IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 February 2025, accepted 20 February 2025, date of publication 27 February 2025, date of current version 12 March 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3546255

RESEARCH ARTICLE

C-HIDE: A Steganographic Framework for Robust Data Hiding and Advanced Security Using Coverless Hybrid Image Encryption With AES and ECC

SAHAR A. EL-RAHMAN[1], (Senior Member, IEEE), AHMED E. MANSOUR[2], LEILA JAMEL[3], MANAL ABDULLAH ALOHALI[3], MOHAMED SEIFELDIN[2], AND YASMIN ALKADY[2]

[1]Computer Systems Program-Electrical Engineering Department, Faculty of Engineering-Shoubra, Benha University, Cairo 11672, Egypt
[2]Faculty of Computer Science, Misr International University, Cairo 19648, Egypt
[3]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia

Corresponding author: Leila Jamel (Lmjamel@pnu.edu.sa)

This research project was funded by the Deanship of Scientific Research, Princess Nourah bint Abdulrahman University, through the Program of Research Project Funding After Publication, grant No (44-PRFA-P-114).

ABSTRACT Coverless image steganography conceals information without modifying the carrier image, addressing vulnerabilities in traditional methods. However, existing approaches often require transmitting metadata, raising suspicion and security risks. To overcome these limitations, we propose Coverless Hybrid Image Data Encryption (C-HIDE), a robust steganographic method integrating Advanced Encryption Standard (AES) for data confidentiality and Elliptic Curve Cryptography (ECC) for secure key exchange. The system ensures secure transmission without altering cover images, making embedded data harder to detect. C-HIDE eliminates metadata transmission by enabling both sender and receiver to independently generate synchronized coverless image datasets (CIDs) using random seeds. Encrypted secret data is mapped to images whose hash sequences correspond to segments of the message, with Speeded-Up Robust Features (SURF) ensuring reliable image matching. At the receiver's end, ECC-decrypted AES keys recover the original message while SURF retrieves relevant images. Experimental results demonstrate that C-HIDE achieves an embedding capacity of 574 bits per image, significantly surpassing DCT (256 bits) and DWT (128 bits) techniques. The system maintains 98.5% accuracy under attacks such as noise addition, cropping, and geometric transformations. Furthermore, it enhances security by eliminating metadata transmission, achieving a zero additional information ratio, unlike conventional methods requiring up to 25% extra data. By integrating encryption, minimizing detection, and removing metadata transmission, C-HIDE provides a secure, efficient, and scalable solution for covert communication in real-world applications.

INDEX TERMS Steganography, coverless image steganography, information hiding, information security, concealed communications, cryptography, embedding, encryption technique.

I. INTRODUCTION

With the rapid expansion of digital imagery and the growing dominance of social media platforms [1], image exchange and dissemination have become pivotal in contemporary communication. In specific scenarios, there arises a need to transmit sensitive information covertly to ensure privacy and secure communication. In such instances, image steganography proves to be a crucial tool, enabling the embedding of confidential data into digital images in a manner that renders the hidden content imperceptible. This technique is particularly valuable for secure communication, as it facilitates the discreet transmission of sensitive data within seemingly ordinary images, enabling undetectable

The associate editor coordinating the review of this manuscript and approving it for publication was S. K. Hafizul Islam.

information exchange. Moreover, image steganography is instrumental in intellectual property protection, embedding digital watermarks or copyright metadata that authenticate, trace, and protect the integrity of digital assets. By integrating confidentiality with practicality, image steganography addresses essential challenges in secure digital communication and intellectual property safeguarding.

Image steganography can be classified into two major categories: cover-modified steganography and coverless steganography. In the former, the cover image undergoes modifications to embed the secret data, whereas the latter relies on the inherent properties of the image to embed the secret information without any modifications.

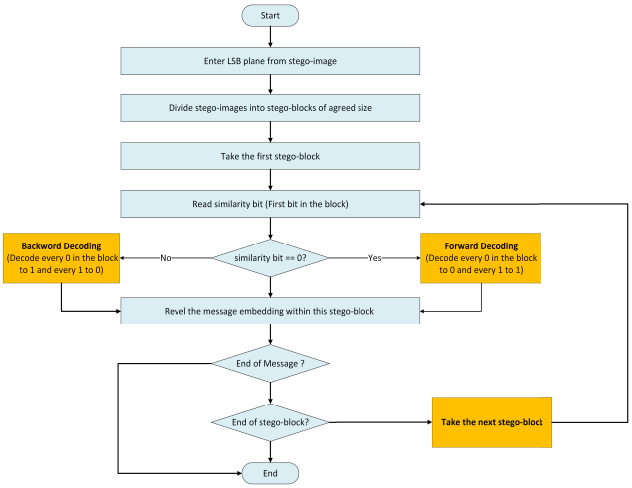

FIGURE 1. Cover-modified steganography.

Cover-modified steganography, a well-established approach in image-based data hiding [2], [3], [4], [5], [6], typically embeds secret information by altering pixel values or specific regions of an image [7], [8], [9], [10], [11]. As illustrated in FIGURE 1, this method capitalizes on image redundancy and the limitations of human visual perception to conceal information. The recipient retrieves the embedded data using a corresponding key and extraction algorithm. Over the years, significant advancements have been achieved in this field [12], [13], [14], [15]. For example, Subramanian et al. [16] developed an end-to-end convolutional neural network (CNN) for information hiding, achieving substantial improvements in capacity. Lan et al. [17] introduced a reversible network based on frequency coefficients, demonstrating resistance to JPEG compression attacks. Additionally, Yang et al. [18] employed a generative adversarial network (GAN) to embed secret messages, mapping the message to latent vectors that generate natural-looking stego-images. The receiver optimizes these latent vectors to recover the original message, demonstrating robustness across various GAN architectures, noise levels, and datasets.

