图中图？采用新型面向键值图隐写术的多图范式

Subhrangshu Adhikary

计算机科学与工程系，B.C. Roy工程学院，杜尔加布尔，西孟加拉邦，印度 – 713206 subhrangshu.adhikary@spiraldevs.com

摘要。 隐写方法一直是研究与开发的热点，旨在将秘密数据隐藏于载体媒体中，使其不被常规可视化察觉。对于 RGB图像，8 位颜色编码的最低有效位（LSB）使得用加密消息的比特替换最后两位成为可能。人们已开发出多种将一幅图像隐藏在另一幅图像中的方法，但在大多数情况下，载荷图像必须处于载体图像可容纳的范围内，而关于如何在多幅图像中隐藏多幅图像的研究文献则寥寥无几。本文提出一种新颖方法，将图像拆分为由键值对组成的 JSON样式字典，并利用元数据图定位整个载体图像集群中载荷图像的不同部分及其位置。该模型可轻松应用于现实场景，在不被察觉的情况下通过公共通信信道私密地共享秘密数据。

关键词： 图像隐写术、键值映射图、最低有效位嵌入、隐私保护、图像处理

1 引言

为了确保数据通过公共通信信道传输时的隐私，人们开展了相关方法的研究，并由此产生了不同的隐写技术 [1]。隐写术是一种将数据隐藏在宿主文件中而不被察觉的方法，尤其适用于直接采用密码加密会引起怀疑的环境 [2]。根据宿主介质的不同，隐写术包括将数据隐藏在图像、声音、文本、视频或其他计算机文件中。图像是最广泛使用的隐写载体媒体之一 [3]。在图像中隐藏数据可以采用不同的方法，通常包括最低有效位（LSB）嵌入、掩蔽与滤波技术、冗余模式编码、加密与散布，以及最后的编码与余弦变换 [4]。在所有这些方法中，最低有效位嵌入是最简单且应用最广泛的技术 [5]。这种方法不会引起怀疑，因为可以在图像中隐藏大量数据，并且隐写图像的大小始终接近原始图像 [6]。在这种方法中，通过用秘密数据替换图像的最低有效位来创建隐写图像。通常使用 1 位会使像素颜色强度改变约

±1 个单位，因此隐写图像几乎无法被区分，但这会使数据存储容量非常有限 [7]。使用 3 位会使像素颜色强度改变最多 ±5 个单位，从而提供较大的数据存储容量，但与原始图像相比，隐写图像会出现明显差异 [8]。因此，通常使用 2 位来存储数据，这会使颜色强度改变最多 ±3 个单位，因此隐写图像与原始图像之间的差异非常小，肉眼无法辨别；此外，使用 2 位也能提供较为充足的数据存储容量 [9]。

JavaScript 对象表示法（JSON）是一种基于键值对字典的数据通信格式，其中使用“{”和“}”标记数据块的起始和结束，键用“..”引号括起，值则根据相应的数据类型书写 [10]。数据可以嵌套，值也可以是数组类型。这种方法可用于存储数据集的元数据，以及与秘密数据中间阶段相关的不同值 [11]。

大多数基于最低有效位（LSB）在图像中隐藏数据的隐写术研究都用于隐藏文本数据。然而，近年来，各种图像矩阵扁平化技术逐渐流行起来，可将图像数据存储在图像中；但当载荷文件较大时，载体媒体便无法容纳秘密图像 [12-13]。其他技术则通过多张载体图像来容纳单张图像的数据，但针对将多张秘密图像分散存储在多张载体图像中的研究仍然很少 [14-15]。这促使我们开发了这种新方法：通过对图像进行扁平映射、将其拆分为数据块，并结合元数据和基于图的映射来组织 JSON，从而将多张秘密图像存储在多张载体图像中。该技术的细节及其性能将在下文讨论。

