基于伪随机数生成器的视频隐写算法

doi:10.3969/j.issn.1674-7100.2024.05.008

王勇智

湖南理工学院
信息科学与工程学院
湖南　岳阳　414006

摘　要：针对视频隐写的安全性和可靠性较低的问题，提出基于伪随机数生成器的视频隐写算法。将伪随机数生成器用于视频帧的选择，以增强隐写过程的随机性和不可预测性。伪随机数生成器产生的序列不同于传统固定模式的帧选择，其输出序列难以预测，使得攻击者难以从外部特征推断嵌入策略，从而降低被统计分析工具和机器学习模型检测的可能性。此外，用校验子格编码将秘密数据编码成冗余信息，以增强秘密数据的完整性，提升数据在复杂通信环境中的抗干扰性。实验结果表明，本算法能较显著提高视频隐写的安全性和隐蔽性，能有效抵抗统计分析攻击，并且在保持高数据嵌入率的同时，确保较低的错误率和较高的图像质量。

关键词：视频隐写技术；密码学；伪随机数生成器；校验子格编码；信息隐藏
中图分类号：TP309；TP391.41　　**文献标志码**：A
文章编号：1674-7100(2024)05-0058-05
引文格式：王勇智 . 基于伪随机数生成器的视频隐写算法 [J]. 包装学报，2024，16(5)：58-62.

1　研究背景

随着信息技术的快速发展，数字媒体已成为人们日常生活和工作交流的重要工具。在此背景下，信息隐藏技术，尤其是视频隐写技术，因其在保密通信中的应用而受到广泛关注[1]。视频隐写技术的核心目标是在不引起视觉可察觉改变的前提下，将秘密信息隐藏于视频文件中。然而，随着检测技术的不断进步，传统的隐写技术面临着越来越多的安全挑战，尤其是在抵抗统计分析和机器学习模型识别方面的能力有待提升[1]。

目前，视频隐写技术主要通过帧选择与帧嵌入两种技术来实现。在帧选择过程中，虽然事先约定特定帧的方法可以在一定程度上保证信息的正确提取，但这种基于明显特征的帧选择方式也增加了被统计分析工具识别的风险。为了解决上述问题，M. Z. Konyar 等[2]提出了一种基于增强型维吉尼亚密码的安全帧选择方法。N. Kar 等[3]利用 DNA 链的随机性从一个全新的角度确定隐写视频的嵌入帧。Fan P. G. 等[4]根据帧量化步长以及帧间互关系提出了一种启发式的帧选择方法。在帧嵌入过程中，通常采用最低有效位（least significant bits，LSB）算法[5-11]。LSB 算法虽然实现简单，但在安全性方面存在明显不足，特别是在面对高级隐写分析工具时，该方法的可检测性较高。为提高安全级别，M. Hacimurtazaoglu 等[12]提出了一种基于多模式密钥块矩阵的 LSB 方法；M. Fateh 等[13]提出了一种基于 LSB 匹配重审视机制的隐写策略；R. J. Mstafa 等[14]利用 Shi-Tomasi 算法[15]检测嵌入视频帧的角点区域，用 LSB 算法进行隐写。研究者们通过改进帧选择和嵌入策略来增强安全性，

收稿日期：2024-05-10
作者简介：王勇智（1970-），男，湖南娄底人，湖南理工学院副教授，主要研究方向为多媒体网络与安全技术，
E-mail：wangyongzhi1970@163.com

虽然这些策略在一定程度上提升了隐蔽性，但是并未从根本上解决隐写过程中数据易受干扰和完整性问题。因此，迫切需要新的方法来提升隐写技术的安全性和隐蔽性。

为了进一步提高隐写技术的安全性和隐蔽性，本文提出基于密码学伪随机数生成器（cryptographically secure pseudo-random number generators，CSPRNG）的视频隐写算法（Secure Frame-CS），在帧选择机制中引入伪随机数生成器，在帧嵌入机制中引入校验子格编码（syndrome-trellis code，STC）[16]。

