Journal of Magnetism and Its Applications

ISSN: 2797-507X

# DUAL-LAYERED DATA SECURITY: COMBINING ENCRYPTION AND IMAGE STEGANOGRAPHY

**Syed Azlan Shah[*1], Ehram Aylia Awan[2], Muhammad Faisal[3], Muhammad Umair Khan[4], Abdul Ahad[5], Muhammad Taha Farooq[6]**

[*1,2,3,4,5,6]*Student, HITEC University*

[*1]azlansyed123@gmail.com, [2]ehramawan35@gmail.com, [3]mfaisal7529@gmail.com, [4]muhammadumairrkhan003@gmail.com, [5]abdulahadkhan3921@gmail.com, [6]tahafarooq12367@gmail.com

**Article History**

**Keywords:**
*AES encryption, image steganography, keyed LSB substitution, hybrid security, IoT, steganalysis, data protection, cryptography, survey*

**Article History**
*Received: 22 August 2026*
*Accepted: 01 November 2026*
*Published: 17 November 2026*

**Copyright** @Author
**Corresponding Author: ***
**Syed Azlan Shah**

**Abstract**

*The rapid expansion of digital communications, cloud services, remote healthcare, and Internet of Things (IoT) applications has intensified the demand for efficient data protection mechanisms, particularly for resource-constrained devices. Cryptography and steganography are complementary information security techniques: cryptography protects message content by rendering it unreadable, while steganography conceals the very existence of communication within an innocuous carrier such as a digital image. Neither technique alone provides comprehensive protection. This survey presents a structured review of eight primary sources spanning 2024–2026 to examine the state of hybrid cryptography-steganography systems for image-based data security. Through systematic comparative analysis, six critical research gaps are identified: the absence of a controlled AES-keyed-LSB protocol, inconsistent evaluation methodologies across studies, conflated security claims, insufficient IoT-specific computational validation, inadequate steganalysis resistance testing, and the lack of standardized baselines. A taxonomy of steganographic techniques (spatial, transform, adaptive, deep learning), cryptographic methods (AES, SPN, chaotic maps, RSA, ECC), and security evaluation approaches is provided. A conceptual reference framework combining AES-256 encryption with keyed LSB substitution is proposed as a design specification for future experimental validation and fair comparison with more complex methods. The survey identifies key challenges including the universal trade-off between capacity, imperceptibility, and security; the steganalysis generalization problem; the deep learning reversibility limitation; and the critical gap in IoT-specific hardware validation. Ten future research directions are proposed to address these challenges.*

## 1. INTRODUCTION

Public and wireless networks are becoming increasingly popular due to the widespread use of digital communications, cloud services, remote healthcare, banking, and Internet of Things (IoT) applications [1], [8] that have been rapidly growing, leading to greater amounts of sensitive information being sent over the network. In such environments, confidentiality, integrity, authentication, and efficient data

protection are demanded, especially when devices are constrained in terms of processing power, memory, bandwidth, or battery capacity [4], [6].

Cryptography and steganography are complementary techniques for information security [7]. The difference between cryptography and steganography is that cryptography hides the content of a message by making it unreadable without the key, while steganography hides the message in plain sight by using a seemingly ordinary carrier, such as a digital image [1], [2], [8], [20].

However, neither of these techniques should be seen as a "cure-all" when used by itself [1]. Encrypted data would be interesting to an attacker since it would signal to the intruder that the communication involved is protected [4], [7]. Likewise, statistical artifacts could be introduced in conventional steganography in the spatial domain, such as the predictable least significant bit (LSB) replacement, which can be identified by regular-singular analysis, chi-square analysis, pixel-difference analysis, and machine learning steganalysis [2], [3], [12], [13].

These challenges are further made worse by the growing use of IoT devices. Sensors, wearable devices, medical equipment, smart-home elements, and industrial controllers are typical examples of IoT devices that communicate over limited wireless channels through which they share sensitive information. These devices are typically limited in memory, processing power, energy, and bandwidth, and require mechanisms capable of securing these devices without imposing an undue processing burden [4], [6].

Thus, hybrid cryptography and steganography systems have received significant research interest. A hybrid system does both: it uses cryptography for confidentiality and steganography for hiding the existence of the communication [7]. Should an attacker be able to detect the hidden payload, the encrypted content ought to still be unreadable without the proper cryptographic key. This layered system can offer more security than cryptography or steganography alone [1], [5], [8].

But when several security methods are used together, it does not necessarily yield a secure and efficient solution. A hybrid system should consider several factors: confidentiality, imperceptibility, embedding capacity, robustness, resistance to steganalysis, computational complexity, memory usage, and transmission latency [1]. The payload will increase the capacity, but also add to the image distortion and ease of detection [2], [5]. Likewise, more sophisticated encryption techniques or embedding methods can make a system more secure but less viable for resource-constrained systems [4], [6].

Various techniques have been studied to date: Advanced Encryption Standard (AES) [2], [10], substitution-permutation networks (SPNs) [6], chaotic maps [6], [7], discrete cosine transform (DCT), discrete wavelet transform (DWT), HUGO [14], WOW, UNIWARD [15], generative adversarial networks, and adaptive embedding algorithms. These methods have different features with regard to security, robustness, imperceptibility, capacity, and computational cost [2]. However, when many techniques are discussed at once, without specifying their role, it may be difficult to clearly determine the research direction, and it may be hard to assess the proposed contribution accurately [1], [5].

### 1.1 Paper Type and Contribution Statement

This paper is positioned as an original survey paper informed by a structured literature review. It is neither a purely systematic review nor an experimental study. The contribution follows a coherent research arc:

1. A structured review of existing hybrid cryptography-steganography literature identifies specific gaps.
2. Those gaps motivate the design of a focused, reproducible AES-keyed-LSB reference framework.
3. The framework is specified in sufficient detail for independent implementation and benchmarking by future researchers.
4. A comprehensive evaluation protocol is defined with controlled baselines, datasets, metrics, and attack models.

The paper does not claim superiority of AES-keyed-LSB over transform-domain, adaptive, chaotic-map, SPN-based, or deep-learning methods. It provides a controlled baseline against which such methods can be fairly compared in future work.

### 1.2 Research Objectives

1. To provide a comprehensive structured review of hybrid cryptography-steganography systems for image-based data security [1], [5], [6].
2. To assess the current state of combining AES encryption with keyed LSB image steganography in terms of image quality, extraction accuracy, and security [2], [5].
3. To examine the effects of payload size and embedding rate on the performance and detectability of stego-images as reported in existing literature [2], [3].
4. To examine whether existing methods are computationally efficient enough for resource-constrained or IoT applications [4], [6].
5. To propose a conceptual reference framework for future experimental validation and fair comparison.

### 1.3 Expected Contributions

1. A well-defined and repeatable reference framework of AES-keyed-LSB, separated from unrelated techniques in the core algorithm [1], [5], [8].
2. A structured comparison against existing methods, reporting security, imperceptibility, capacity, robustness, extraction correctness, and computational cost as documented in the literature [2], [5].
3. A standardized baseline protocol against which transform-domain, adaptive, chaotic-map, SPN-based, and deep-learning steganography methods can be fairly compared in future studies [2], [3], [6].

### 1.4 Scope and Research Boundaries

The focus of this survey is strictly on AES encryption and keyed LSB image steganography [1], [5], [6]. Advanced techniques such as HUGO, WOW, UNIWARD, DCT, DWT, chaotic maps, SPNs, and GANs are discussed as related techniques or future comparison techniques [2], [3]. This narrow focus results in a clear research problem, a well-defined contribution, and a measurable assessment process [1], [5].

The central question is: Is it possible to hide AES-encrypted data with keyed LSB image steganography under acceptable image quality, extraction accuracy, statistical steganalysis resistance, and computational efficiency for resource-constrained or IoT applications? The answer will be evaluated based on a repeatable implementation specification, controlled baselines, clearly defined datasets, varying payload sizes, explicit attack models, and multidimensional performance evaluation [1], [2], [3], [5].