2 方法论

所提出的方法论用于在经过多个中间步骤的多个图像中隐藏和提取多个图像。具体细节将在下文中说明。

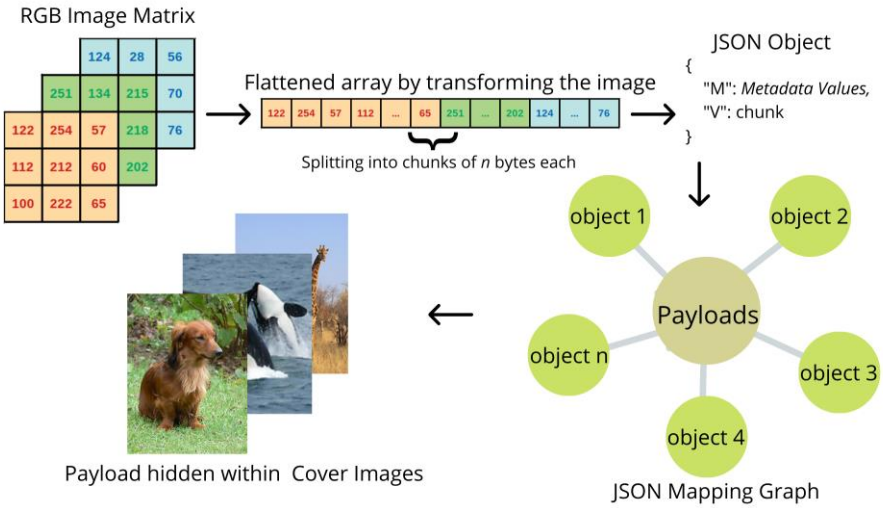

图 1. 所提出的多图像范式方法的表示过程：首先将图像的 RGB矩阵展平并划分为大小为 *n* 字节的数据块，然后将这些数据块与图像的元数据属性一起转换为 JSON 对象。随后，利用这些对象以字符串形式创建 JSON映射图，最后通过最低有效位插入法将该字符串嵌入载体图像中

2.1 处理载荷图像

所提出算法中最重要的部分，是对载荷图像进行处理，以便以一种即使将数据分散到多个图像中之后也能轻松恢复的方式将其嵌入其中 [16]。为此，采用了 flatmap技术，将单个图像矩阵转换为一维数组。在此过程中，将每种颜色（即红色、绿色和蓝色）的矩阵分别转换为一维数组：依次追加每一行，最后再依次追加各颜色对应的一维数组。对每个载荷图像重复执行相同的过程。

完成此步骤后，根据载体图像的载体尺寸，将这些一维数组分别划分为相应大小的数据块。如果数据块大小过小，JSON图元数据会占用大量数据，而在此过程中仅有很少的像素保持空闲。如果数据块大小过大，JSON图元数据的大小虽然较小，但载体图像中会有大量像素保持空闲。因此，综合考虑这些因素，实验采用了 512 字节的数据块。

2.2 映射图与 JSON键值对字典

将载荷图像展平并划分为大小合适的数据块后，使用 JSON 创建映射图。为此，JSON 中的前两个键值对包含载荷图像和载体图像的数量。接下来，嵌套JSON 对象的子对象包含每幅图像 [17-18] 的详细信息。其中，元数据包含原始载荷图像的形状，包括高度、宽度、颜色映射表、数据块数量等。相应的图像数据键则包含一个元组数组，其中记录了数据块在图中的位置，编号为

用于识别载荷图像以及每个 512 字节的处理后的数据块。随后使用此 JSON 生成最终字符串，以嵌入载体图像中[19-20]。

2.3 将数据嵌入载体图像的最低有效位

在完成载荷图像的处理并为每个载荷图像准备好 JSON 图字符串后，将准备好的载荷字符串插入每个图像像素 [21-22] 的最低两个有效位中。根据通用的隐写术最低有效位插入方法，载荷字符串中的每个位将按照载体图像的可编码容量，依次连续嵌入载体图像中。因此，生成隐写图像 [23-24]。

2.4 载荷图像提取

生成隐写图像后，还需要对其进行解码以提取载荷。为此，分别对所有隐写图像的最低有效位进行解码，并根据每个隐写图像的 JSON 字符串中的图映射，将其组合到所需位置。随后，对组合后的字符串进行排列，分别合并每个图像被拆分的数据块；然后，根据图像的元数据，将扁平化一维数组重塑为图像矩阵，最终提取出隐藏图像 [25-26]。

3 结果与讨论

通过组合构成映射图的扁平化 RGB 矩阵数据块的 JSON对象，完成了载荷字符串的最低有效位嵌入。该文本已在 8 张载体图像和 2 张载荷图像上执行。8 张载体图像分别包括狗、鲸鱼、长颈鹿、马、松鼠、骆驼、老虎和鱼的照片，2 张载荷图像则包括猫和鹦鹉的照片，如图 2 所示。组合这 8 张图像后，在每个点使用 2 个最低有效位时，共有 38115048 个、每个包含 2 位的槽位可用于存储数据。组合后的 2 张载荷图像需要 35047586 个 2 位槽位的空间；然而，由于 JSON映射图的创建和填充，约需额外 5% 的空间，使载荷字符串大小达到 37228972。这使可用空间的利用率达到 97.67%。在配备 Intel i3 6th Gen CPU 和 12 GB 随机存取存储器的计算机上，该方法对图像进行编码需要 74.7 秒，解码需要 19.1 秒。



