)=\sum_{i=0}^{t}\sigma_i x^i \tag{6}$$

伴随多项式 $S(x)$可以表示为：

$$S(x)=\sum_{i=0}^{n-k}s_i x^i=\sum_{i=0}^{n-k}\left(\sum_{j=1}^{t}y_j x_j^i\right)x^i \qquad s_0=1 \tag{7}$$

令 $w(x)=S(x)\sigma(x)$，由于 $w(x)$的次数不会超过 $2t$，因此，有：

$$w(x)=\sum_{i=0}^{2t}w_i x^i \qquad w_0=1 \tag{8}$$

且：

$$\sum_{i=0}^{t}s_{t-i+j}\sigma_i=0 \qquad j=1,2,\cdots,t \tag{9}$$

由于错误位置多项式 $\sigma(x)$ 的次数为 t，$w(x)$ 的次数不会超过 t，可知在伴随多项式 $S(x)$中仅需求幂次小于 t 的项参与计算，从而有：

$$w(x)\equiv(S(x)\sigma(x))\bmod(x^{2t+1}) \tag{10}$$

这里采用迭代的方法求解错误位置多项式 $\sigma(x)$ 和 $w(x)$ 。迭代算法步骤如下所述。

1）初始化：$\sigma^{(-1)}(x)=1$，$w^{(-1)}(x)=0$，$d_{-1}=1$，$D(1)=0$ 和 $\sigma^{(0)}(x)=1$，$w^{(0)}(x)=1$，$d_0=s_1$，$D(0)=0$。

2）在第 j 次迭代后，$j \leftarrow j+1$，计算 $d_j = s_{j+1} + \sum_{i=1}^{k} s_{j+1-i}\sigma_i^{(j)}$，其中 k 表示多项式 $\sigma(x)$ 的次数。

3）判断 d_j 是否等于 0，如果等于 0，则使用递推计算式：

$$\begin{aligned} &\sigma^{(j+1)}(x) = \sigma^{(j)}(x) \\ &w^{(j+1)}(x) = w^{(j)}(x) \\ &(j+1) - D(j+1) = j - D(j) \end{aligned} \tag{11}$$

然后进入第 7 步；否则进入第 4 步。

4）选择 j 之前的第 i 行。

5）判断 $d_i \neq 0$ 且 $i - D(i)$ 最大，如果不是，返回第 4 步；否则进入第 6 步。

6）迭代计算。

$$\begin{aligned} &\sigma^{(j+1)}(x) = \sigma^{(j)}(x) - d_j d_i^{-1} x^{j-i} \sigma^{(i)}(x) \\ &w^{(j+1)}(x) = w^{(j)}(x) - d_j d_i^{-1} x^{j-i} w^{(i)}(x) \end{aligned} \tag{12}$$

7）判断 j 是否等于 $2t$，如果不等，返回第 2 步；否则进入第 8 步。

8）完成迭代，得到最终的 $\sigma(x)$ 和 $w(x)$ 。

$$\begin{aligned} &\sigma(x) = \sigma^{(j+1)}(x) \\ &w(x) = w^{(j+1)}(x) \end{aligned} \tag{13}$$

1.2.2　方案设计

为了能够实现快速准确的解码识读，需要设计一套符合编码方案的解码算法。该解码方案如下所述。

1）对经过可靠性编码得到的码云原图进行局部截取，得到部分印刷量子点点阵掩膜图像。

2）为了消除可视化效果，需要对截取得到的印刷量子点点阵掩膜图像进行信息解调处理，得到置乱图像。

3）对置乱图像进行帧同步信息检测[26]。若检测到同步信息，则对其进行解交织编码得到印刷量子点点阵本原图像；若没有检测到同步信息，则需要判断反置乱次数是否超限，若超限，那么需要移动到下一位进行处理，若没有超限，则只需要修改反置乱迭代次数，产生一个新的反置乱数据进行反置乱处理。