## 2. SURVEY METHODOLOGY

### 2.1 Research Approach

This study employs a structured literature review to identify, categorize, and critically analyze existing work on hybrid cryptography-steganography systems, image steganography techniques, and IoT-specific security constraints. The review follows a transparent and reproducible protocol inspired by the PRISMA guidelines [9], as applied by Apau et al. [3] in their systematic review of 125 articles. The screening was conducted by the authors on a focused set of databases.

### 2.2 Search Strategy

The literature search targeted the following electronic databases:

- IEEE Xplore
- ACM Digital Library
- ScienceDirect
- Wiley Online Library
- Springer Link
- ResearchGate (for supplementary sources)

Search terms included combinations of:

- (“steganography” AND “cryptography” AND “hybrid”)
- (“image steganography” AND “AES” AND “LSB”)
- (“encryption” AND “steganography” AND “IoT”)
- (“steganalysis” AND “statistical attacks” AND “image”)

- ("keyed embedding" AND "image security")

The search period covered publications from 2019 to 2026.

### 2.3 Inclusion and Exclusion Criteria

**Inclusion Criteria:**

1. Peer-reviewed journal articles or top-tier conference papers
2. Published in English
3. Focus on image steganography, cryptography, or their combination
4. Report quantitative performance metrics (PSNR, MSE, SSIM, BER, execution time, or equivalent)
5. Published between 2019 and 2026

**Exclusion Criteria:**

1. Non-English publications
2. Studies focused exclusively on audio, video, or text steganography without an image component
3. Papers without quantitative evaluation
4. Duplicate publications

### 2.4 Study Selection

Eight primary sources were selected for detailed analysis based on their direct relevance to the proposed AES-keyed-LSB framework, hybrid crypto-steganographic design, IoT constraints, and steganalysis evaluation. These sources span the period 2024–2026 and include both survey/review papers and original experimental studies. Although the search window extended from 2019 to 2026, the sources retained for detailed analysis are the most recent ones that satisfied all inclusion criteria.

### 2.5 Data Extraction

For each included study, the following data were extracted:

- Publication year, venue, and authors
- Steganographic technique (spatial, transform, adaptive, deep learning)
- Cryptographic algorithm used
- Cover media type and dataset
- Performance metrics reported
- Security evaluation methods
- IoT applicability assessment
- Identified limitations

### 2.6 Quality Assessment

Selected papers were assessed for:

- Clarity of research objectives
- Adequacy of methodology description
- Reproducibility of experiments
- Comprehensiveness of evaluation metrics
- Statistical validity of results
- Disclosure of limitations

## 3. LITERATURE REVIEW AND BACKGROUND

### 3.1 Image Steganography

The method of hiding a secret message in an image where the presence of the secret message is not easily detected is called image steganography. To embed the payload, the cover image is modified to form a stego-image, and the receiver who is supposed to extract the payload applies the extraction procedure to the stego-image to recover the payload. The main design criteria are: imperceptibility, embedding capacity, robustness, security, and computational efficiency [1], [2], [3], [18].

The image steganography techniques can be divided into two categories: spatial domain techniques and transform domain techniques. The spatial domain approaches deal with the pixels of the image itself, as opposed to the transform domain approaches which manipulate the coefficients obtained from transforms such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Spatial techniques are usually easier and quicker, while transform domain techniques might be more robust to some image processing tasks but are more complicated [1], [3], [7], [18].

### 3.2 LSB Steganography

One of the spatial-domain techniques is Least Significant Bit (LSB) substitution, in which some low-order bits of the image are substituted by secret bits. LSB can provide a high degree of imperceptibility while requiring little computational resources, as the low-order bits in a pixel value only change slightly when altered. Such properties are attractive for lightweight and resource-limited applications [3], [4], [6].

The biggest drawback of conventional LSB substitution is its predictability. If the embedding is sequential or not sufficiently random, then the statistics of the embedded pixels can be altered in a manner that can be detected [1], [2], [3]. These changes can be utilized to differentiate cover images from stego-images through regular-singular analysis [13], chi-square analysis [2], [12], pixel-difference analysis [3], and machine-learning-based steganalysis methods. Higher payload results in higher capacity as well as higher distortion and detectability [1], [2], [3].

Randomized embedding or keyed embedding uses a pseudo-random sequence, dependent on the secret, to select embedding positions as a solution to part of the problem. However, keyed position selection is not inherently secure; the performance of the pseudorandom generator, payload rate, distribution of the cover image, and the detector used for evaluation all influence the security result [1], [2], [3], [6].

Banoori et al. [5] demonstrated that up to 4 LSBs can be used before significant quality degradation occurs, reporting PSNR values ranging from 62.55 dB (4-LSB) to 87.876 dB (1-LSB) across various test images. Alaklabi et al. [6] confirmed that 1-bit LSB achieves PSNR of 85.738 dB for small payloads (19 bytes) and 59.320 dB for 10 KB payloads using their SPN+CLM+LSB system.

### 3.3 Cryptography and AES

To secure the content of information, it is possible to encrypt the information using an algorithm and a secret key, which is called cryptography. In the case of bulk data processing, symmetric encryption is less expensive in terms of computational complexity than public-key encryption [3] and uses a single secret key for encryption and decryption [7], [8].

In this survey, Advanced Encryption Standard (AES) is identified as the most relevant basic encryption technique [3]. AES is a symmetric block cipher with keys of 128 bits, 192 bits, and 256 bits, and 128-bit blocks [10]. Since it is efficient, standardized, and widely employed, it is suitable to encrypt the payload prior to embedding it in the stego-medium [3], [5], [8].

Ahmed et al. [8] provide a comprehensive classification of cryptographic algorithms into symmetric-key cryptography (AES, DES, 3DES, RC4, Blowfish), asymmetric/public-key cryptography (RSA, DSA, ElGamal, ECC), and hash functions (SHA-1, SHA-2 family, MD5). They note that hybrid cryptography refers to the integration of multiple algorithms to enhance efficiency and address limitations inherent in individual algorithms [8].

The implementation should clearly indicate AES mode, AES key length, nonce/initialization vector procedure, padding behavior, and integrity protection. The authentication tag should be embedded in or transmitted with the ciphertext when authenticating. In an authenticated mode such as Galois/Counter Mode (GCM), a nonce should be different in each encryption [3], [11].

### 3.4 Hybrid Cryptography-Steganography

A combination of encryption and steganography is called a hybrid system. First, the secret message is encrypted, and the encrypted message (ciphertext) is then written into a cover medium. Once the ciphertext is received, the receiver fetches the received data and then decrypts it. There are two complementary approaches: hiding and encryption of the information [3], [5], [8].

According to Haverkamp and Sarmah [1], some of the application areas in which hybrid systems have been studied include healthcare, IoT, cloud, UAV, automotive, e-commerce, and others. They also find that there are limitations and trade-offs to consider in hybrid designs regarding security, image quality, capacity, computation, latency, and usability. Therefore, it is important to consider multiple factors other than the strength of the encryption or PSNR to assess a proposed hybrid system [1]. Their systematic analysis found that 42% of the identified articles incorporated a Reversible Data Hiding (RDH) technique, indicating growing interest in lossless recovery.

Banoori et al. [5] employ AES, image-transposition, pixel shuffling, XOR processing, and LSB embedding. Their results show the potential of AES-based hybrid image steganography, but by using several operations, the importance of clearly specifying the algorithm and separating the contribution of each operation is increased [3], [5]. Their method achieved an average PSNR of 80.49 dB across comparative analysis with state-of-the-art methods (Table 5 in [5]).

Alaklabi et al. [6] investigate a lightweight approach that relies on an SPN and chaotic maps. Their work is similar because it demonstrates that low-complexity hybrid protection is of interest, but distinct from the focused AES-keyed-LSB proposal because it uses a fundamentally different cryptographic architecture [3], [6]. Their system achieved average total execution time of 0.0113 seconds for small text and 0.0162 seconds for 10 KB embedding.

