AI & CYBER FORUM
AN INTERNATIONAL JOURNAL
OPEN ACCESS
ISSN 3117-6399
Review Article
Check for updates

Robust Hybrid Image Steganography Using Combined LSB and Discrete Wavelet Transform with Cryptographic Data Protection

Pankaj Nandan

Department of Computer Applications, Government Degree College, Ramkote, Jammu and Kashmir, 184205, India

Corresponding author: **Pankaj Nandan** | E-mail: **prof.pankajnandan@gmail.com**

Citation: Pankaj Nandan (2025). Robust Hybrid Image Steganography Using Combined LSB and Discrete Wavelet Transform with Cryptographic Data Protection. *AI & Cyber Forum: An International Journal.* **DOI: https://doi.org/10.51470/AI.2025.4.2.21**

Received 18 June 2025 | Revised 16 July 2025 | Accepted 28 July 2025 | Available Online August 12, 2025

Abstract

The increasing demand for secure digital communication has intensified research into image steganography, particularly techniques capable of concealing confidential information within digital images while maintaining visual quality and resistance to unauthorized detection. Conventional Least Significant Bit (LSB) substitution offers simplicity, high embedding capacity and low computational complexity; however, its susceptibility to image processing operations, statistical analysis and deliberate steganalysis limits its application in security-sensitive environments. In contrast, Discrete Wavelet Transform (DWT)-based steganography provides frequency-domain embedding capabilities that can improve imperceptibility and robustness but may involve greater computational complexity and trade-offs in payload capacity. Hybrid approaches combining LSB substitution and DWT have therefore attracted attention as a means of exploiting the complementary advantages of spatial- and frequency-domain techniques. The review also discusses the influence of image characteristics, embedding capacity, peak signal-to-noise ratio, structural similarity, robustness and steganalysis resistance on overall system performance. Furthermore, emerging developments involving artificial intelligence, optimization algorithms, deep learning-based detection and advanced cryptographic frameworks are considered. The integration of transform-domain embedding with cryptographic protection represents a promising direction for developing secure and robust image steganography systems, although performance depends strongly on embedding strategy, image content, attack models and cryptographic implementation.

Keywords: *Image steganography; Least Significant Bit; Discrete Wavelet Transform; hybrid steganography; cryptography; information security.*

1. Introduction

The rapid expansion of digital communication, cloud computing, online transactions and distributed information systems has substantially increased the volume of sensitive information transmitted through public networks. Confidential documents, personal records, financial information, research data and institutional communications require protection against unauthorized access, interception and manipulation. Traditional cryptographic techniques provide confidentiality by transforming readable information into an unintelligible representation through encryption algorithms. Although encryption protects the contents of transmitted information, it does not necessarily conceal the existence of communication. An encrypted message may attract attention because its presence and structure can be readily identified. This limitation has encouraged the development of information-hiding techniques that conceal the existence of secret communication within apparently ordinary digital media [1].

Steganography is a branch of information security concerned with concealing secret information within a carrier medium, such as an image, audio signal, video sequence or text document. Unlike conventional cryptography, which primarily transforms the representation of information, steganography attempts to make the presence of the information difficult to detect. Digital images are particularly suitable carriers because of their widespread availability, high data redundancy and complex spatial and frequency characteristics. Minor modifications to selected image components can often accommodate secret information without producing perceptually significant changes. Consequently, image steganography has become an important research area in secure communication, digital media protection, information authentication and covert data transmission. Among the available image-steganography methods, Least Significant Bit substitution is one of the most widely studied spatial-domain approaches.

© ***Authors:*** *Published in AI & Cyber Forum: An International Journal under the CC BY-NC-ND 4.0 license (http://creativecommons.org/licenses/by-nc-nd/4.0/). No commercial use or modifications permitted.*

The technique embeds secret information by modifying the least significant bits of selected pixel values. Since these modifications generally produce small numerical differences, the resulting stego-image can retain visual characteristics similar to those of the original cover image. LSB techniques are relatively easy to implement and can support comparatively high embedding capacity. However, direct LSB substitution is vulnerable to image compression, filtering, resizing, cropping, noise addition and statistical steganalysis [2].