4）对印刷量子点点阵本原图像进行并串变换，将二维数据转换为一维数据，然后去掉同步信息。

5）进行 BCH 解码和解奇偶校验编码，得到加密数据。

6）对解码后的数据进行信息解密，识读出原始明文信息。

解码方案设计流程见图 2。

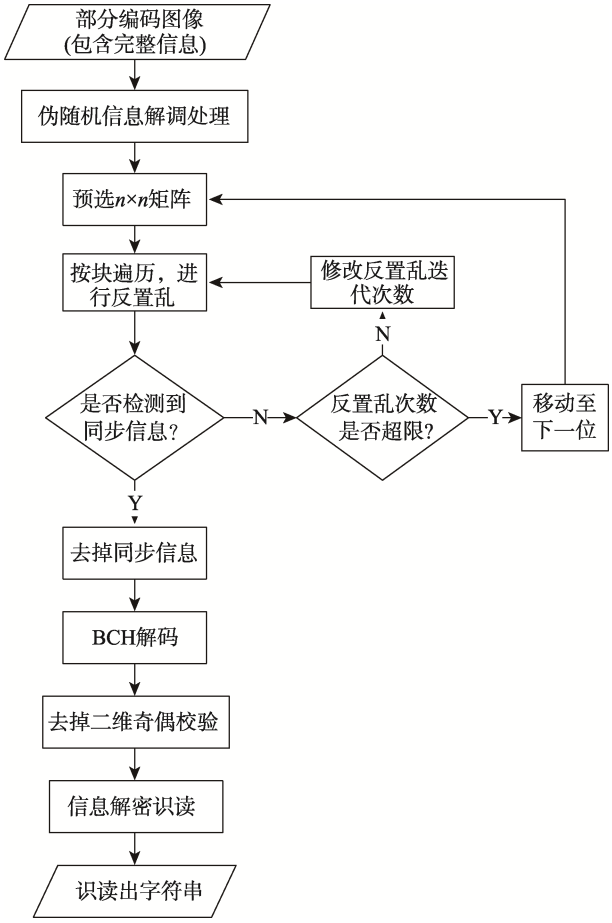


图 2　解码方案设计
Fig.2 Decoding scheme design

2　算法实现

2.1　印刷量子点信息隐藏算法

对待隐藏的明文信息进行信息预处理、信息加密、多重检纠错编码和信息调制，可以得到印刷量子点阵掩膜图像。具体算法实现如下所述。

1）信息预处理。对待隐藏的防伪标识、网址、序列号、文本或商标等不同格式的明文信息进行预处理，使之成为规范的十六进制序列码组。

2）DES 信息加密。为了满足在进行信码分组时每 64 位二进制数据为一组，需要将得到的十六进制码流进行补零直到达到要求。对得到的十六进制码流数据进行 DES 信息加密，密钥为 8765432112345678，得到与之唯一对应的十六进制码流序列，再转为二进制数据。为了提高二进制码流的安全性，在其头部和尾部分别加上 6 位二进制数据作为同步头和同步尾。DES 加密后输出二进制码流流程见图 3。

3）二维奇偶校验编码。将二进制数据进行串并变换，得到二维的二进制数据矩阵，对该矩阵进行二维的奇偶校验产生二维奇偶校验码，得到校验信息数据。二维奇偶校验编码对信息数据进行内层检错，当

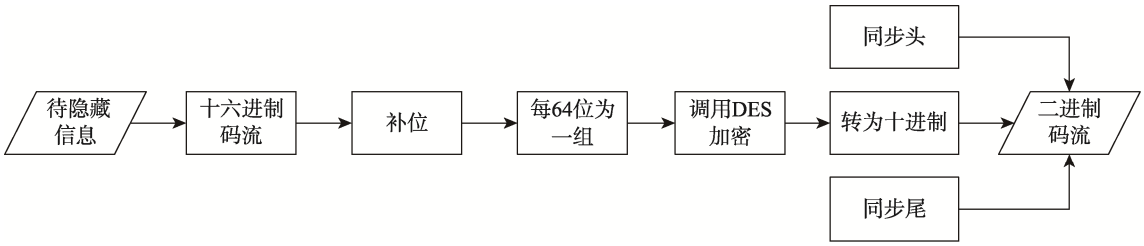


图 3　DES 加密处理流程
Fig.3 DES encryption processing flow

信息在传输过程中出现误码时可以及时发现，以保证信息传输的准确性。

4）BCH 编码。对步骤 3 中得到的校验信息数据进行(7,4)BCH 编码，得到编码后的二进制信息数据，再在其末尾加入 13 位的巴克码作为帧同步码组信息，作为完整待隐藏信息的记录标志。将一维编码后的数据进行串并变换，得到二维的信息数据，即印刷量子防伪点阵本原图像。

5）多重复制拼接。为满足与载体图像尺寸匹配，需要对印刷量子点阵本原图像进行 $m\times m$（具体 m 取值需要按照实际应用情况而定）的周期性复制和多重拼接，得到一个满铺图像。

6）交织编码（伪随机信息置乱）。为解决印刷量子点阵图样排列因相对规则而引起的信息安全漏洞，防止不法分子对其进行伪造、抄袭或者非法拷贝，对复制拼接的输出图像进行伪随机信息置乱。伪随机置乱是指采用不同迭代次数的伪随机交织编码，对每个区域的图像进行交织迭代置乱运算，得到一个随机性排列的图像。

7）信息调制。对伪随机信息置乱后的图像进行信息调制，得到信息记录容量大、可靠性高的单像素印刷量子点防伪点阵掩膜图像。

2.2　印刷量子点信息识读算法

文中采用的识读算法是分块识读算法，截取部分的码云原图进行解码识读，可以提高印刷量子点的信息识读速度。印刷量子点信息识读是量子点图像生成的逆过程，具体算法实现如下所述。

1）信息解调与解置乱。首先随机截取包含完整明文信息的印刷量子点阵掩膜图像进行信息解调，得到置乱图像，对该图像进行帧同步信息检测，如果检测到同步信息，则进行伪随机信息解置乱，得到印刷量子点阵本原图像；如果没有检测到同步信息，则需要检测解置乱次数是否超限，如果超限则移动到下一位重新按块遍历，否则直接修改解置乱次数，再进行同步信息检测。

