Symmetric Encryption Framework for Reversible Data Hiding in the Encrypted Domain

Zechen Zhao *

School of Management Science and Engineering, Beijing Information Science and Technology University, Beijing, 102206, China

* Corresponding Author Email: mm1589653680@outlook.com

Abstract. In the context of the deep integration of digitalization and cloud computing, the demands for privacy protection and value-added services for multimedia data have become increasingly prominent. Reversible Data Hiding in Encrypted Images (RDHEI) technology, which can embed secret data into an encrypted carrier and losslessly recover the original carrier, has emerged as a key research direction in information security. As the core underpinning of RDHEI, the diversity and performance differences of symmetric encryption frameworks directly determine the upper limit of the technology's practical application. However, existing research has largely focused on optimizing single frameworks, lacking a systematic review of their principles, strategies, and complementarity. Conducting such a comprehensive study is of significant value for technology selection and future breakthroughs. This paper focuses on symmetric encryption frameworks in RDHEI, systematically reviewing three typical categories from four perspectives: technical principles, encryption mechanisms, embedding strategies, and performance complementarity. These frameworks include full bit-plane partitioning with pixel prediction, those based on the Binary Symmetric Channel (BSC) and polar codes, and 3D model octree subdivision with multiple Most Significant Bit (MSB) prediction. The research herein not only provides a clear reference for RDHEI technology selection but also points towards the future direction of dynamic framework fusion, offering a new path to overcome bottlenecks in the information security domain by balancing capacity, complexity, and reversibility through modular design.

Keywords: Reversible Data Hiding in Encrypted Images (RDHEI), Symmetric encryption framework, Binary Symmetric Channel (BSC), Octree subdivision.

1. Introduction

With the deep integration of digitalization and cloud computing technologies, the demand for transmitting and storing multimedia data, such as images and 3D models, has surged. The dual requirements of privacy protection and data value-add have become an industry focus. On one hand, to prevent data leakage, multimedia data must be securely transmitted through encryption, which is the foundation of privacy protection. On the other hand, scenarios like copyright authentication and data provenance require embedding additional information into encrypted data without compromising the integrity of the original data. The proliferation of computing and mobile devices has dramatically increased the risk of privacy breaches for multimedia data (images, 3D models, etc.), necessitating a synergistic approach of "encryption + data hiding" to achieve both privacy protection and value-added services (for example, copyright authentication, data provenance). Reversible Data Hiding in Encrypted Images (RDHEI) technology has become a key solution due to its "reversibility" [1], and this tension has driven the development of the technology.

RDHEI refers to the technology that allows for embedding secret data into encrypted carriers like images and 3D models, and subsequently enables the accurate extraction of the secret data and lossless recovery of the original carrier. Its core lies in the reversibility of the entire “encryption-embedding-recovery" process. Symmetric encryption is the primary method supporting this technology. Represented by stream and block ciphers, it constructs an embedding space through bit-level or block-level operations such as bitwise XOR and block scrambling, reserving redundancy for data embedding while ensuring the security of the ciphertext. Early symmetric encryption techniques laid the foundation for RDHEI [2]. Subsequently, they evolved towards more refined and multi-

dimensional optimizations, such as adapting to the characteristics of various carriers like 3D models, introducing channel coding theory to enhance stability, and progressively balancing embedding capacity, security, and computational complexity, leading to a more mature technological framework [3].

Although current research has made progress in optimizing individual symmetric encryption frameworks, it lacks a systematic review of the differences in principles, performance boundaries, and complementarity among different frameworks. This paper focuses on symmetric encryption frameworks within RDHEI, reviewing three typical categories: full bit-plane partitioning with pixel prediction, those based on the Binary Symmetric Channel (BSC) and polar codes, and 3D model octree subdivision with multiple Most Significant Bit (MSB) prediction. The study is conducted from the perspectives of technical principles, encryption mechanisms, embedding strategies, and performance complementarity. It aims not only to provide a clear reference for technology selection but also to support the promotion of dynamic framework fusion and to help overcome bottlenecks in the field of information security.