Transform-domain techniques provide an alternative strategy by embedding information within selected frequency coefficients rather than directly modifying pixel values. The Discrete Wavelet Transform is particularly useful because it decomposes an image into multiple frequency sub-bands at different spatial resolutions. A two-dimensional DWT generally produces four sub-bands: approximation coefficients (LL), horizontal detail coefficients (LH), vertical detail coefficients (HL) and diagonal detail coefficients (HH). These sub-bands provide different characteristics for information embedding. The approximation sub-band contains much of the image's low-frequency information, whereas the detail sub-bands represent variations and high-frequency structures. Appropriate coefficient selection can help balance visual imperceptibility, embedding capacity and resistance to selected image-processing operations. The combination of LSB and DWT offers an opportunity to integrate spatial-domain simplicity with frequency-domain adaptability. In a hybrid architecture, DWT may be used to identify suitable frequency components, while LSB substitution can be applied to selected transform coefficients or coefficient representations [3]. Alternatively, the two methods may be used in separate embedding stages, depending on the architecture. Such combinations can provide greater flexibility in selecting embedding locations, controlling distortion and distributing secret information. Nevertheless, hybridization alone does not guarantee improved security or robustness.

2. Fundamentals of Digital Image Steganography

Digital image steganography is an information-hiding technique in which confidential data are concealed within an ordinary digital image, commonly referred to as the cover image, to minimize the possibility of unauthorized detection. The fundamental objective is to embed secret information without introducing perceptually significant modifications to the original image. A typical image-steganography system involves three principal components: the cover image, the secret message and the resulting stego-image. During the embedding process, the secret information is converted into a binary sequence and incorporated into selected image components according to a predefined algorithm. The resulting stego-image is subsequently transmitted to the intended receiver, who applies the corresponding extraction procedure to recover the hidden information. Depending on the embedding technique, modifications may be introduced directly into pixel values or into frequency-domain coefficients obtained through mathematical transformations.

The overall effectiveness of a steganographic system is determined by several interrelated characteristics, including imperceptibility, embedding capacity, robustness and security. Imperceptibility refers to the extent to which embedding modifications remain visually undetectable, whereas embedding capacity represents the quantity of information that can be concealed within the carrier image [4]. Robustness describes the ability to preserve and recover embedded information following image-processing operations, including compression, filtering, resizing and noise addition. Security, meanwhile, concerns the resistance of the embedding mechanism to unauthorized detection, extraction and manipulation. These characteristics frequently involve competing requirements, as increasing the amount of embedded information may introduce greater image distortion or statistical detectability. Consequently, the development of effective image-steganography systems requires an appropriate balance between payload capacity, perceptual quality and resistance to potential attacks.

Image-steganography techniques are broadly classified into spatial-domain and transform-domain approaches according to the representation in which information is embedded. Spatial-domain methods directly modify pixel intensities or their binary representations, with Least Significant Bit substitution being one of the most commonly investigated techniques. In this approach, secret information is embedded by replacing selected least significant bits of image pixels with corresponding message bits. Since the modification generally produces only a small numerical change in pixel intensity, the visual appearance of the resulting image can remain largely unchanged. Spatial-domain techniques are computationally efficient and relatively straightforward to implement, making them suitable for applications requiring simple embedding and extraction procedures. However, their dependence on individual pixel values makes them vulnerable to image compression, filtering, geometric transformations and statistical steganalysis. Transform-domain techniques address some of these limitations by embedding information within mathematical representations of the image rather than modifying pixel values directly. Common transformations include the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT), each of which provides different characteristics for frequency-based information embedding. Among these approaches, DWT is particularly relevant because it decomposes an image into multiple frequency sub-bands at different spatial resolutions, allowing the embedding algorithm to select coefficients according to their frequency characteristics and perceptual sensitivity [4]. The Discrete Wavelet Transform and LSB substitution offer complementary capabilities that can be integrated within hybrid image-steganography architectures. While DWT provides a multiresolution representation for identifying suitable frequency components, LSB substitution offers a relatively simple mechanism for incorporating binary information into selected pixel or coefficient representations.