2）多重检纠错解码。对印刷量子点阵本原图像进行并串变换，将二维数据转换为一维二进制数据，去掉同步信息后进行(7,4)BCH 解码，对得到的解码序列去掉二维奇偶校验，得到二进制的密文信息。

3）信息解密识读。根据码流长度对二进制密文信息进行分组，将分组后的二进制码流序列先转换为字符数组，再转换成十六进制码流，按照 DES 解密算法进行解密，生成原始隐藏的明文信息。

3　实验测试

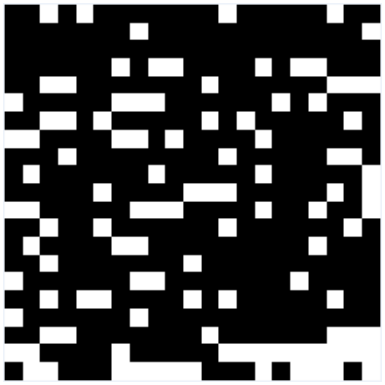
3.1　印刷量子点图像生成与识读

例如要隐藏的信息为 20 个字符的网址信息，经过预处理后变为 40 个十六进制码流，为了满足在进行信码分组时每 64 位二进制数据为一组，需要将得到的十六进制码流进行补零直到达到要求，补齐后为 48 个十六进制码流。进行 DES 加密得到 384 位二进制码流序列，加上同步头和同步尾后得到 396 位。将 396 位二进制数据进行串并变换，得到二维的二进制数据矩阵，对该矩阵进行二维奇偶校验编码得到 441 位校验信息数据，见图 4a。对校验信息数据进行(7,4)BCH 编码，得到 777 位编码后的二进制信息数据，再在其末尾加入 13 位的巴克码作为群同步码组信息，作为完整待隐藏信息的记录标志。将一维编码后的数据进行串并变换，得到二维的信息数据，即印刷量子防伪点阵本原图像，见图 4b。

对点阵本原图像进行 4×4 的周期性复制拼接，见图 5a，由该图可以看到其具有很明显的纹理特征，这样很容易引起信息安全漏洞，因此需要再对其进行交织迭代置乱运算，得到一个随机性排列的图像，见图 5b。

对伪随机信息置乱后的图像进行信息调制，得到信息记录容量大、可靠性高的单像素印刷量子点防伪点阵掩膜图像，图像尺寸为 348×348，见图 6a。图 6b 是从图 6a 中截取的一块包含完整信息的印刷量子点防伪点阵掩膜图像。

为解决印刷量子点点阵图样排列因相对规则而引起的信息安全漏洞，需要对得到的图像进行交织置乱处理，但不同的交织置乱次数得到的印刷量子点阵图像的排列也会有所不同。如图 7 所示，将印刷量子点点阵本原图像可视化为量子点图像，再对其进行 4×4 的周期性复制拼接，对得到的拼接图像分别进行置乱次数为 5 和 14 的交织置乱处理。



$$\begin{bmatrix}
0&0&1&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&1&1&0&0&0&0&1&0&1&1&0&0&0\\
0&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1\\
1&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&0&1&0&0&0\\
0&0&1&1&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&1&0\\
1&1&0&0&0&0&1&1&0&1&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1&0\\
0&1&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&0&0&1&0&0&0&0&1&1&1&0&0&0&0&0&1&0&1\\
1&1&0&0&0&0&0&1&1&1&0&0&0&0&1&0&0&1&0&0&1\\
0&0&1&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0\\
0&1&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&1&0&1&1&0&0&0&0&1&0&1&0&0&0&0&0&1&0&0\\
1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1\\
1&1&0&0&0&0&1&0&0&0&0&0&1&1&1&1&1&1&1&1&1\\
0&1&1&0&0&0&1&1&1&1&1&0&0&0&1&0&1&1&1&0&1
\end{bmatrix}$$