2. Overview of Symmetric Encryption Frameworks

2.1. Symmetric Encryption Framework Based on Full Bit-Plane Partitioning and Pixel Prediction

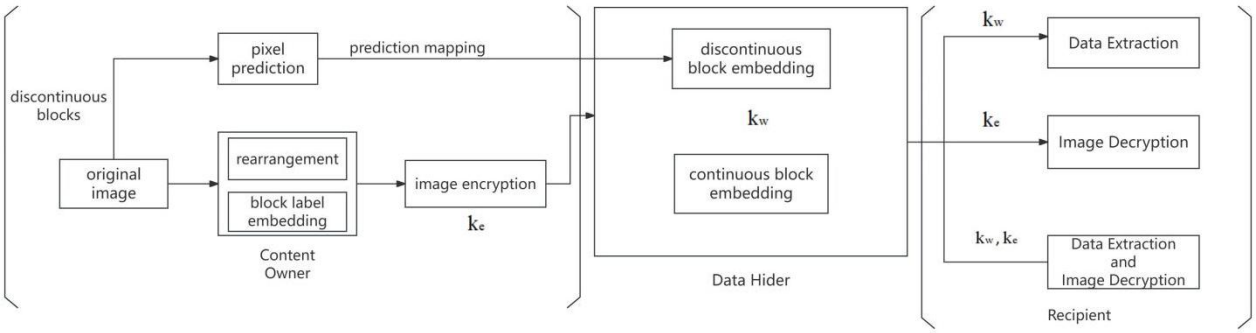

Figure 1. Symmetric Encryption Framework Based on Full Bit-Plane Partitioning and Pixel Prediction [4]

The symmetric encryption framework (Figure1) based on full bit-plane partitioning and pixel prediction operates on the eight bit-planes of a grayscale image. Its core principle is to achieve reversible embedding through fine-grained partitioning and the exploitation of pixel correlations. The process begins with preprocessing by the content owner: each bit-plane is partitioned into continuous and non-continuous blocks of a fixed size (for example, 4×4). Continuous blocks consist of pixels that are all 0s or all 1s, while non-continuous blocks contain both 0 and 1 pixels. Block labels are generated to record the partitioning result. Subsequently, the image is rearranged in the order of "non-continuous blocks first, followed by continuous blocks" to ensure an orderly subsequent embedding operation.

The encryption phase employs a stream cipher mechanism ($e_{i,j,k} = r_{i,j,k} \oplus b_{i,j,k}$ a pseudo-random sequence r generated by the stream cipher is XORed with the carrier image bit-plane b to encrypt the image and ensure ciphertext security). A pseudo-random sequence is XORed bit-by-bit with the bit-plane pixels. While this disrupts global redundancy, it intentionally preserves local correlation within the blocks. This design is analogous to the idea behind the classic Prediction Error Expansion algorithm, where maintaining inter-pixel correlation lays the foundation for reversibility. For non-continuous blocks, the content owner generates a prediction map using a 3-neighbor pixel prediction model (the central pixel P is predicted based on the sum of surrounding pixels Q, V, and R; P is predicted as 0 if the sum is 0 or 1, and as 1 if the sum is 2 or 3), marking the positions of correctly predicted pixels.

The data hider's embedding operation is targeted. In continuous blocks, the bottom-right pixel is reserved as a recovery reference, and data is directly embedded in the remaining positions. In non-continuous blocks, data is embedded only at pixel locations where the prediction map value is 1; incorrectly predicted pixels are left unchanged. At the receiving end, to extract the data, the image is rearranged according to the block labels, the original pixel values are inferred using the prediction map, and lossless recovery is completed through decryption with the stream cipher. Throughout this process, a dual-key mechanism (an encryption key for decryption and a hiding key to locate embedded positions) ensures the separation of operations, while the exploitation of correlation through pixel prediction effectively reduces the distortion introduced to the carrier by embedding [4].

