



Study on Taste Visualization Schemes of Random Number Spectrum

Wei Qian

School of Information Technology and Engineering, Tianjin University of Technology and Education, Tianjin, China

Email address:

weiqian@tute.edu.cn

To cite this article:

Wei Qian. Study on Taste Visualization Schemes of Random Number Spectrum. *Science Innovation*. Vol. 10, No. 6, 2022, pp. 202-206.

doi: 10.11648/j.si.20221006.14

Received: November 1, 2022; **Accepted:** November 29, 2022; **Published:** December 8, 2022

Abstract: The use of random numbers can be seen everywhere in life and the performance directly affects the security of cryptosystems. So the research on properties of random numbers plays an important role in the field of information security. The inherent nature abstraction of random number spectrum makes it difficult to become aware of the distribution tendency. The available methods of visualization, such as Poincare plot, random walk, variant map and so on, seldom confront directly the original random number spectrum and lack taste. The paper put forward a taste visualization scheme of random number spectrum whose mission is to display the intrinsic distribution characteristics of the spectrum intuitively by using simple and interesting methods. The scheme unfolds the original random number spectrum along the two dimensional surface and three dimensional space with concise, vivid and ingenious properties, and makes use of thresholds to constrain iteration rounds and plot scales to ensure good visuals, and its results aim for promoting readers' intuitive experience and reducing the cognitive work. Especially the random chips can lead the readers to perceive the distribution of the spectrum figuratively, and stimulate the pleasant psychological feelings.

Keywords: Random Number Spectrum, Visualization, Taste

随机数谱的趣味可视化方法研究

韦潜

天津职业技术师范大学信息技术工程学院, 天津, 中国

邮箱

weiqian@tute.edu.cn

摘要: 随机数的运用在生活中随处可见, 随机数性能的好坏直接影响密码系统的安全, 随机数品质的研究在信息安全领域显得至关重要。随机数谱固有的抽象性很难感知其分布特征, 现有的可视化方法, 比如Poincare散点图、随机游走、变值转换等等, 较少直面原始的随机数谱, 且缺少趣味内涵。随机数谱趣味可视化方法旨在运用简单有趣的形式, 将数谱的内在分布特征直观展现出来。该方法将原始随机数谱沿二维平面和三维空间顺次铺展, 融入简洁、清晰、奇巧的趣味内涵, 并且引入阈值约束迭代轮次和绘图规模, 以确保良好的视觉效果, 获得的随机图谱有助于提升读者的直观体验, 减轻认知负担, 尤其是随机切片有益于引领读者形象感知数谱的分布特征, 同时激发愉悦的心理情愫。

关键词: 随机数谱, 可视化, 趣味

1. 引言

公元前一千多年的商朝，人们利用灼烧随机龟裂进行占卜[1]，《易经》中有蓍草起卦的记载[2]，骰子是产生随机数的有效工具[3]，最早的骰子发现于中东的一座公元前24世纪的墓穴里[4]。随机数的运用早已进入人们的生活。

2. 问题提出

随机数是这样的一些数，如果选取数序列 $\xi_1, \xi_2, \dots, \xi_n$ 处在0与1之间，这些数顺次有同样的概率在区间(0,1)内出现[5]。古籍《说文解字》中称“谱，籍禄也”。随机数谱就是对依照某种方法获得的随机数序列的记录。随机数谱固有的抽象性，使人很难直观感知其分布特征。可视化[6]可以将随机数谱的分布模式转换成直观的结果。

随机数谱中的每一个元素，以点坐标的方式绘制在一维数轴上，可以直观表现随机效果。但是，如果随机点多了就会影响视觉效果。

以时间为x轴坐标，随机数谱为y轴坐标，将随机数谱沿着时间轴展开，形成二维随机图谱。如果数据量不大，可以用线把点连接起来以显示趋势。只是随着时间的延伸，图谱会变得越来越长。

