A SYSTEMATIC REVIEW OF MULTI-MEDIA CRYPTOSTEGANOGRAPHY: TECHNIQUES, CONSTRAINTS, AND ARCHITECTURAL REQUIREMENTS FOR WEB DEPLOYMENT

Kareena U, Koustubha Nagaraj, Muskaan Sheikh. Soujanya K

0. Abstract

0.1. Introduction and Background

The online space expands quicker all the time. That kind of expansion pulls in constant threats from folks aiming to grab data they should not touch. Regular encryption alone does not cut it anymore. We really need stronger options. Steganography covers up the very existence of any message in the first place. It gives a solid method for sharing info without anyone noticing[1]. Even so, things like the web remain wide open and easy to hit. Fresh types of attacks on networks show up regularly too. That means we must layer in tough defenses that fit together well. Such an approach keeps information secure and unaltered as it moves around. Environments full of constant surveillance or pattern hunting require nothing less.

0.2. Purpose and Research Gap

While numerous studies investigate steganography within individual media types (image or video), a comprehensive, multi-media assessment that systematically integrates constraints, specifically, mandatory pre embedding cryptography and constraints imposed by web application deployment that remains undeveloped in the extant literature[2]. This systematic literature review (SLR) addresses this gap by synthesizing the state of the art across four primary digital media: Image, Audio, Video. This paper seeks to answer the fundamental question: How do different multimedia steganography techniques compare in terms of data capacity, imperceptibility, and robustness?

0.3. Methodology

This review synthesizes findings from seminal and contemporary academic work. The analysis focused on schemes evaluated across the core performance metrics of Capacity, Imperceptibility (quantified by metrics like PSNR and SSIM), and Robustness(resistance to steganalysis and file modifications). We systematically categorize methodologies based on their domain(spatial vs transform) and addressed technical constraints critical for reliable web system deployment.

0.4. Principal Findings

The analysis yields critical comparative findings that shape the development of robust steganographic systems:

1. **Trend Towards LSB and Capacity Trade-Offs:** There is a confirmed, significant historical and persistent trend towards the Least Significant Bit (LSB) technique, particularly in web-based image systems, owing to its inherent simplicity and high capacity in the spatial domain[3, 4]. However, this popularity is tempered by its vulnerability; complex transform domain techniques, such as Discrete Cosine Transform (DCT) often offer better imperceptibility (higher PSNR) and stronger robustness against attack, though usually at the expense of lower payload capacity. Furthermore, utilizing high-quality, high resolution images is critical, as the increased pixel count directly translates to substantially superior data hiding capacity (payload)[5, 6, 7].

2. **The Audio Integrity Constraint:** Reliability in audio steganography demands the use of uncompressed Pulse Code MOdulation (PCM) formats, specifically WAV, because lossy compression formats (eg. MP3) introduce significant data loss and risk file corruption due to magnified changes upon decompression, rendering them unsuitable for guaranteed data integrity[8].

3. **Video Utility:** Video offers the highest capacity medium, leveraging techniques from both image and audio steganography.

0.5. Conclusion and Implication

The development of viable covert communication systems for web development necessitates a combined Cryptosteganographic architecture, where pre-encryption messages confidentiality and integrity regardless of a successful steganalysis attack[9, 10]. Future research must prioritize adaptive algorithms that maintain low computational complexity- critical for real time web deployment- while adhering to strict media format constraints, particularly the use of uncompressed media to prevent payload destruction.

I. Foundational Concepts and Architectural Necessity

1.1 Differentiation and Convergence of Steganography and Cryptography

Information security systems fundamentally rely on mechanisms to protect data during exchange. Two primary methodologies dominate this field: cryptography and steganography. Cryptography functions by mathematically transforming a message into an unintelligible format(ciphertext), ensuring that only authorized parties possessing the correct key can read the contents. Its primary goal is to maintain the secrecy of the content. Conversely, steganography operates on the principle of covertness- it conceals the existence of the message itself within an innocuous cover object (such as image, video, audio), rendering the communication invisible to all but the intended recipient.

A critical difference between the two fields lies in the security guarantees they provide. While steganography primarily offers confidentiality (covertness), cryptography inherently provides confidentiality, integrity (ensuring the message has not been tampered with), and non-repudiation. In modern network security, where data integrity is as crucial as confidentiality, neither methodology is sufficient alone. The increasing prevalence of statistical steganalysis mechanisms designed to detect hidden messages in digital media necessitates a layered defensive approach.

1.2. The Layered Defence: Cryptosteganographic Systems

The convergence of steganography and cryptography is essential for creating robust, modern security systems, often termed Cryptosteganographic architectures. In this layered approach, the secret message is first encrypted using a string algorithm (such as AES) to ensure its confidentiality and integrity[9]. This ciphertext is then embedded into the cover medium using a steganographic algorithm. The process utilizes a stego-key, which often functions as a password for decryption and extraction, resulting in the final stego-medium.