In recent advancements, related research has enhanced security through full bit-plane scrambling and double encryption (block-wise classified scrambling + traversal matrix encryption). Combined with pixel prediction techniques to differentiate between continuous and non-continuous blocks, this achieves separable reversible data hiding. The scheme features a large key space and high sensitivity, with the average PSNR of marked encrypted images reaching 64.64dB and an actual average embedding capacity of 2.5 bpp. It allows for lossless image recovery and data extraction and can also resist attacks such as salt-and-pepper noise and cropping. This further unleashes the potential for the synergistic utilization of bit-plane redundancy [5].

2.2. Symmetric Encryption Framework Based on the Binary Symmetric Channel (BSC) and Polar Codes

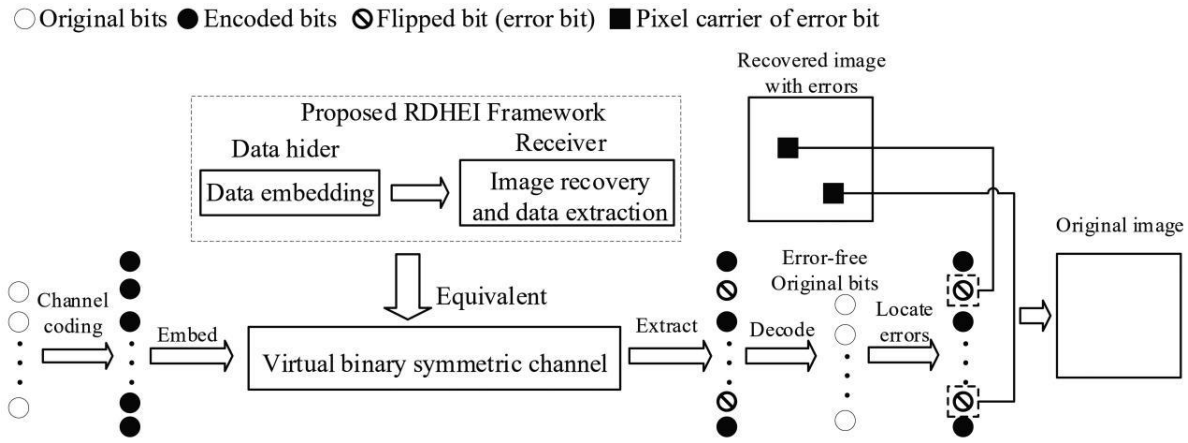

Figure 2. Symmetric Encryption Framework Based on the Binary Symmetric Channel (BSC) and Polar Codes [6]

The symmetric encryption framework (Figure 2) based on the Binary Symmetric Channel and polar codes innovatively models the data embedding and extraction process as a transmission over a virtual Binary Symmetric Channel. Its core is to ensure reversibility through the error-correction mechanism of polar codes. The content owner's encryption operation uses a stream cipher, generating a pseudo-random sequence to be XORed with the image pixel bits. This completely destroys the original redundancy, making the ciphertext exhibit noise-like characteristics. This processing simulates the noise interference in a channel, providing a basis for subsequent modeling.

During the embedding process, the data hider must first encode the secret data with polar codes. Specifically, the secret data is divided into several groups, and each group is processed by polar codes to generate code blocks containing redundant information. The redundancy introduced in this process makes subsequent error correction possible. Subsequently, the data hider selects carrier pixels using a data hiding key and embeds the encoded secret data into specified LSB planes (for example, from the 3rd to the 6th bit). The embedding rule is: if the secret data bit is 1, the target bit of the corresponding pixel is flipped; if it is 0, it remains unchanged.

The processing flow at the receiving end reflects the core logic of the framework. First, the encryption key is used to decrypt the image, obtaining a plaintext image containing the embedded information. For each pixel that could potentially contain data, the receiver generates two candidate

values: the original decrypted value and the value after bit-flipping. By using a predicted value from reference pixels (obtained by interpolating adjacent unmodified pixels), the receiver determines which candidate value is closer to the original state, thereby preliminarily extracting the secret data and recovering the pixels. Since predictions may contain errors, the extracted secret data will have errors. At this point, the polar code decoder comes into play, correcting the errors using a successive cancellation decoding algorithm to obtain the correct secret data. Simultaneously, based on the corrected code stream, the receiver can reverse-engineer the original embedding operation and precisely recover all pixel values, achieving full reversibility.

