IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/44AI/2024/4444924/
Vol. 2024 (22), Article ID 4444924

Mathematical Modeling in Color Difference Analysis in Consecutive Video Frames for Steganography*

Marcin PERY and Robert WASZKOWSKI

Military University of Technology, Faculty of Cybernetics
Institute of Computer and Information Systems
Kaliskiego St. 2, 00-908 Warsaw, Poland

Correspondence should be addressed to: Marcin PERY, marcin.pery@wat.edu.pl

* Presented at the 44th IBIMA International Conference, 27-28 November 2024 Granada, Spain

Abstract

This study investigates spatial domain video steganography, driven by the increasing demand for secure data embedding techniques that leverage inherent video properties to remain undetectable. Traditional approaches in the literature often neglect the detailed statistical characterization of naturally occurring pixel color differences across video frames, creating a significant gap in understanding how these variations can be systematically analyzed and effectively applied to steganographic methods. To address this deficiency, the study develops a comprehensive mathematical model for video files, introducing a function to compute inter-frame color differences and constructing a formalized color difference histogram. This innovative metric enables precise characterization of video files by analyzing the frequency and distribution of pixel color variations, offering a novel perspective on video content analysis. The findings confirm that the proposed model reliably captures the statistical patterns of color differences, providing a robust and scalable framework for improving steganographic techniques. By leveraging these patterns, the model enhances the resilience and imperceptibility of spatial domain steganography against detection and tampering. Future research will extend this framework to diverse video datasets, exploring its adaptability and uncovering additional insights into natural color variation dynamics and their potential applications in secure information encoding. This work lays the foundation for further advancements in the integration of statistical analysis and steganographic innovation.

Keywords: steganography, video steganography, mathematical model of video, information encoding

Introduction

Steganography represents an advanced method of information security (Shannon, 1948) that focuses on concealing data within ordinary digital media to obscure its existence. This technique enables covert communication, ensuring that unauthorized individuals remain unaware of the hidden content (Kahn, 1967). The primary objective of steganography is to protect sensitive information by rendering its presence undetectable, thereby preventing unauthorized access and facilitating secure exchanges (Johnson, et al., 1998). Unlike cryptography, which centers on encrypting the content of messages, steganography targets the concealment of the communication itself, making it particularly valuable in contexts where overt encryption may attract scrutiny or be restricted.

Steganographic methods achieve data concealment by altering specific properties of digital media, such as pixel values in images, frequency components in audio files, or even characteristics of network packets (Sencar, et al., 2004). The success of these methods hinges on the invisibility of the alterations to the original medium, ensuring that the modified version, known as the steganogram, appears statistically indistinguishable from the unmodified medium. The choice of a suitable technique depends on various factors, including the nature of the cover medium, the size of the embedded message, and the required robustness against detection or tampering Katzenbeisser, et al., 2000).

Cite this Article as: Marcin PERY and Robert WASZKOWSKI, Vol. 2024 (22) "Mathematical Modeling in Color Difference Analysis in Consecutive Video Frames for Steganography " Communications of International Proceedings, Vol. 2024 (22), Article ID 4444924, https://doi.org/10.5171/2024.4444924

Techniques for embedding data within images and videos can be broadly classified into spatial and transform domain approaches (Cox, et al., 2007; Kadhim, et al., 2019). Spatial domain methods involve direct manipulation of pixel attributes, such as color or brightness, to encode hidden data. While these methods are relatively straightforward to implement, they are more vulnerable to detection through statistical or visual analysis (Chan, et al., 2004). Transform domain techniques, in contrast, operate on the frequency components of media, modifying coefficients derived from transformations such as the Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). These approaches often enhance robustness against compression and processing, providing greater resistance to steganalysis (Chang, et al., 2002).

The evolution of steganographic methods continues to be driven by the growing demand for secure communication and data protection in the digital era (Johnson, et al., 2001). As steganalysis techniques become increasingly sophisticated, researchers strive to develop innovative approaches to bolster the security and resilience of steganography (Petitcolas, et al., 1999). This ongoing advancement ensures the relevance of steganography for diverse applications, including digital watermarking, copyright protection, and secure information transmission. Such efforts are essential to maintaining the utility and reliability of steganography as a critical tool in information security (Fridrich, 2009; Anderson, et al., 1998).