### 3.5 Steganography for IoT

The presence of constraints in IoT environments is increased due to the limited memory, processing power, energy, bandwidth, and storage capabilities of sensors, wearables, medical devices, smart-home systems, and industrial controllers. A secure desktop method might not be feasible on an IoT device if it demands too much time, memory, or energy to run [3], [4], [6].

Driss et al. [4] provide the most comprehensive survey of steganography in IoT, identifying that image-based steganography accounts for 62% of IoT steganography studies, followed by network-based (20%), quantum (8%), audio (5%), text (3%), and video (2%). They emphasize that spatial domain techniques, particularly LSB substitution, are the most widely used due to their simplicity, low computational requirements, and high embedding capacity, making them ideal for resource-constrained IoT devices. However, these techniques lack robustness against attacks and compression.

The features of lightweight processing, low latency, low communication overhead, scalability, and attack resistance on wireless or heterogeneous networks are emphasized in the IoT steganography literature. LSB is appealing in this respect because of its simplicity of implementation, but statistical detection and image manipulation need to be explicitly measured [3], [4].

### 3.6 Steganalysis and Security Evaluation

Steganalysis tries to find out if a carrier has hidden information and, if it does, to find the embedding method or estimate its payload. The statistical methods involve analyzing relationships between the pixels, histograms, pair distributions, and others. These include: RS analysis [13], chi-square analysis [12], pixel-difference analysis, and sample-pair analysis. In modern steganalysis, classifiers that rely on machine learning and deep learning are used [2], [3], [16].

Kombrink et al. [2] provide the most comprehensive survey of steganalysis, reviewing 456 references. They demonstrate that one of the greatest challenges in steganalysis is generalizability: often one scheme can detect the presence of one specific hiding method. Their topological sorting analysis shows that no single steganalysis method is applicable to the majority of steganography methods. They also note that many deep-learning-based steganography methods are not completely reversible, rendering them impractical for actual covert communication [2].

Apau et al. [3] found that GAN-based methods dominate recent research (17 out of 125 papers), followed by Adaptive Edge Detection (AED, 14 papers). They observed that previously preferred traditional techniques such as LSB algorithms are receiving less attention, while AI-powered algorithms including Machine Learning, Deep Learning, CNN, and Genetic Algorithms are recently dominating image steganography research.

The question of security can be divided into two separate questions: can the payload be made confidential when not supplied with the AES key, and can its presence be detected? AES responds to the first question, and keyed embedding and steganalysis experiments to the second question. These properties have a connection but are not synonymous [1], [3], [6].

### 3.7 Performance Measures

MSE, PSNR, and SSIM [1], [2], [3], [5] are commonly used metrics for the assessment of image quality. The average squared difference between corresponding cover and stego-image pixels is used to measure MSE. PSNR is a measure of the relationship between signal and noise expressed in decibels, based on MSE. SSIM can be used to compare structural similarity and to give complementary perceptual information. The lower the distortion, the higher the PSNR or SSIM. However, they are not necessarily resistant to steganalysis [2].

The capacity should be specified in bytes followed by bits per pixel (bpp), which includes the overheads of headers, payload length, nonce/initialization vector, and authentication tag. The bit error rate, byte error rate, message-recovery accuracy, and authenticated decryption success should be used to evaluate extraction [3]. The robustness and efficiency of an IoT platform should be separately measured based on the specified image attack, execution time, memory consumption, latency, and energy consumption [4].

## 4. SYSTEMATIC LITERATURE ANALYSIS

### 4.1 Overview of Selected Studies

Table 1 summarizes the eight primary sources, their focus, strengths, and limitations relevant to this research.

**Table 1. Critical comparison of reviewed studies**

| Study | Primary Focus | Strength | Limitation Relevant to This Research |
|---|---|---|---|
| Haverkamp and Sarmah (2024) [1] | Cryptography and steganography fusion | Identifies application domains and security-performance trade-offs | Hybrid systems vary substantially, making controlled comparison difficult |
| Kombrink et al. (2024) [2] | Image steganography methods and steganalysis | Broad taxonomy of spatial, transform, adaptive, and deep learning approaches | Shows that detector generalization and realistic datasets remain difficult |
| Apau et al. (2024) [3] | Resistance to statistical steganalysis | Systematic review of methods designed to resist statistical attacks | Studies use inconsistent datasets, payloads, metrics, and attack models |
| Driss et al. (2025) [4] | Steganography in IoT | Emphasizes energy, memory, latency, and heterogeneity constraints | IoT suitability requires measurements on a specified platform |
| Banoori et al. (2025) [5] | AES-based hybrid image steganography | Demonstrates an AES and LSB-oriented hybrid design | Multiple processing operations make component-level attribution difficult |
| Alaklabi et al. (2026) [6] | SPN, chaotic maps, and LSB | Targets lightweight hybrid security | Uses a different core architecture from the focused AES-LSB proposal |
| Majeed et al. (2025) [7] | Survey of encryption and steganography | Reviews chaotic, S-box, DNA, spatial, transform, and neural methods | Highlights many alternatives but does not establish one controlled implementation |

| Study | Primary Focus | Strength | Limitation Relevant to This Research |
|---|---|---|---|
| Ahmed et al. (2025) [8] | General cryptography and steganography review | Explains complementary security services and hybrid designs | Broad coverage requires a more narrowly defined experimental framework |

### 4.2 Taxonomy of Steganographic Techniques

Based on the systematic analysis of all eight sources, steganographic techniques are classified as shown in Figure 1.

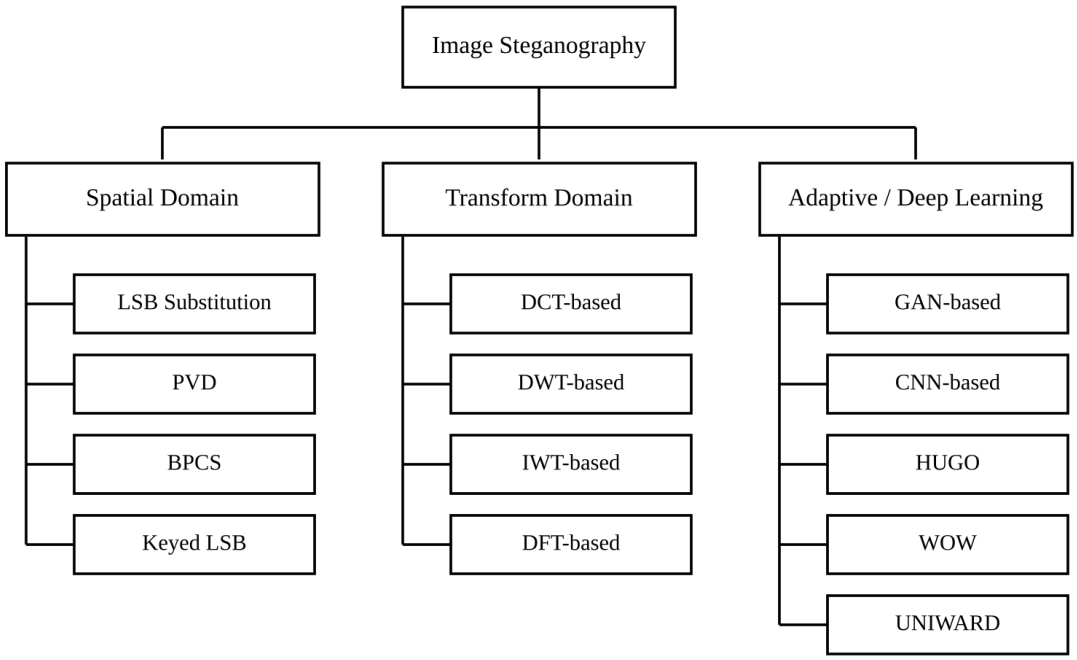



**Figure 1. Taxonomy of image steganography techniques.**

#### *4.2.1 Spatial Domain Techniques*

- **LSB Substitution:** The most fundamental technique. Banoori et al. [5] demonstrated that up to 4 LSBs can be used before significant quality degradation. Alaklabi et al. [6] confirmed PSNR > 85 dB for small payloads at 1-LSB. Driss et al. [4] found spatial domain techniques account for 62% of IoT steganography studies.
- **Pixel Value Differencing (PVD):** Apau et al. [3] reported PVD achieving the highest embedding capacity (8.88 bpp) but with reduced PSNR (25 dB).
- **Keyed/Random LSB:** Uses pseudo-random sequences for embedding position selection, reducing predictability [2], [6].