3. Least Significant Bit Substitution in Digital Image Steganography

Least Significant Bit (LSB) substitution is one of the most widely used spatial-domain techniques for digital image steganography because of its simplicity, low computational complexity, and relatively high data-hiding capacity. The technique is based on modifying the least significant bits of selected pixel values to represent the binary sequence of a secret message. In an 8-bit grayscale image, each pixel is represented by an intensity value ranging from 0 to 255, and changing its least significant bit generally produces a maximum intensity variation of one level. Such a small modification is often imperceptible to human vision, particularly when embedding is distributed across a sufficiently large number of pixels. In RGB images, the same principle can be applied independently to the red, green, and blue colour channels, thereby increasing the potential embedding capacity. However, the selection of colour channels and the number of bits modified per pixel must be carefully controlled because excessive modification can introduce visible distortion and increase the statistical detectability of the stego-image [5]. The conventional LSB embedding process involves converting the secret message into a binary sequence and replacing selected least significant bits of the cover image pixels with the corresponding message bits. The simplest implementation uses sequential pixel positions, although this approach may create identifiable patterns when a large amount of information is embedded. To overcome this limitation, pseudo-random pixel selection can be employed, with the selection sequence generated from a secret key. Key-based pixel selection distributes the embedded information across the image and makes extraction more difficult for an unauthorized recipient. Other improvements include adaptive LSB substitution, in which the number of embedded bits is adjusted according to local image characteristics. Textured and edge-rich regions can generally tolerate small pixel modifications more effectively than smooth regions, where even minor changes may be statistically detectable. Consequently, adaptive embedding strategies attempt to improve the balance between payload capacity and visual quality by allocating more data to suitable image regions while restricting modifications in relatively uniform areas. Despite its advantages, conventional LSB substitution has important limitations, particularly regarding robustness and resistance to steganalysis. Since the hidden information is stored directly in pixel values, operations such as JPEG compression, filtering, resizing, cropping, and format conversion may modify or remove embedded bits. Furthermore, statistical analysis of pixel-value distributions can reveal unusual patterns associated with LSB replacement, especially when the embedding rate is high. The method is also vulnerable to deliberate manipulation if the embedding positions and message structure are not adequately protected. Several enhanced LSB approaches have therefore been investigated, including randomized embedding, edge-based pixel selection, multi-bit substitution, adaptive embedding, and combinations with transform-domain techniques [6].

4. Discrete Wavelet Transform for Image Steganography

The Discrete Wavelet Transform (DWT) is an important frequency-domain technique used in digital image processing, compression, denoising, and information hiding. Unlike spatial-domain methods that directly modify pixel values, DWT represents an image through frequency-related sub-bands at different spatial resolutions. A two-dimensional DWT decomposes an image into four principal sub-bands, namely LL, LH, HL, and HH. The LL sub-band represents the low-frequency approximation of the original image, while the LH, HL, and HH sub-bands contain directional high-frequency information associated with horizontal, vertical, and diagonal image details, respectively. This decomposition enables the identification of different image components according to their frequency characteristics and provides flexibility in selecting suitable regions for data embedding. The transform can also be applied repeatedly to the LL sub-band to produce multilevel decomposition, allowing the image to be analysed at progressively different resolutions [7]. In image steganography, the selection of an appropriate wavelet sub-band is a major factor influencing the performance of the embedding process. The LL sub-band contains the principal structural information of the image and is generally more sensitive to modifications because changes in this region can affect the overall visual appearance. In contrast, the high-frequency sub-bands contain edge and texture information, where appropriately controlled modifications may be less perceptible. Embedding secret information in LH, HL, or HH coefficients can therefore provide opportunities to improve visual imperceptibility, although these regions may be more vulnerable to certain image-processing operations. For example, compression and filtering can suppress high-frequency components, potentially damaging the embedded information. The choice of sub-band must consequently consider the intended balance between imperceptibility, embedding capacity, and resistance to image manipulation. Wavelet families such as Haar, Daubechies, Symlets, and biorthogonal wavelets may produce different coefficient distributions and reconstruction characteristics, making wavelet selection another important design consideration. The general DWT-based embedding procedure begins with the transformation of the cover image into its wavelet coefficients. The secret payload is then mapped to selected coefficients using an embedding rule, which may involve coefficient modification, quantization, threshold-based adjustment, or bit-level substitution. After embedding, the inverse discrete wavelet transform (IDWT) is applied to reconstruct the stego-image in the spatial domain. At the receiver's end, the stego-image is transformed again using the corresponding DWT configuration, and the embedded information is extracted from the designated coefficients.