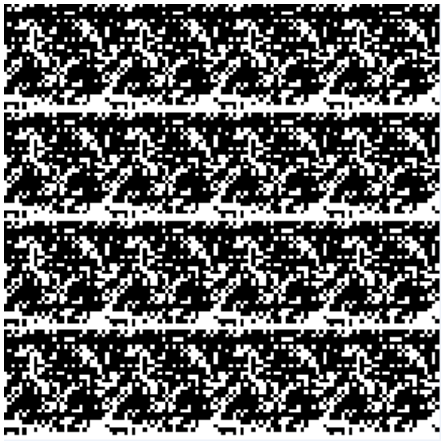
a 二维奇偶校验图像及对应数值矩阵

$$\begin{bmatrix}
0&0&1&0&1&1&0&1&0&0&0&1&0&1&0&0&0&0&0&0&1&0&0&0&1&0&1&0\\
0&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&1&1&0&0&1&0&0&0&1&0&1&0&1&0&1&1&0&0&1&0&0&1\\
0&1&0&0&1&1&1&0&1&0&0&0&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0\\
0&0&0&1&1&1&0&1&1&1&0&0&0&1&0&0&0&0&1&0&1&1&1&1&0&0&0&1\\
0&0&0&0&0&0&0&1&0&1&0&0&1&1&0&0&0&0&0&0&0&1&1&0&1&0&0&1\\
0&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&0&0&1&0&1&1&0&0&1&0\\
0&0&1&0&1&0&1&1&0&0&0&1&1&0&0&0&1&0&1&0&1&0&0&1&1&1&0&0\\
0&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
1&0&1&0&0&1&1&1&0&1&0&0&1&0&1&1&0&0&0&0&0&0&0&0&1&0&0&1\\
1&1&0&0&0&1&0&1&1&0&0&0&0&0&0&0&1&0&0&1&1&1&0&0&1&0&1&1\\
1&0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&0&0\\
1&0&0&0&1&0&1&0&0&1&1&1&0&1&1&0&0&0&1&0&1&0&1&0&0&1&1&1\\
0&0&1&1&1&0&0&0&1&0&1&1&0&0&1&0&0&1&1&1&0&0&0&0&0&0&0&1\\
0&0&1&0&1&0&0&0&1&0&1&1&0&0&1&0&1&1&0&0&0&0&0&1&1&0&0&0\\
0&1&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&0\\
1&1&0&0&0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&0&0&0&0&0&0&1&0&1\\
1&0&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&0&0&0&1&0&0&0&1&0&1&1&0\\
1&0&0&0&1&0&1&0&0&1&0&1&1&0&0&1&0&0&1&1&1&0&0&0&0&0&0&1\\
0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&0&0&0&0&0&0&1&1&1\\
1&1&1&1&1&0&0&0&1&0&1&0&1&0&0&1&1&1&0&0&0&1&0&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&0&1&1&0&0&0&1&0&0&1&1&1&0&1&1&1&1&0\\
0&0&0&0&1&0&1&1&0&1&1&1&0&1&0&0&1&0&0&0&1&0&1&1&1&1&1&0\\
0&1&1&0&1&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{bmatrix}$$