Despite these innovations, traditional steganography methods often degrade the visual quality of carrier images and are susceptible to detection by steganalysis tools [19], [20], [21]. To overcome these limitations, coverless steganography has emerged as a viable alternative. Unlike its counterpart, coverless steganography leaves the carrier image unaltered, allowing it to evade detection by conventional steganalysis techniques. Instead, it establishes a relationship between secret information and carrier images through predefined mapping rules. Notably, coverless steganography does not eliminate the need for a carrier image but ensures that the image remains unmodified during the transmission of the hidden information.

In coverless image steganography, secret messages are encoded as binary data, and specific images are selected to represent these bits based on predefined mapping rules. Using the same rules, the receiver decodes the binary data from the selected images and reconstructs the original message. As the images remain unaltered, the concealed information is much harder to detect, making this technique highly suitable for covert communication, such as secure information exchange, intelligence sharing, and clandestine operations.

Coverless steganographic algorithms based on hash sequences can be categorized into generative-based and mapping-based methods. Generative-based methods create images corresponding to specific hash sequences, while mapping-based approaches establish fixed associations between hash sequences and images. Zhou et al. [21] pioneered generative-based methods by generating hash sequences from pixel block averages in scanned sub-images. Building on this, Zhang et al. [22] enhanced the technique using discrete cosine transform (DCT) coefficients, and Liu et al. [23] further advanced it by leveraging discrete wavelet transform (DWT) decomposition to analyze low-frequency components for hash sequence generation.

Generative-based coverless steganography algorithms, including those utilizing DCT and DWT [24], heavily depend on the pixel-level attributes of images. Consequently, even minor disturbances to the image can disrupt the hash sequence's consistency, compromising system reliability. In contrast, mapping-based algorithms improve robustness by constructing unique coverless image datasets (CIDs) for both sender and receiver. This enables the receiver to accurately locate corresponding images in the CID and extract associated hash sequences using predefined mapping rules, enhancing resilience against image disturbances.

Zheng et al. [25] expanded on coverless steganography by employing Scale-Invariant Feature Transform (SIFT) features for hash sequence generation. Yuan et al. [26] improved this approach by integrating SIFT with bagged features. To address geometric distortions, Luo et al. [27] introduced a faster region-based convolutional neural network (faster-RCNN). Additionally, Liu et al. [28] suggested transmitting disguised images instead of steganographic ones to address security concerns.

Beyond coverless steganography, several recent works have explored alternative approaches to enhance data security and robustness in steganographic systems. These

include encryption-steganography hybrids, generative-based steganographic techniques, and novel spatial domain methodologies.

Xiaoxiao Hu et al. [29] propose a novel robust generative image steganography scheme that leverages the Stable Diffusion model to enable zero-shot text-driven stego image generation, addressing the limitations of existing approaches in terms of visual quality and robustness under lossy transmission conditions. By introducing a dual-key mapping module, the framework enhances security and resilience against unknown channel attacks, adhering to Kerckhoff's principle. The proposed method demonstrates significant improvements in extraction accuracy, robustness, and image quality, offering a promising solution for secure and efficient covert communication in real-world scenarios.

A recent study [30] introduced a double data security algorithm that combines encryption with steganography for enhanced protection. It uses a two-stage encryption scheme based on a fractional-order memristive neural network and embeds encrypted data within 3D geometries. The approach outperforms AES-256 in efficiency and security, making it a robust solution for secure data storage and transmission.

Another significant advancement is seen in image-in-image steganography, which enhances both security and visual imperceptibility.

Recent advancements in image-in-image steganography have focused on improving both security and efficiency. LiDiNet, introduced in [31], presents a novel approach by leveraging multiple invertible neural networks (INNs) to achieve seamless image hiding and recovery. Its innovative invertible convolutional layer enhances information fusion, while adaptive coordination spatial-wise attention modules improve robustness. With its lightweight structure, LiDiNet outperforms traditional methods in visual quality and resistance to steganalysis, making it a promising solution for secure image embedding.

Despite advancements in generative-based coverless steganography, challenges persist. Key issues include the need for large image databases to store hash sequences, leading to higher storage requirements and associated costs. Managing these databases is complex, as data quality critically impacts algorithm performance. Additionally, selecting specific image regions for hash sequence generation necessitates transmitting supplementary information, which increases security risks and the likelihood of tampering or detection.

Similarly, spatial domain steganography has seen novel enhancements to improve both embedding capacity and security.

The secured spatial steganography algorithm in [32] enhances data security through multi-layer encryption, QR code transformation, and DNA coding before embedding data in an RGB cover image. Experimental results show high embedding capacity, robustness against attacks, and strong imperceptibility, making it effective for secure communication.

To mitigate these challenges, mapping-based coverless image steganography algorithms have gained prominence [33], [34], [35], [36]. A notable example is the Deep Cross-Modal Hashing Convolutional Neural Network (DCMH-CNN) by Zou et al. [37], which employs deep hashing and convolutional neural networks for feature extraction and data mapping. DCMH-CNN uses CNNs to extract high-dimensional image features, encoding them as deep hashes for representation. These are clustered into compact CIDs using K-means, and a mapping table links images in the CID to hash sequences. At the receiver's end, the same CNN extracts features from received images to decode the corresponding secret information using predefined mapping rules.