Successful recovery generally depends on consistent wavelet selection, decomposition level, coefficient locations, embedding strength, and synchronization between the sender and receiver. A secret key may additionally be used to determine the coefficient selection pattern, improving access control and reducing the likelihood of unauthorized extraction [8].

5. Hybrid LSB–DWT Image Steganography

Hybrid LSB–DWT image steganography combines the spatial-domain simplicity of Least Significant Bit substitution with the frequency-domain representation provided by the Discrete Wavelet Transform. The central objective of this combination is to exploit the advantages of both techniques while reducing some of their individual limitations. Conventional LSB methods offer straightforward implementation and relatively high embedding capacity but are often vulnerable to image-processing operations and statistical steganalysis. DWT-based approaches provide frequency-selective embedding and multiresolution analysis, although their performance depends strongly on coefficient selection and embedding strength. By integrating these techniques, hybrid frameworks can be designed to select suitable image regions or transform coefficients for embedding and subsequently use LSB substitution to represent the encrypted or encoded payload. However, the actual performance of a hybrid system depends on its specific architecture, embedding rule, and extraction procedure; combining two techniques does not inherently ensure greater security or robustness [9]. Several implementation strategies can be considered for hybrid LSB–DWT steganography. In one approach, the cover image is first decomposed into wavelet sub-bands, after which selected coefficients are converted or represented in a suitable numerical format for LSB-based embedding. The modified coefficients are then used to reconstruct the stego-image through the inverse transform. This design allows the embedding locations to be selected according to frequency characteristics, while LSB substitution provides a relatively simple mechanism for modifying the selected coefficient representations. In another approach, DWT is used primarily as a region-selection or analysis mechanism. The transform identifies suitable frequency components or image regions, but the actual payload is embedded into the corresponding spatial-domain pixels after an inverse transformation or region mapping procedure. These approaches should be distinguished because modifying wavelet coefficients and modifying spatial-domain pixels selected through wavelet analysis are technically different operations. Each requires a clearly defined embedding algorithm and a corresponding extraction procedure to ensure that the hidden information can be recovered accurately. The embedding process in a hybrid framework generally begins with the preparation of the secret message, which may include text, documents, images, or other digital information.

The payload can first be encrypted using a standard cryptographic algorithm, such as the Advanced Encryption Standard in an authenticated encryption mode, before being converted into a binary sequence. The cover image is then subjected to DWT decomposition, and suitable sub-bands or coefficients are selected according to the chosen embedding strategy. LSB substitution is subsequently applied to the selected coefficient representations or mapped pixel locations, depending on the architecture. A secret key may control both the cryptographic operation and the pseudo-random selection of embedding positions.

The effectiveness of hybrid LSB–DWT systems must be examined through a balanced evaluation of imperceptibility, capacity, robustness, computational efficiency, and resistance to steganalysis. A hybrid method may improve visual quality by restricting embedding to selected frequency components or image regions, but this outcome depends on the number of modified coefficients and the embedding strength. Similarly, the use of DWT may improve the organization of embedding locations without necessarily protecting the payload against compression, cropping, or geometric transformations. If LSB substitution is applied directly to transform coefficients, even small changes in coefficient representation may be affected by coefficient scaling, rounding, or inverse transformation. Therefore, the complete embedding and extraction pipeline must be evaluated rather than assuming that the advantages of the individual techniques will automatically be retained in their combination. Comparative studies should include conventional LSB, standalone DWT, and hybrid LSB–DWT methods under identical image datasets, payload sizes, and attack conditions [10]. A further consideration is the relationship between hybrid embedding and cryptographic protection. Steganography conceals the presence of a message, whereas cryptography protects the information contained within that message. Integrating encryption with hybrid LSB–DWT embedding can therefore provide complementary layers of protection.

6. Cryptographic Data Protection in Image Steganography

Cryptography provides an additional layer of security in image steganography by protecting the actual content of the hidden message. While steganography conceals the existence of communication, cryptography transforms the message into an unreadable format that can only be accessed using the appropriate decryption key. Integrating encryption with hybrid LSB–DWT techniques can therefore improve the confidentiality of transmitted information. Before embedding, the secret message is converted into ciphertext using a standard encryption algorithm such as the Advanced Encryption Standard (AES). Authenticated encryption modes, particularly AES-GCM, are useful because they provide both confidentiality and integrity verification.