#### *4.2.2 Transform Domain Techniques*

- **DCT-based:** Most frequently used transform method [2]. Provides higher robustness against compression but lower capacity than spatial methods.
- **DWT-based:** Offers multi-resolution decomposition. Driss et al. [4] noted DWT provides better robustness against noise and geometric attacks.
- **IWT-based:** Avoids floating-point precision problems of DWT [2].

#### *4.2.3 Adaptive and Deep Learning Techniques*

- **GAN-based:** Dominant in recent research (17/125 papers in Apau et al. [3]). Provides high security but limited embedding capacity (typically 0.4–0.5 bpp) and high computational complexity.
- **CNN-based:** Used for both steganography and steganalysis [2], [3].
- **Adaptive methods (HUGO, WOW, UNIWARD):** Minimize embedding distortion by adapting to image content [2], [14], [15].

### 4.3 Cryptographic Methods in Hybrid Systems

Table 2 compares the cryptographic algorithms used in the reviewed hybrid systems.

**Table 2. Cryptographic algorithms used in reviewed hybrid systems**

| Algorithm | Type | Key Size | Used In | Advantages | Limitations |
|---|---|---|---|---|---|
| AES | Symmetric block cipher | 128/192/256-bit | [1], [4], [5], [8] | Standardized, efficient, widely adopted | Requires key management |
| SPN + Chaotic Map | Lightweight symmetric | Variable (SHA2-256 derived) | [6] | Fast, low computational cost | Non-standard, limited cryptanalysis history |
| RSA | Asymmetric | 1024–4096-bit | [1], [8] | No key exchange needed | Computationally expensive |
| Chaotic Maps (Logistic, Henon) | Stream cipher equivalent | Initial conditions | [6], [7] | High sensitivity, fast | Finite precision issues |
| ECC | Asymmetric | 256-bit equivalent | [4] | Smaller keys than RSA | Complex implementation |
| XOR-based | Symmetric | Variable | [1] | Extremely fast and simple | Weak on its own; vulnerable if the key is reused |

### 4.4 Performance Metrics Comparison

Table 3 lists the key performance metrics reported across the reviewed studies. The ranges shown are indicative values commonly used in the literature rather than fixed standards.

**Table 3. Key performance metrics reported across studies**

| Metric | Definition | Typical Range (Good) | Studies Reporting |
|---|---|---|---|
| PSNR (dB) | Peak Signal-to-Noise Ratio | > 40 dB (good), > 50 dB (excellent) | All 8 studies |
| MSE | Mean Square Error | < 1.0 (good) | [1], [3], [5], [6] |
| SSIM | Structural Similarity Index | > 0.95 (good) | [1], [3], [5], [6] |
| BPP | Bits Per Pixel (capacity) | 0.5–4.0 bpp | [3], [4], [5], [6] |
| BER | Bit Error Rate | < 0.01 (good) | [1], [4] |
| Execution Time | Total embed/extract time | < 0.1 s (real-time) | [4], [6] |
| RS Analysis | Regular-Singular detection | < 5% difference | [3], [5] |

| Metric | Definition | Typical Range (Good) | Studies Reporting |
|---|---|---|---|
| NPCR | Number of Pixel Change Rate | > 99.6% | [7] |
| UACI | Unified Average Changing Intensity | 33.4% | [7] |
| Entropy | Information randomness | 8.0 (max for 8-bit) | [7] |

### 4.5 Security Evaluation Methods

Table 4 summarizes the steganalysis and security evaluation approaches used in the reviewed studies.

**Table 4. Steganalysis and security evaluation approaches**

| Attack/Evaluation | Type | Studies Using | Purpose |
|---|---|---|---|
| RS Analysis | Statistical | [3], [5] | Detect LSB-based embedding |
| Chi-Square ($\chi^2$) | Statistical | [3], [5] | Detect sequential embedding patterns |
| Histogram Analysis | Visual/Statistical | [5], [6] | Detect distribution anomalies |
| PDH (Pixel Difference Histogram) | Statistical | [6] | Detect LSB modification patterns |
| ML-based Steganalysis | Intelligent | [2], [3] | Detect subtle embedding artifacts |
| Key Sensitivity | Cryptographic | [5], [6] | Verify encryption robustness |
| Key Space Analysis | Cryptographic | [5], [7] | Assess brute-force resistance |
| Noise/Cropping Attacks | Robustness | [5], [6] | Test resilience to manipulation |
| JPEG Compression | Robustness | [4], [5] | Test survival under lossy compression |

### 4.6 IoT-Specific Findings

Figure 2 and Table 5 relate the IoT device constraints identified by Driss et al. [4] to the resulting design requirements for steganography.

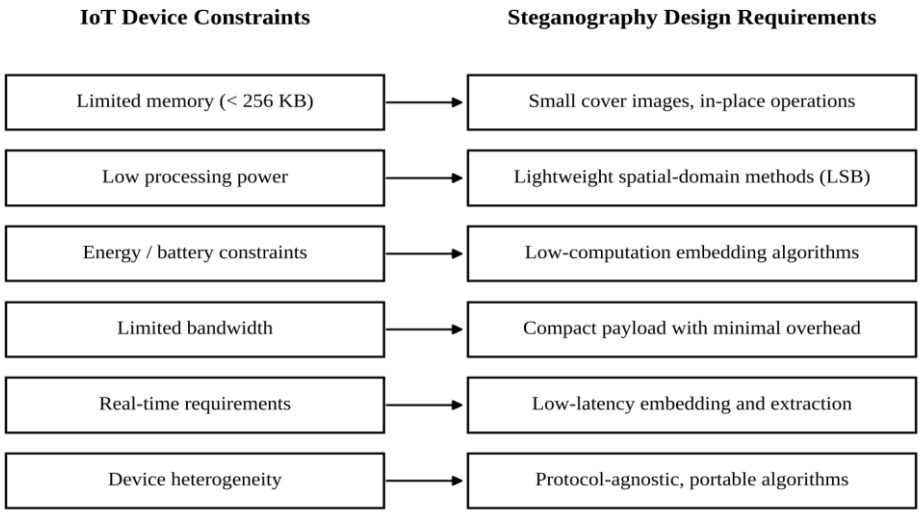



**Figure 2. IoT constraints and their impact on steganography design.**

**Table 5. IoT constraints identified from Driss et al. [4]**

| Constraint | Impact on Steganography | Affected Studies |
|---|---|---|
| Limited memory (< 256 KB typical) | Restricts cover image size and algorithm complexity | [1], [4] |
| Low processing power | Favors spatial domain over transform/DL methods | [4], [6] |
| Energy constraints (battery) | Requires lightweight algorithms | [4], [6] |
| Bandwidth limitations | Restricts payload size | [1], [4] |
| Real-time requirements | Demands low-latency embedding/extraction | [4], [6] |
| Device heterogeneity | Requires protocol-agnostic solutions | [4] |

Driss et al. [4] found that image-based steganography accounts for 62% of IoT steganography studies due to simplicity and low computational requirements, despite vulnerability to statistical attacks. Haverkamp and Sarmah [1] found that among the seven IoT-focused articles in their review, three did not utilize time-based analysis metrics, making it challenging to assess computational performance.