2 算法设计

2.1 嵌入算法

Secure Frame-CS 算法的主要改进思路为使用 CSPRNG 来优化帧选择过程，并利用 STC 增强信息嵌入的安全性和完整性，从而有效抵抗统计分析和增强数据的抗篡改能力。

2.1.1 帧选择机制

CSPRNG 可提升帧选择机制的随机性与安全性。CSPRNG 能在相同的种子下，生成完全相同的随机数据序列，从而确保接收方与发送方之间的一致性。且此随机数据序列无法被外部预测。因此，CSPRNG 非常适用于需要高安全性的应用，如用于加密和隐写技术。伪随机数据序列的生成过程为

$$R_i = H(seed||i), \tag{1}$$

式中：i 是随机数序列中的索引；R_i 是第 i 个随机数；H 是一个安全的哈希函数，如 SHA-256；$seed$ 是种子值。

在帧选择机制中，选取视频的 3 个主要特征作为 CSPRNG 的种子输入：帧数 N、分辨率 R 以及时间长度 T。这些特征代表了视频的基本物理和时间属性，能够为生成伪随机数提供一个独特的、与视频内容紧密相关的种子，并且这些特征与内容无关，不会受到隐写操作的影响，保证了秘密数据的可提取性。此外，引入了一个接收方与发送方事先约定好的秘密字符串 K，以进一步增强种子的安全性。种子值的计算公式为

$$seed = \mathrm{md5}(N + R + T + K), \tag{2}$$

式中 md5 是 md5 散列算法。

最终嵌入帧 f_{target} 的计算公式为

$$f_{\mathrm{target}} = R_i \,\%\, N, \tag{3}$$

式中 % 是取余操作。

2.1.2 帧嵌入机制

在视频隐写技术中，一旦选定了合适的帧，接下来就是将信息有效地嵌入到这些帧中。为此，本文采用了 STC 作为帧嵌入机制。STC 是一种高效的编码技术，结合了编码理论与图理论，能提高隐写过程中的安全性和数据的完整性。

STC 的核心是利用子格结构在给定的数据集中创建冗余，从而实现数据的错误检测和纠正。在隐写背景下，STC 能够最小化嵌入影响，同时能最大化数据负载的隐蔽性。具体来说，STC 通过构建一个特定的格（trellis）来定义数据嵌入的可能性。这个格由所有可能的秘密信息构成，每个信息都与特定的格点相对应。STC 的嵌入过程主要涉及以下几个关键步骤。

1）建立格结构：首先，建立一个子格结构。它定义了所有可能的嵌入点集合。每个点代表视频帧中的一个像素点，这些点的选择基于对像素修改导致的视觉和统计影响的预测。

2）生成校验矩阵：为了实现精确控制，生成一个校验矩阵 $\boldsymbol{H}$。该矩阵用于将编码后的数据映射到选定的像素点上。校验矩阵反映出视频帧的特性，如亮度、色彩分布等，能确保修改这些像素时对整体视频质量的影响最小。

3）选择嵌入位置：使用生成的校验矩阵，通过解决特定方程，确定哪些像素最适合嵌入信息，以最小化对帧质量的影响。该方程为

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{s}\boldsymbol{H}^{\mathrm{T}}, \tag{4}$$

式中：$\boldsymbol{x}$ 是目标帧中选定像素点的原始值；$\boldsymbol{s}$ 是经过编码的待嵌入信息。

确定嵌入位置后，采用 LSB 方法将由小到大排列的 STC 对帧进行嵌入，即

$$y_i = (x_i \,\&\, \sim 1) | b_i, \tag{5}$$

式中：b_i 是待嵌入的位（0 或 1）；& 和 | 分别是按位与和或操作；~1 是对数字 1 取反，以确保 x_i 的最低位被清零，同时不影响其他位的数据。

为确保接收方能准确地识别出嵌入位置，本文采用信息嵌入 UV 分量、嵌入位置信息保存于 Y 分量的策略。Y 分量主要代表图像的亮度信息，其对视觉变化的敏感度较低，因此在 Y 分量中嵌入位置信息不易被肉眼察觉。这种方法不仅确保了发送方与接收方之间的信息同步，还有效地保护了嵌入信息的隐蔽性，同时也最大化了数据嵌入的容量。因此，