The primary operational advantage of this integration is resilience. Should a covert channel be detected by advanced steganalysis, the underlying payload being encrypted remains unintelligible and secure. By pre-encrypting the data, the security architecture ensures that the failure of covertness does not equate to a failure of confidentiality. This combination provides a powerful dual defense mechanism vital for securing data transmission over inherently unsafe communication channels like the internet[10].

II. Comparative Analysis of Multimedia Steganography Techniques

This section systematically addresses the research question by comparing different multimedia steganography techniques baked on three fundamental performance metrics: Capacity, Imperceptibility and Robustness[4].

2.1 Defining the Performance Triad: Capacity, Imperceptibility and Robustness

Evaluation of any steganographic scheme rests upon a triad of core performance metrics:

1. **Imperceptibility (Quality) :** This measures the extent to which the hidden message alters the cover object. High imperceptibility is quantified using objective quality metrics like the Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index Measure (SSIM)[11, 12]. A higher PSNR generally indicates lower visual or aural distortion.
2. **Payload Capacity :** This refers to the maximum volume of secret data that can be embedded into the cover object, often measured in bits per pixel (bpp). Higher capacity is desirable for large data transmission[4, 12].
3. **Robustness :** This is the resistance of the system both to malicious detection (Steganalysis) and to incidental attacks, such as image compression, filtering or format conversion. Robustness is crucial for maintaining message integrity during transmission[4].

2.2 Image Steganography: The Trade-off between Spatial and Transform Domains

Image steganography is primarily categorized into two domains: spatial and transform. The comparison between the widely used Least Significant Bit (LSB) technique (spatial domain) and the Discrete Cosine Transform (DCT) technique (transform domain) reveals a direct trade-off among the three core metrics.

LSB vs. DCT Comparison

Metric	LSB (Spatial Domain)	DCT (Transform Domain)	Finding
CAPACITY	High/Superior	Low/Very mall	LSB is often preferred for applications requiring maximum payload, potentially achieving up to 4bpp
IMPERCEPTIBILITTY	Good, but typically lower PSNR	Higher PSNR / Minimal Distortion	DCT alters frequency coefficients, leading to less noticeable distortion and better quality metrics than basic LSB
ROBUSTNESS	Low (Highly susceptible to steganalysis)	Higher (More robust to compression / filtering)	LSB's simple, deterministic embedding introduces statistical anomalies easily detected by universal steganalysis.

The sustained popularity of LSB, particularly in web-based applications, is primarily due to its simplicity and speed, making it low-complexity for deployment[3, 13]. However, this comes at the cost of robustness, leading researchers to shift towards complex, AI-driven techniques to defeat advanced statistical steganalysis.

Capacity Enhancement via Image Quality

A significant finding is that capacity is directly linked to the quality and resolution of the cover image. High-quality, high-resolution images are confirmed to provide superior payload capacity because they contain a greater number of redundant pixels for embedding[4, 6]. State-of-the-art algorithms have demonstrated embedding efficiencies exceeding 5.22 bits per pixel (bpp) by leveraging high-quality cover images[14]. However, embedding must adhere to a strict PSNR threshold (e.g., 30 dB) to maintain imperceptibility, as maximizing capacity without regard for quality compromises covertness[12].

2.3 Audio Steganography: The Integrity Constraint and Capacity

Audio steganography employs methods like LSB coding, parity coding and echo hiding. LSB coding is the simplest method for embedding and extraction in audio files, often used to achieve high data rates.

The WAV Format Imperative

A mandatory constraint dictates that reliable audio steganography must utilize uncompressed formats, specifically WAV files based on Pulse Code Modulation (PCM), rather than compressed formats like MP3.

- **WAV (Uncompressed):** Changes in the least significant bits of raw PCM data do not significantly affect the audio playback or break the file structure, ensuring both imperceptibility and integrity. WAV files possess a high native bitrate (e.g., 1411 kbps at 16 bit), providing a large, table data reservoir and are better suited for editing and data hiding.
- **MP3 (Lossy Compression):** MP3 compression reduces file size by removing data (psychoacoustic modeling). If a secret payload is embedded and the file is subsequently compressed or decompressed, the embedded changes are magnified, risking file corruption or the destruction of the hidden message (data loss)[15].

Therefore, while LSB provides high capacity in audio, the technique's Robustness against incidental data destruction is only maintained if the cover media is strictly uncompressed (WAV)[8].

2.4 Video Steganography: Scale and Utility

Video Steganography: Highest Capacity
Video offers the highest payload capacity because it is a combination of sequential image frames and an audio track. Techniques used include LSB and DCT applied to individual frames, as well as manipulating motion vectors or coefficients in compressed video.

- **Capacity:** Extremely high.
- **Robustness:** High complexity. Robustness is a major challenge due to video compression (encoding) during transmission. Advanced techniques, including those based on Generative Adversarial Networks (GANs) and deep learning, are increasingly necessary to achieve high visual quality and strong robustness against popular video compressions.