### 4.7 Critical Synthesis

The systematic analysis reveals the following key observations:

1. **Trade-off universality:** All studies confirm the fundamental trade-off between embedding capacity, imperceptibility, and security [1], [3], [5], [6], [7], [8]. Ahmed et al. [8] noted that "capacity and security are reciprocal."
2. **Hybrid superiority:** Combining cryptography with steganography is consistently reported to provide stronger security than either technique alone [1], [5], [6], [8], although these claims are rarely tested under a common protocol. Haverkamp and Sarmah [1] found that 42% of reviewed articles incorporated Reversible Data Hiding (RDH).
3. **Computational cost concern:** Alaklabi et al. [6] achieved average total execution time of 0.0113 seconds for small text and 0.0162 seconds for 10 KB embedding. Banoori et al. [5] require multiple sequential operations (transposition, magic matrix, XOR, LSB, then AES), making component-level attribution difficult.
4. **Detection vulnerability:** Kombrink et al. [2] demonstrated that no single steganalysis method generalizes across multiple steganographic schemes, and spatial domain methods remain most vulnerable.
5. **Standardization gap:** Apau et al. [3] identified that only 27% (34/125) of reviewed papers employed encryption, and only 13% implemented data compression, indicating inconsistent security layering.
6. **GAN dominance with limitations:** Apau et al. [3] found GAN is the most preferred technique (17/125 papers), but Kombrink et al. [2] noted that many DL approaches are not completely reversible, making them impractical for actual covert communication.

### 4.8 Research Gap

Based on the structured review of eight primary sources spanning 2024–2026, several critical gaps in the existing literature are identified:

**Gap 1: Absence of a Controlled, Reproducible AES-Keyed-LSB Protocol.** While Banoori et al. [5] demonstrate an AES-based hybrid steganography system, their framework incorporates multiple simultaneous operations (transposition, magic matrix, XOR, and LSB) without isolating the contribution of each component. Similarly, Alaklabi et al. [6] propose an SPN and chaotic map architecture that is fundamentally different from AES-keyed-LSB. No existing study provides a narrowly defined, reproducible AES-keyed-LSB protocol with controlled baselines (sequential LSB and AES-only transmission) under standardized conditions.

**Gap 2: Inconsistent Evaluation Across Studies.** Apau et al. [3] conducted a systematic review of 125 articles and found that studies use inconsistent datasets, payload sizes, performance metrics, and attack models. Haverkamp and Sarmah [1] similarly identified that hybrid systems vary substantially in their evaluation criteria, making controlled comparison difficult. Specifically, 73% of the papers reviewed by Apau et al. [3] were published between 2018–2023, yet no unified benchmark exists for evaluating crypto-steganographic fusion.

**Gap 3: Separation of Security Claims.** Kombrink et al. [2] demonstrated that steganalysis generalization remains the greatest challenge in the field, with no single detection method applicable across multiple steganographic schemes. However, existing hybrid studies often conflate encryption security (confidentiality) with steganographic security (undetectability). The proposed framework explicitly separates these: AES addresses confidentiality, while keyed embedding and steganalysis experiments address detectability [1], [2], [6].

**Gap 4: IoT-Specific Computational Validation.** Driss et al. [4] comprehensively surveyed steganography in IoT and identified that resource constraints (memory, processing power, energy, bandwidth) are critical yet under-evaluated. Their survey found that 62% of IoT steganography studies use image-based methods, but very few report execution time, memory usage, or energy consumption on actual IoT hardware. Haverkamp and Sarmah [1] confirmed that 3 out of 7 IoT-focused articles did not utilize time-based analysis metrics.

**Gap 5: Statistical Steganalysis Resistance Not Systematically Tested.** Apau et al. [3] found that while GAN-based methods dominate recent research (17 out of 125 papers), traditional LSB methods remain vulnerable to RS and Chi-Square attacks. The proposed keyed-LSB method does not assume undetectability by default but requires explicit experimental validation against statistical (Chi-Square, RS) and machine-learning-based steganalysis detectors [2], [3].

**Gap 6: Lack of Standardized Baseline for Future Comparison.** Ahmed et al. [8] and Majeed et al. [7] provide broad surveys of cryptography and steganography techniques but do not establish a controlled experimental baseline. No existing work provides a standardized AES-keyed-LSB protocol against which transform-domain, adaptive, chaotic-map, SPN-based, or deep-learning steganography methods can be fairly compared in future studies.

This survey identifies these six gaps to guide future research. Specifically, no existing study provides a narrowly defined, reproducible AES-keyed-LSB protocol with controlled baselines under standardized conditions. This survey proposes a conceptual reference framework (Section 5) that addresses these gaps at the design level, providing a structured basis against which future experimental studies can be compared.

## 5. PROPOSED REFERENCE FRAMEWORK

### 5.1 Purpose and Scope

Based on the gaps identified in Section 4.8, this section proposes a conceptual reference framework for a dual-layer security system combining AES-256 encryption with keyed LSB image steganography. This framework is not implemented or experimentally evaluated in this survey. Rather, it serves as:

1. A structured design specification that future researchers can implement and benchmark.
2. A standardized baseline architecture against which transform-domain, adaptive, chaotic-map, SPN-based, and deep-learning steganography methods can be fairly compared.
3. A reference for identifying which components of existing hybrid systems contribute to security, imperceptibility, and computational efficiency.

### 5.2 Framework Architecture

The proposed reference framework consists of two layers, shown in Figure 3. Tables 6 and 7 specify the parameters of each layer.

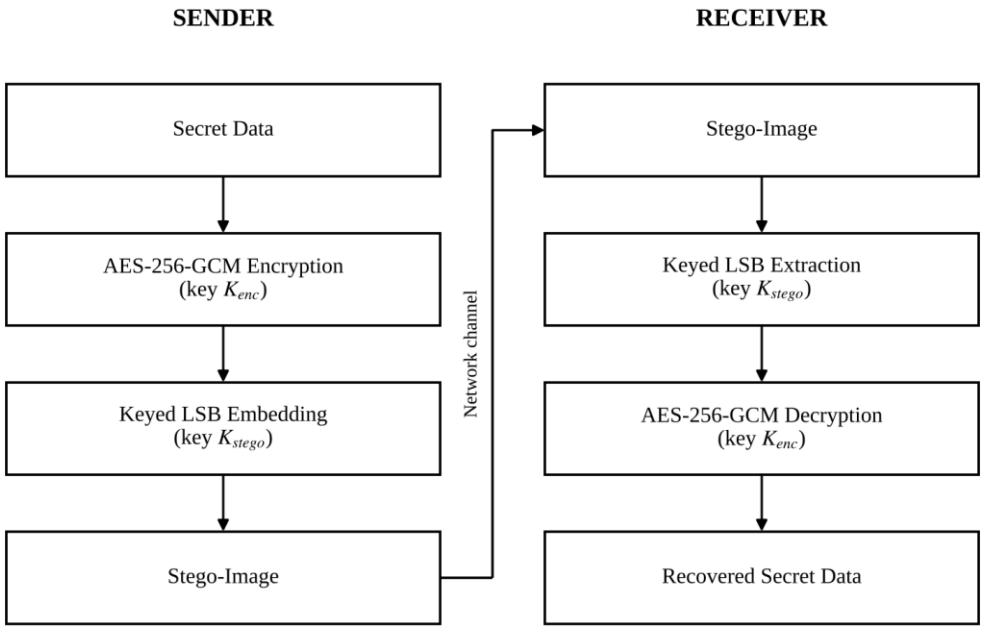



**Figure 3. Dual-layer data security system architecture.**

**Layer 1 — Cryptographic Protection (AES-256-GCM):**

**Table 6. Layer 1 specification: cryptographic protection**

| Parameter | Specification |
|---|---|
| Algorithm | AES-256 in Galois/Counter Mode (GCM) [10], [11] |
| Key length | 256 bits |
| Nonce | 96-bit, unique per encryption session |
| Authentication tag | 128-bit (integrated in GCM) |
| Rationale | AES-GCM provides authenticated encryption in a single standardized primitive, reducing implementation risk [5], [8]. AES is selected for its NIST standardization, hardware acceleration availability, and widespread adoption in hybrid systems [1], [5], [8]. |