视频能在不降低质量的前提下，实现高效且安全的传输。

2.2 解密提取机制

在完成视频隐写后，接收方需要从嵌入视频中正确提取出秘密信息。此过程涉及几个关键步骤，包括定位嵌入帧、定位嵌入位置以及提取嵌入数据。具体流程如图 1 所示。

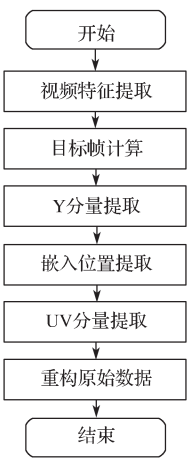

图 1 信息提取机制流程图

Fig. 1 Information extraction mechanism flow chart

给定一个嵌入视频，首先要分析视频并提取关键信息，如帧数、分辨率和时长，这些信息将用于计算种子值；其次，利用 CSPRNG 计算出目标帧的索引；然后，将目标帧的 YUV 三通道分离，并从 Y 通道提取嵌入位置列表；最后，根据列表从 UV 通道提取数据，并重构原始的秘密数据，即将 b_i 依次组合成嵌入字节列表，得到嵌入数据。数据提取公式为

$$b_i=y_i\&1。\tag{6}$$

3 实验结果与分析

3.1 性能评价指标

视频隐写性能评价指标有误码率（bit error rate，BER）、峰值信噪比（peak signal-to-noise ratio，PSNR）、结构相似性指标（structural similarity，SSIM）。BER 是发送的秘密信息与接收的实际信息相异的比特数占总比特数的比率，表示隐写系统在传输过程中信息丢失的程度。PSNR 是丢失的报文占报文发送总量的比例，表示网络传输的可靠性。丢包率越低，网络传输越可靠。SSIM 是一种结构感知的图像质量评价指标，它考虑了图像的亮度、对比度和结构等因素，与人眼感知到的图像质量一致。SSIM 的取值范围为 [0, 1]，值越接近 1 表示图像质量越好。对于视频而言，PSNR、SSIM 均为所有帧的均值。

3.2 实验设置

为评估视频隐写效果，选用 10 个常用的 YUV 视频文件作为评估数据集。视频分辨率为 352 × 288、176 × 144，帧数为 150~2101 帧，时长为 6~84 s，具体数据如表 1 所示。

表 1 评估数据集信息表

Table 1 Evaluation dataset information table

文件名	分辨率	帧数	时长 /s
Akiyo	352 × 288	300	12
Bridge-Close	352 × 288	2000	80
Bridge-Far	352 × 288	2101	84
Bus	352 × 288	150	6
Carphone	176 × 144	382	9
Claire	176 × 144	494	11
Coastguard	352 × 288	300	12
Container	352 × 288	300	12
Flower	352 × 288	250	10
Foreman	352 × 288	300	12

使用 Python 实现 SecureFrame-CS 算法，并采用 OpenCV2 库进行相关的视频操作。采用 RandomGen 库实现密码学伪随机数生成器，种子值由视频帧数、分辨率与固定字符串拼接生成，并对种子值的每个字符计算 ASCII 编码值。矩阵操作均通过 NumPy 库进行实现。采用 Hill 算法 [17] 计算 STC，其中极大值设置为 1×10^8，均值滤波器选择 15 × 15，以保证对嵌入所产生影响的计算稳健性和适应性。