图 2。图中展示了左侧的 8 幅隐写图像，它们在未被明显察觉的情况下隐藏了右侧的两幅载荷图像

隐写图像在视觉上与原始图像没有明显差异。然而，观察其颜色强度直方图时，差异十分明显。图 3 展示了一张图像（例如鲸鱼图像）与其隐写对应图像的直方图对比。可以观察到，尽管原始图像与隐写图像之间不存在可察觉的视觉差异，但二者的直方图存在显著差异，表明最低有效位发生了修改。原始图像中所有像素特定强度值的计数最大值约为 110000，而隐写图像中的最大值约为 175000。分别观察各个颜色通道可以发现，对于原始图像和隐写图像，红色在接近 110 的强度值处出现次数最多；但红色值在原始图像中出现的最高次数约为 78000，在隐写图像中约为 123000。同样，对于绿色，两张图像的强度最大值均出现在约 140 处，但该强度值在原始图像中出现的最高次数约为 76000，在隐写图像中约为 125000。最后，对于蓝色，两张图像的最大值均出现在接近 165 的强度值范围内，但原始图像的最大值约为 80000，隐写图像的最大值约为 124000。

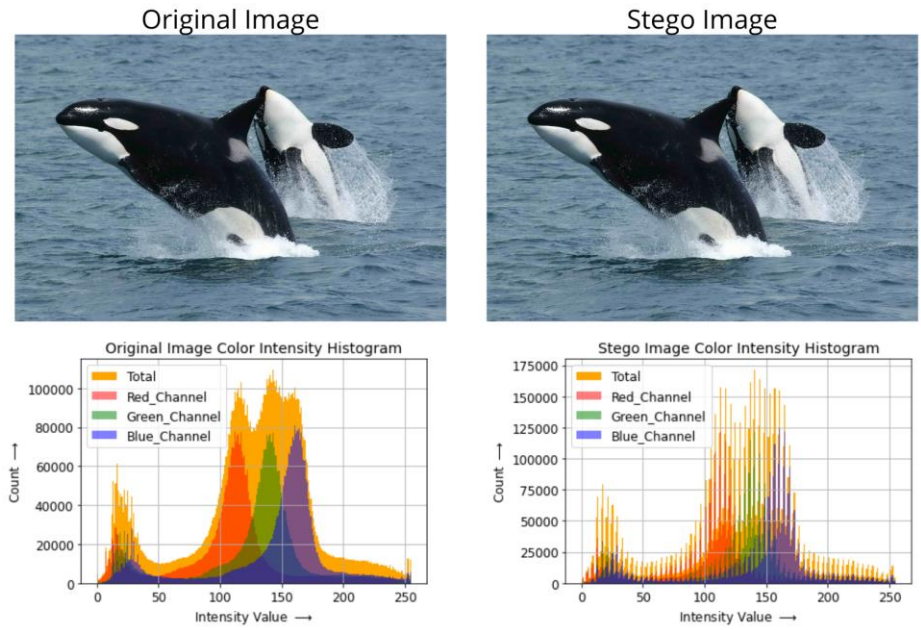

图3。原始图像与隐写图像并排对比，以及它们各自的颜色强度直方图

仔细观察可以发现，原始图像的直方图呈均匀分布，没有突然出现的尖峰；而隐写图像的直方图则呈离散分布，几乎以规则的间隔出现空隙。这是因为在自然图像中，除不同颜色、纹理或强度之间的明显边界外，相邻像素值的变化都很平滑。另一方面，隐写图像的最后两位已被修改，使得每个相邻像素之间以及全部三个颜色矩阵中的强度都产生了 ±3 的差异。这破坏了颜色变化的自然连续性，使直方图呈离散分布。这也是最低有效位方法的局限之一：尽管图像间的差异无法通过视觉辨别，但只需一个简单的直方图，就能轻易检测出图像是否经过隐写处理。因此，除了使用隐写术，还建议结合密码学技术加密载荷，以全面保护数据。这一现象也解释了为什么隐写图像中所有颜色的颜色强度最大值都远高于原始图像：颜色强度值中的空隙被叠加到了隐写图像直方图的尖峰上。

