Computer Science and Application 计算机科学与应用, 2018, 8(11), 1657-1664
Published Online November 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.811182

Hans汉斯

The Mean-Based Ciphertext Domain Reversible Information Hiding Is Improved by Pixel Correlation

Shiyi Zhao, Yuan Yuan

Country Graduate School of Tangshan, Southwest Jiaotong University, Tangshan Heibei
Email: 1206412183@qq.com, 1586523750@qq.com

Received: Oct. 17th, 2018; accepted: Oct. 30th, 2018; published: Nov. 6th, 2018

Abstract

This paper improves the image encryption algorithm and the image embedding capacity. The document divided image into the block columned by 256 * 1. The number of blocks determines the number of bits embedded. The original block is too large, resulting in relatively few embedded data. Therefore, this paper divides the block as small as possible and modifies the embedding method and extracts the information completely according to the neighboring pixels of the average pixel. Using this method, the embedded information increases. Experimental results show that the embedding capacity obtained by this method is almost ten times of that. In this part, we mainly discuss the method of making space after encryption in the algorithm of reversible information hiding based on encryption domain. The proposed scheme is also simple and easy to operate with security and reversibility and privacy protection.

Keywords

Encrypted Image, Image Recovery, Information Hiding, Reversible Data Hiding

通过像素相关性改进的基于均值的密文域可逆信息隐藏

赵师毅，袁　圆

西南交通大学唐山研究生院，河北 唐山
Email: 1206412183@qq.com, 1586523750@qq.com

收稿日期：2018年10月17日；录用日期：2018年10月30日；发布日期：2018年11月6日

文章引用：赵师毅，袁圆. 通过像素相关性改进的基于均值的密文域可逆信息隐藏[J]. 计算机科学与应用, 2018, 8(11): 1657-1664. DOI: 10.12677/csa.2018.811182

摘　要

这篇文献改进了图像加密算法，提高了图像的嵌入容量。原文献中将图像按列分为256 * 1大小的块，嵌入的信息和块的多少有关。原文中分块太大而导致嵌入的信息相对较少，所以，本文将块尽可能地分小，并修改了嵌入方法并根据均值像素的相邻像素完全提取信息，使得嵌入的信息增加。本分主要讨论的是基于加密域的可逆信息隐藏的算法中的加密后腾出空间的方法。实验结果表明，修改后的算法嵌入的数据比原文多了十多倍，提出的方案同样简单易操作并具有安全性和可逆性、隐私保护性。

关键词

图像加密，图像恢复，信息嵌入，可逆信息隐藏

1. 引言

随着人们对隐私保护也越来越重视，但是普遍的图像可逆信息隐藏算法存在着容量不足的问题。因此本文将致力于改进图像的嵌入容量，增加图片的嵌入信息，并且使得恢复出来的图像和原始图像的像素误差不大。

可逆信息隐藏按嵌入域分可以分为空域和变换域这两种类型。空域指的是直接图像的像素进行操作，而变换域指的是通过一系列可逆的变换方式(如 DCT 变换等)对图像进行操作。可逆信息隐藏也可以分为加密图像的可逆信息隐藏和未加密图像的可逆信息隐藏。通常，基于未加密图像的可逆信息隐藏中使用的是差值扩展和直方图平移的方法。而加密域的可逆信息隐藏又可以分为加密前腾出空间和加密后腾出空间的方法。接下来，我们主要讨论的是基于加密域的可逆信息隐藏的算法中的加密后腾出空间的方法。加密后腾出空间的算法又可以分为联合算法和可分离算法。联合算法必须是在解密后的图像中提取信息，然后再恢复图像。而可分离算法可以在含有隐藏信息的加密图像中提取信息，再根据加密密钥解密图像，并得到恢复的图像。

2. 本文提出的算法

2.1. 计算均值

将图像按列进行分块，记分块后剩余的像素为 Rest。计算每一个块的均值，将均值像素代替每一个块的第一个像素。再将计算过均值的块和剩余的块合并成图像 J。分块取平均值(avg.m):[J,p] = avg(origin_img,x)传入：原始图像、分块大小，返回：计算均值后的图像及分块个数