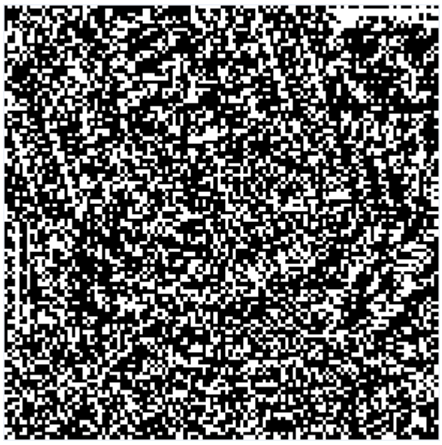
b 印刷量子点阵本原图像及对应数值矩阵

图 4　检纠错编码输出

Fig.4 Output diagram of check and correct code



a 4×4 复制拼接图像



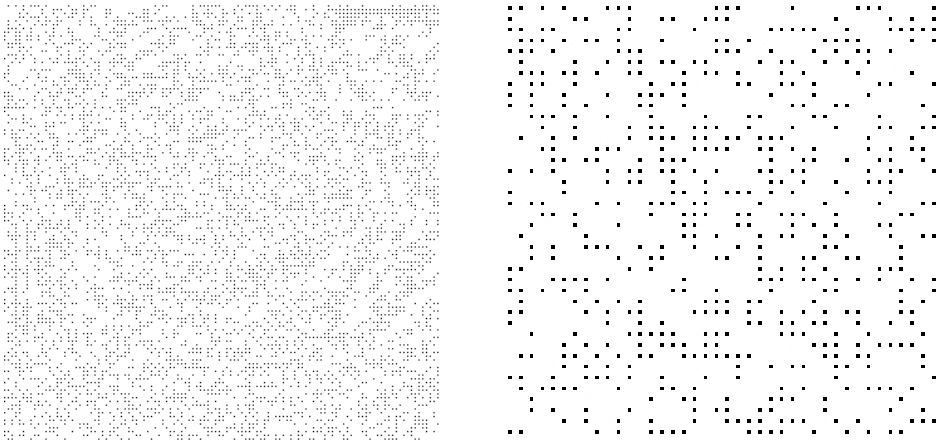
b 交织迭代置乱图像

图 5　伪随机信息置乱输出

Fig.5 Output diagram of pseudo-random information scrambling

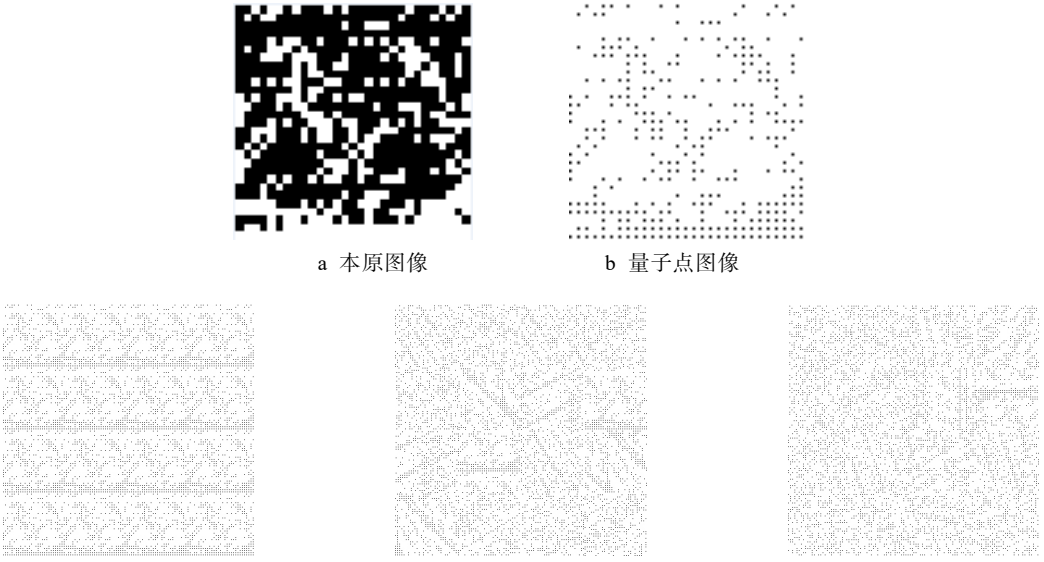
由图 7c，d，e 可知，量子点图像经过周期性复制拼接过后得到的图像纹理特征明显，很容易引起信息安全漏洞，对其进行交织置乱过后伪随机性明显比拼接后的图像要好，但是对比置乱次数为 5 和 14 得到的图像，可以看出置乱次数为 14 的图像的伪随机性明显比置乱次数为 5 的图像的伪随机性要好。

对随机截取的部分码云原图进行信息解调，得到如图 8a 所示的置乱图像，再对该图像进行解交织置乱，得到如图 8b 所示的印刷量子点阵本原图像。



a 码云原图　　b 截取的局部码云原图

图 6　印刷量子点防伪点阵掩膜图像
Fig.6 Printing quantum dot anti-counterfeiting lattice mask image



a 本原图像　　b 量子点图像

c 复制拼接图像　　d 交织置乱（次数为 5）　　e 交织置乱（次数为 14）

图 7　不同交织置乱次数生成的码云图像对比
Fig.7 Comparison of code cloud images generated by different times of interleaving and scrambling

a 信息解调图像　　b 解交织置乱图像

图 8　解码后的输出图像
Fig.8 Decoded output image

对解码得到的印刷量子点点阵本原图像去掉同步信息后进行 BCH 解码，对得到的解码序列去掉二维奇偶校验，得到二进制的密文信息，再对其进行 DES 解密识读出原始明文信息。借助 Matlab 仿真工具可完整识读并提取出原始 20 个字符的明文信息，并且识读时间为 0.567 138 s，信息识读与响应结果见图 9。

图 9　信息识读与响应结果
Fig.9 Result of information reading and response

基于可靠性信道编码的印刷量子点点阵掩膜图像是一种基于最小墨点的半色调网点图像，可以很好地隐藏于载体图像中，且不影响图像质量，具有一定的抗复制功能。要想复制或者拷贝纹理图像，就需要采用高精度的复印设备进行复印，或者用高精度的拍照设备抓取纹理图像后，再将拍到的图像缩放到与原图一样的尺寸进行打印或印刷，但是在复制或相应的工艺处理过程中，微小的信息记录载体-墨点的空间特性信息就会全部或部分丢失，造成信息缺损或者污损，进而达到信息防伪的目的。将印刷量子点阵掩膜图像以满铺的形式非关联盲植入载体图像中，得到的效果见图 10。

为了验证文中提出算法的检纠错能力，对得到的印刷量子点防伪点阵掩膜图像先随机加入噪声和突

图 10　非关联盲植入输出图像
Fig.10 Uncorrelated blind implant output image

发噪声，再对其进行信息解码识读的实验，实验仿真所用的印刷量子点图像尺寸为 87×87。加入随机噪声的实验仿真结果见表 2，加入突发噪声的实验仿真结果见表 3。

由表 2 和表 3 可知，对加入不同程度随机噪声和突发噪声的印刷量子点防伪点阵掩膜图像进行信息解码识读与响应实验，仍然可以完整地识读和提取出原始明文信息，并且解码正确率都能达到 93%以上。这表明文中提出的算法具有较强的纠错能力，在具有一定污损的情况下仍然可以很好地保证信息的完整性，并且能够提取出完整信息，具有很好的实用价值。

为验证嵌入印刷量子点图像的防伪攻击鲁棒性，进行了多种类型、多种强度的攻击，并且将提取出的印刷量子点图像进行解码识读实验，选用原始图像尺寸为 512×512，水印尺寸为 87×87。利用归一化值（NC, Normalized Correlation）对提取的印刷量子点图像的性能进行评价。不同类型攻击后提取印刷量子点的解码识读效果及 NC 值见表 4。

表 2　加入不同数量随机噪点后的信息识读与响应结果
Tab.2 Information reading and response results after adding different amounts of random noise