The encrypted binary sequence is then embedded into the selected image coefficients or pixel locations using the chosen hybrid approach. Effective cryptographic protection also depends on secure key management. Encryption keys and embedding-position keys should be generated and stored securely, and their distribution must be restricted to authorized users. A pseudo-random number generator can be used to determine embedding locations, reducing the predictability of the hidden-data distribution. However, cryptographic protection does not prevent steganalysis or guarantee successful message extraction after image manipulation [11]. Therefore, encryption, embedding-position randomization, and reliable extraction should be treated as complementary security components rather than interchangeable mechanisms.

7. Extraction and Recovery of Hidden Information

The extraction process is essential for recovering the original secret message from the stego-image. In a hybrid LSB–DWT framework, the authorized receiver first obtains the stego-image and applies the same wavelet decomposition and parameter configuration used during embedding. The selected sub-bands, coefficients, or mapped pixel locations are then examined to recover the embedded binary sequence. Where pseudo-random embedding positions have been used, the corresponding secret key is required to reproduce the selection pattern. The extracted bitstream is subsequently reconstructed into ciphertext or the original encoded payload, depending on the embedding design. If encryption has been applied, the recovered ciphertext is decrypted using the appropriate cryptographic key. For authenticated encryption, the authentication tag must also be verified to determine whether the encrypted payload has been modified. Successful recovery depends on accurate synchronization between the embedding and extraction procedures, including the wavelet family, decomposition level, coefficient selection, embedding strength, and payload length. Image compression, cropping, filtering, and resizing may introduce extraction errors, particularly when the embedded information is not designed to withstand such operations [12]. Consequently, reliable recovery mechanisms and error-control techniques may be incorporated to improve the accuracy of information retrieval.

8. Performance Evaluation and Quality Assessment

The performance of hybrid LSB–DWT image steganography should be evaluated using multiple quantitative and qualitative parameters. Imperceptibility is commonly measured through Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index Measure (SSIM). PSNR estimates the difference between the original cover image and the resulting stego-image, while SSIM evaluates structural similarity. Higher PSNR and SSIM values generally indicate better visual preservation, although they do not independently establish resistance to steganalysis.

Embedding capacity is another important parameter, commonly expressed in bits per pixel (BPP) or as the total number of hidden bits. Recovery performance can be evaluated using the Bit Error Rate (BER), which measures the proportion of incorrectly extracted bits. Robustness should be examined by applying common image-processing operations, including JPEG compression, filtering, noise addition, cropping, resizing, and brightness adjustment. Computational time and memory requirements are also relevant, particularly for applications involving large images or resource-constrained devices. A meaningful evaluation should compare conventional LSB, standalone DWT, and hybrid LSB–DWT methods using the same cover images, payload sizes, and experimental conditions. In addition, steganalysis-based testing is necessary to investigate whether the embedded information can be detected statistically or through machine-learning techniques. No single metric can establish the overall security of a steganographic system; therefore, visual quality, capacity, robustness, extraction accuracy, and detectability should be considered together.

9. Security Threats and Steganalysis

Despite improvements in hybrid image steganography, several security threats can affect the confidentiality and successful recovery of hidden information. Statistical steganalysis attempts to identify modifications in pixel values or transform coefficients that may indicate the presence of embedded data. Traditional LSB substitution can produce detectable statistical patterns, particularly when embedding capacity is high or pixel selection is predictable. More advanced steganalysis approaches use machine-learning and deep-learning models to identify subtle image features associated with steganographic modifications. Such methods present challenges for hybrid systems because frequency-domain transformations do not automatically eliminate statistical traces. Image-processing attacks also represent a significant threat. Lossy compression, filtering, noise addition, cropping, resizing, and geometric transformations may alter the embedded information and reduce extraction accuracy [13]. Unauthorized access to cryptographic or embedding-position keys can further compromise system security. To address these risks, hybrid frameworks should incorporate randomized embedding locations, controlled embedding strength, authenticated encryption, secure key management, and suitable error-correction mechanisms. Their effectiveness must be verified through systematic testing against both conventional image-processing attacks and modern steganalysis techniques.

10. Applications of Hybrid LSB–DWT Image Steganography

Hybrid LSB–DWT image steganography has potential applications in areas where confidential information must be transmitted or stored without attracting unnecessary attention. In secure communication, it can be used to conceal encrypted messages within digital images shared through communication networks.