This framework breaks through the traditional design philosophy that relies on carrier redundancy. By modeling embedding errors as channel noise, it uses the channel polarization properties of polar codes to achieve efficient error correction. Its essence lies in transforming the information hiding problem into a channel coding problem, which represents a distinct difference and innovation compared to the classic histogram shifting algorithm that achieves reversibility through statistical properties [6].

Current research based on virtual BSC channel modeling and polar code encoding has effectively improved performance in complex interference scenarios. By using a flag bit transmission channel and systematic polar codes, data can be extracted independently in the encrypted domain, enhancing the capacity and fidelity of Vacating Room After Encryption (VRAE) RDHEI, with the MSB plane embedding rate reaching 0.6866 bpp [7]. Furthermore, by constructing a flag bit transmission channel combined with systematic polar codes, secret data can be extracted independently in the encrypted domain. While ensuring the reversibility of the carrier image and error-free extraction of secret information, this significantly improves the capacity of the secret information and the fidelity of the marked image, providing technical support for ciphertext hiding in complex environments like 5G communications and the IoT. This continues the BSC framework's approach of balancing anti-interference with security while adapting to the characteristics of high-resolution professional images [8].

2.3. Symmetric Encryption Framework for 3D Models Based on Octree Subdivision and Multiple Most Significant Bit (MSB) Prediction

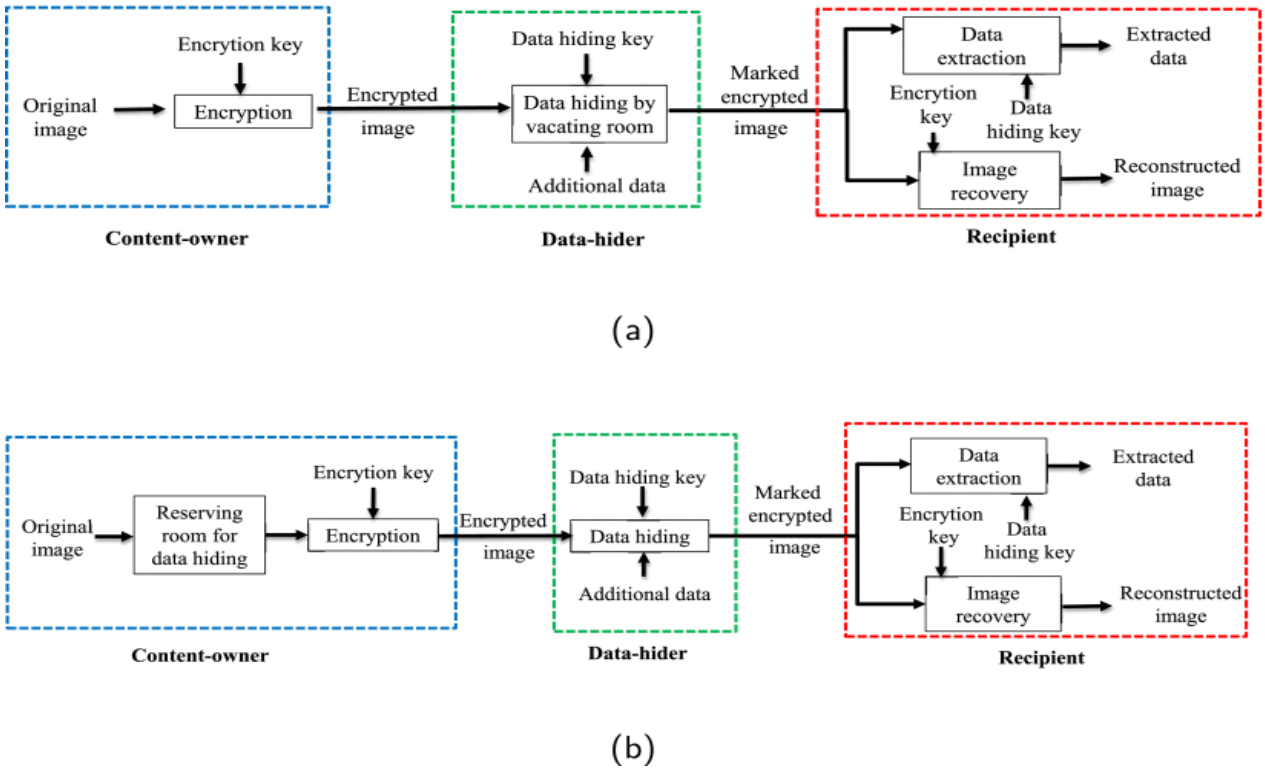

Figure 3. Two frameworks of RDH-ED methods. (a) VRAE. (b) RRBE.[9]