3.3 性能分析

用 SecureFrame-CS 算法对评估数据集进行隐写并测试其性能，算法性能（BER、PSNR、SSIM、是否成功提取信息）如表 2 所示。由表 2 可知：1）所有视频的误码率为 0%。这意味着所有隐写信息都能被完整且准确地提取，没有发生任何传输错误或数据丢失的现象。在数据传输上的高可靠性为隐写信息准确无误地从视频中提取提供了保障。2）所有视频的隐写信息均被成功提取。这证明了本文方法在实际应用中的稳定性和一致性。3）所有视频的 PSNR 值均为无穷大。这意味着隐写后的视频与原始视频在视觉上没有任何差异，隐写过程没有引入任何可检测的视觉失真。对于实际应用，这一点尤为重要，

因为它确保了隐写技术对视频内容质量的影响极小，使得隐写信息在视觉上完全不可察觉。4）所有视频的 SSIM 值均为 0.99，接近 1。这表明隐写后的视频在结构上与原视频高度一致，几乎没有任何变化。高 SSIM 值进一步验证了隐写技术的隐蔽性和非侵入性，使得隐写信息在保持视频质量的前提下能被有效嵌入和提取。总之，本文提出的视频隐写技术在不同视频上的广泛适用性、稳定性和安全性，说明其不仅在理论上是可行的，而且也能满足实际应用需求。

表 2　算法性能

Table 2　Experimental algorithm results

文件名	BER/%	是否成功提取信息	PSNR	SSIM
Akiyo	0	是	∞	0.99
Bridge-Close	0	是	∞	0.99
Bridge-Far	0	是	∞	0.99
Bus	0	是	∞	0.99
Carphone	0	是	∞	0.99
Claire	0	是	∞	0.99
Coastguard	0	是	∞	0.99
Container	0	是	∞	0.99
Flower	0	是	∞	0.99
Foreman	0	是	∞	0.99

4　结语

本文提出了基于密码学伪随机数生成器和校验子格编码的视频隐写技术。通过引入密码学伪随机数生成器和校验子格编码技术，在视频帧中精确控制信息嵌入位置和过程，以有效提高隐写信息的隐蔽性和安全性。实验结果表明，本算法不仅保持了视频的视觉质量，还能提供高度的数据保密性和稳定性。

本算法具有广泛的应用前景，能用于需要高安全性的保密通信场景，如军事、政府和企业通信等，还适用于高干扰环境中的信息传递、高质量视频传输的应用场景，如高清电视广播和视频会议等。然而，视频隐写技术在实际应用中还面临一些挑战。首先，系统的计算复杂性和资源消耗需要得到有效管理，以确保在不同设备和平台上的可行性。其次，算法实时处理能力是实现广泛应用的重要步骤。最后，兼容性方面，需确保与现有视频标准和协议的良好互操作性，并制定相应的标准化流程以促进技术的普及应用。此外，在应用过程中需平衡安全性与合法性，确保技术不被滥用，维护其正当用途。

参考文献：

[1] 王智瀚，严李强，姚致远 . 基于多维码技术的隐蔽信息传输方法 [J]. 信息安全与通信保密，2023，21(9)：45-55.
WANG Zhihan，YAN Liqiang，YAO Zhiyuan. Covert Information Transmission Method Based on Multi-Dimensional Code Technology[J]. Information Security and Communications Privacy，2023，21(9)：45-55.

[2] KONYAR M Z，SOLAK S. Efficient Data Hiding Method for Videos Based on Adaptive Inverted LSB332 and Secure Frame Selection with Enhanced Vigenere Cipher[J]. Journal of Information Security and Applications，2021，63：103037.

[3] KAR N，MANDAL K，BHATTACHARYA B. Improved Chaos-Based Video Steganography Using DNA Alphabets[J]. ICT Express，2018，4(1)：6-13.

[4] FAN P G，ZHANG H，ZHAO X F，et al. Exploring Frame Difference to Enhance Robustness for Video Steganography on Social Networks[J]. Security and Communication Networks，2023，2023(1)：6295486.