2.2. 加密图像

产生与图像大小的伪随机数记为 R，将图像中除均值像素外的所有像素用公式(3)计算加密像素值得到加密图像 E。加密图像(encrypted.m)：E = encrypted (J, R, x)。传入：均值图像、加密密钥(伪随机数)、分块大小返回：加密图像

$$E(i,j)=\left(J(i,j)+R(i,j)\right)\bmod 256 \tag{3}$$

2.3. 嵌入信息

对加密图像 E 中的像素嵌入信息。如果一个块的嵌入信息为 1，则将加密图像中该块中除均值像素外的二进制加 1010，如果嵌入信息为 0，则不改变加密图像的像素值。1010 即为十进制的 10，如果我们相加的数太小了，那么在块分小了之后，如果嵌入为 1，那么除均值像素外的像素累计加的数太小，导致在算均值位置的原始像素与我们嵌入 0 算出的结果相差不大，或者更平滑如果相加的数太大了，也有同样的问题。或者是如果原始图像中均值像素和周围像素相差太大，那么算出的结果可能是错误的值相关性更大。如果像素值为 255，二进制为 11111111，加上 1010 为 1001。像素值大于 245 的计算方法如 255。将嵌入信息后的加密图像记为 C。

2.4. 解密图像

将图像 C 中每一个块中除均值以外的像素值用公式(4)进行解密，得到含有隐藏信息的解密图像 D。

$$D(i,j)=\left(C(i,j)-R(i,j)\right)\bmod 256 \tag{4}$$

其中，R (i, j)和加密时的伪随机数是一样的。解密图像(decrypted.m):D = decrypted (C, R, x)传入：嵌入信息后的加密图像、加密密钥、分块大小返回：解密图像。

2.5. 提取信息恢复图像

对于含有隐藏信息的加密图像中的每一个块，我们并不知道嵌入的数据为 0 还是 1，将原始的块记为 B0 作为嵌入为 0 的块，将除均值外像素二进制减去 1010 后的块记为 B1 作为嵌入为 1 的块。如果在像素值小于等于 9，在减 1010 时，在最高位添一个 1 相减，例如：9 的二进制为 00001001，在最高位添一个 1 变成：100001001，再将这个数减去 1010 得到 11111111，即 255。其他小于 9 的数字也是同样的计算方式。

通过公式(5)计算两种情况下的均值像素记为 first0 和 first1。

$$\text{first}=\text{round}\left(s1j*x-\sum_{i=2}^{x}sij\right) \tag{5}$$

其中，s1j 代表每一个块的均值像素值，x 为分块大小，sij 为块中的像素值。

在嵌入为 0 和嵌入为 1 的情况下，计算块中每一个像素的预测值，并将他们与对应的像素值求绝对值后相加。在嵌入为 0 的情况下，计算该像素相邻四个像素的均值记为 A0。在嵌入为 1 的情况下，计算该像素相邻四个像素的均值记为 A1。如图 1 所示，如果均值像素位于图像边缘，则取它上下左右在图像范围内的像素。通过公式(6)判断嵌入为 0 还是 1。

$$f0=\text{abs}\left(x0-A0\right) \tag{6}$$

$$f1=\text{abs}\left(x1-A1\right) \tag{7}$$

其中 x0 为嵌入为 0 时对应的像素值，而 x1 为嵌入为 1 时对应的像素值。因为像素之间的相关性，未嵌入信息的像素要比嵌入信息后的像素更平滑，所以，若 f0 > f1 则嵌入为 1，均值像素为 x1，原始块为 B1；若 f0 < f1 则嵌入为 0，均值像素为 x0，原始块为 B0。正确提取信息后，图像得到完美恢复。

3. 仿真实验结果

该算法测试的图像均为 512 * 512 大小，分块最小能分到 20 * 1，嵌入数据为 13,107 比特，是文献[1]