In healthcare, the approach may support the discreet transmission of medical reports, diagnostic information, and patient-related records, provided that appropriate privacy and regulatory safeguards are maintained. Digital watermarking and copyright protection represent other possible applications, where ownership information or authentication data can be embedded into images to support content verification and intellectual property protection. The technique may also be useful in military communication, digital forensics, confidential document exchange, and cloud-based information storage. Combining steganography with encryption can provide an additional layer of protection when sensitive digital information is exchanged over potentially insecure networks [14]. However, practical implementation requires consideration of image quality, payload size, processing time, and resistance to image manipulation. These applications should therefore be supported by appropriate security testing and should not replace established encryption, access-control, or data-protection systems.

12. Conclusion

Hybrid image steganography combining Least Significant Bit substitution and Discrete Wavelet Transform provides a flexible approach to digital information hiding by integrating spatial-domain embedding with multiresolution frequency analysis. LSB techniques offer computational simplicity and relatively high embedding capacity, whereas DWT enables frequency-dependent coefficient selection and adaptive embedding. Their combination may provide improved control over image distortion and robustness against selected processing operations when supported by an appropriate embedding and extraction architecture. The integration of cryptographic data protection further strengthens the security framework by ensuring that concealed information remains confidential even if the hidden payload is successfully extracted. Authenticated encryption, secure key management and key-dependent embedding locations can contribute to a more comprehensive protection strategy. Nevertheless, the effectiveness of such systems depends on the embedding design, image characteristics, payload size, transformation conditions and resistance to modern steganalysis, hybrid LSB–DWT steganography with cryptographic protection represents a promising research direction, but its practical security and robustness must be demonstrated through systematic comparative experimentation rather than inferred solely from theoretical advantages.

References

1. Anderson, R., & Petitcolas, F. A. P. (1998). On the limits of steganography. IEEE Journal on Selected Areas in Communications, 16(4), 474–481. https://doi.org/10.1109/49.668971
2. Apau, R., Asante, M., Twum, F., Ben Hayfron-Acquah, J., & Peasah, K. O. (2024). Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. PLOS ONE, 19(9), e0308807. https://doi.org/10.1371/journal.pone.0308807
3. Bachrach, M., & Shih, F. Y. (2011). Image steganography and steganalysis. WIREs Computational Statistics, 3(3), 251–259. https://doi.org/10.1002/wics.152
4. Chan, C.-K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. Pattern Recognition, 37(3), 469–474. https://doi.org/10.1016/j.patcog.2003.08.007
5. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, 90(3), 727–752. https://doi.org/10.1016/j.sigpro.2009.08.010
6. Eid, W. M., Alotaibi, S. S., Alqahtani, H. M., & Saleh, S. Q. (2022). Digital image steganalysis: Current methodologies and future challenges. IEEE Access, 10, 81123–81145. https://doi.org/10.1109/ACCESS.2022.3202905
7. Fridrich, J. (2009). Steganography in digital media: Principles, algorithms, and applications. Cambridge University Press. https://doi.org/10.1017/CBO9781139192903
8. Fridrich, J., & Kodovský, J. (2012). Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 7(3), 868–882. https://doi.org/10.1109/TIFS.2012.2190402
9. Kombrink, M. H., Geradts, Z. J. M. H., & Worring, M. (2025). Image steganography approaches and their detection strategies: A survey. ACM Computing Surveys, 57(2), Article 33. https://doi.org/10.1145/3694965
10. Mallat, S. G. (1989). A theory for multiresolution signal decomposition: The wavelet representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 11(7), 674–693. https://doi.org/10.1109/34.192463
11. Mandal, P. C., Mukherjee, I., Paul, G., & Chatterji, B. N. (2022). Digital image steganography: A literature survey. Information Sciences, 609, 1451–1488. https://doi.org/10.1016/j.ins.2022.07.120
12. National Institute of Standards and Technology. (2007). Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC (NIST Special Publication 800-38D). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-38D
13. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—A survey. Proceedings of the IEEE, 87(7), 1062–1078. https://doi.org/10.1109/5.771065
14. Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: From error visibility to structural similarity. IEEE Transactions on Image Processing, 13(4), 600–612. https://doi.org/10.1109/TIP.2003.819861