




Editorial

Data Hiding and Its Applications: Digital Watermarking and Steganography

David Megías ^{1,*}, Wojciech Mazurczyk ² and Minoru Kuribayashi ³

¹ Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC), CYBERCAT-Center for Cybersecurity Research of Catalonia, Castelldefels, 08860 Barcelona, Spain

² Institute of Computer Science, Warsaw University of Technology, Nowowiejska 15/19, 00-665 Warsaw, Poland; wojciech.mazurczyk@pw.edu.pl

³ Graduate School of Natural Science and Technology, Okayama University, Okayama 700-8530, Japan; kminoru@okayama-u.ac.jp

* Correspondence: dmegias@uoc.edu

Data hiding techniques [1] have been widely used to provide copyright protection, data integrity, covert communication, non-repudiation, and authentication, among other applications. In the context of increased dissemination and distribution of multimedia content (text, audio, video, etc.) over the internet, data hiding methods, such as digital watermarking and steganography, are becoming more and more relevant in providing multimedia security. Due to the complementary nature of general requirements of these methods, i.e., imperceptibility, robustness, security, and capacity, many data hiding schemes attempt to obtain optimal performance.

There are many potential applications of data hiding techniques. Copyright protection via content proof of ownership, owner identification or transaction tracking (digital fingerprinting), broadcast monitoring, content authentication including tampering detection or localization, copy control, device control, and legacy enhancement stand out among the applications of digital watermarking. On the other hand, secret communications are the focus of steganography, either for military reasons, for dissidents, or for criminal organizations. The military and criminal applications of steganography have led to an increased interest of the academic community in steganalysis, i.e., the techniques used to detect steganographic communications.

Apart from the classical applications of data hiding, mentioned above, new application scenarios have emerged in the last few years [2]. These new applications of data hiding include privacy-preserving transaction tracking, digital watermarking for data provenance, digital watermarking for forensics, network flow watermarking, network steganography, VoIP steganography, steganography for criminals and terrorists, and steganography for malware injection, among others.

The goal of this special issue is to focus on the improvement of data hiding algorithms and their different applications (either the traditional or the emerging ones), bringing together researchers and practitioners from different research fields, including data hiding, signal processing, cryptography, or information theory, among others, to contribute with original research outcomes that address current challenges in data hiding methods. The list of topics/keywords covered by this special issue is the following:

- Steganography
- Steganalysis
- Digital watermarking
- Zero watermarking
- Digital fingerprinting
- Coverless data hiding
- Reversible data hiding and applications



Citation: Megías, D.; Mazurczyk, W.; Kuribayashi, M. Data Hiding and Its Applications: Digital Watermarking and Steganography. *Appl. Sci.* **2021**, *11*, 10928. <https://doi.org/10.3390/app112210928>

Received: 10 November 2021

Accepted: 17 November 2021

Published: 19 November 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

- Forensic aspects of data hiding
- Embedding capacity/payload
- Emerging applications of data hiding in IoT and Big Data
- Applications of data hiding
- Ownership Proof/Copyright Protection
- Covert channels
- Traitor-tracing
- Extraction/detection
- Data integrity
- Distortion measurement
- Transform coding
- Information theory
- Information entropy
- Signal processing
- Data segmentation

In response to the call for papers, nineteen papers were submitted to this special issue among which twelve were accepted for publication. These twelve papers include two review papers/surveys and ten contributions that address several research challenges of data hiding schemes.

In one of the accepted papers, Qureshi and Megías [3] present a systematic review and future directions for blockchain-based multimedia content protection schemes using data hiding techniques. The survey provides a detailed analysis of multimedia content protection applications using blockchain and proposes a taxonomy to classify these applications based on the technical aspects of blockchain, content protection techniques, digital rights management, digital watermarking and fingerprinting, and performance criteria. The paper concludes that there is a relevant research gap regarding blockchain-based multimedia copyright protection systems. In addition, the paper discusses some technical challenges and outlines future research directions.

