基于加密图像的可逆信息隐藏

彭青梅 * ** 禹谢华 * ***
PENG Qing-mei YU Xie-hua

摘 要 加密图像的可逆信息隐藏对于数据处理过程中的信息安全可以起到双重保险的作用，加密对数据信息进行保护，而嵌入的秘密数据可以起到在解密后监视多媒体数据的传输中是否被篡改，验证其完整性和原始载体的无损恢复。本文阐述了信息隐藏技术，介绍可逆信息隐藏技术的研究现状，分析了基于加法同态的直方图多峰值平移的可逆信息隐藏算法与基于 Paillier 同态公钥加密与预测误差的可逆信息隐藏算法。

关键词 信息隐藏；可逆；加密图像

doi：10.3969/j.issn.1672-9528.2018.12.017

1 信息隐藏技术概述

信息隐藏技术是把秘密信息隐藏在多媒体信息中的一种方法。图像是最适合信息隐藏的数据载体。信息隐藏的方法主要有数字水印技术、隐写术等。

信息隐藏可以分为有损信息隐藏与可逆信息隐藏信息隐藏技术，区别在于接收端是否能无失真恢复载体。有损信息隐藏技术可以应用于多媒体数据的版权保护场景，接收端提取秘密数据后不能完全恢复载体。可逆信息隐藏可应用在多媒体数据的非法篡改后，可以验证其完整性并无损恢复，比如医疗诊断信息等，在接收端提取秘密信息后可以无失真恢复载体。

如图 1 所示，信息隐藏技术的分类：根据信息隐藏的载体是否会造成永久性失真分为有损信息隐藏和可逆信息隐藏，可逆信息隐藏又根据信息隐藏是否有加密分为密文域可逆信息隐藏和非密文可逆信息隐藏。

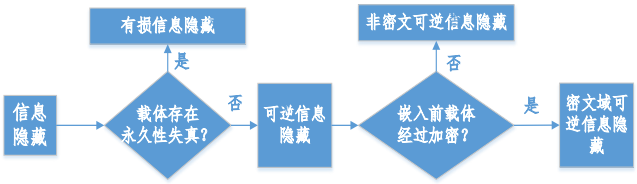

图 1 信息隐藏技术的分类

* 福建师范大学闽南科技学院 福建泉州 362332
** 华侨大学 福建厦门 361005
*** 厦门大学信息科学与技术学院 福建厦门 361005
[基金项目] 课题项目：2018 福建省中青年教师教育科研项目“科技类”课题，项目编号：JT180830；课题项目：2018 年泉州市科协资助项目，批准文号：泉科协【2018】65 号

2 加密图像的可逆信息隐藏的意义

随着信息技术的不断发展，通信、信息安全领域的研究可以从不同的角度去探究，多媒体数据在通信的传输中，极易遭受到了非法截取、内容篡改等。多媒体数据涉及到的内容，小到版权保护和隐私保护，如医疗诊断信息、所有权信息、身份验证数据或软件序列号，大到国家军事国防方面的图像信息。因此，保护信息安全变得尤其的重要。

图像的加密和信息隐藏是保护信息安全的研究方向。密码学是通过加密可以保证数据内容的安全性。信息隐藏技术是通过嵌入秘密数据来验证其多媒体数据的完整性。

加密图像的可逆信息隐藏对于数据处理过程中的信息安全可以起到双重保险的作用，加密对图像数据内容进行保护，而嵌入的秘密数据可以起到在解密后监视多媒体数据的传输中是否被篡改，验证其完整性和原始载体的无损恢复，可以应用的场景，如远程医学诊断、云环境下加密数据标注、司法上的数字取证等。

3 可逆信息隐藏研究现状

可逆信息隐藏技术的研究中，Tian[1] 提出了可逆信息隐藏技术的差分展开机制，通过将相邻像素差加倍并调整奇偶校验，将秘密数据嵌入到原始图像中。Ni[2] 等人首先提出了基于直方图平移的可逆信息隐藏方法，对图像直方图中的峰值点平移，修改像素值实现了可逆的秘密数据嵌入。M.Thodi 和 J.J.Rodriguez[3] 中引入了预测误差扩展策略，充分利用图像像素冗余，取得了不错的率失真性能。Qin[4] 等根据图像局部复杂度的分布自适应地选择参考像素，并提出了基于

?1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

预测的直方图平移的方案，该方案可以获得数据嵌入时预测误差的集中直方图。J. Fridrich 和 M. Goljan[5] 提出对图像压缩腾出空间来嵌入秘密信息实现可逆信息隐藏。