中的 12 倍左右。以 Lena 图像为例，该算法的仿真结果如图 2 所示。

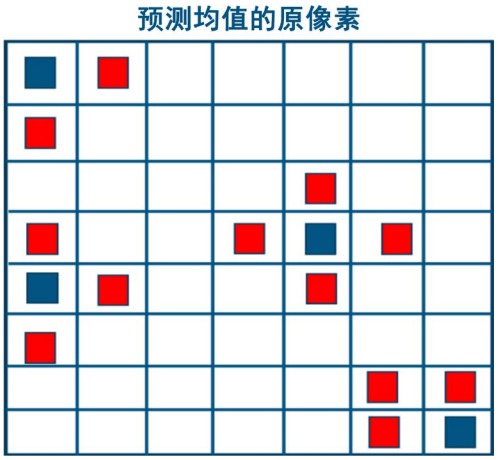
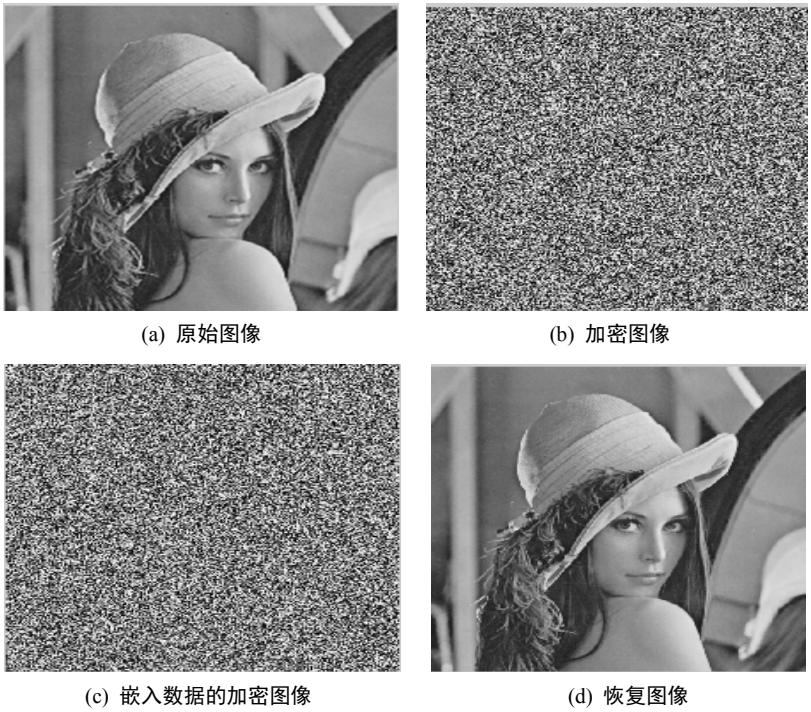


Figure 1. Pixel prediction
图 1. 像素预测



(a) 原始图像　(b) 加密图像

(c) 嵌入数据的加密图像　(d) 恢复图像

Figure 2. The simulation results
图 2. 仿真结果

通过上述仿真结果我们可以看到加密后的图像看不见原始的内容，从而确保原始图像的隐私。对应的直方图如图 3 所示。

从上述的直方图的结果可以看出，嵌入的加密图像和数据的直方图与原始图像的直方图有很大的不同，加密后嵌入信息的直方图像素分布均匀，无法识别原始图像的内容。恢复图像的直方图与原始图像相同，说明了我们算法的可逆性。