Although mapping-based algorithms like DCMH-CNN enhance database efficiency and security, they are not without limitations. Repeated occurrences of specific secret segments may necessitate reusing the same images, compromising communication secrecy. Synchronization of CNN models between sender and receiver also requires parameter exchange, introducing vulnerabilities and transmission complexity. Furthermore, robustness against adversarial attacks such as cropping, translation, noise, and severe rotation remains a significant challenge.

To address these challenges, the proposed Coverless Hybrid Image Data Encryption (C-HIDE) system integrates mapping-based techniques with hybrid encryption to enhance security, robustness, and capacity. By eliminating the need for metadata transmission, C-HIDE reduces security risks. It utilizes random seeds to generate synchronized CIDs, mapping secret information to binary hash sequences. AES and Elliptic Curve Cryptography (ECC) are employed for encryption and secure key exchange, while Speeded-Up Robust Features (SURF) facilitate reliable image retrieval from CIDs. This approach addresses traditional steganography's challenges, such as large database requirements and metadata transmission, offering a more secure, efficient, and robust solution.

Experimental results indicate that C-HIDE outperforms existing coverless steganography algorithms in embedding capacity, robustness, and security. By combining cryptographic methods with coverless steganography, C-HIDE ensures effective covert communication, even in the presence of advanced steganalysis tools. In summary, C-HIDE provides a novel, practical framework for secure information concealment, addressing critical challenges in steganography and delivering enhanced performance.

The structure of this paper is organized as follows: Section II discusses preliminaries, including the definitions of coverless steganography, steganalysis, encryption with AES-ECC, coverless steganography algorithm based on SURF. Section III presents the proposed C-HIDE system, which is based on image block matching and the Dense Convolutional

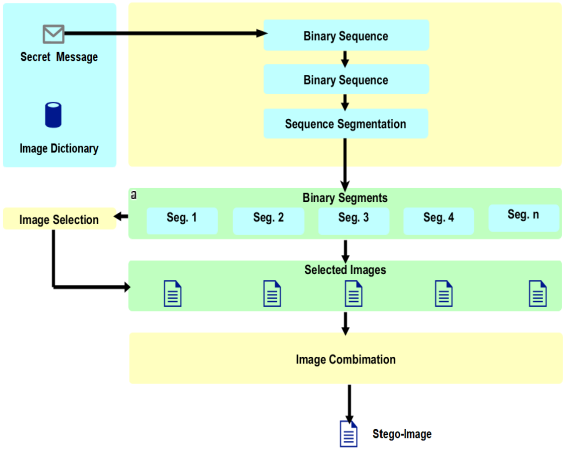

FIGURE 2. Cover steganography.

Network. In Section IV, the performance of this method is evaluated and compared with existing approaches in terms of robustness, accuracy, efficiency, and capacity. Finally, Section V provides a summary of the proposed method along with future research directions.

II. PRELIMINARIES

A. COVERLESS STEGANOGRAPHY

Coverless image steganography is an innovative technique for concealing information without modifying the carrier medium, thereby eliminating the vulnerabilities associated with traditional steganography. In conventional methods, hidden data often alters the statistical properties of carrier files, making them susceptible to detection by steganalysis tools. In contrast, coverless steganography maps the secret message directly to unaltered, publicly available images, bypassing the need for modifications and significantly reducing the risk of detection as shown in FIGURE2.

The core concept of coverless steganography [38], [39] lies in associating data segments with features or hash sequences extracted from images. These selected images act as carriers for the hidden information, and their intrinsic properties ensure the security of the transmission. However, despite its promise, coverless steganography faces notable challenges. Many existing methods demand extensive image databases to ensure adequate mapping capacity, which can lead to increased resource requirements. Additionally, some techniques rely on transmitting auxiliary metadata, such as block locations or mapping parameters, to enable data recovery at the receiver's end. This reliance on metadata not only raises security concerns but also increases the risk of interception during communication. Moreover, existing single-dataset approaches often reuse the same images for transmitting different segments of the hidden data. This repetitive usage can raise suspicion and compromise the covert nature of the communication. To address these issues, the proposed Coverless Hybrid Image Data Encryption (C-HIDE) method introduces a secure and robust framework by leveraging synchronized datasets, random seed generation, and advanced hybrid encryption techniques. These innovations ensure the elimination of metadata transmission and enhance the security and scalability of coverless steganography.

B. STEGANALYSIS

Steganalysis involves detecting the presence of steganography and extracting hidden information. Unlike steganography, which focuses on embedding data covertly, steganalysis aims to reveal the existence of secret information within an image and, if possible, extract it. Traditional steganalysis techniques primarily target LSB-based methods in the spatial domain and approach in the DCT transform domain. These methods rely on identifying statistical anomalies introduced by data embedding to determine the presence of hidden information.