The symmetric encryption framework (Figure 3) for 3D models, based on octree subdivision and multiple Most Significant Bit (MSB) prediction, is specifically designed for the spatial characteristics of 3D mesh models. Its core strategy is to achieve reversible embedding by exploiting spatial redundancy through adaptive partitioning and high-order bit prediction. The process begins with the content owner normalizing the 3D model's vertex coordinates, converting floating-point values into integers within a fixed range to eliminate scale discrepancies. An octree is then used to recursively partition the model into non-overlapping sub-blocks based on a maximum depth and a vertex count threshold, which enhances the spatial correlation among vertices within each sub-block. This concept is similar to the use of local redundancy in image partitioning.

Within each sub-block, vertices are divided into a reference set (containing one randomly selected vertex) and an embedding set (the remaining vertices). The multiple MSB prediction process compares the binary representations of these two sets bit-by-bit, starting from the most significant bit. The high-order bits preceding the first point of mismatch constitute the embedding space, and the length of this predictable sequence is determined by the degree of spatial correlation. During encryption, a stream cipher is applied via XOR operation only to the non-embeddable bits, preserving the redundancy in the embeddable bits. The data hider then embeds Huffman-coded auxiliary information into the base bits and inserts the secret data into the reserved space using bit replacement.

At the receiver's end, the encryption key is used to decrypt the non-embeddable bits. With the data hiding key, the auxiliary information is extracted to reconstruct the sub-blocks and the prediction map. The receiver then re-executes the multiple MSB prediction using the reference set to reverse-engineer the original high-order bits of the embedding set, achieving lossless model recovery. This approach of enhancing local correlation is analogous to the Prediction Error Expansion (PEE) algorithms used in 2D images, as both depend on carrier redundancy, but this framework is specifically adapted to the spatial properties of 3D models.

This framework follows the Reserving Room Before Encryption (RRBE) paradigm (corresponding to Figure 3b), which differs from the Vacating Room After Encryption (VRAE) paradigm (Figure 3a). VRAE first encrypts the data and then modifies the ciphertext to create space, a process that can lead to recovery errors because encryption destroys redundancy. In contrast, RRBE first reserves room by exploiting redundancy—using methods like octree subdivision and MSB prediction—and then encrypts the remaining data. This ensures the embedding space is accessible, enabling high capacity and lossless recovery, making it better suited for the high capacity and fidelity demands of 3D models [9].

Recent studies have optimized the octree subdivision and multiple MSB prediction strategies, reducing the proportion of reference vertices to free up more redundant space, achieving an average 40% increase in embedding capacity compared to similar algorithms. Furthermore, a lightweight, multi-user scheme based on threshold secret sharing has been proposed, which is resistant to single-point failures and requires encrypting only 6.12% of the data compared to related methods, making it suitable for distributed storage scenarios for 3D models. These advancements complement the core design logic of "enhancing correlation through subdivision" within the 3D model framework, driving the technology towards higher-dimensional mapping and cross-carrier fusion [10].

3. Comparative Analysis and Discussion of Typical Symmetric Encryption Frameworks

3.1. Core Differences from Encryption Mechanisms to Embedding Strategies

From the perspective of encryption mechanisms, all three frameworks utilize stream ciphers to ensure ciphertext security, but they differ in their handling of carrier redundancy and key coordination. The full bit-plane partitioning and pixel prediction framework [4] intentionally preserves local, intra-block correlation within bit-planes to reserve embedding redundancy, requiring only the coordination of a dual-key (encryption and hiding) system; the BSC and polar code framework [6] completely destroys original redundancy, modeling the encryption noise as a virtual Binary Symmetric Channel,

and in addition to the dual keys, it requires synchronized polar code parameters to support error correction; the octree subdivision and multiple MSB prediction framework [9], designed for 3D models, preserves spatial correlation of vertices within sub-blocks through octree partitioning, and its keys must be adapted to the sub-block division information to correctly match the reference and embedding sets.