**Layer 2 — Steganographic Concealment (Keyed LSB):**

**Table 7. Layer 2 specification: steganographic concealment**

| Parameter | Specification |
|---|---|
| Embedding method | LSB substitution with key-dependent pseudo-random position selection |
| PRNG | Cryptographically secure pseudo-random number generator (CSPRNG) seeded with a 256-bit embedding key |
| Position selection | Fisher–Yates shuffle [19] using PRNG output |
| Embedding depth | 1-LSB per pixel (primary) |
| Rationale | Keyed embedding reduces the predictability of sequential LSB while maintaining low computational complexity suitable for IoT [4], [6]. |

### 5.3 Key Separation

Two independent keys are defined:

- $K_{enc}$ (256-bit): AES-256-GCM encryption/decryption
- $K_{stego}$ (256-bit): CSPRNG seed for embedding position selection

These keys serve independent security functions: $K_{enc}$ protects confidentiality; $K_{stego}$ protects covertness. The effective security of the composed system depends on the construction, key independence, attack model, and which keys the adversary possesses. No "combined key space" claim is made, as this would be an oversimplification of the composed security.

### 5.4 Conceptual Workflow

The sender-side embedding process is shown in Figure 4 and Table 8, and the receiver-side extraction process in Figure 5 and Table 9.

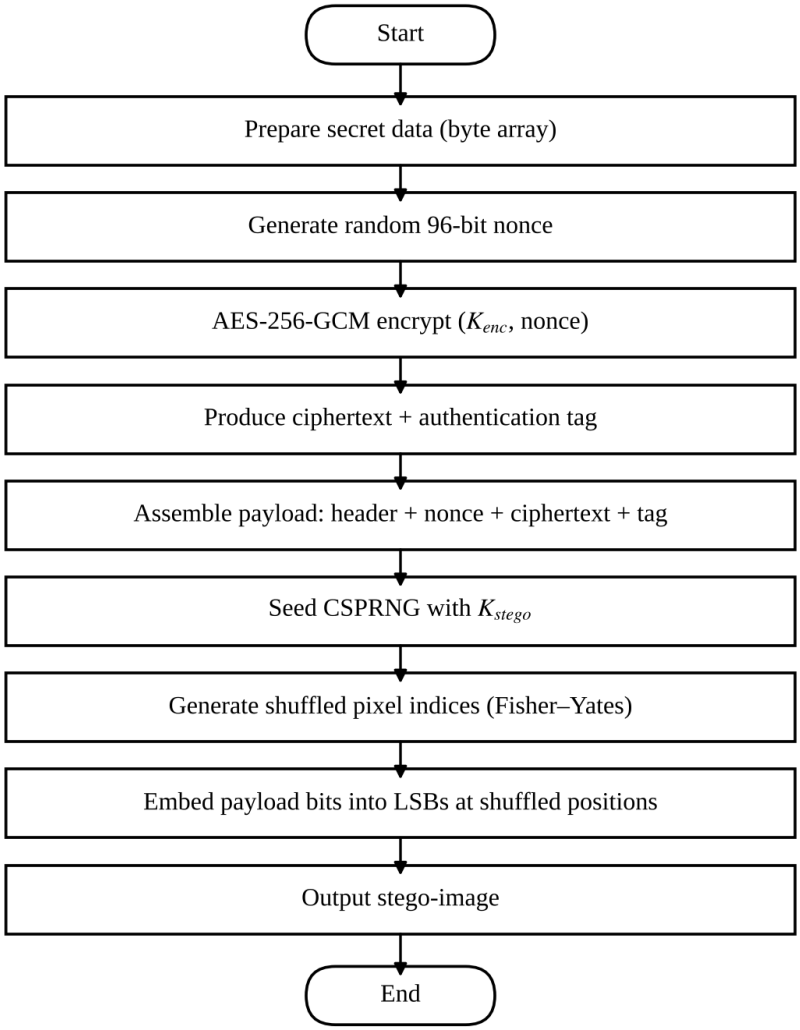



**Figure 4. Embedding process flowchart (sender side).**

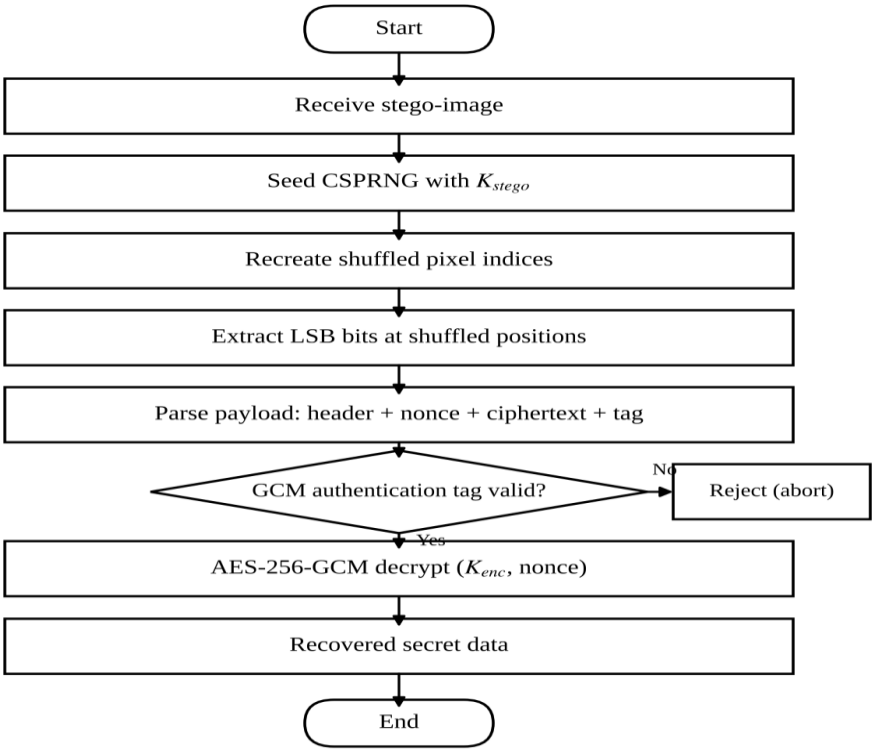



**Figure 5. Payload extraction and decryption flowchart (receiver side).**

**Sender Side (Embedding):**

**Table 8. Sender-side embedding steps**

| Step | Operation |
|---|---|
| 1 | Secret data is prepared as a byte array |
| 2 | AES-256-GCM encrypts the data using $K_{enc}$ and a random nonce, producing ciphertext + authentication tag |
| 3 | Payload is assembled: [Header ‖ Nonce ‖ Ciphertext ‖ Auth Tag] |
| 4 | $K_{stego}$ seeds a CSPRNG to generate a shuffled pixel index array |
| 5 | Payload bits are embedded into the LSBs at the shuffled positions |
| 6 | Stego-image is transmitted |

**Receiver Side (Extraction):**

**Table 9. Receiver-side extraction steps**

| Step | Operation |
|---|---|
| 1 | $K_{stego}$ recreates the shuffled pixel index array |
| 2 | LSB extraction recovers the raw bitstream |
| 3 | Payload is parsed into Header, Nonce, Ciphertext, Auth Tag |
| 4 | GCM authentication tag is verified; if invalid, reject |
| 5 | AES-256-GCM decrypts the ciphertext using $K_{enc}$ and Nonce |

| Step | Operation |
|---|---|
| 6 | Original secret data is recovered |

### 5.5 Threat Model

Table 10 lists the considered threats and the corresponding mitigations.