Various steganalysis tools analyze how embedding affects an image's statistical properties. Examples include SPAM [40], SRM [41], and their variants [42], [43]. Recently, deep neural networks (DNNs) have revolutionized steganalysis, garnering significant attention. One notable contribution is by Qian et al., who introduced the Gaussian Neural Convolutional Neural Network (GNCNN) for spatial-domain steganography detection [44]. By using a Gaussian function as the activation function instead of ReLU or sigmoid, GNCNN achieved performance on par with SRM [45].
Xu et al. investigated CNN architecture design for steganalysis and demonstrated that well-designed CNNs could outperform traditional approaches. Similarly, Ye et al. developed a supervised CNN-based steganalysis application, achieving better results than SRM [38]. Furthermore, Chen et al. proposed a phase-aware CNN for JPEG steganalysis by integrating a phase separation model, significantly improving detection accuracy [39]. These advanced techniques are often employed to assess the robustness and anti-steganalysis capabilities of coverless steganography methods.

In the realm of steganography, a critical steganalysis tool that is frequently referenced in academic literature is 'StegExpose.' This tool is designed to detect various forms of steganography by analyzing the statistical properties of images and identifying inconsistencies that suggest the presence of hidden data. Given that the proposed C-HIDE framework employs coverless steganography a technique that does not alter the visual characteristics of the carrier images there are inherent advantages in terms of detection resistance. The C-HIDE method utilizes publicly available images as carriers, ensuring that the statistical properties remain largely unchanged. Additionally, because C-HIDE avoids metadata transmission, it minimizes opportunities for steganalysis tools like StegExpose to identify any hidden information. Preliminary assessments indicate that C-HIDE's reliance on synchronized coverless image datasets and the direct mapping of encrypted message segments to image hashes enhances its immunity to detection by StegExpose,

thereby providing a more secure alternative in the landscape of steganographic practices.

C. ENCRYPTION WITH AES-ECC

To ensure secure communication, the proposed method integrates the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) into a hybrid encryption framework. This combination capitalizes on the strengths of both symmetric and asymmetric encryption methods, providing robust data protection and secure key exchange mechanisms. AES is a symmetric encryption algorithm renowned for its efficiency and high-level security. It encrypts data using a shared secret key, offering various key lengths (128, 192, or 256 bits) to balance security and performance. AES is widely adopted in secure communication systems due to its resistance to brute-force attacks and its ability to handle large volumes of data efficiently. ECC, on the other hand, is an asymmetric encryption technique designed for secure key exchange. ECC relies on the mathematical properties of elliptic curves to achieve high levels of security with smaller key sizes compared to traditional algorithms like Rivest–Shamir–Adleman (RSA). This makes ECC particularly suitable for applications where computational resources or bandwidth are limited. The hybrid AES-ECC approach begins with the use of ECC to establish a shared secret between the sender and receiver. The shared secret (Kshared)is computed using the sender's private key and the receiver's public key as in Eq. 1, and vice versa:

$$K_{\text{shared}} = d_A \cdot Q_B = d_B \cdot Q_A \tag{1}$$

where dA and dB are the private keys, and QA and QB are the corresponding public keys. This shared secret is then processed through a Key Derivation Function (KDF) to generate a symmetric AES key K_{AES} as in Eq. 2:

$$K_{AES} = K_{DF}(K_{shared}) \tag{2}$$

The AES key is subsequently used to encrypt the secret data into ciphertext, ensuring data confidentiality. This hybrid encryption framework combines the computational efficiency of AES with the robust key exchange capabilities of ECC. By integrating AES-ECC into the C-HIDE system, the proposed method guarantees the security of the transmitted data even under active surveillance or interception, making it a highly effective solution for secure and covert communication.

D. COVERLESS STEGANOGRAPHY ALGORITHM BASED ON SURF

Coverless image steganography by leveraging multi-sub-CIDs, SURF-based image retrieval, and binary mapping. Each component plays a critical role in achieving secure and reliable data hiding and extraction. Below, each component is described in detail.

1) PREPROCESSING THE ORIGINAL IMAGE DATASET

The initial step of the algorithm focuses on preprocessing a publicly available image dataset. This step ensures that both the sender and receiver utilize a consistent dataset, thereby eliminating the need for transmitting metadata. The images in the dataset are arranged in ascending order based on their average pixel values, creating a standardized sequence. This sorting facilitates deterministic mapping during the embedding and retrieval processes. Furthermore, each image is assigned a new name corresponding to its sequence number in the sorted order. This preprocessing stage streamlines subsequent operations and guarantees that both parties reference the same sorted dataset.

2) CONSTRUCTING MULTI-SUB-CIDS

To eliminate the repeated use of identical images, the algorithm partitions the sorted dataset into multiple Coverless Image Datasets (CIDs). A random array, generated through a fixed random seed, specifies the sequence numbers of images to be included in each CID. For example, if the random array is "2150, 200, 81, …, 125, …, 1617," the images corresponding to these indices are selected from the sorted dataset to construct the first CID as shown in Fig. 3. Once the first CID is created, the selected images are removed from the sorted dataset. The same random array is then applied to the remaining images to produce the next CID. This process continues until the desired number of sub-CIDs is generated. The fixed random seed ensures that both the sender and receiver independently generate identical CIDs without requiring additional synchronization. Dividing the dataset into multiple sub-CIDs significantly reduces the risk of reusing the same images for different secret messages, thereby lowering the likelihood of detection by adversaries.