选取了九张 512 * 512 图像进行测试，包括了 lena，zelda，Man，airplane，couple，sailboat，baboon，

goldhill，barbara 图像。用文献[1]的算法块大小与信息提取错误的趋势如图 4 所示，采用本文的算法仿真分析改进后的错误趋势如图 5 所示。

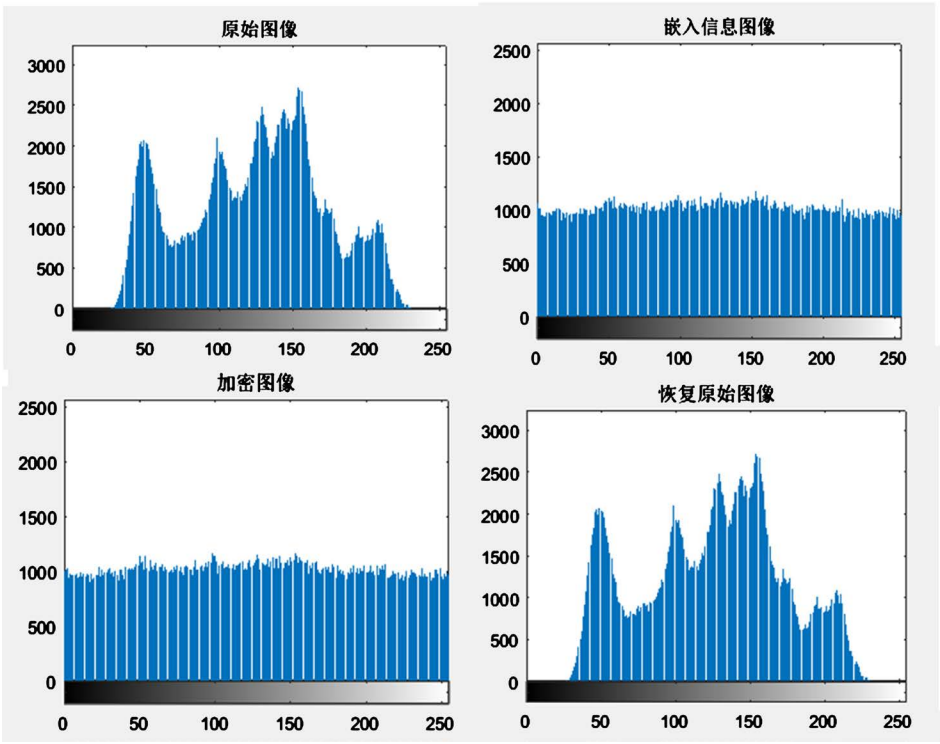


Figure 3. Histogram results
图 3. 直方图结果

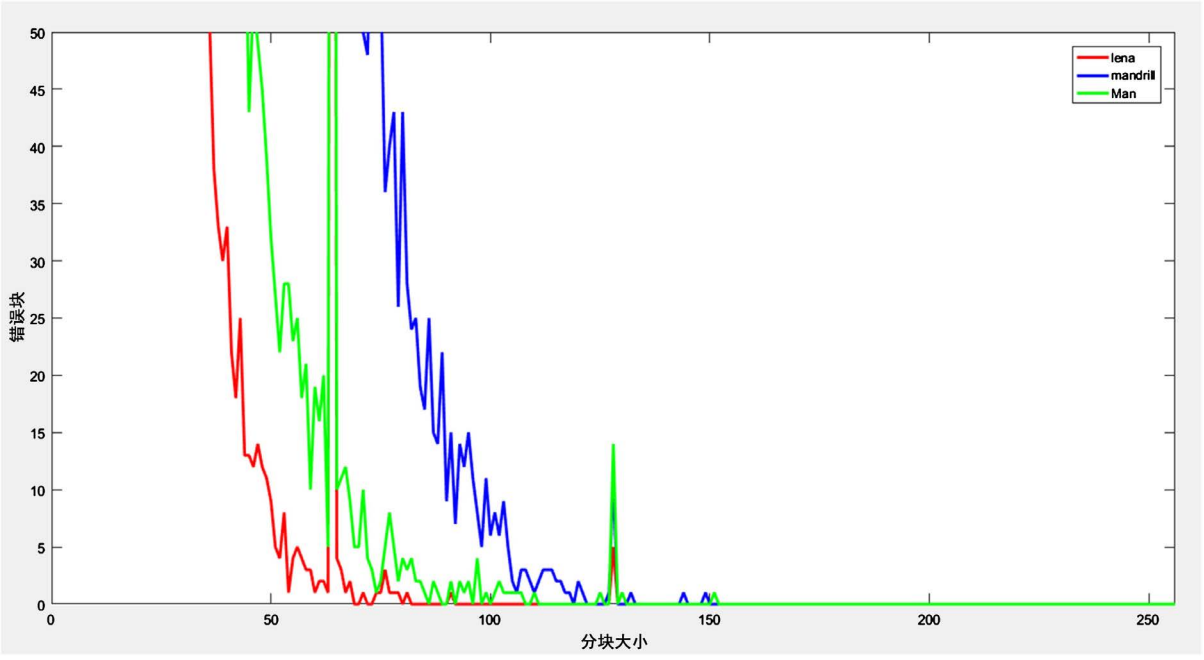