In another survey paper, Caviglione [4] presents a systematic literature review of the most recent approaches for counteracting network covert channels. Network covert channels are increasingly used to distribute malware (stegomalware) and the detection of these kinds of attacks is difficult since those channels typically carry very low data rates, and it is difficult to identify where the secret information is hidden. Apart from the literature review, the paper identifies the major research challenges and the most promising development trends and discusses the advancements needed for building a more robust and consistent framework to obtain protection against network covert channels and stegomalware.

Among the research papers, four of them focus on new watermarking applications, including watermarking for 3D models [5], a watermarking scheme robust against screen-cam attacks [6], a watermarking protocol based on blockchain [7], and a watermarking framework to protect Deep Learning (DL) models [8].

In Ref. [5], Botta et al. present an algorithm for integrity protection of 3D models represented as a set of vertices and polygons. The proposed approach uses fragile watermarking on the vertices of the 3D model introducing a very small watermarking noise. The watermark is embedded into a secret vector space defined by the Karhunen-Loève transform obtained from a key image. The proposed method outperforms the state-of-the-art techniques in terms of performance, especially distortion and security.

Chen et al. [6] present a screen-cam robust image watermarking scheme using feature-based synchronization. Taking pictures of a screen with mobile phones or cameras is one of the main methods to leak image information. The paper analyzes the distortions caused by the screen-cam process and classifies them into five categories, namely, linear distortion, gamma tweaking, geometric distortion, noise attack, and low-pass filtering attack. After that, a watermark synchronization method is proposed based on the construction of a local square feature region (LSFR), a Gaussian function, a modified Harris-Laplace detector, and

a speeded-up robust feature (SURF) orientation descriptor. Then, the message is embedded in each selected LSRF with an embedding algorithm using a non-rotating embedding method and a preprocessing procedure to modulate the discrete Fourier transform (DFT) coefficients. This approach makes it possible to improve watermark detection from the captured information. The effectiveness of the method against screen-cam attacks is shown and the scheme outperforms the state-of-the-art techniques not only against screen-cam attacks, but also when they are combined with other desynchronization attacks.

In Ref. [7], Frattolillo presents a watermarking protocol based on blockchain. “Buyer friendly” and “mediated” watermarking protocols can ensure both correct content protection and the easy participation of buyers in the transactions to purchase multimedia content, offering an alternative to more traditional “buyer and seller” watermarking protocols. In this paper, a new watermarking protocol is proposed combining the “buyer friendly” and “mediated” approaches with blockchain technology. The resulting protocol supports limited and balanced participation of buyers and content providers in transactions of protected digital content and avoids the need for a trusted third party directly involved in transactions. This reduces the risk of protocol violations by the buyers or the sellers by colluding with other parties. The proposed approach achieves security properties that are comparable to those of the state-of-the-art schemes, which require trusted third parties. Although the performance is somewhat penalized by the consensus mechanism of the blockchain, the next generations of the blockchain will make it possible to implement better algorithms and improve performance.

Jebreel et al. [8] propose KeyNet, an asymmetric key-style framework for watermarking DL models. DL models are used to solve many complex engineering tasks, including computer vision, speech recognition, natural language processing, or stock market analysis. Building representative and highly accurate DL models is a very costly task that involves devoting significant computational resources to process large amounts of proprietary training data, which is also hard to collect. Hence, the owners of DL models seek compensation for the incurred costs from commercial exploitation of such models, but this makes DL models attractive for attackers who try to steal them and use them in an illegal manner. KeyNet is a novel watermarking framework that satisfies the main requirements for an effective and robust watermarking of DL models. In the proposed framework, any sample in a watermark carrier set can take more than one label based on where the owner signs it, where the signature is the hashed value of the owner’s information, and her model. Then, multitask learning (MTL) is used to learn the original classification task and the watermarking task together. Furthermore, a private model is added to the original one to act as a private key. Both models are trained together to embed the watermark while preserving the accuracy of the original classification task. To extract a watermark from a model, the prediction of the marked model on a signed sample is passed to the private model which can provide the position of the signature. The proposed KeyNet framework is then tested on several data sets to show its effectiveness and performance. The obtained results illustrate that KeyNet preserves the utility of the DL model while embedding a robust watermark. The watermarking application is carried out in an innovative way that makes it possible to embed a large amount of information, to establish a strong link between the owner and her marked model, to prevent attackers from overwriting the watermark without losing accuracy in the original task, and to uniquely fingerprint several copies of a pre-trained DL model for a large number of users in the system.