3) ESTABLISHING THE MAPPING RULE OF HASH SEQUENCES

A pivotal aspect of the algorithm is establishing a one-to-one mapping between the images in the CIDs and their corresponding binary hash sequences. Each image within a CID is assigned a unique binary sequence, ranging from "000…0" to "111…1." The length of each binary sequence (L) is determined by the total number of images (M) in the CID and is calculated as in Eq. 3:

$$L = Log_2(M) \tag{3}$$

This mapping guarantees that every binary segment of the secret message is uniquely associated with a specific image in the CID. The distinctiveness of the mapping rule is vital for accurately reconstructing the original message at the receiver's end, ensuring reliable communication. Additionally, the use of a predefined mapping rule eliminates the necessity for transmitting supplementary metadata, thereby bolstering security by minimizing the risk of adversaries intercepting or exploiting auxiliary information.

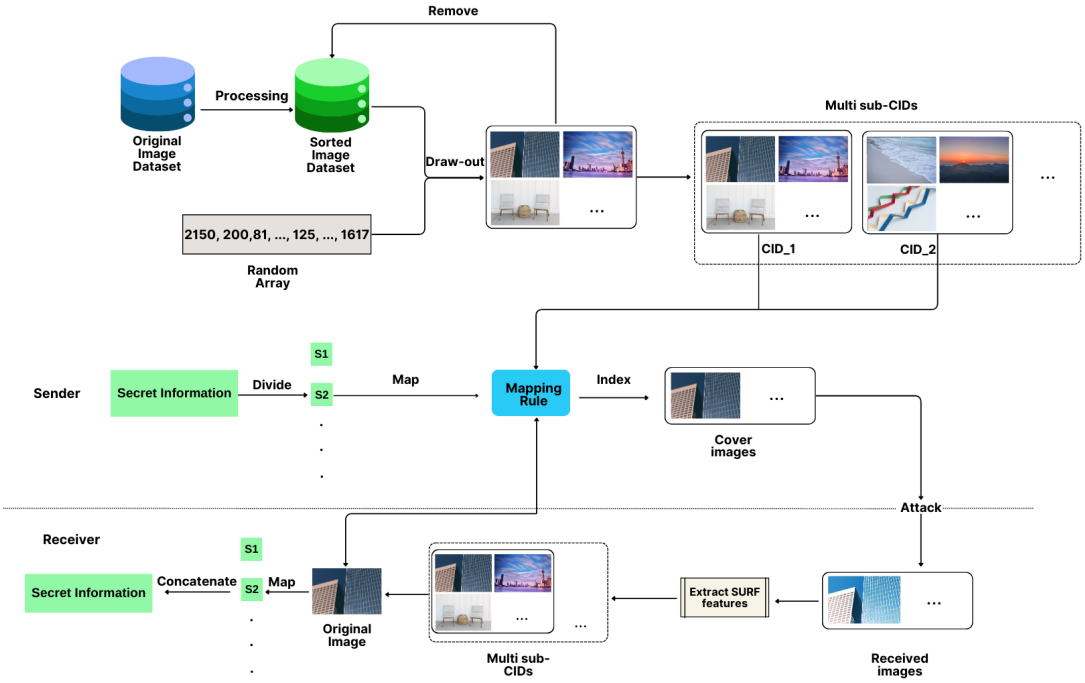

FIGURE 3. Robust coverless image steganography algorithm utilizing image retrieval based on SURF features.

4) SECRET INFORMATION EMBEDDING

The process of embedding the secret message involves selecting specific images from the CIDs using a predefined mapping rule. Initially, the secret message is divided into binary segments, each matching the length of the hash sequences.

5) IMAGE RETRIEVAL USING SURF

Retrieving the correct images from the transmitted set is a crucial step at the receiver's end. The algorithm utilizes Speeded-Up Robust Features (SURF) to facilitate robust and accurate image matching. SURF identifies key features within the received images, even if they have undergone various distortions such as rotation, cropping, or noise. These features are then matched with the original images in the CIDs using the nearest distance method. This robustness against attacks ensures reliable image retrieval, even under challenging conditions. By integrating SURF, the algorithm significantly enhances the resilience of the steganography process, effectively withstanding geometric transformations and other types of image alterations.

6) SECRET INFORMATION EXTRACTION

The final stage focuses on reconstructing the hidden message at the receiver's end. After identifying the original images through SURF-based matching, the predefined mapping rule is applied to extract the associated binary hash sequences. These sequences are concatenated to generate the complete binary representation of the secret message. Any padding added during the embedding process is subsequently removed to accurately recover the original message. This approach guarantees secure and efficient retrieval of the hidden data, even if the transmitted images have been subjected to alterations during transmission.

E. IMAGE DATASETS FOR STEGANOGRAPHIC RESEARCH

In steganographic research, the selection of datasets plays a crucial role in evaluating the robustness, imperceptibility, and efficiency of embedding techniques. Below, we discuss prominent image datasets often employed in this domain, highlighting their characteristics, including the number of images, resolution, and diversity of content.

1) BOSSBase (BREAK OUR STEGANOGRAPHY SYSTEM)

The BOSSBase dataset [45] is a benchmark in steganographic research, containing 10,000 grayscale images, each with a resolution of 512×512 pixels. The dataset was designed to test the limits of steganography and steganalysis algorithms. Its uniform resolution and grayscale format make it particularly suitable for spatial and transform domain techniques, ensuring a controlled environment for algorithm evaluation.

2) ALASKA DATASET

The ALASKA dataset [46]is specifically designed for steganography and steganalysis research, containing natural images and their stego versions created using various algorithms. It includes high-resolution images that simulate real-world scenarios, providing a robust testing ground for assessing the resistance of steganographic methods to detection.