Poincare散点图[7, 8]以随机数谱的前后相邻点组成 (x,y) 坐标序列，方法简单有效。但是不管x坐标序列和y坐标序列来自同一随机数谱或是不同的随机数谱，都会与最初的随机数谱有所区别。

随机游走模型[9-11]以一种有趣的方式模拟随机数谱，但是对于(0,1)之间的随机数实现起来不够简单直观，并且动感游走会显得趣味更浓。

变值转换法将随机数谱转化为变值序列[12, 13]，进而形成绘图所需要的二维点坐标 (x,y) 。该方法借助变值反映随机数的分布，但是获得的随机图谱直接表现变值的分布，而不是最初的随机数谱。

本文提出随机数谱的趣味可视化方法，以简洁有趣的方式将随机数谱的分布特征展现出来，可以提升读者的直观体验，减轻认知负担。

3. 随机数谱的趣味可视化方法

趣而生乐，乐而生欢，趣问促思。将趣味设计[14, 15]融入随机数谱的可视化方法中，不仅可以将随机数谱内在的复杂度[16]进行转化，而且可以唤醒读者的愉悦情绪，发现被习惯意识所蒙蔽的事实。

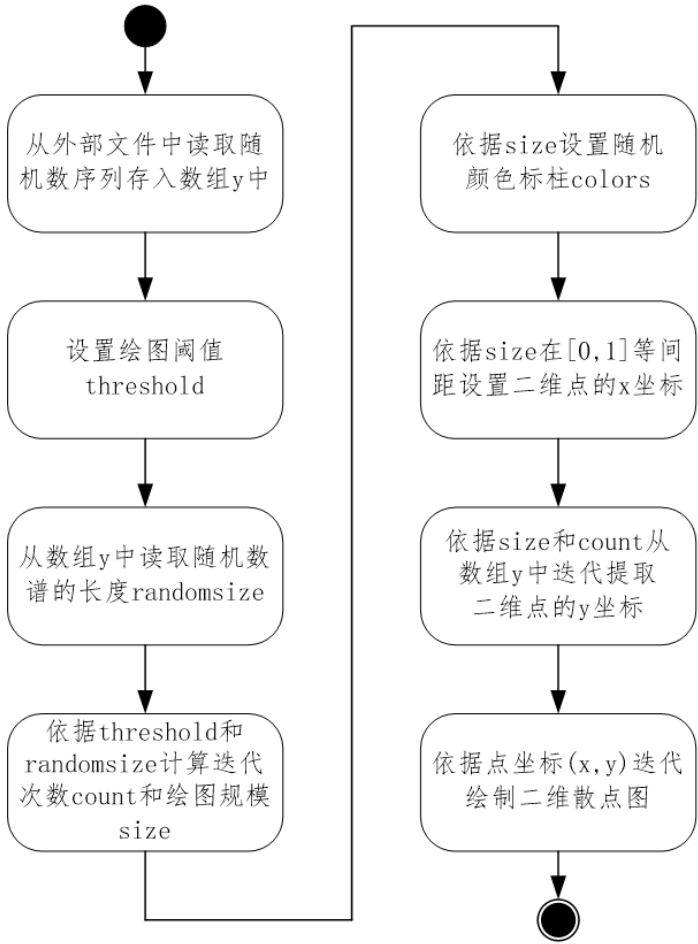


图1 二维可视化方法。

3.1. 二维可视化方法

设计思想为将一维随机数谱沿二维平面顺次展开，具体方法描述如图 1 所示。该方法使用阈值 threshold 限制绘图规模 size ，以保证获得清晰的视觉效果； x 坐标在 $[0,1]$ 区间按照绘图规模 size 轻巧展开，与随机数谱构成二维平面点的坐标 (x,y) ；依据超出阈值 threshold 的随机数谱剩余部分的长度，调整绘图规模 size ，将剩余随机数谱绘制在最后一张图上。