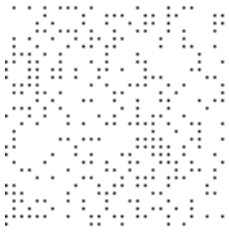
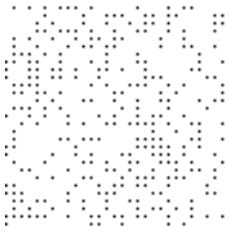
噪点数量	量子点图像	加噪后图像	信息识读与响应	解码正确率/%
170			Command Window 行位置：列位置：置乱次数：1,1,13 提取信息为：https://www.csdn.net Elapsed time is 0.690535 seconds.	97.75
180			Command Window 行位置：列位置：置乱次数：1,1,13 提取信息为：https://www.csdn.net Elapsed time is 0.896897 seconds.	97.62

表 3　加入不同面积突发噪声后的信息识读与响应结果

Tab.3 Information reading and response results after adding burst noise of different areas

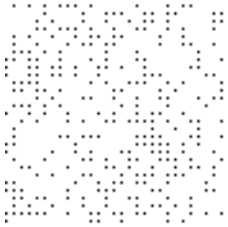
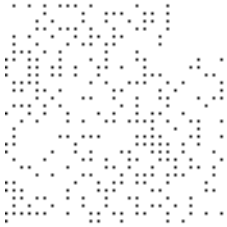
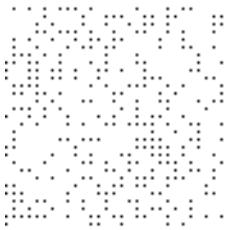
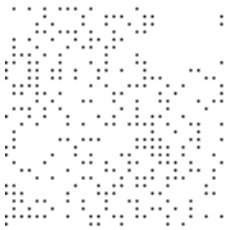
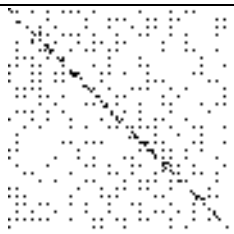
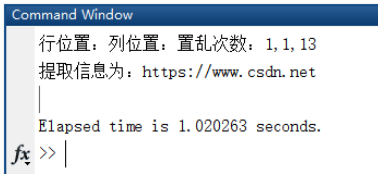
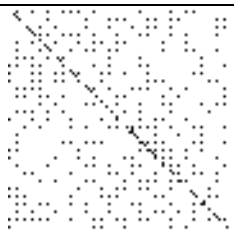
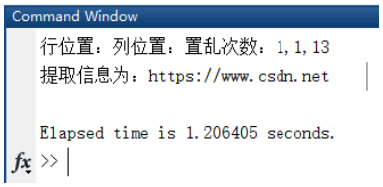
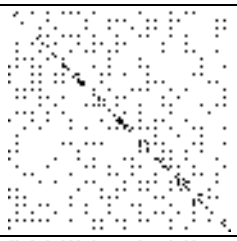
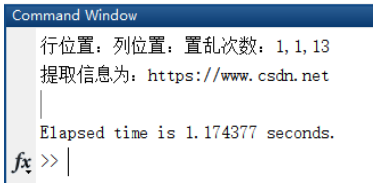
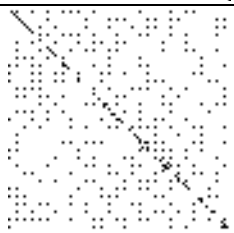
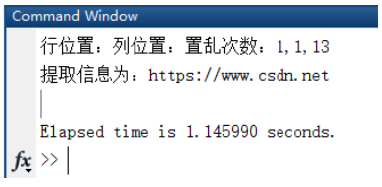
遮盖面积	量子点图像	加噪后图像	信息识读与响应	解码正确率/%
20×20				94.72
23×23				93.01

表 4　不同类型攻击后提取印刷量子点的信息识读以及 NC 值

Tab.4 Information reading and NC values of printed quantum dots were extracted after different types of attacks

类型	攻击图像	提取图像	信息识读与响应	NC 值
剪切攻击				0.8854
降低对比度攻击				0.9252
高斯噪声方差 0.01				0.9077
JPEG 图片压缩 20%				0.9159

由表 4 可知，对载体图像进行不同类型的攻击实验后，提取出的印刷量子点图像的 NC 值都在 0.88 以上，表现出较好的性能，并且对提取的印刷量子点进行解码识读时都能够识读出完整的明文信息。

3.2　实验对比分析

对文献[19]中的算法进行优化，将印刷量子点可视化为单个像素（1×1）的最小成像单元，然后将文

献[19]中的算法与文中算法和基于(7,4)汉明编解码算法进行实验对比。待隐藏信息为 20 个字符信息，通过分析它们的纠错能力、编码效率和解码识读时间，验证文中提出的编解码算法优劣。在纠错能力都为 1 和编码效率都为 4/7 的情况下，不同解码算法对印刷量子点块的解码识读时间对比见表 5。

由表 5 可知，截取 87×87，120×120，135×135 和 180×180 包含完整信息块的印刷量子点点阵掩膜图像进行解码识读时，文中算法的解码识读时间明显低于(7,4)汉明解码和文献[19]中算法的解码识读时间，并且随着印刷量子点点阵掩膜图像块的尺寸越大，解码识读出完整信息块所需的时间也越长。说明在纠错能力和编码效率相同的情况下，文中提出算法的解码识读的性能要优于汉明码和文献[19]的解码识读的性能。