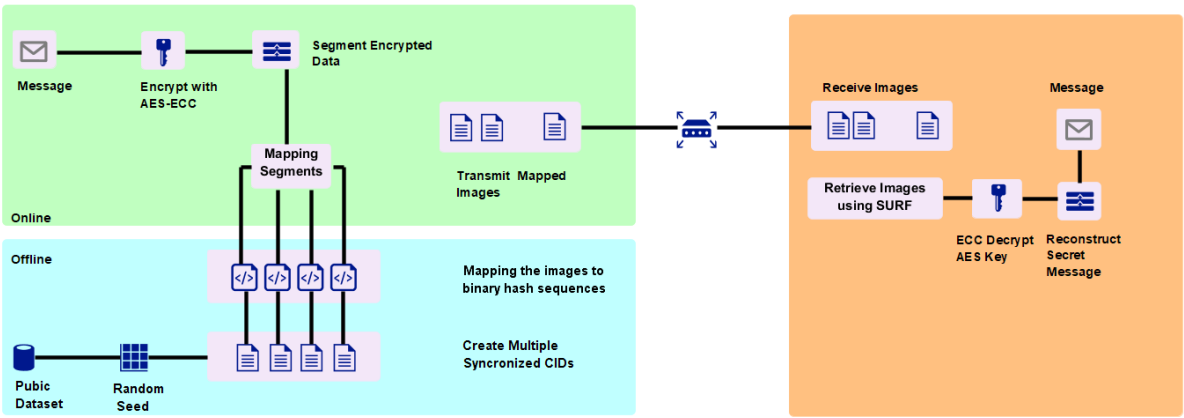

FIGURE 4. C-HIDE proposed system.

3) UCID (UNCOMPRESSED COLOUR IMAGE DATASET)

The UCID dataset [47] comprises 1,336 uncompressed images with varying resolutions, making it a valuable resource for evaluating image steganography techniques. The images in this dataset include a wide variety of content, such as landscapes, urban scenes, and objects, ensuring diversity in testing scenarios. Its uncompressed format preserves image quality, allowing precise assessment of distortion introduced by embedding algorithms.

4) MS-COCO (MICROSOFT COMMON OBJECTS IN CONTEXT)

The MS-COCO dataset [48] consists of over 330,000 images annotated with object and scene labels. These images cover a wide range of natural and artificial scenes, providing a rich resource for steganographic methods that rely on semantic features. The diversity in content, resolution, and complexity makes this dataset suitable for testing robustness and imperceptibility under realistic conditions.

5) CALTECH 101/256

The Caltech datasets [49] feature 101 or 256 categories of objects, with each category containing multiple images. These datasets provide images with varying resolutions and content complexity, making them ideal for evaluating the adaptability of steganographic techniques to diverse image types. The Caltech datasets are widely used for training and testing spatial-domain embedding algorithms.

6) DRESDEN IMAGE DATABASE

The Dresden Image Database [50] comprises over 14,000 images captured using different devices, including smartphones and cameras. The dataset focuses on forensic and steganographic research, allowing the evaluation of embedding techniques under varying device-specific characteristics. The images are available in diverse resolutions, reflecting real-world usage scenarios.

7) INRIA HOLIDAY DATASET

The INRIA Holiday dataset [51] contains 1,491 images featuring natural landscapes, urban scenery, buildings, and tourist photographs. These high-resolution images exhibit rich visual features and diversity, including variations in environments, lighting conditions, and shooting angles. The dataset's diversity makes it ideal for testing robustness and imperceptibility in challenging conditions.

8) ImageNet DATASET

The ImageNet dataset [52] includes over 15 million images spanning more than 1,000 categories, such as animals, objects, plants, and scenes. Each image is labeled with a category, making this dataset highly versatile for tasks like image classification and object detection. The large scale and diversity of ImageNet provide a robust testing environment for steganographic techniques, particularly those relying on semantic content.

9) OPEN IMAGES DATASET

The Open Images dataset [53]contains approximately 9 million images with annotations for objects, relationships, and scenes. Its large size and comprehensive labeling make it a valuable resource for evaluating algorithms that incorporate contextual or semantic features into steganography. The dataset includes images of varying resolutions and quality, reflecting real-world scenarios.

10) WANG DATASET (COREL DATASET)

The Wang dataset [54], also known as the Corel dataset, contains 1,000 images grouped into 10 categories. These images have consistent quality and resolution, making the dataset suitable for controlled testing of steganographic methods. The small scale and defined categories make it an accessible choice for preliminary evaluations.

Each of these datasets has unique characteristics that cater to specific aspects of steganographic research. Datasets like

BOSSBase and ALASKA provide controlled environments for rigorous testing, while diverse datasets such as MS-COCO, INRIA Holiday, and ImageNet simulate real-world scenarios, ensuring the robustness and practicality of developed methods. These datasets collectively form a foundation for advancing the field of image steganography.

III. C-HIDE PROPOSED SYSTEM

The proposed C-HIDE system introduces an innovative framework that combines coverless image steganography with advanced cryptographic techniques to address the limitations of existing methods. By eliminating the need for metadata transmission and leveraging hybrid encryption with AES and ECC, the system enhances data confidentiality and secure key exchange. Additionally, the use of Speeded-Up Robust Features (SURF) ensures reliable image retrieval, making the system robust against image processing attacks such as noise, rotation, and cropping. The C-HIDE framework utilizes a publicly available image database to create multiple synchronized Coverless Image Datasets (CIDs), enabling the mapping of encrypted message segments to images without altering their content as shown in FIGURE 4. This approach ensures effective covert communication while bypassing traditional steganalysis tools. The following subsections detail the components and processes of the C-HIDE system, highlighting its secure, scalable, and efficient design. Algorithm III-B illustrates all steps of the C-HIDE algorithm.