加密图像的可逆信息隐藏，是将加密技术和信息隐藏技术两者结合起来，分别从内容和存在的不同角度保护信息的安全性，主要有两种情况：第一种，先加密原始图像，在加密图像后嵌入秘密信息；第二种，先在原始图像嵌入秘密信息再加密，得到密文图像。比如在云服务端，可以在用户加密过的图像内容中嵌入额外的数据，图像内容所有者在保护隐私不泄密的同时，这样，经过标记的加密图像就可以在云上进行有效的管理，经过授权的接收方可以正确提取嵌入的数据，并能无损地恢复原始明文图像。因此，对加密图像的可逆信息隐藏方案，从加密后的图像中找到空间进行数据隐藏，保证数据提取和图像恢复。

文献 [8]-[10] 张和项提出的基于公钥加密的可逆信息隐藏算法就是利用公钥加密的加法同态性设计出了加密可逆信息隐藏算法，文献 [11] 中肖也提出了利用具有加法同态性的加密算法处理原文图像后，再利用多层差值直方图平移进行秘密数据嵌入。在加密图像信息隐藏领域引入了同态加密技术的早期算法，引用 Okamoto-Uchiyama 公钥密码 [14] 来加密原文数据，通过利用加密系统的同态属性适应性替换量化后的密文图像 DCT 系数来嵌入数字水印。

同态算法尤其是全同态加密技术的计算复杂度与密文扩展极大地影响了加密图像秘密数据嵌入的效率，这种情况可以引入密文压缩技术有效提高嵌入效率，Zhang[7] 提出了一种独立可分的加密域图像的可逆信息隐藏算法，是利用密文压缩技术实现可分离的代表算法，一种典型的加密图像的可逆信息隐藏方案。

4 加密图像的可逆信息隐藏

加密图像的可逆信息隐藏研究，提出研究内容包括以下两个方面：

4.1 基于加法同态的直方图多峰值平移的可逆信息隐藏算法。

Subramanyam 等人提出的加密算法 [6]，这种加密算法具有加法同态性。加密原始图像 M，由一个秘密种子 s 用 RC4 算法得到密钥流 K。加密算法对每一个像素进行模加运算得到加密图像 C：

C=E(M,K)=(M+K)mod256=($m_{i,j}+k_{i,j}$)mod256= $C_{i,j}$

$i=1,2,3,...,n$

$j=1,2,3,...,n$

初始灰度图像 M；随机产生密钥流 K；n 表示图像的像素个数；$m_{i,j}$ 表示 M 的第 i 行 j 列个像素；$C_{i,j}$ 表示 C 的第 i 行 j 列个像素；$k_{i,j}$ 表示 K 的第 i 行 j 列的值。

加密图像 C 的相邻像素模减得到差值：

$$\begin{aligned} d_{i,j} &= (c_{i,j+1}-c_{i,j}) \bmod 256 \\ &= ((m_{i,j+1}+k_{i,j+1}) \bmod 256-(m_{i,j}+k_{i,j}) \bmod 256) \bmod 256 \\ &= (m_{i,j+1}+k_{i,j+1}-m_{i,j}-k_{i,j}) \bmod 256 \end{aligned}$$

（在构造 $k_{i,j}$ 时，令组成相邻像素对的 $k_{i,j}$ 相同）

因此，$d_{i,j}=(m_{i,j+1}-m_{i,j}) \bmod 256$

由上可知，密文域像素模减的差值和明文域像素模减的差值是一样的，差值构成差值直方图。通过多层差值直方图平移进行信息嵌入。本文提出了将图像分块通过不同的扫描方式得到最优最多峰值之和的差值直方图，进行多层平移信息嵌入，可以根据不同的载体图像提高信息嵌入容量。

4.2 基于 Paillier 同态公钥加密与预测误差的可逆信息隐藏算法。

同态性加密算法首先由 Rivest 等人所提出 [12]。现有的基于 Paillier 同态公钥加密的可逆信息隐藏算法计算复杂度高，运算成本较大，例如文献 [8]。于此，文献 [13] 提出了一种新的加密图像的可逆信息隐藏算法，先在原始图像预留空间嵌入秘密数据，图像加密前，将载体图像分为嵌入像素和参考像素，通过嵌入像素点的四个相邻的上下左右参考像素值来计算它的预测像素值，实际像素值与预测像素值运算获得预测误差值。把预测误差值小于阈值 T 的嵌入像素定位为目标像素，可以映射成一张目标像素定位表。