**Table 10. Threat model and mitigations**

| Threat | Mitigation |
|---|---|
| Passive eavesdropper | Steganography hides communication existence |
| Active steganalyst | Keyed embedding + low embedding rate resist detection |
| $K_{stego}$ compromise | AES encryption renders extracted content unreadable |
| $K_{enc}$ compromise | Attacker cannot locate payload within image |
| Image manipulation | Robustness limited to lossless operations (inherent LSB limitation) |
| Brute-force | AES-256 key space ($2^{256}$) renders exhaustive search infeasible |

### 5.6 Design Rationale

**Table 11. Design decisions and their justification**

| Decision | Choice | Justification |
|---|---|---|
| AES mode | GCM | Single standardized AEAD primitive; no manual MAC composition needed [8], [11] |
| No additional transforms | Excluded (magic matrix, transposition, DWT) | Isolates contribution; reduces complexity for IoT [4], [6]. Banoori et al. [5] use multiple operations making component-level attribution difficult. |
| 1-LSB primary | Minimizes distortion | Alaklabi et al. [6] confirmed PSNR > 85 dB for small payloads at 1-LSB |
| CSPRNG position selection | Eliminates sequential predictability | Addresses vulnerability to RS and Chi-Square analysis [2], [3] |

### 5.7 Positioning Relative to Existing Work

**Table 12. Positioning of the proposed framework relative to existing work**

| Aspect | Proposed Framework | Banoori et al. [5] | Alaklabi et al. [6] |
|---|---|---|---|
| Operations | 2 (AES + keyed LSB) | 5+ (transposition, magic matrix, XOR, LSB, AES) | 4 (SPN, CLM, XOR, LSB) |
| Standardization | AES-256-GCM (NIST) | AES + custom operations | SPN + Chaotic (non-standard) |
| IoT suitability | High (minimal operations) | Low (multiple sequential steps) | Medium |
| Reproducibility | Full specification | Partial | Full |
| Purpose in this survey | Reference baseline for future comparison | Reviewed study | Reviewed study |

### 5.8 Evaluation Protocol for Future Implementation

The following evaluation protocol is specified for future researchers who implement this framework:

- **Datasets:** USC-SIPI [5], [6], BOSSbase v1.01 [2], [17], ALASKA2 [2]

- **Payload sizes:** 1 KB, 5 KB, 10 KB, 25 KB, 50 KB
- **Imperceptibility metrics:** PSNR, SSIM, MSE
- **Security metrics:** RS analysis, Chi-Square test, ML-based steganalysis (SRM features [16] + ensemble classifier), key sensitivity
- **Robustness:** JPEG compression (QF = 95, 90, 80, 70, 50), Gaussian noise, salt-and-pepper noise, cropping, resizing, median filtering
- **Computational efficiency:** AES encryption/decryption time, embedding/extraction time, total end-to-end latency, memory usage
- **Baselines:** Sequential LSB (no encryption), AES-only transmission (no hiding), Random LSB without key

## 6. CHALLENGES AND OPEN ISSUES

Based on the systematic analysis of the reviewed literature, the following challenges and open issues are identified:

### 6.1 Trade-off Universality

Figure 6 illustrates the fundamental trade-off among imperceptibility, embedding capacity, and security.

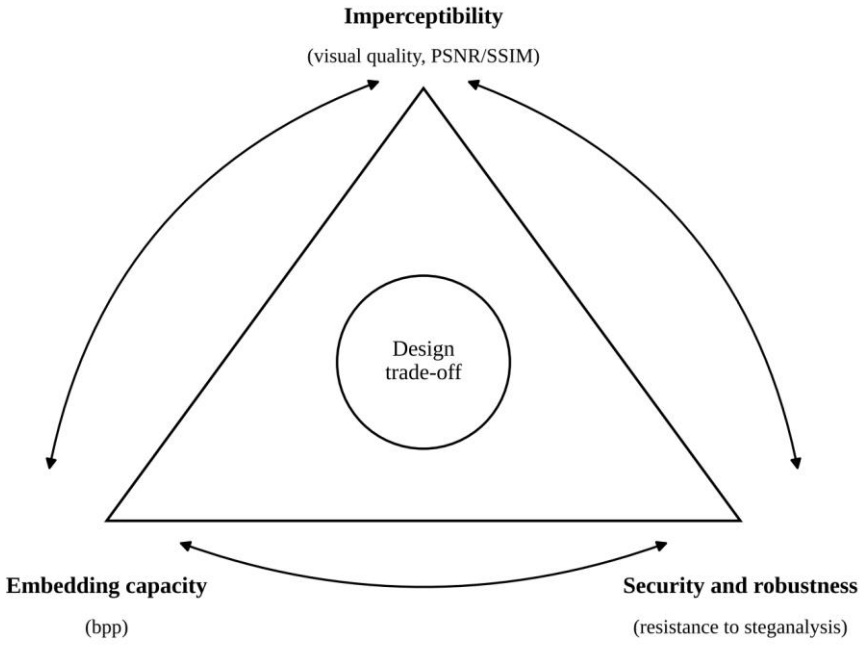



**Figure 6. Fundamental trade-off in image steganography.**

All reviewed studies confirm the fundamental trade-off between embedding capacity, imperceptibility, and security [1], [3], [5], [6], [7], [8]. Ahmed et al. [8] noted that "capacity and security are reciprocal." Increasing payload improves capacity but degrades image quality and increases detectability. No existing method simultaneously optimizes all three. Apau et al. [3] identified this trade-off as the central challenge in image steganography, noting that techniques proposed to achieve high hiding capacity result in image distortion that ultimately reduces security.

### 6.2 Inconsistent Evaluation

Apau et al. [3] found that studies use inconsistent datasets, payload sizes, performance metrics, and attack models. Haverkamp and Sarmah [1] confirmed that hybrid systems vary substantially in evaluation criteria. This makes controlled comparison across studies extremely difficult. A unified benchmark does not exist. The four benchmark datasets most commonly used are BOSSbase, USC-SIPI, Seam Carving Original Q75, and 24 KODAK image databases [3].

### 6.3 IoT-Specific Validation Gap

Driss et al. [4] found that while 62% of IoT steganography studies use image-based methods, very few report execution time, memory usage, or energy consumption on actual IoT hardware. Haverkamp and Sarmah [1] found that 3 out of 7 IoT-focused articles did not utilize time-based analysis metrics. This leaves the practical feasibility of most proposed methods unverified for resource-constrained environments.

### 6.4 Steganalysis Generalization

Kombrink et al. [2] demonstrated that no single steganalysis method generalizes across multiple steganographic schemes. Their topological sorting analysis showed that detection performance varies significantly depending on the specific steganographic method, dataset, and embedding rate. This means that security claims based on a single steganalysis test are insufficient. They strongly recommend that future research always compare new schemes with previous ones to enable relative performance judgment.

### 6.5 Deep Learning Reversibility Problem

Kombrink et al. [2] identified that many deep-learning-based steganography methods (GAN, CNN, autoencoder) are not completely reversible. Without reversibility, the hidden information cannot be reliably extracted, rendering these methods impractical for actual covert communication despite their superior imperceptibility and security. They note: "if no one can extract the hidden information, there is no use for the steganographic method."

### 6.6 Lack of Standardized Baselines

No existing work provides a standardized AES-keyed-LSB protocol against which more complex methods (transform-domain, adaptive, chaotic-map, SPN-based, deep-learning) can be fairly compared. This makes it impossible to determine whether the added complexity of advanced methods provides proportional security benefits. Alaklabi et al. [6] also noted the need for "a unified benchmark that supports fair and transparent evaluation of different steganography methods."

### 6.7 Cryptographic Construction Precision

Many hybrid studies do not specify the exact cryptographic mode, nonce/IV handling, authentication mechanism, or key separation procedure. This lack of precision makes it difficult to assess the actual security of the cryptographic layer and to reproduce the results. Apau et al. [3] found that only 27% of reviewed papers employed encryption, and only 13% implemented data compression.