A. SYSTEM COMPONENTS

1) PUBLIC IMAGE DATASET

The proposed C-HIDE algorithm uses a publicly available image dataset as the basis for carrier images. This ensures accessibility and eliminates the need to create proprietary datasets. Both the sender and receiver preprocess this dataset identically, ensuring that the same images are used for encoding and decoding without requiring metadata transmission.

2) RANDOM SEED GENERATOR

a random seed generates consistent random sequences for both the sender and receiver. These sequences are used to index images from the dataset, ensuring that identical Coverless Image Datasets (CIDs) are created without the need for metadata exchange. To generate the random sequence, a random seed is used as the starting point. This can be achieved in Eq. 4:

$$S = rng(R) \tag{4}$$

When given a random seed R, the random sequence S is generated. This sequence is used to index images from the sorted dataset, ensuring that both sender and receiver independently construct identical sub-datasets (CIDs).

3) COVERLESS IMAGE DATASETS (CIDS)

The random sequence S is applied iteratively to the sorted dataset to create multiple CIDs. The sorted dataset is divided into multiple CIDs using random sequences. So the proposed C-HIDE selects images indexed by S from the dataset to form the first CID. Then remove the selected images and repeat with the same sequence to construct additional CIDs. If I = I1, I2, ….., In represents the sorted dataset, then the first CID CID1 is in Eq. 5:

$$CID_1 = \{I_{S1}, I_{S2}, \ldots.., I_{SK}\} \tag{5}$$

where S_i is the i^{th} index in the random sequence S.

4) BINARY HASH MAPPING

Each image in the CIDs is mapped to a unique binary hash sequence. The hash sequences serve as a bridge between the secret message and the carrier images. The length of the hash sequence L depends on the number of images M in the CID as illustrated in Eq. 3. For mapping Rule a CID containing M images, the binary hash sequences range from 000 . . . 000 to 111 . . . 111. Each image I_j in the CID corresponds to a unique binary hash sequence $H(I_j)$ as shown in FIGURE 5.

5) ADVANCED ENCRYPTION STANDARD (AES)

AES encrypts the secret message into ciphertext, ensuring its confidentiality. The encryption process transforms the plaintext message into a secure, unreadable format, which is then embedded into the CIDs.

6) ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

ECC facilitates the secure exchange of the AES encryption key. By generating a shared secret between the sender and receiver, ECC ensures that only authorized parties can decrypt the hidden message as illustrated in Eq. 2.

7) SPEEDED-UP ROBUST FEATURES (SURF)

SURF extracts distinctive features from images to enable robust image retrieval. It ensures that transmitted images can be accurately identified even if they have been subjected to noise, cropping, or other transformations. For image I, SURF extracts key points K and descriptors D as in Eq. 6:

$$(K, D) = SURF(I) \tag{6}$$

B. PROCESSES OF THE C-HIDE SYSTEM

The processes performed by the C-HIDE proposed system are detailed as followers, as well as the pseudocode for hiding data using C-HIDE is illustrated in Algorithm III-B.

1) PREPROCESSING AND CID CONSTRUCTION

First, use a publicly available image database as the base for both sender and receiver. I = I1, I2,…, In, as the base for encoding and decoding. Secondly, a random seed generates consistent random sequences for both the sender and receiver to ensure identical datasets without metadata transmission. For example in MATLAB, using $rng(42)$ followed by Eq. 7:

$$randi([0, M-1], 1, K) \tag{7}$$

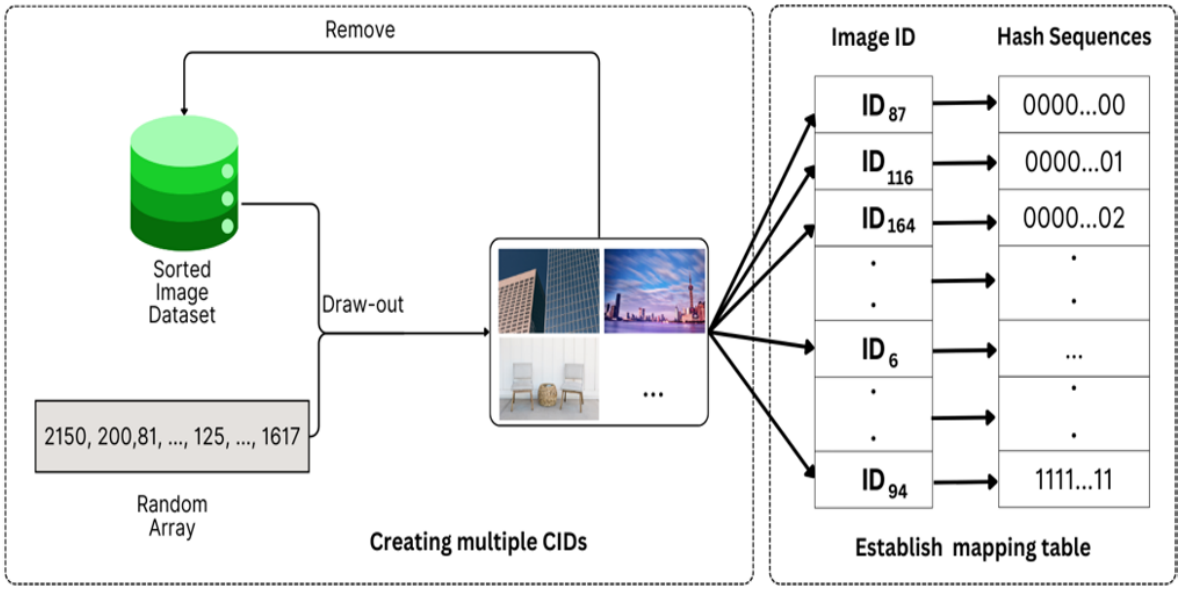

FIGURE 5. Binary hash mapping.