In steganography, various modeling approaches exist. Zöllner, et al. (1998) provides a foundational framework for analyzing steganographic security, focusing on undetectability. Their model demonstrates the feasibility of information-theoretically secure steganography under conditions like randomized embedding and independence between the message, cover, and steganograms, also introducing an attacker model that lacks information on the embedding process. Similarly, Cachin (1998) presents a model for assessing security with a passive adversary, framing detection as a hypothesis testing problem and quantifying security through relative entropy between cover and steganogram distributions. Defining "perfect" security as zero relative entropy, Cachin establishes theoretical security bounds and presents a universal steganographic system requiring no specific knowledge about cover.

This study presents a straightforward, functional model of video files as covers in video steganography, enabling the definition of functions within the proposed model that can serve as metrics for evaluating the characteristics of the analyzed video files.

Mathematical model

In simplified terms, a video can be considered a sequence of consecutive images, commonly referred to as frames. However, in practical applications, the way videos are stored is far more complex, as it depends heavily on the codec employed. Most modern video codecs do not store each frame as a complete image; instead, they use sophisticated algorithms to detect and encode only the differences between successive frames.

This method, which relies on motion estimation and prediction, drastically reduces the storage requirements and improves efficiency. For the purposes of this study, a simplified video model was utilized, avoiding the complexities of inter-frame compression. Specifically, the Motion JPEG (MJPEG) format was chosen, as it stores each frame as a complete image, devoid of advanced compression mechanisms. This decision enables a direct and detailed examination of pixel color differences between consecutive frames, which is a critical aspect of the research on spatial domain video steganography. By focusing on uncompressed or lightly compressed frame data, the study ensures that the results are not influenced by the artifacts or alterations introduced by complex encoding processes, thus providing a clearer foundation for analyzing and developing steganographic techniques.

Video

We define the *video* v^i as an i-element vector (see Eq. 1).

$$v^i = [v_1, v_2, \ldots, v_i] \tag{1}$$

$$\bigwedge_{i \in \{1 \ldots Z\}} v^i \in \mathcal{V}$$

$$Z \in \mathbb{N}$$

where: v_i – the i-th frame of the video v,
v^i – the i -elements of vector of frames,
$\mathcal{V}$ – the set of all videos.

We can regard a video as a vector of frames, formed by sequentially appending each frame from the first to the last. (see Eq. 2).

$$\bigwedge_{i\in\{1\ldots Z\}} v^i = \begin{cases} [v_1] & ,i = 1 \\ v^{i-1} \oplus v_i & ,i \in \{2\ldots Z\} \end{cases} \tag{2}$$

where: Z – number of frames in the video v.

Frame

We define the *frame* v_i as a matrix of vectors of pixels (see Eq. 3).

$$v_i = \begin{bmatrix} p^i_{0,0} & \cdots & p^i_{X-1,0} \\ \cdots & p^i_{x,y} & \cdots \\ p^i_{0,Y-1} & \cdots & p^i_{X-1,Y-1} \end{bmatrix} \tag{3}$$

$$\bigwedge_{i\in\{1\ldots Z\}} v_i \in \{0\ldots 255\}^{3^{X\times Y}}$$

$$X, Y \in \mathbb{N}$$

where: $p^i_{x,y}$ – the (x, y) pixel of the i-th frame v_i,
$X \times Y$ – dimensions of frames,
$\{0\ldots 255\}^{3^{X\times Y}}$ – the set of all frames, which are $X \times Y$ matrixes of 3-elements vectors of numbers from $\{0\ldots 255\}$

Pixel

We define the pixel $p^i_{x,y}$ as a 3-elements vector of bytes representing colors (see Eq. 3).