4 结论

隐写方法用于将消息隐藏在另一种载体媒体中而不被察觉。最低有效位（LSB）插入方法是一种流行的

用于隐藏数据的隐写方法，通过利用极低有效位将数据隐藏在图像中。人们已采用不同方法将一幅图像隐藏在另一幅图像中，但这些方法的可编码容量有限。本文提出一种解决这一问题的方法：引入一种基于 JSON映射图 的新方法，将多幅图像编码到多幅图像中。

该方法对RGB图像矩阵使用flatmap技术，然后将数据拆分为每个包含*n*字节的数据块，并使用这些数据块和图像的元数据创建JSON对象。最后，利用由此创建的对象生成映射图，进而生成可编码的载荷字符串。随后，通过最低有效位插入法将这些字符串嵌入载体图像中。该方法在视觉上无法区分，但可以通过直方图检测出来，因此还建议对载荷字符串进行密码加密，以提高安全性。

该方法可以轻松地以任意顺序将大型载荷图像文件嵌入多张载体图像中，随后将这些图像组合起来以恢复载荷文件。隐写图像可以通过公共通信信道进行共享，而不会在视觉上被察觉，从而维护隐私。此外，还可以改进该模型，使其能够在不被察觉的情况下将超大数据文件嵌入图像中，并通过使峰值分布更加均匀来减少离散直方图峰值。

致谢。本研究是The Gyanam Project的一部分，由Spiraldevs Automation Industries Pvt. Ltd.、印度与CubicX、印度共同合作完成。

参考文献

1. Gutub, A. 和 Al-Ghamdi, M., 2020年。利用多媒体图像隐写术隐藏份额，以优化基于计数的秘密共享。*Multimedia Tools and Applications*，*79*(11)，第7951-7985页。2. Duan, X.、Guo, D.、Liu, N.、Li, B.、Gou, M. 和 Qin, C., 2020年。结合图像椭圆曲线密码学与深度神经网络的新型大容量图像隐写方法。*IEEE Access*，*8*，第25777-25788页。3. Gutub, A. 和 Al-Shaarani, F., 2020年。基于最低有效位和离散小波变换隐写术比较的高效多图像秘密隐藏实现。*Arabian Journal for Science and Engineering*，*45*(4)，第2631-2644页。4. Adhikary S.、Ghosh R.、Ghosh A.（2021年）使用可穿戴传感器和机器学习进行无临床干预的步态异常检测。载于：Muthukumar P.、Sarkar D.K.、De D.、De C.K.（编）《Innovations in Sustainable Energy and Technology》。Advances in Sustainability Science and Technology。Springer，新加坡。https://doi.org/10.1007/978- 981-16-1119-3 31. 5 。5. Almazaydeh, L., 2020年。基于改进的最低有效位替换的安全RGB图像隐写。*International Journal of Embedded Systems*，*12*(4)，第453-457页。6. Islam, M.A.、Riad, M.A.A.K. 和 Pias, T.S., 2021年1月。使用视觉密码学增强图像隐写术的安全性。载于：*2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*（第694-698页）。IEEE。