目标像素定位后，图像进行 Paillier 同态加密：

$C(i,j)=g^{m(i,j)} \cdot (r(i,j))^n \bmod n^2$

再把秘密数据用相同的密钥和加密算法加密，信息隐藏者将待嵌入的额外信息组成伪像素，根据定位表的位置信息，替换目标像素的值，完成秘密信息嵌入。发送方不需要发送定位表。接收方拥有相应的密钥，图像解密前，都可以根据目标像素定位表来提取秘密信息。图像解密后，可以通过四个相邻像素的预测误差值提取秘密信息并恢复图像。

5 总结

本文阐述信息隐藏技术，介绍可逆信息隐藏技术的研究现状，分析介绍了基于加法同态的直方图多峰值平移的可逆信息隐藏算法与基 Paillier 同态公钥加密与预测误差的可逆信息隐藏算法。此次加密图像的可逆信息隐藏仅限于理论研究阶段，在具体的实施过程中可能会遇到一些实际问题，这

?1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

就需要在实验验证算法的过程中从实际出发，不断调整改进算法的思路，客观的对理论进行更正和完善；其次，是在前人研究的基础上进行的创新，部分问题仍需进一步斟酌研究。

参考文献：

[1] Tian J. Reversible data embedding using a difference expansion[J]. IEEETransactions on Circuits and Systems for Video Technology, 2003, 13(8):890−896.

[2] Ni Z, Shi Y Q, Ansari N, and W. Su, “Reversible data hiding,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, 2006.

[3] M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible watermarking,” IEEE Transactions on Image Processing., vol. 16, no. 3, pp. 721–730, 2007.

[4] C. Qin, C. C. Chang, Y. H. Huang, and L. T. Liao, “An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 23, no. 7, pp. 1109–1118, 2013.

[5] J. Fridrich and M. Goljan, “Lossless data embedding for all image formats,” in SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, vol. 4675, pp. 572–583, 2002.

[6] Subramanyam A.V, Emmanuel S, Kankanhalli M. Robust watermarking of compressed and encrypted JPEG2000 images[J]. IEEE Transactions on Multimedia, 2012, 14(3): 703-716.

[7] Zhang X. Separable reversible data hiding in encrypted image[J]. IEEE Trans. Inf.Forensics and Security, 2012, 7(2): 826-832.

[8] ZHANG X P，LOONG J，WANG Z，et al．Lossless and reversible data hiding in encrypted images with public key cryptography［J］．IEEE Transactions on Circuits and Systems for Video Technology，2015，26(9) : 1622 — 1631．

[9] ZHANG X．Commutative reversible data hiding and encryption［J］．Security and Communication Networks，2013，6 (11) :1396 — 1403．

[10] 项世军，杨乐．基于同态加密系统的图像鲁棒可逆水印算法．软件学报，2018,29(4). http://www.jos.org.cn/1000-9825/5406.htm Xiang SJ, Yang L. Robust and reversible watermarking algorithm in encrypted image with homomorphic cryptosystem. Ruan Jian Xue Bao/Journal of Software, 2018,29(4).

[11] 肖迪，王莹，常燕廷，等．基于加法同态与多层差值直方图平移的密文图像可逆信息隐藏算法 [J]. 信息网络安全，2016（4）：9-16.XIAO Di, WANG Ying, CHANG Yanting, et al. Reversible Data Hiding in Encrypted ImageBased on Additive Homomorphism and Multi-level Difference Histogram Shifting[J]. Netinfo Security, 2016(4):9-16

[12] R. L. Rivest, A. Shamir, and L. M. Adleman, —A method for obtaining digitalsignature and public-key cryptosystems, ‖ Commun. Assoc. Comput. Mach.,vol. 21, no. 2, pp.120–126, 1978.

[13] 项世军，罗欣荣． 同态公钥加密系统的图像可逆信息隐藏算法［J］．软件学报，2016， 27(6) : 1592 — 1601．

[14] OKAMOTO．T，UCHIYAMA．S．A new public-key cryptosystem as secure as factoring［C］Proceedings of the 1998 International Conference on the Theory and Application of Cryptographic Tech- niques．Berlin: Springer，1998: 308 — 318．

[15] Kuribayashi M, Tanaka H. Fingerprinting Protocol for Images Based on Additive Homomorphic Property[J]. IEEE Trans. Image Processing, 2005, 14(12):2129-2139.

【作者简介】

彭青梅（1989-），女，硕士研究生，助教，网络工程师，研究方向：网络安全；

禹谢华（1982-），男，汉族，湖南邵东人，硕士，副教授。研究方向：人工智能、无线传感器网络、信息与网络安全。

（收稿日期：2018-12-11）

?1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net