3.2. 三维可视化方法

设计思想为将一维随机数谱沿三维空间顺次展开，单轮迭代具体方法描述如图2所示。该方法使用阈值 threshold 限制绘图规模 size ，以保证视图清晰；在 $[0,1]$ 区间按照绘图规模 size 轻巧布局 x 坐标和 y 坐标，与随机数谱构成三维空间点的坐标 (x,y,z) ；绘制随机数谱沿 XOZ 平面的切片，并使平面切片顺次沿 y 轴展开，最终构成三维空间随机图谱。

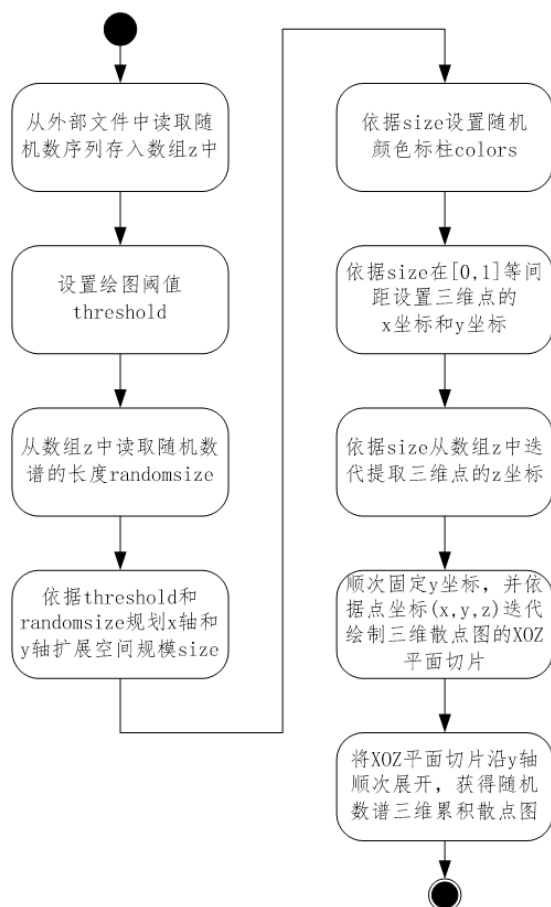


图2 三维可视化方法。

4. 实验与结果

实验采用 Windows 7 旗舰版 64 位操作系统，Intel(R) Core(TM) i3-3240 CPU 3.40GHz 处理器，安装内存 (RAM) 4.00 GB。实验在 Visual Studio Code 1.70.1 编辑器环境下，使用 Python 3.8.10 64-bit 完成。