Regarding embedding strategies, all methods must select positions and ensure reversibility, but they follow different paths. The full bit-plane framework [4] relies on intra-block pixel correlation, embedding data in pixel bits with zero prediction error and using a "prediction map" to reverse the process and restore the original values; the BSC and polar code framework [6] does not depend on carrier correlation, instead selecting LSB planes for embedding, treating errors as "channel noise," and using polar code decoding for error correction; and the 3D model framework [9] leverages the spatial association of vertices within sub-blocks, embedding data in the consistent MSB planes identified through prediction and recovering the original coordinates by re-predicting from the reference set.

These differences, as summarized in Table 1, reflect adaptations to different carriers and scenarios: the full bit-plane framework focuses on local image redundancy to increase capacity, the BSC framework enhances robustness against interference, and the 3D framework is tailored for non-image carriers, providing a logical basis for technological complementarity.

Table 1. Feature Comparison of Different Symmetric Encryption Frameworks

Framework Type	Core Features of Encryption Mechanism	Core Features of Embedding Strategy
Full Bit-plane Partitioning and Pixel Prediction	Stream cipher (bitwise XOR on bit-planes). Disrupts global redundancy but preserves intra-block local correlation. Dual-key: encryption + hiding	Embedding location: Specific bit-planes of continuous and non-continuous blocks. Reversibility mechanism: It leverages intra-block pixel correlation to identify pixels with zero prediction error for embedding. Reversibility is achieved by restoring the original values using the prediction map.
BSC and Polar Codes	Stream cipher (pixel bit XOR). Destroys redundancy, modeled as a virtual BSC; requires synchronization of polar code parameters.	Embedding location: Specific LSB planes. Reversibility mechanism: It leverages channel coding; polar code error correction is used to counteract noise, and the original pixels are recovered by correcting errors during the decoding process.
Octree Subdivision and Multiple MSB Prediction	Stream cipher (bitwise processing of 3D vertex coordinates). Disrupts topological redundancy but preserves sub-block spatial correlation. Key synchronization is adapted to the 3D structure.	Embedding location: Multiple MSB planes of vertex coordinates. Reversibility mechanism: It uses multiple MSB prediction, leveraging the spatial correlation of vertices within sub-blocks. The original coordinates are recovered by re-predicting from the reference set.

3.2. Complementary Performance Characteristics

The performance differences among symmetric encryption frameworks in RDHEI are essentially a result of differentiated trade-offs between capacity, robustness, carrier compatibility, and security. This trade-off creates technological complementarity, allowing various frameworks to excel in different scenarios and collectively build a technical system that covers multiple requirements [2].

3.2.1. The Complementary Balance of Embedding Capacity and Robustness

The conflict between embedding capacity and robustness is a core trade-off. The full bit-plane partitioning and pixel prediction framework achieves a high embedding rate of 3.0875 bits per pixel (bpp) on the BOSSbase dataset by dividing eight bit-planes into continuous and non-continuous blocks and leveraging local pixel correlation to select embedding locations. It excels at exploiting

carrier redundancy and performs exceptionally well on low-texture images [4]. However, its reliance on prediction accuracy means that in complex-texture images (like Baboon), an increase in prediction errors reduces the available embedding space, limiting its robustness.

Complementing this is the BSC and polar code framework, which models the embedding process as a virtual noisy channel and uses polar code error correction to counteract interference, ensuring reversibility even in complex images. Although the redundancy introduced by channel coding results in a lower embedding rate, its advantage in robustness within noisy environments is significant [6]. Together, these two frameworks cover a spectrum of needs, from high-capacity, low-interference scenarios to low-capacity, high-robustness applications.