Figure 4. Block size and information extraction error trend
图 4. 块的大小与信息提取错误的趋势

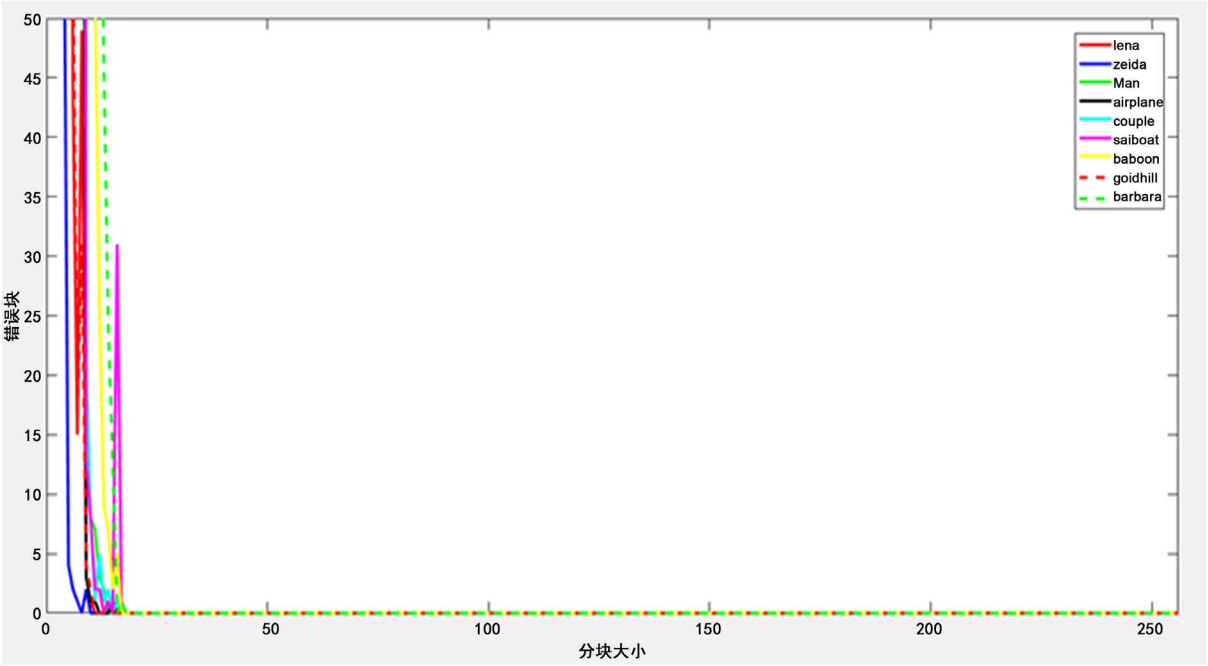


Figure 5. Block size and information extraction error trend
图 5. 块的大小与信息提取错误的趋势

分块出现错误的原因：放均值的像素与周围像素相差太大，导致预测的不准确。块分小了，剩余像素累计加 1 的值变小了，与未加 1 得出的均值位原始像素差距不大，可能会更接近预测的像素。