4.1. 随机数谱二维可视化实验

随机数谱的长度为 5500，阈值 threshold 设置为 2000。正态分布随机数谱的单轮迭代可视化效果如图3所示，随机数谱剩余部分的可视化效果如图4所示。

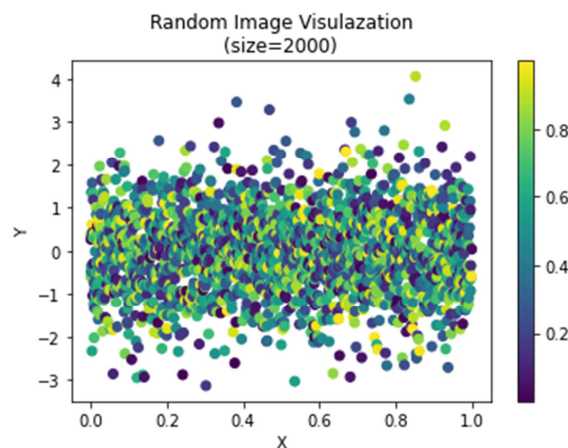


图3 正态随机数谱的二维可视化（规模=2000）。

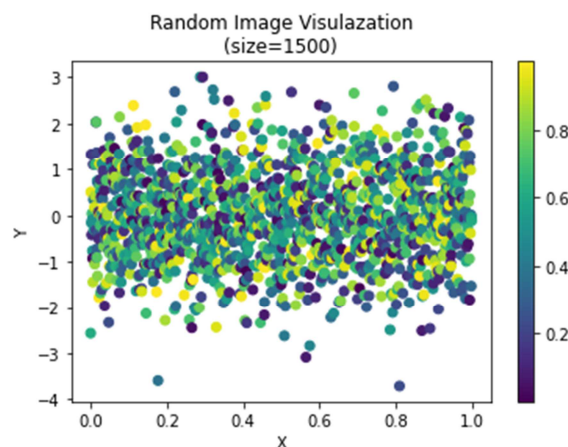


图4 正态随机数谱的二维可视化（规模=1500）。

均匀分布随机数谱的单轮迭代可视化效果如图5所示，随机数谱剩余部分的可视化效果如图6所示。

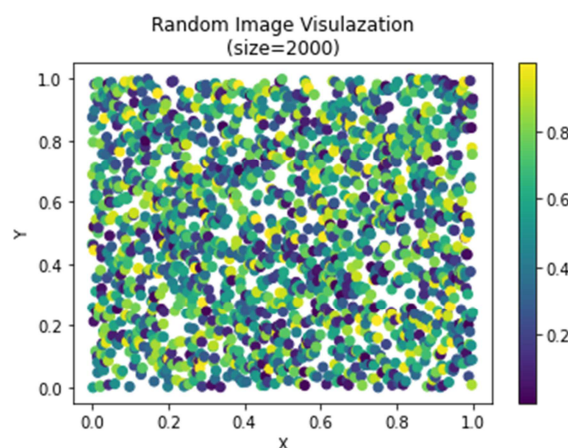


图5 均匀随机数谱的二维可视化（规模=2000）。

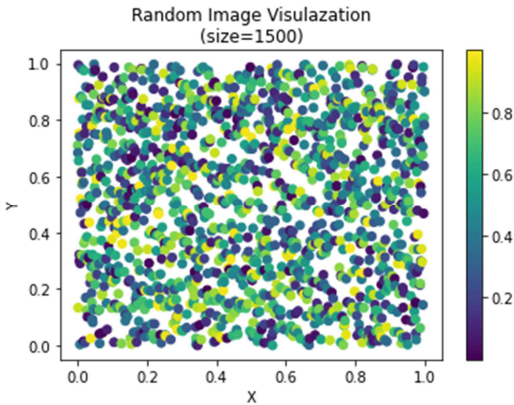


图6 均匀随机数谱的二维可视化（规模=1500）。

4.2. 随机数谱三维可视化实验

随机数谱的长度为10000，阈值threshold设置为10000。
若随机数谱的长度在阈值以内，则单轮绘制三维随机图谱；
若随机数谱的长度超过阈值，则迭代绘制三维随机图谱。
正态分布随机数谱的三维可视化效果如图7至图10所示，
均匀分布随机数谱的三维可视化效果如图11至图14所示，
分别展示一个切片、三个切片、五个切片和十个切片的效果。