### 6.8 Computational Complexity of Adaptive Methods

Apau et al. [3] observed that adaptive embedding techniques such as CNN, DL, and GAN were reported to have higher computational complexity than both spatial domain and transform domain methods. This is particularly problematic for IoT applications where real-time processing and energy efficiency are critical [4].

## 7. FUTURE RESEARCH DIRECTIONS

Based on the gaps and challenges identified in this survey, the following future research directions are recommended:

1. **Experimental validation of the proposed reference framework:** Implement the AES-256-GCM + keyed-LSB framework described in Section 5 and report actual PSNR, SSIM, MSE, BER, execution time, and steganalysis resistance measurements on standardized datasets (USC-SIPI, BOSSbase).
2. **Controlled baseline comparison:** Use the proposed framework as a baseline to fairly compare against transform-domain (DCT, DWT), adaptive (WOW, UNIWARD, S-UNIWARD), chaotic-map, SPN-based, and deep-learning steganography methods under identical conditions.
3. **IoT hardware validation:** Measure execution time, memory usage, and energy consumption on actual IoT platforms (Raspberry Pi, ESP32, Arduino) to verify real-time feasibility [4], [6].

4. **Comprehensive steganalysis evaluation:** Test against multiple statistical (RS, Chi-Square) and ML-based steganalysis detectors at varying embedding rates to provide a complete security assessment [2], [3].
5. **Adaptive embedding integration:** Investigate content-adaptive cost functions that adjust embedding based on image texture and complexity to improve the capacity-security trade-off [2].
6. **Deep learning reversibility:** Address the reversibility limitation of GAN and CNN-based steganography to make these methods practically usable for covert communication [2].
7. **Post-quantum cryptography:** Evaluate quantum-resistant encryption algorithms as alternatives to AES for long-term security in hybrid crypto-steganographic systems [4].
8. **Blockchain integration:** Explore decentralized key management and stego-image authentication using blockchain technology [4]. Apau et al. [3] also recommended blockchain as a future direction.
9. **Unified benchmark creation:** Develop a standardized benchmark dataset and evaluation protocol for fair comparison of crypto-steganographic systems, addressing the inconsistency identified by Apau et al. [3] and Alaklabi et al. [6].
10. **Multi-cover and multi-domain extension:** Extend the framework to distribute payloads across multiple images or combine image, audio, and network steganography for increased security [2], [8].

## 8. CONCLUSION

This paper presented a structured survey of hybrid cryptography-steganography systems for image-based data security, with a focus on IoT-constrained environments. Through a review of eight primary sources spanning 2024–2026, the survey provided a comprehensive taxonomy of steganographic techniques (spatial, transform, adaptive, deep learning), cryptographic methods (AES, SPN, chaotic maps, RSA, ECC), and security evaluation approaches (RS analysis, Chi-Square, ML-based steganalysis, PDH).

Six critical research gaps were identified: the absence of a controlled AES-keyed-LSB protocol, inconsistent evaluation across studies, conflated security claims, insufficient IoT-specific computational validation, inadequate steganalysis resistance testing, and the lack of standardized baselines.

A conceptual reference framework combining AES-256-GCM with keyed LSB substitution was proposed as a design specification for future experimental validation. This framework is positioned not as a superior alternative to existing methods, but as a controlled, reproducible baseline against which more complex techniques can be fairly compared.

The survey identified key challenges including the universal trade-off between capacity, imperceptibility, and security; the steganalysis generalization problem; the deep learning reversibility limitation; and the critical gap in IoT-specific hardware validation. Ten future research directions were proposed to address these challenges.

The proposed method is not claimed to be superior to all existing approaches. Rather, it serves as a controlled, reproducible baseline platform for future comparative studies. The narrow focus ensures clear attribution of results, measurable evaluation, and practical IoT applicability.

## REFERENCES

I. Haverkamp and D. K. Sarmah, “Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis,” *Int. J. Inf. Secur.*, vol. 23, no. 4, pp. 2607–2635, Aug. 2024, doi: 10.1007/s10207-024-00853-9.

M. H. Kombrink, Z. J. M. H. Geradts, and M. Worring, “Image steganography approaches and their detection strategies: A survey,” *ACM Comput. Surv.*, vol. 57, no. 2, Art. 33, Oct. 2024, doi: 10.1145/3694965.

R. Apau, M. Asante, F. Twum, J. B. Hayfron-Acquah, and K. O. Peasah, “Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review,” *PLoS ONE*, vol. 19, no. 9, p. e0308807, Sep. 2024, doi: 10.1371/journal.pone.0308807.

M. Driss, L. Berriche, S. B. Atitallah, and S. Rekik, “Steganography in IoT: A comprehensive survey on approaches, challenges, and future directions,” *IEEE Access*, vol. 13, pp. 74844–74875, 2025, doi: 10.1109/ACCESS.2025.3564120.

S. Z. Banoori et al., "An improved hybrid image steganography method using AES algorithm," *Sci. Rep.*, vol. 15, no. 1, p. 44515, Dec. 2025, doi: 10.1038/s41598-025-28140-0.

A. Alaklabi, M. A. Hafeez, and A. Munir, "Fast and lightweight hybrid image encryption and steganography leveraging an SPN, chaotic maps, and LSB substitution," *J. Cybersecur. Priv.*, vol. 6, no. 1, p. 31, Feb. 2026, doi: 10.3390/jcp6010031.

N. D. Majeed, A. J. Al-Askery, F. S. Hasan, and S. Abood, "A survey on steganography and image encryption techniques," *Electr. Eng. Tech. J.*, vol. 2, no. 1, pp. 11–24, Jan. 2025, doi: 10.51173/eetj.v2i1.13.

H. A. Ahmed, A. Mahfoud, and O. I. Al-Sanjary, "Comprehensive review of cryptography and steganography algorithms," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 29s, pp. 212–228, 2025.

M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, Art. no. n71, Mar. 2021, doi: 10.1136/bmj.n71.

National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication 197, Nov. 2001 (updated May 2023), doi: 10.6028/NIST.FIPS.197-upd1.

M. Dworkin, "Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC," NIST Special Publication 800-38D, Nov. 2007, doi: 10.6028/NIST.SP.800-38D.

A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Information Hiding (IH 1999)*, Lecture Notes in Computer Science, vol. 1768. Berlin, Germany: Springer, 2000, pp. 61–76, doi: 10.1007/10719724_5.

J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and gray-scale images," *IEEE MultiMedia*, vol. 8, no. 4, pp. 22–28, Oct.–Dec. 2001, doi: 10.1109/93.959097.

T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Information Hiding (IH 2010)*, Lecture Notes in Computer Science, vol. 6387. Berlin, Germany: Springer, 2010, pp. 161–177, doi: 10.1007/978-3-642-16435-4_13.

V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP J. Inf. Secur.*, vol. 2014, Art. no. 1, Jan. 2014, doi: 10.1186/1687-417X-2014-1.

J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 868–882, Jun. 2012, doi: 10.1109/TIFS.2012.2190402.

P. Bas, T. Filler, and T. Pevný, "Break our steganographic system: The ins and outs of organizing BOSS," in *Information Hiding (IH 2011)*, Lecture Notes in Computer Science, vol. 6958. Berlin, Germany: Springer, 2011, pp. 59–70, doi: 10.1007/978-3-642-24178-9_5.

A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, Mar. 2010, doi: 10.1016/j.sigpro.2009.08.010.

R. Durstenfeld, "Algorithm 235: Random permutation," *Commun. ACM*, vol. 7, no. 7, p. 420, Jul. 1964, doi: 10.1145/364520.364540.

N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security & Privacy*, vol. 1, no. 3, pp. 32–44, May/Jun. 2003, doi: 10.1109/MSECP.2003.1203220.