4. 实验分析比较

文献[2]提出了采用传统的 RDH 方案和统一嵌入置乱方案两种 RDH 方法在加密图像中嵌入信息。[3]在[2]的基础上该方案获得了最佳的视觉质量和增强的嵌入率。测试结果和相关性被展示，概述了提议的技术与传统技术的可行性和重点。文献[4]提出了一种基于加密 JPEG 位流的可逆数据隐藏框架，其次，嵌入的有效载荷比文献[3]还要大。文献[5]中的方法无需对原始图像进行预处理，即可将附加数据直接嵌入到加密图像中。文献[6]根据隐藏密钥选取部分加密像素，用 LDPC 码对选中像素的 MSB 进行 Slepian-Wolf 编码，为信息隐藏预留空间，该算法能无损重建原始图像，提高了嵌入率，不过，压缩像素 MSB 导致了解密图像质量不高的问题(例如嵌入率为 0.05 bpp 时，Baboon 图像的解密图像 PSNR 不到 25 dB)。文献[7]根据相邻像素间的位置关系，将加密像素分为三个集合，压缩每个集合中像素的 3 LSB，为信息隐藏预留空间，此外，该算法中提出的渐进图像解密机制提供了更好的率失真性能，*i.e.*，在相同解密图像 PSNR 值下，更大的信息嵌入率。此外，文献[8] [9]基于位替换(替换加密像素的某些比特为秘密比特)的方法也实现了信息隐藏。其中，文献[8]将密文图像 LSBs 位平面中的部分比特替换为秘密信息，用经被替换比特和嵌入秘密比特调制生成的伪随机序列修改 LSBs 位平面中余下比特，该算法虽然实现了信息提取与图像解密恢复的可分离，但信息提取会出现错误；文献[9]提出一种基于预测误差的可分离 RDH-EI 算法，用 XOR 加密原始图像，通过替换加密像素的最高位(或次高位)隐藏信息，基于预测误差的方法重建原始图像，该可分离 RDH-EI 算法具有较高信息隐藏容量，能以一定概率无损重建原始图像。不过，文献[9]的可分离算法解密图像质量较低，即使嵌入率低至约 0.016 bpp，平滑图像(如 Lena)和纹理图像(如 Baboon)的解密图像与原始图像的 PSNR 分别仅为 35 dB 和 24 dB 左右。[1]是将图像按列分块，并计算每一个块的均值，将均值放在每一个块的第一个像素的位置，采用 mod256 对图像进行加密，嵌

入信息为 1 时则将每一个块除均值像素外的像素加 1，嵌入为 0 则保持不变，在提取信息恢复图像时，根据数学公式对整个块进行判断嵌入的信息为 1 还是 0，提取信息后便能完全恢复图像。综合以上文献的的处理方法和嵌入信息量的算法综合考虑提出了本文的算法，主要在提升信息的嵌入率。

在文献[1]中，嵌入的信息的大小与分块的个数有关，即分多少个块嵌入多少比特的信息。文献[1]中分块大小为 256 * 1，那么 512 * 512 大小的图像只能嵌入 1024 比特的数据。相比于其他算法来说，嵌入的容量太少了。经过实验仿真分析发现文献[1]中分块最小为 229 左右，最多能嵌入 1144 比特的数据，如果块小于 229，则提取的信息错误率会上升，导致我们恢复出来的图像和原始图像的 PSNR 降低。经过对像素的分析，我们发现，块分小了之后，通过原算法的提取方式算出的区间不准确。[1]的提取公式如下公式(1) (2)所示：

$$B \in \left(\frac{(x+1)A}{x} - \frac{255}{x}, \frac{(x+1)A}{x} \right) \text{提取为 } 0 \tag{1}$$

$$B \in \left(\frac{(x+1)A}{x}, \frac{(x+1)A}{x} + \frac{255}{x} \right) \text{提取为 } 1 \tag{2}$$