3.2.2. The Gradient Complementarity of Computational Complexity and Security

Balancing computational complexity and security is key to practical application. The full bit-plane partitioning framework uses a stream cipher and simple block partitioning, resulting in low complexity (concentrated in pixel prediction and block label management), making it suitable for resource-constrained terminals. Its security relies on the separation of the dual keys [4]. The BSC and polar code framework has higher complexity due to polar code encoding and decoding (especially for long codes), but since the encryption phase completely destroys carrier redundancy, its ciphertext entropy approaches 8, providing superior security [6]. The 3D model framework has the highest complexity due to octree subdivision and multiple MSB prediction, yet it maintains acceptable security when processing large-scale point clouds through sub-block isolation and key synchronization. This gradient of trade-offs is suitable for a range of scenarios, from lightweight terminals to high-performance servers.

The balance of capacity and robustness, full carrier coverage, and the gradient adaptation of complexity and security together constitute the complementarity of these frameworks. This provides flexibility for technology selection and also points the way for future integrated frameworks: to synergistically optimize capacity, robustness, and compatibility by integrating their respective advantages [3].

4. Conclusion

The core value of RDHEI technology lies in achieving reversible information extraction while ensuring the privacy and security of the carrier through the synergistic adaptation of diverse symmetric encryption strategies. The development of this technology has consistently revolved around balancing capacity, complexity, and reversibility. Existing research, following different technical paths, has formed a complementary system of performance that covers multiple carriers and scenarios, providing support for information security needs in complex environments and demonstrating the vitality and diversity of the research field. Future work needs to promote the dynamic fusion of these technical frameworks. Through modular design and intelligent adaptation, performance in specific scenarios can be optimized, practical applications can be expanded, and cross-disciplinary technologies can be integrated. How to balance capacity, complexity, and reversibility in complex scenarios, as well as integrate with emerging technologies to expand application boundaries, is not only a challenge but also provides broad opportunities for innovation and development in this field.

References

[1] Puteaux P, Ong SY, Wong KS, Puech W. A survey of reversible data hiding in encrypted images – The first 12 years. Journal of Visual Communication and Image Representation, 2021, 77: 103085.

[2] Ou B, Li Xiaolong, Ni Rongrong, et al. Research development of reversible data hiding in images. Journal of Beijing Jiaotong University, 2022, 46 (01): 1 - 10.

[3] Ge Y, Sun J, Zhang M. Research progress of reversible data hiding in encrypted domain. 7th International Conference on Information Science, Computer Technology and Transportation (ISCTT), Xishuangbanna, China, 2022: 1 - 10.

[4] Zhou X, Wu F, Chen Z, Ren S. High embedding rate full-plane reversible data hiding in encrypted images. Journal of Image and Graphics, 2021, 26 (5): 1147 - 1156.

[5] Weng CY, Yang CH. Reversible data hiding in encrypted image using multiple data-hiders sharing algorithm. Entropy, 2023, 25 (2): 209.

[6] Chen K, Guan Q, Zhang W, Yu N. Reversible data hiding in encrypted images based on binary symmetric channel model and polar code. IEEE Transactions on Dependable and Secure Computing, 2023, 20 (6): 4519 - 4535.

[7] Chen K, Guan Q, Zhang W, Yu N, Lu W. Separable reversible data hiding in encrypted images based on systematic polar code and flag bit transmission channel model. IEEE Transactions on Dependable and Secure Computing, 2025. doi: 10.1109/TDSC.2025.3591657.

[8] Liu R, Zhou Q, Liu J, Zhang Y, Hui Z, Zhang X. Separable reversible data hiding in encrypted images for remote sensing images. Entropy, 2023, 25 (12): 1632.

[9] Hou G, Ou B, Long M, Peng F. Separable reversible data hiding for encrypted 3D mesh models based on octree subdivision and multi-MSB prediction. IEEE Transactions on Multimedia, 2024, 26: 2395 - 2407.

[10] Zhang C, Ou B, Peng F, Zhao Y, Li K. A survey on reversible data hiding for uncompressed images. ACM Computing Surveys, 2024, 56 (7): 180.