Then, four other papers present different advances in steganography and steganalysis: a high-capacity block-based steganographic scheme for images [9], an evaluation of the false-negative rate of the Stegdetect tool [10], a steganographic scheme for the MIDI format [11], and a reversible and plausible deniable covert channel for one-time passwords (OTP) based on hash chains [12].

Wu et al. [9] propose an efficient and high-capacity block-based steganographic method using optimal selection for palette images. The main goal of steganography is to provide a large steganographic payload with statistically undetectable methods. A

typical approach to reduce statistical detectability in steganography is to increase the embedding efficiency, defined as the number of bits that can be hidden per embedding change. Methods with higher embedding efficiency are less detectable since, under the same capacity, they change less pixel values compared to lower efficiency methods. Block-based steganography methods are designed in order to improve the embedding efficiency under a limited capacity, but they often skip the blocks with larger distortion and require a location map to record the blocks that carry embedded data. The method proposed in this paper applies block-based steganography for palette images and does not require a location map. The proposed scheme embeds several bits in a block with, at most, a pixel change, which minimizes the embedding noise. This makes it possible to embed data in all the blocks of the image, leading to a larger capacity compared with other schemes known from the literature. Experimental results comparing the proposed scheme with other works evidence an improvement in the trade-off between embedding efficiency and capacity.

In Ref. [10], Aziz et al. analyze the false negative rates of Stegdetect, a modern automated steganalysis tool. Steganalysis is a collection of techniques aiming at detecting whether some media carries secret information previously hidden using steganography. Detecting steganography is essential to fight against secret criminal communications or malware that is transmitted using covert steganographic channels. In the paper, an extensive analysis of Stegdetect is conducted by embedding random messages in 2000 JPEG images using JPHide steganography to establish the false-negative rate of the tool. The study concludes that the sensitivity parameter of Stegdetect is a key factor of the false-negative rates. The false-negative rates with Stegdetect are high for sensitivity values between 0.1 and 3.4. The best detection results for JPHide are obtained with a sensitivity value of 6.2. The paper concludes that the sensitivity parameter of Stegdetect needs to be adjusted carefully in forensic activities when many images are analyzed to reduce false-negative rates.

Järpe and Weckstén present *Velody 2* [11], a new musical steganographic scheme for the MIDI format by modifying the velocity parameter considering constraints in capacity and security. The major drawback of most MIDI steganographic schemes is their lack of resilience against steganalysis since most existing methods leave traces that do not appear naturally in MIDI files. The proposed scheme is based on embedding information into the velocities of the note-on events to mimic the behavior of some available digital audio software suites. Data embedding is carried out by setting velocities to values within a narrow interval to be specified which removes potential mood swings in the velocity parameter of the music. The use of the technique is restricted to organ and harpsichord music, which are naturally performed with constant or close to constant velocities, but the method can be used with little artificial effects on other types of music. Regarding resilience against steganalysis, *Velody 2* is shown to leave very little traces and is comparable with the best MIDI steganographic methods in state-of-the-art methods. As audibility is concerned, it is shown that 30 listeners could not significantly guess which files contain embedded information. As far as embedding rate is concerned, *Velody 2* outperforms the methods proposed in recent works.