其中 B 为含有隐藏信息的解密图像中每一个块的均值，x 为分块的大小，A 为块中第一像素值，也就是该块中所有原像素的均值。从公式中，我们得知，如果 x 过于小，那么 255/x 偏大，该区间可能存在重合部分或者 B 不在该区间上等情况，所以，如果块分小了之后用该方法提取信息是不准确的。

5. 结论

本文的加密方法和文献[1]是一样的。在嵌入信息时将加密图像除均值外的像素改变大一点，在提取信息时，通过均值像素的相邻像素对均值像素的预测从而正确提取信息并且恢复原始图像。但是文献[1]中的算法提取信息，则块分小了(分母变大了)，区间的值不准确(X 为块的大小)。

在这篇文献中，基于文献[1]改进的算法被提出了。修改了嵌入方法并且通过相邻像素的相关性提取信息完美恢复了图像，通过此操作提高了它的嵌入容量，降低了信息提取的错误率。该方法的实验结果表明嵌入容量比文献[1]大得多，并且致我们恢复出来的图像和原始图像的 PSNR 值变化不大，这说明在加密和解密的过程中图像的画质得到了很好的保护。此外在直方图中可以直观的看出加密和嵌入信息后的直方图均匀。并且通过本文的算法，在仿真分析结果可以看出块的大小与信息提取错误的趋势明显下降且更加稳定。因此在文献[1]的基础上，提出了一种基于相邻像素的预测来判断均值像素的值，并且恢复原始图像。本文的算法改进过程为计算均值、加密图像、嵌入信息、解密图像、提取信息恢复图像，成功的实现了增大嵌入容量，提取正确信息的效果。

参考文献

[1] Zhang, W.M., Wang, H., Hou, D.D. and Yu, N.H. (2016) Reversible Data Hiding in Encrypted Images by Reversible Image Transformation. *IEEE Transactions on Multimedia*, **18**, 1469-1479.

[2] Yi, S. and Zhou, Y. (2015) An Improved Reversible Data Hiding in Encrypted Images. *IEEE China Summit and International Conference on Signal and Information Processing*, Chengdu, 12-15 July 2015, 225-229. https://doi.org/10.1109/ChinaSIP.2015.7230396

[3] Qian, Z.X., Xu, H.S., Luo, X.Y. and Zhang, X.P. (2018) New Framework of Reversible Data Hiding in Encrypted JPEG Bitstreams. *IEEE Transactions on Circuits & Systems for Video Technology*, **99**, 1-1. https://doi.org/10.1109/TCSVT.2018.2797897

[4] Agrawal, S. and Kumar, M. (2017) Mean Value Based Reversible Data Hiding in Encrypted Images. *Optik*, **130**, 922-934. https://doi.org/10.1016/j.ijleo.2016.11.059

[5] Xiang, S.J. and Luo, X. (2017) Efficient Reversible Data Hiding in Encrypted Image with Public Key Cryptosystem.

EURASIP Journal on Advances in Signal Processing, **2017**, 59.

[6] Qian, Z.X. and Zhang, X.P. (2016) Reversible Data Hiding in Encrypted Images with Distributed Source Encoding. *IEEE Transactions on Circuits and Systems for Video Technology*, **26**, 636-646. https://doi.org/10.1109/TCSVT.2015.2418611

[7] Qian, Z.X., Zhang, X.P. and Feng, G.R. (2016) Reversible Data Hiding in Encrypted Images Based on Progressive Recovery. *IEEE Signal Processing Letters*, **23**, 1672-1676. https://doi.org/10.1109/LSP.2016.2585580

[8] Zhang, X.P., Qin, C. and Sun, G.L. (2012) Reversible Data Hiding in Encrypted Images Using Pseudorandom Sequence Modulation. *Proceedings of IWDW*, LNCS, Berlin, 358-367.

[9] Wu, X.T. and Sun, W. (2014) High-Capacity Reversible Data Hiding in Encrypted Images by Prediction Error. *Signal Processing*, **104**, 387-400. https://doi.org/10.1016/j.sigpro.2014.04.032