$$p^i_{x,y} = \left[red^i_{x,y}, green^i_{x,y}, blue^i_{x,y}\right] \tag{4}$$

$$\bigwedge_{i\in\{1\ldots Z\}} \bigwedge_{\substack{x\in\{0\ldots X-1\} \\ y\in\{0\ldots Y-1\}}} \begin{cases} p^i_{x,y}[0] = red^i_{x,y} & \in \{0\ldots 255\} \\ p^i_{x,y}[1] = green^i_{x,y} & \in \{0\ldots 255\} \\ p^i_{x,y}[2] = blue^i_{x,y} & \in \{0\ldots 255\} \end{cases}$$

$$\bigwedge_{i\in\{1\ldots Z\}} v_i \in \{0\ldots 255\}^{3^{X\times Y}}$$

where: $red^i_{x,y}, green^i_{x,y}, blue^i_{x,y}$ – colors of the pixel $p^i_{x,y}$.

Considering the above definitions, we can define the set of all videos $\mathcal{V}$ in accordance with (Eq. 5).

$$\mathcal{V} = \{0\ldots 255\}^{3^{X\times Y}{}^*} \tag{5}$$

where: $\{0\ldots 255\}^{3^{X\times Y}{}^*}$ – the set of all videos, which are vectors of $X \times Y$ matrixes of 3-elements vectors of numbers from$\{0\ldots 255\}$.

Measures of frame difference

Frame Difference

A mathematically defined model for video frames, as shown above, enables the measurement of differences between consecutive video frames as a matrix of vectors representing individual pixel colors in the RGB space. The function $diff$ is defined as the mapping of a specific video and a selected frame number to a matrix of integers from $\{-255\ldots255\}$ (see Eq. 6).

$$diff: \mathcal{V} \times \{2..Z\} \to \{-255\ldots255\}^{X \times Y} \tag{6}$$

$$diff(v,i) := \begin{bmatrix} p^i_{0,0} - p^{i-1}_{0,0} & \cdots & p^i_{X-1,0} - p^{i-1}_{X-1,0} \\ \cdots & p^i_{x,y} - p^{i-1}_{x,y} & \cdots \\ p^i_{0,Y-1} - p^{i-1}_{0,Y-1} & \cdots & p^i_{X-1,Y-1} - p^{i-1}_{X-1,Y-1} \end{bmatrix}$$

$$v \in \mathcal{V}, i \in \{2\ldots Z\}$$

where: v – video,
i – the index of frame in the v video,
$p^i_{x,y}$ – the (x, y) pixel in i-th frame,
$p^{i-1}_{x,y}$ – the (x, y) pixel in $(i-1)$-th frame.

Color Difference Histogram

To analyze the properties of video files in the spatial domain represented in the RGB color space, we will use the color difference histogram. This histogram hist is defined as a function that maps video files and a given color in the RGB color space to the Cartesian product of all possible color differences between consecutive frames and the frequency of their occurrence (see Eq. 7).

$$hist: \mathcal{V} \times \{0,1,2\} \to \{-255\ldots255\} \times [0,1] \tag{7}$$

$$hist(v, color) := \bigcup_{d \in \{-255\ldots255\}} \left\{ d, \sum_{\substack{i \in \{2\ldots Z\} \\ x \in \{0\ldots X-1\} \\ y \in \{0\ldots Y-1\}}} \frac{\{1\}_{d = diff(v,i)_{x,y}[color]}}{X \cdot Y \cdot (Z-1)} \right\}$$

$$v \in \mathcal{V}, color \in \{0,1,2\}$$

where: v – video,
i – the index of frame in the v video,
$diff(v, i)$ – the frame difference between i-th and $(i-1)$-th frames,
$color$ – index of color in an RGB pixel vector,
$X \times Y$ – dimensions of frames,
$\mathcal{V}$ – the set of all videos,
Z – number of frames in the video v.

Conclusions

This study introduced a mathematical model for video files that supports the definition of a function to calculate color differences between consecutive frames. Based on this function, a formal description of a color difference histogram was developed, providing a distinctive metric to characterize video files by the frequency of color changes between frames.

Theoretical Contributions

The study contributes theoretically by establishing a mathematical model of a video file and defining a function that determines the histogram of color differences across consecutive frames. This histogram serves as a formal tool for analyzing color variations within video content.