Keller and Wendzel [12] present a work on reversible and plausibly deniable covert channels OTP based on hash chains. A covert channel (CC) is an unforeseen communication channel in a system design that enables several actions related to cybercrime, such as information theft, barely detectable channels for commanding and controlling botnets, and secret criminal communications. The paper presents a covert channel between two devices where one device authenticates itself with Lamport's OTP based on a cryptographic hash function. The proposed channel provides plausible deniability, i.e., the communicating parties can deny the existence of the covert channel and reversibility, i.e., the reconstruction of the original carrier message to the state before the steganographic data was embedded, and it can be applied in different contexts, such as traditional TCP/IP communications, Internet of Things (IoT) environments, blockchain-based systems, and local inter-process communications that rely on hash chains. Countermeasures to detect such a covert channel are also presented, but such detection is difficult because hash values appear to be random

binary strings and deviations are hard to detect. Experimental results are presented to evaluate the channel's performance, to conduct statistical tests using the NIST suite, and to determine the channel's stealthiness (by running a test for matching hash values between legitimate and covert environments). The experiments show that the proposed channel might be detectable under realistic conditions only if no encryption is applied and authentication data are collected over a longer time span. The exact time spans depend on the deployed variant of the covert channel, which, in turn, is affected by the width of the selected hash function.

Finally, two other application scenarios are presented in the remaining papers of this special issue. First, an adaptive reversible data hiding scheme is proposed [13] and, second, a Machine Learning (ML)-based solution for the detection of propaganda and misinformation spread using mixed-code text is presented [14].

In [13], Chen et al. propose an adaptive reversible data hiding scheme using absolute moment block truncation coding (AMBTC) and Quantization Level Difference (QLD). Reversible data hiding makes it possible to recover the original (cover) object after data extraction in the receiving end, being a very valuable application field when images must be protected even from the slightest modification (such as in medical and military applications). The proposed method provides a large embedding capacity with a reduced quality loss for the modified images and uses QLD together with an interpolation technique to adaptively embed the secret information into pixels of AMBTC-compressed block, except for the positions of two replaced quantization levels. The proposed method obtains good performance for embedding capacity and still meets the requirement for better-modified image quality when the image is complex thanks to the use of QLD. The experimental results show that the proposed method outperforms the referenced approaches regarding distortion in terms of peak signal-to-noise ratio (PSNR) and hiding capacity.

Finally, Tundis et al. [14] present an algorithm for the detection of hidden propaganda in mixed-code text over the internet. The internet has become a widely used tool for spreading misinformation and propaganda. Although mechanisms to track potentially fake information exist, various ways have been found to avoid such kind of detection. An example of the approaches used to bypass detection is to use mixed-code language, which consists of text written in an unconventional way combining different languages, symbols, scripts, and shapes, often substituting the usual alphabet letters. The message is still readable by humans, but algorithms often fail in their detection. The article proposes a machine learning (ML) approach for character identification to detect and analyze whether some content includes propaganda or disinformation hidden using mixed-code text. The paper first proposes a possible categorization of different types of existing mixed code. The study is focused on the analysis of one type of *Text as Art Form* written on a single row by adopting a methodological approach centered on two main aspects, namely mixed code text analysis and hidden propaganda detection. Regarding the mixed code text analysis, a four-step algorithm that supports both the identification of mixed code in the text along with its normalization into natural language is proposed. As the hidden propaganda detection is concerned, a Convolutional Neural Network (CNN) classifier is designed. The overall performance of the tests is on a publicly available dataset containing a collection of 15,847 textual propaganda and nonpropaganda-related items. The experimental results are very remarkable in terms of performance (accuracy, precision, F1-score, and recall), overcoming the achievements of the reference works.

In general, this special issue covers recent trends in both traditional and emerging applications of data hiding and constitutes a good sample of the current state-of-the-art results in this field.

Author Contributions: The authors contributed equally to the different steps of this research. All authors have read and agreed to the published version of the manuscript.