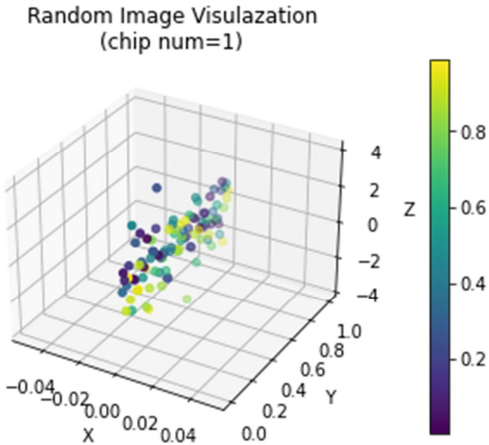


图7 正态随机数谱的三维可视化（切片数=1）。

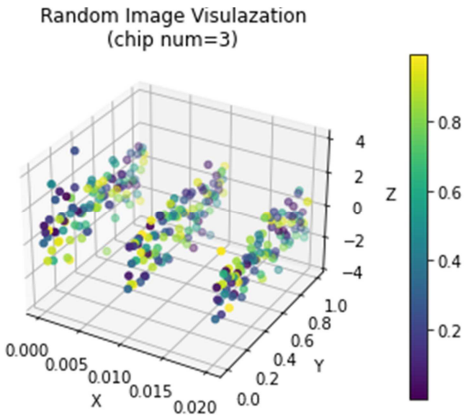


图8 正态随机数谱的三维可视化（切片数=3）。

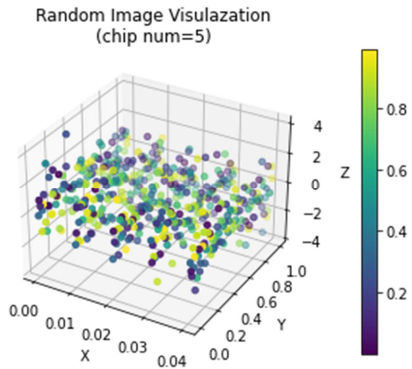


图9 正态随机数谱的三维可视化（切片数=5）。

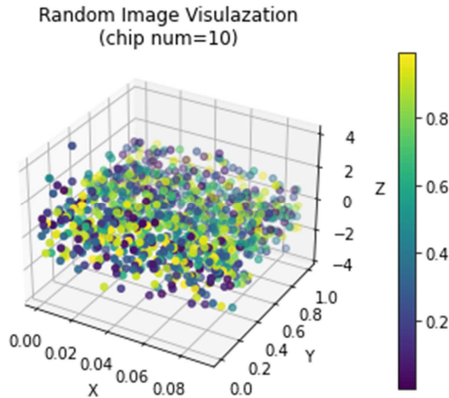


图10 正态随机数谱的三维可视化（切片数=10）。

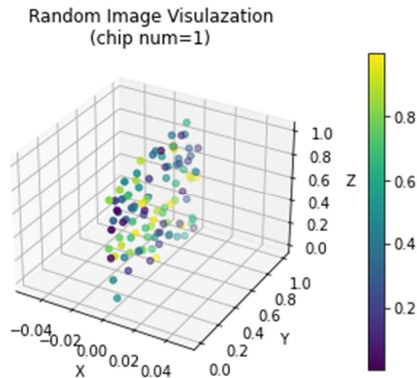


图11 均匀随机数谱的三维可视化（切片数=1）。

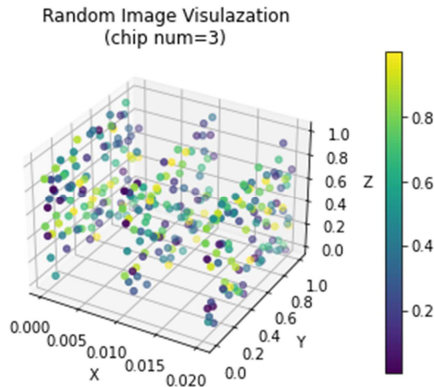


图12 均匀随机数谱的三维可视化（切片数=3）。

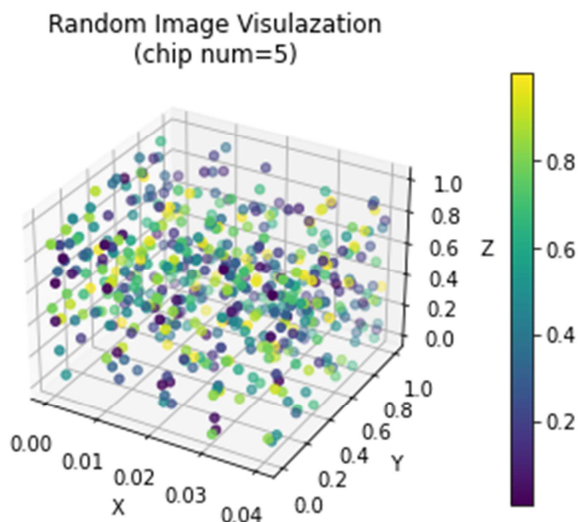


图13 均匀随机数谱的三维可视化（切片数=5）。

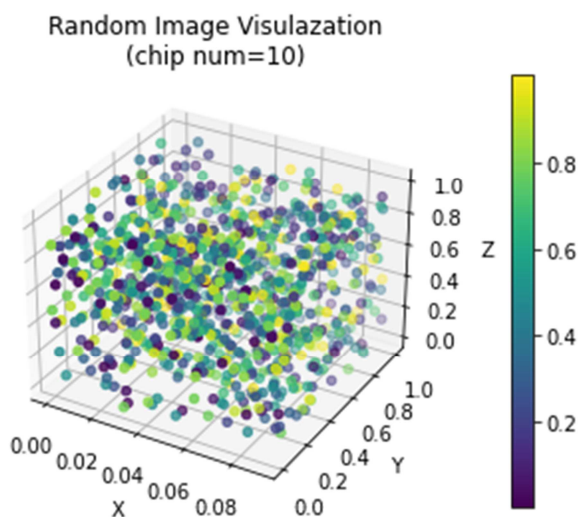


图14 均匀随机数谱的三维可视化（切片数=10）。

5. 结论

趣味可视化方法将原始随机数谱顺次沿二维平面和三维空间铺展，方法简洁轻巧直观，既可以感知随机数谱的总体分布趋势，又可以体验动态变化轨迹，降低读者认知负担，增添愉悦情趣。

致谢

本文为教育部高等教育司产学研协同育人项目《密码趣味研习场景下总体国家安全观的认知教育探索与实践》(202102602014)的阶段性成果之一。

参考文献

- [1] 懿恭. 我们最古的书: 甲骨文-龟册 [J]. 文物参考资料, 1954, (05): 24-28.
- [2] 贾连翔. 清华简《筮法》与楚地数字卦演算方法的推求[J]. 深圳大学学报 (人文社会科学版), 2014, 31 (03): 57-60.
- [3] GALTON F. Dice for statistical experiments [J]. Nature, 1890, 42 (1070): 13-14.
- [4] TASHIAN C. A brief history of random numbers [EB/OL]. (2017-03-10) [2022-10-10]. <https://tashian.com/articles/a-brief-history-of-random-numbers/>
- [5] 金星南. 在原子核物理学中的蒙特卡罗方法 [J]. 物理通报, 1963, (05): 225-232.
- [6] Nathan Yau. 数据之美[M]. 张伸, 译. 北京: 中国人民大学出版社, 2014: 66-71.