根据表 4 可知文中算法得到的印刷量子点图像对多种类型、多种强度的攻击的鲁棒性，利用文献[19]算法和基于(7,4)汉明编解码算法也进行鲁棒性实验，测试印刷量子点图像的尺寸都为 87×87。提取出不同算法的水印图像对比见表 6。将提取出的不同算法水

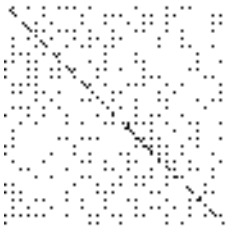
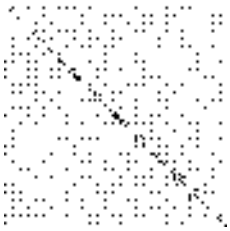
表 5　不同解码算法对印刷量子点块的解码识读时间对比

Tab.5 Comparison of decoding and reading time of printed quantum dot blocks with different decoding algorithms

纠错能力	编码效率	尺寸	不同解码算法的解码识读时间/s		
			文中算法	(7,4)汉明码	文献[19]
1	4/7	87×87	0.567 138	0.837 730	1.137 716
1	4/7	120×120	3.121 176	3.325 333	5.336 535
1	4/7	135×135	5.726 797	5.992 078	8.966 412
1	4/7	180×180	18.695 213	19.067 011	30.064 045

表 6　提取出不同算法的水印图像对比

Tab.6 Comparison of the watermark images extracted by different algorithms

类型	文中算法	(7,4)汉明码	文献[19]
剪切攻击			
降低对比度攻击			
高斯噪声方差 0.01			
JPEG 图片压缩 20%			

印图像的 NC 值进行对比，结果见表 7。

由表 6 和表 7 可知，文中算法得到的印刷量子点图像针对不同类型攻击的鲁棒性要比文献[19]算法和基于(7,4)汉明编解码算法得到图像的鲁棒性要好，NC 值更高。

对 BCH 编码的纠错能力、编码方式和信码分组形式与汉明编码和 RS 编码进行了对比，见表 8。设信息码长为 n，信息位为 m，最小码距为 d。

表 7 NC 值对比
Tab.7 Comparison of NC value

类型	文中算法	(7,4)汉明码	文献[19]
剪切	0.8854	0.8848	0.8875
降低对比度	0.9252	0.9252	0.9241
高斯噪声方差 0.01	0.9077	0.9072	0.9077
JPEG 图片压缩 20%	0.9159	0.9133	0.9121

表 8 3 种信道编码性能对比
Tab.8 Comparison of three channel coding performance

性能参数	BCH 编码	汉明编码	RS 编码
纠错能力（t）	$t=(d-1)/2$ 可自主定义	$t=1$ 不可自主定义	$t=(d-1)/2$ 纠正随机错误效果差
编码效率（R）	$R=(n-m)/n$	$R=(n-m)/n$	$R=(n-m)/n$
编码方式	bit 位	bit 位	字符位
信码分组	灵活性高	灵活性低	灵活性低

由表 8 可知，在纠错能力方面，BCH 编码和 RS 编码都可以纠正随机错误和突发错误，而汉明编码只能纠正单个随机错误，但是 RS 编码在纠正随机错误的效果比较差。在编码方式方面，BCH 编码和汉明编码都是基于 bit 位的编码，而 RS 编码是基于字符位的编码；在信码分组方面，BCH 编码的灵活性高，而汉明编码和 RS 编码的灵活性较低。综上所述，BCH 编码的性能在总体上要优于汉明编码和 RS 编码。

4 结语

针对打印信息污损和图像识读信息误判引起的误码率高这一突出问题，设计一种基于印刷量子点的多重组合信息可靠性编解码算法，该算法采用二维奇偶校验编码+BCH 编码+交织编码+帧同步组合方式来实现半色调信息防伪与信息隐藏，具有良好的抗复制性、信息隐藏效果好、数据记录容量大等显著优势。实验结果表明，该算法的检纠错能力较强，鲁棒性好，信息解码识读与响应速度快，并且比基于汉明码和 RS 码的性能要好。

BCH 编码在信道编码中不是最好的编码方式，所以在未来的工作中将考虑使用性能更优的信道编码方式，比如卷积编码，利用卷积编码与二维奇偶校验编码和交织编码进行结合，实现可靠性更高、纠错能力更强、信息容量更大的半色调信息防伪与信息隐藏。

参考文献：

[1] TSENG H W, CHANG C C. Hiding Data in Halftone Images[J]. Informatica, 2005, 16(3): 419—430.

[2] CHEN Fang-fang, ZHU Jian-le, CAO Peng, et al. Print Anti-Replication Technology Based on AM/FM Hybrid Halftone[C]// 2017 IEEE 17th International Conference on Communication Technology (ICCT), IEEE, 2017: 329—332.

[3] PUNEET G, MADHUR G, CARL S, et al. Clustered-Dot Halftoning with Direct Binary Search[J]. IEEE Signal Processing Magazine, 2013, 22(2): 473—487.

[4] XUE Y, LIU W, LU W, et al. Efficient Halftone Image Steganography Based on Dispersion Degree Optimization[J]. Journal of Real-Time Image Processing, 2019, 16(3): 601—609.