III. Synthesis, Challenges and Conclusion

3.1. Comparative Performance Synthesis Across Media

MEDIA TYPE	DOMINANT TECHNIQUE DOMAIN	CAPACITY PROFILE	IMPERCEPTIBILITY PROFILE	ROBUSTNESS PROFILE
IMAGE	Spatial (LSB) & Transform(DCT)	High (LSB)to Moderate (DCT)	Excellent (DCT) to Good (LSB)	Low (LSB) to Moderate (DCT).
AUDIO	LSB / PCM based	High, based on bitrate (WAV)	High (minimal artifacts in WAV)	High only if WAV format is strictly maintained.
VIDEO	Frame / Motion detector	Highest	High (requires advanced algorithms to combat compression)	Highly complex; must resist temporal and compression artifacts.

3.2. Challenges in Universal Steganalysis and System Robustness

The most formidable challenge is the continuous competition between hiders and detectors. The vulnerability of traditional LSB techniques mandates a shift toward adaptive, data-aware algorithms to maintain forensic robustness against universal steganalysis[13]. For web deployment, the challenge lies in balancing the superior Robustness of complex, AI-driven algorithms against the required low Complexity for real-time processing and rapid transmission.

3.3. Recommendations for Next-Generation Cryptosteganographic Systems

Based on the comparative analysis of technical constraints and security vulnerabilities:

1. **Mandatory Integrated Security Architecture:** All development efforts must adopt the layered Cryptosteganographic architecture, ensuring data integrity and confidentiality with cryptography (e.g., AES) regardless of the steganographic layer's success[9, 10].

2. **Adaptive Algorithm Focus:** Future research must prioritize adaptive algorithms that achieve better Imperceptibility and Robustness than traditional LSB by dynamically selecting embedding locations, yet remain computationally efficient for web deployment.

3. **Adherence to Uncompressed Media Standards:** For audio, developers must strictly adhere to the use of uncompressed WAV formats, recognizing that Robustness and message integrity are destroyed by using lossy compression (MP3)[8].

IV. REFERENCES

[1]. J. Bah l and R. Ramakishore, "LSB Technique and Its Variations Used In Audio Steganography: A Survey," International Journal of Engineering Research & Technology (IJERT), vol. 02, no. 04, April 2013.

[2]. E.G. Satish, N. Sreenivasa, E. Naresh, P. Ramesh Naidu, and A.C. Ramachandra, "Multimedia Multilevel Security by Integrating Steganography and Cryptography Techniques," ITM Web Conf., vol. 57, 2023, Art. no. 01012. Doi: 10.1051/itmconf/20235701012.

[3]. S. Rahman et al., "A novel and efficient digital image steganography technique using least significant bit substitution," Scientific Reports, col. 15, no. 1, 2025.

[4]. H Kaur and J Rani, "A Survey on different techniques of steganography," MATEC Web of Conferences, vol. 57, 2016.

[5]. M. H. Mohamed and L. M. Mohamed, "High Capacity Image Steganography Technique based on LSB Substitution Method," Applied Mathematics & Information Sciences, vol. 10, no. 1, 2016.

[6]. A. A. Zakaria et al., "High-Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution," Applied Sciences, vol. 8, no. 11, 2018.

[7]. M. Pelosi and C. Easttom, "Positive Identification of LSB image Steganography using Cover Image Comparisons," Journal of Digital Forensics, Security and Law, vol. 15, no. 2, 2021.

[8] .B. E. Sánchez Rinza, L. G. Munive Morales, and A. Jaramillo Núñez, "LSB Algorithm to Hide Text in an Audio Signal," COMPUTACIÓN Y SISTEMAS (COMP. Y SIST.), vol. 26, no. 1, Jan/Mar. 2022.

[9] . D. K. Sarmah and N. Bajpai, "Proposed System for data hiding using Cryptography and Steganography," International Journal of Computer Applications, vol. 8, no. 9, Sept. 2010.

[10]. A. U. Zaman, "Security during transmission of Data Using Web Steganography," Starred Paper (Master's Thesis), St. Cloud State University, 2018.

[11]. Z. N. Sultani and B. N. Dhannoon, "Image and Audio Steganography based on indirect LSB," Kuwait Journal of Science, vol. 48, no. 4, 2021.

[12]. R. S. Hameed et al., "High Capacity Image Steganography System based on Multi-layer Security and LSB Exchanging Method," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 13, no. 8, 2022.

[13]. R. Apau et al., "Image Steganography Techniques for Resisting Statistical Steganalysis Attacks: A systematic literature review," PLoS One, vol. 19, no. 9, 2024.

[14]. S. Zhang et al., "A High-Capacity Steganography Algorithm Based on Adaptive Frequency Channel Attention Networks," Sensors (Basel), vol. 22, no. 20, 2022.

[15]. E. A. Alsolami, "Audio Steganography Method using Least Significant Bit (LSB) Encoding Technique," Journal of Theoretical and Applied Information Technology, vol. 100, no. 12, 2022.