- [7] SUSHMA N B, GHANSHYAM D J, MONICA X, et al. Poincare plot: a simple and powerful expression of physiological variability [J]. MGM Journal of Medical Sciences, 2021, 8 (4): 435-441.
- [8] Ahmed S, Bhuiyan T A, Kishi T, et al. Human activity classification based on angle variance analysis utilizing the Poincare plot [J]. Applied Sciences, 2021, 11 (16): 7230. <https://doi.org/10.3390/app11167230>
- [9] PEARSON K. The problem of the random walk [J]. Nature, 1905, 72 (1865): 294.
- [10] Bellaachia A, Al-Dhelaan M. Random Walks in Hypergraph [J]. International Journal of Education and Information Technologies, 2021, 15 (2): 13-20.
- [11] Spitzer F. Principles of random walk, second edition [M]. New York: Springer-Verlag, 1976: 35-39.
- [12] 郑智捷. 多元逻辑函数的基础等价变值表示 [J]. 云南民族大学学报, 2011, 20 (5): 396-397.
- [13] ZHENG Z J. Novel pseudo random number generation using variant logic framework [C]// Edith Cowan University. Proceedings of the 2nd International Cyber Resilience Conference. Perth: Edith Cowan University, 2011: 100-104.
- [14] 方红梅. 梁启超趣味论研究[D]. 武汉: 武汉大学, 2008: 119-129.
- [15] 刘花弟. 设计与趣味研究 [D]. 南昌: 江西师范大学, 2004: 19.
- [16] SAFFER D. Designing for interaction, second edition: creating innovative applications and devices [M]. Berkeley: New Riders, 2009: 136-137.