[5] 王朔中，张新鹏，张卫明 . 以数字图像为载体的隐写分析研究进展 [J]. 计算机学报，2009，32(7)：1247-1263.
WANG Shuozhong，ZHANG Xinpeng，ZHANG Weiming. Recent Advances in Image-Based Steganalysis Research[J]. Chinese Journal of Computers，2009，32(7)：1247-1263.

[6] ELTAHIR M E，KIAH L M，ZAIDAN B B，et al. High Rate Video Streaming Steganography[C]//2009 International Conference on Information Management and Engineering. Kuala Lumpur：IEEE，2009：550-553.

[7] RAMALINGAM M. Stego Machine-Video Steganography Using Modified LSB Algorithm[J]. Journal of Information and Communication Convergence Engineering，2011，5(2)：170-173.

[8] TARUN M V S，RAO K V，MAHESH M N，et al. Digital Video Steganography Using LSB Technique[J]. Iconic Research And Engineering Journals，2020，3(10)：14-17.

[9] JAYAKANTH K，NANDHINI S，SOMAYA A M，et al. Video Steganography：Recent Advances and Challenges[J]. Multimedia Tools and Applications，2023，82(27)：41943-41985.

[10] KUMAR H，MAMORIA P，KUMARI S，et al. Video Steganography Techniques: A Comprehensive Review and

Performance Evaluation[C]//International Conference on Cryptology & Network Security with Machine Learning. Singapore：Springer，2023：35-48.
[11] BATTISTI F，CARLI M，NERI A，et al. A Generalized Fibonacci LSB Data Hiding Technique[C]//3rd International Conference on Computers and Devices for Communication (CODEC-06). Calcutta：University of Calcutta，2006(4)：671-683.
[12] HACIMURTAZAOGLU M，TUTUNCU K. LSB-Based Pre-Embedding Video Steganography with Rotating & Shifting Poly-Pattern Block Matrix[J]. PeerJ Computer Science，2022，8：e843.
[13] FATEH M，REZVANI M，IRANI Y. A New Method of Coding for Steganography Based on LSB Matching Revisited[J]. Security and Communication Networks，2021(5)：6610678.
[14] MSTAFA R J，YOUNIS Y M，HUSSEIN H I，et al. A New Video Steganography Scheme Based on Shi-Tomasi Corner Detector[J]. IEEE Access，2020，8：161825-161837.
[15] SHI J B，TOMASI C. Good Features to Track[C]//1994 Proceedings of IEEE Conference on Computer Vision and Pattern Recognition. Seattle：IEEE，1994：593-600.
[16] FILLER T，JUDAS J，FRIDRICH J. Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes[J]. IEEE Transactions on Information Forensics and Security，2011，6(3)：920-935.
[17] LI B，WANG M，HUANG J W，et al. A New Cost Function for Spatial Image Steganography[C]//2014 IEEE International Conference on Image Processing (ICIP). Paris：IEEE，2014：4206-4210.

（责任编辑：邓　彬）

Research on Video Steganography Techniques Based on Cryptographically Secure Pseudo-Random Number

WANG Yongzhi

（School of Information Science and Engineering，Hunan Institute of Science &Technology，Yueyang Hunan 414006，China）

Abstract：In response to the issues of low security and reliability associated with video steganography, a video steganography algorithm is proposed based on a pseudo-random number generator (PRNG). The PRNG is utilized for selecting video frames, thereby enhancing the randomness and unpredictability of the steganographic process. The sequence generated by the PRNG, unlike traditional fixed-pattern frame selection, is difficult to predict, making it challenging for attackers to infer the embedding strategy from external features, thereby reducing the likelihood of detection by statistical analysis tools and machine learning models. Additionally, check digit lattice coding is employed to encode secret data into redundant information, enhancing the integrity of the secret data and improving its resistance to interference in complex communication environments. Experimental results demonstrate that this algorithm significantly enhances the security and concealment of video steganography, and effectively resists statistical analysis attacks. Moreover, while maintaining a high data embedding rate, it ensures a low error rate and high image quality.

Keywords：video steganography；cryptography；pseudo-random number generator；check lattice encoding；information hiding