Funding: The authors acknowledge the funding obtained from the EIG CONCERT-Japan call to the project Detection of fake news on Social Media platforms "DISSIMILAR" through grants

PCI2020-120689-2 (Spanish Government), JPMJSC20C3 (Japanese Government) and EIG CONCERT-JAPAN/05/2021 (National Centre for Research and Development, Poland). The first author also acknowledges the funding to the project RTI2018-095094-B-C22 “CONSENT” by the Spanish Ministry of Science and Innovation.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We acknowledge the authors of Refs. [3–14] for their valuable contributions to this special issue.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cox, I.; Miller, M.; Jeffrey, A.; Fridrich, J.; Kalker, T. *Digital Watermarking and Steganography*, 2nd ed.; Morgan Kaufmann: Burlington, MA, USA, 2008. [[CrossRef](#)]
2. Megías, D. Data hiding: New opportunities for security and privacy? In Proceedings of the European Interdisciplinary Cybersecurity Conference (EICC 2020), Rennes, France, 18 November 2020; Article No.: 15. pp. 1–6. [[CrossRef](#)]
3. Qureshi, A.; Megías, D. Blockchain-Based Multimedia Content Protection: Review and Open Challenges. *Appl. Sci.* **2021**, *11*, 1. [[CrossRef](#)]
4. Caviglione, L. Trends and Challenges in Network Covert Channels Countermeasures. *Appl. Sci.* **2021**, *11*, 1641. [[CrossRef](#)]
5. Botta, M.; Cavagnino, D.; Gribaudo, M.; Piazzolla, P. Fragile Watermarking of 3D Models in a Transformed Domain. *Appl. Sci.* **2020**, *10*, 3244. [[CrossRef](#)]
6. Chen, W.; Ren, N.; Zhu, C.; Zhou, Q.; Seppänen, T.; Keskinarkaus, A. Screen-Cam Robust Image Watermarking with Feature-Based Synchronization. *Appl. Sci.* **2020**, *10*, 7494. [[CrossRef](#)]
7. Frattolillo, F. A Watermarking Protocol Based on Blockchain. *Appl. Sci.* **2020**, *10*, 7746. [[CrossRef](#)]
8. Jebreel, N.; Domingo-Ferrer, J.; Sánchez, D.; Blanco-Justicia, A. KeyNet: An Asymmetric Key-Style Framework for Watermarking Deep Learning Models. *Appl. Sci.* **2021**, *11*, 999. [[CrossRef](#)]
9. Wu, H.; Chen, L.; Ching, Y. Block-Based Steganography Method Using Optimal Selection to Reach High Efficiency and Capacity for Palette Images. *Appl. Sci.* **2020**, *10*, 7820. [[CrossRef](#)]
10. Aziz, B.; Jung, J.; Lee, J.; Chun, Y. A False Negative Study of the Steganalysis Tool Stegdetect. *Appl. Sci.* **2020**, *10*, 8188. [[CrossRef](#)]
11. Järpe, E.; Weckstén, M. Velody 2—Resilient High-Capacity MIDI Steganography for Organ and Harpsichord Music. *Appl. Sci.* **2021**, *11*, 39. [[CrossRef](#)]
12. Keller, J.; Wendzel, S. Reversible and Plausibly Deniable Covert Channels in One-Time Passwords Based on Hash Chains. *Appl. Sci.* **2021**, *11*, 731. [[CrossRef](#)]
13. Chen, Y.; Chang, C.; Lin, C.; Wang, Z. An Adaptive Reversible Data Hiding Scheme Using AMBTC and Quantization Level Difference. *Appl. Sci.* **2021**, *11*, 635. [[CrossRef](#)]
14. Tundis, A.; Mukherjee, G.; Mühlhäuser, M. An Algorithm for the Detection of Hidden Propaganda in Mixed-Code Text over the Internet. *Appl. Sci.* **2021**, *11*, 2196. [[CrossRef](#)]