Practical Implications

The proposed model offers significant potential for investigating the statistical properties of video files, providing a robust foundation for analyzing natural pixel color variations across consecutive frames. This capability can directly aid in the development and refinement of spatial domain video steganography techniques, specifically those that leverage pixel color differences in the RGB space for encoding information. By characterizing these variations with precision, the model allows researchers to design more resilient and imperceptible steganographic methods.

Future Research

We propose applying the model to conduct experimental research on video files with varied characteristics, such as color profiles and motion dynamics, by:
- generating histograms for these files, and
- analyzing the properties of the resulting histograms.

This approach will further validate the model's applicability and reveal insights into the natural color variation patterns in different video content types.

Author Contributions

The results of the work were obtained mainly by the first author under the scientific supervision of the second one.

Acknowledgment

The work was partially financed by the Military University of Technology in Warsaw, Poland as part of the project No. UGB 22-701.

References

- Anderson, R. and Petitcolas, F. (1998) 'On the limits of steganography' *IEEE Journal on Selected Areas in Communications*, 16(4), 474-481, ISSN 0733-8716, DOI 10.1109/49.668971
- Cachin, C. (1998) 'An Information-Theoretic Model for Steganography' *Springer, Information Hiding - Lecture Notes in Computer Science*, 1525, DOI 10.1007/3-540-49380-8_21
- Chan, C. and Cheng, L. (2004) 'Hiding data in images by simple LSB substitution' *Elsevier, Pattern Recognition*, 37(3), 469-474, ISSN 0031-3203, DOI 10.1016/j.patcog.2003.08.007
- Chang, C., Chen, T. and Chung, L. (2002) 'A steganographic method based upon JPEG and quantization table modification' *Information Sciences*, 141(1-2), 123-138, ISSN 0020-0255, DOI 10.1016/S0020-0255(01)00194-3
- Cox, I., Miller, M. and Kalker, T. (2007) Digital Watermarking and Steganography, Morgan Kaufmann Publishers, Burlington, USA, ISBN 0123725852
- Fridrich, J. (2009) Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, Cambridge, UK, DOI 10.1017/CBO9781139192903.014
- Johnson, N. and Jajodia, S. (1998) 'Exploring Steganography: Seeing the Unseen' *IEEE Computer*, 31(2), 26-34, ISSN 0018-9162, DOI 10.1109/MC.1998.4655281
- Johnson, N., Duric, Z. and Jajodia, S. (2001) 'Information Hiding: Steganography and Watermarking - Attacks and Countermeasures' *Springer*, ISBN 978-0-7923-7204-2, DOI 10.1007/978-1-4615-4375-6, 2001
- Kadhim, I., Premaratne, P., Vial, P. and Halloran, B. (2019) 'Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research' *Neurocomputing*, 335, 299-326, ISSN 0925-2312, DOI 10.1016/j.neucom.2018.06.075
- Kahn, D. (1967) The Codebreakers: The Story of Secret Writing, Macmillan, NYC, USA, ISBN 978-0025604605
- Katzenbeisser, S. and Petitcolas, F. (2000) Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, USA, ISBN 978-1-58053-035-4

- Petitcolas, F., Anderson, R. and Kuhn, M. (1999) 'Information hiding - a survey' *Proceedings of the IEEE*, 87(7), 1062-1078, ISSN 0018-9219, DOI 10.1109/5.771065
- Sencar, H., Ramkumar, M. and Akansu, A. (2004) 'Data Hiding Fundamentals and Applications' *Elsevier Academic Press*, ISBN 9780120471447, DOI 10.1016/B978-0-12-047144-7.X5000-5
- Shannon, C. (1948) 'A Mathematical Theory of Communication' *Bell System Technical Journal*, 27(3), 379-423, ISSN 0005-8580, DOI 10.1002/j.1538-7305.1948.tb01338.x
- Zöllner, J., Federrath, H., Klimant, H., Pfitzmann, A., Piotraschke, R., Westfeld, A. and Wolf, G. (1998) 'Modeling the Security of Steganographic Systems' Information Hiding, Second International Workshop, vol. 1525, Lecture Notes in Computer Science, Springer, Berlin, 1998, pp. 344–354