[5] DING H, YANG Y. Data Hiding in Color Halftone Images Based on New Conjugate Property[J]. Computers & Electrical Engineering, 2018, 70: 302—316.

[6] YI Xu-mei, CAO Peng. The Shapes of Halftone-AM-Dots Based on Information Hiding[C]// 2011 2nd International Symposium on Intelligence Information Processing and Trusted Computing, IEEE, 2011: 59—62.

[7] MINNEBO L, VELDE K, DELABASTITA P. FM Screening with Sub-Dot Phase Modulation: U.S. Patent Application 10/662, 460[P]. 2004-05-13.

[8] CROUNSE K. Halftone Method and System Using Hybrid AM/FM Screening for Highlight/Shadow Tonal Regions: US, Patent Application 10/337, 031[P]. 2004-07-08.

[9] FU M S, AU O C. Data Hiding Watermarking for Halftone Images[J]. IEEE Transactions on Image Processing, 2002, 11(4): 477—484.

[10] KIM C, SHIN D, SHIN D. Data Hiding in a Halftone Image Using Hamming Code (15, 11)[C]// Asian Conference on Intelligent Information and Database Systems, Springer, Berlin, Heidelberg, 2011: 372—381.

[11] MA Z, LI F, ZHANG X. Data Hiding in Halftone Images Based on Hamming Code and Slave Pixels[J]. Journal of Shanghai University (Natural Science Edition), 2013, 19(2): 111—115.

[12] JANA B, GIRI D, MONDAL S K. Partial Reversible

Data Hiding Scheme Using (7, 4) Hamming Code[J]. Multimedia Tools and Applications, 2017, 76(20): 21691—21706.

[13] JANA B, GIRI D, MONDAL S K. Dual Image Based Reversible Data Hiding Scheme Using (7, 4) Hamming Code[J]. Multimedia Tools and Applications, 2018, 77(1): 763—785.

[14] CAO Ze-kun, YIN Zao-xia, HU Hong-he, et al. High Capacity Data Hiding Scheme Based on (7, 4) Hamming Code[J]. Springer Plus, 2016, 5(1): 1—13.

[15] LIEN B K, CHEN S K, WANG W S, et al. Dispersed Data Hiding Using Hamming Code with Recovery Capability[J]. Journal of Symbolic Logic, 2015, 63(4): 1565—1581.

[16] 葛乃馨. 半色调信息隐藏防伪研究[D]. 南京: 南京林业大学, 2019: 13—49.
GE Nai-xin. Research on Halftone Information Hiding Anti-Counterfeiting[D]. Nanjing: Nanjing Forestry University, 2019: 13—49.

[17] 刘丽, 杨文杰, 汪雅婷, 等. 信息技术在印刷包装防伪上的应用研究进展[J]. 包装工程, 2019, 40(9): 216—223.
LIU Li, YANG Wen-jie, WANG Ya-ting, et al. Research Progress on Application of Information Technology in Printing and Packaging Anti-Counterfeiting[J]. Packaging Engineering, 2019, 40(9): 216—223.

[18] 陈方方. 半色调复合防伪方法及算法研究[D]. 北京: 北京印刷学院, 2020: 32—55.
CHEN Fang-fang. Research on Half-Tone Composite Anti-Counterfeiting Method and Algorithm[D]. Beijing: Beijing Institute of Graphic Communication, 2020: 32—55.

[19] 朱建乐. 盲同步印刷量子点信息隐藏编解码技术研究[D]. 北京: 北京印刷学院, 2019: 12—38.
ZHU Jian-le. Research on Information Hiding Encoding and Decoding Technology of Blind Synchronous Printing Quantum Dot[D]. Beijing: Beijing Institute of Graphic Communication, 2019: 12—38.

[20] WANG Li-qi, SUN Zhong-hua, ZHU Shi-xin. Hermitian Dual-Containing Narrow-Sense Constacyclic BCH Codes and Quantum Codes[J]. Quantum Information Processing, 2019, 18(10): 1—40.

[21] HOCQUENGHEM A. Codes Correcteurs D'Erreurs[J]. Chiffres, 1959, 2(2): 147—156.

[22] BOSE R C, RAY-CHAUDHURI D K. On a Class of Error Correcting Binary Group Codes[J]. Information and Control, 1960, 3(1): 68—79.

[23] SINGH G. A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security[J]. International Journal of Computer Applications, 2013, 67(19): 33—38.

[24] WANG X, TANG S. Bit-Level Soft-Decision Decoding of Double and Triple-Parity Reed-Solomon Codes Through Binary Hamming Code Constraints[J]. IEEE Communications Letters, 2014, 19(2): 135—138.

[25] HSU P, HOLCOMB T W, LIN C L. Motion Vector Coding and Decoding in Interlaced Frame Coded Pictures: US, Patent 7, 924, 920[P]. 2011-04-12.

[26] HU H T, LEE T T. Frame-Synchronized Blind Speech Watermarking Via Improved Adaptive Mean Modulation and Perceptual-Based Additive Modulation in DWT Domain[J]. Digital Signal Processing, 2019, 87: 75—85.