7. AlKhodaidi, T. 和 Gutub, A., 2021年。改进图像隐写术分配，以提高多媒体基于计数的秘密共享的安全性。Multimedia Tools and Applications，80(1)，第1143-1173页。8. Adhikary S.、Chaturvedi S.、Chaturvedi S.K.、Banerjee S.（2021年）利用人工智能进行COVID-19传播预测与影响分析，以实现可持续全球卫生评估。载于：Siddiqui N.A.、Bahukhandi K.D.、Tauseef S.M.、Koranga N.（编）《Advances in Environment Engineering and Management》。《施普林格地球与环境科学会议录》。Springer，Cham。https://doi.org/10.1007/978-3-030-79065-3_30。9. Liao, X.、Yin, J.、Chen, M. 和 Qin, Z., 2020年。基于图像纹理特征的多图像隐写自适应载荷分配。《IEEE可靠与安全计算汇刊》。10. Hureib, E.S. 和 Gutub, A.A., 2020年。通过结合椭圆曲线密码学与图像隐写术增强医疗数据安全。《国际计算机科学与网络安全杂志》(IJCSNS)，20(8)，第1-8页。11. Sukumar, A.、Subramaniyaswamy, V.、Ravi, L.、Vijayakumar, V. 和 Indragandhi, V., 2020年。基于RIWT-拉普拉斯金字塔和直方图移位并使用深度学习的鲁棒图像隐写方法。《多媒体系统》，第1-16页。12. Shah, P.D. 和 Bichkar, R., 2021年。基于遗传算法的不可感知图像隐写技术与直方图失真最小化。载于《国际计算智能、数据科学与云计算会议论文集：IEM-ICDC 2020》（第62卷，第267页）。施普林格·自然。13. Kumar, S.、Kumar, S.、Singh, N.K.、Majumder, A. 和 Changder, S., 2018年8月。一种在彩色图像中隐藏文本数据的新方法。载于《2018年第7届国际可靠性、信息通信技术与优化国际会议（趋势与未来方向）》（ICRITO）（第577-581页）。IEEE。14. Mukherjee, S. 和 Sanyal, G., 2020年。结合N数码加密的图像隐写术。Multimedia Tools and Applications，79(39)，第29951-29975页。15. Alexan, W.、El Beheiry, M. 和 Gamal–Eldin, O., 2020年。三维图像隐写中不同数学序列的比较研究。《国际计算与数字系统杂志》，9(4)，第545-552页。16. Lu, S.P.、Wang, R.、Zhong, T. 和 Rosin, P.L., 2021年。基于可逆神经网络的大容量图像隐写术。载于《IEEE/CVF计算机视觉与模式识别会议论文集》（第10816-10825页）。17. Pramanik, S.、Singh, R.P. 和 Ghosh, R., 2020年。双正交小波变换和遗传算法在图像隐写术中的应用。Multimedia Tools & Applications，79。18. Cogranne, R.、Giboulot, Q. 和 Bas, P., 2020年6月。通过最小化统计可检测性实现隐写术：JPEG和彩色图像的案例。载于《2020年ACM信息隐藏与多媒体安全研讨会论文集》（第161-167页）。19. Vishnu, B.、Namboothiri, L.V. 和 Sajeesh, S.R., 2020年3月。结合像素值差异和边缘检测的增强型图像隐写术。载于《2020年第四届计算方法与通信国际会议》（ICCMC）（第827-832页）。IEEE。20. Adhikary S.、Chaturvedi S.K.、Banerjee S.、Basu S.（2021年）理化特征对海洋叶绿素分析与学习技术的影响。载于：Siddiqui N.A.、Bahukhandi K.D.、Tauseef S.M.、Koranga N.（编）《Advances in Environment Engineering and Management》。《施普林格地球与环境科学会议录》。Springer，Cham。https://doi.org/10.1007/978-3-030-79065-3_29。21. Kweon, H.、Park, J.、Woo, S. 和 Cho, D., 2021年。带私钥的深度多图像隐写术。《电子学》，10(16)，第1906页。22. Das, A.、Wahi, J.S.、Anand, M. 和 Rana, Y., 2021年。使用深度神经网络的多图像隐写术。arXiv预印本，arXiv:2101.00350。

23. Hong T.V.T.、Do P.（2019）SAR：一种具有文本流突发检测与可视化功能的基于图的系统。载于：Vasant P.、Zelinka I.、Weber GW.（编）《智能计算与优化》。ICO 2018。《智能系统与计算进展》，第866卷。Springer，Cham。https://doi.org/10.1007/978-3-030-00979-3_4。 24. Joshua Thomas J.、Pillai N.（2019）基于双向循环神经网络的图像描述生成深度学习框架。载于：Vasant P.、Zelinka I.、Weber GW.（编）《智能计算与优化》。ICO 2018。《智能系统与计算进展》，第866卷。Springer，Cham。 https://doi.org/10.1007/978-3-030- 00979-3 22。25 。Zaman S.U.、Karim R.、Arefin M.S.、Morimoto Y.（2020）采用混合加密提高数据安全性的分布式多云存储系统。载于：Vasant P.、Zelinka I.、Weber GW.（编）《智能计算与优化》。ICO 2019。《智能系统与计算进展》，第1072卷。Springer，Cham。https://doi.org/10.1007/978-3-030- 33585-4 6。26 。Lakhno V.、Akhmetov B.、Ydyryshbayeva M.、Bebeshko B.、Desiatko A.、Khorolska K.（2021）用于识别网络攻击的决策支持系统知识数据库构建模型。载于：Vasant P.、Zelinka I.、Weber GW.（编）《智能计算与优化》。ICO 2020。《智能系统与计算进展》，第1324卷。Springer，Cham。 https://doi.org/10.1007/978-3-030-68154-8_42。