where M is the total number of images and K is the desired sequence length. So $randi([0, 500], 1, 256)$ produces a random sequence of length 256. Thirdly, the dataset is divided into multiple CIDs. Each CID contains a fixed number of images. Then, calculate the average pixel value because Each image in the dataset is sorted based on its average pixel value. The average pixel value for an image Ij is computed using the formula (8):

$$\text{AvgPixel}(I_j) = \frac{1}{W \times H} \sum_{x=1}^{W} \sum_{y=1}^{H} I_j(x, y) \tag{8}$$

where W is the width of the image. H is the height of the image. $I_j(x, y)$ is the pixel value at coordinates (x, y) in the image I_j.

This formula calculates the sum of all pixel values in the image and then divides it by the total number of pixels (width times height) to get the average. Then random sequences and segmenting into multiple $CIDs(CID1, CID2, \ldots, CIDN)$ as shown in FIGURE 6.

2) BINARY HASH MAPPING

Each image I_j in the CID is mapped to a unique binary hash sequence $H(I_j)$. The length of the hash sequence L depends on the number of images M in the CID. As formulated in (9)

$$H(I_j) = \{0, 1\}^L \tag{9}$$

where $L = log2M$ and M is the total number of images in the CID.

3) ENCRYPTION OF SECRET INFORMATION

The first phase in the encryption process is AES when the secret message M is encrypted using AES to produce

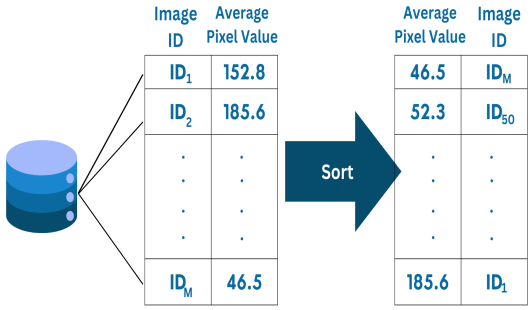

FIGURE 6. Preprocessing and CID construction.

ciphertext C as formed in Eq. 10:

$$C = AES(M_{SECRET}, K_{AES}) \tag{10}$$

where K_{AES} is the AES encryption key. The second phase in the encryption process is ECC when ECC facilitates secure key exchange. A shared secret K_{shared} is generated using ECC as formulated in Eq. 1.

4) EMBEDDING THE ENCRYPTED DATA

The ciphertext C is divided into segments $C1, C2, \ldots, CN$ each corresponding to a binary hash sequence as in Eq. 11:

$$C = \bigcup_{i=1}^{N} C_i \tag{11}$$

Each segment C_i is mapped to an image I_j in the CID whose hash sequence $H(I_j)$ matches the binary representation of C_i.

Algorithm 1 C-HIDE System

Require: Secret data S, synchronized random seed Seed, synchronized coverless image databases CID_A and CID_B, AES key K_AES, ECC public/private key pairs (K_pub_A, K_priv_A) and (K_pub_B, K_priv_B)

Ensure: Transmitted encrypted stego-images {I_S1, I_S2, …, I_Sn} and recovered secret data S at the receiver

****Sender Side**** Encrypt the secret data S using AES encryption:

Ciphertext C = AES_Encrypt(S, K_AES)

Divide the ciphertext C into segments:

C = {C1, C2, …, Cn}, where each segment matches the hash sequence length

Independently generate a synchronized coverless image dataset (CID_A):

Use the random seed Seed to generate CID_A

Map each ciphertext segment Ci to an image in CID_A:

Compute hash sequence Hi for each image I in CID_A using SURF feature extraction:

Find images I_Si in CID_A where Hi corresponds to Ci

Encrypt the AES key K_AES using ECC for secure transmission:

Encrypted Key K_AES_enc = ECC_Encrypt(K_AES, K_pub_B)

Transmit the stego-images {I_S1, I_S2, …, I_Sn} and K_AES_enc to the receiver

****Receiver Side**** Independently generate a synchronized coverless image dataset (CID_B):

Use the random seed Seed to generate CID_B, ensuring it matches CID_A

Decrypt the AES key K_AES:

K_AES = ECC_Decrypt(K_AES_enc, K_priv_B)

Retrieve ciphertext segments from received stego-images:

For each received stego-image I_Si, compute its hash sequence Hi:

Match Hi with CID_B to find the corresponding ciphertext segment Ci

Reconstruct the ciphertext C:

Combine all retrieved segments C = {C1, C2, …, Cn}

Decrypt the secret data S:

S = AES_Decrypt(C, K_AES)

****End****

5) TRANSMITTING COVER IMAGES

The selected images $I_{t1}, I_{t2}, \ldots, I_{tn}$ corresponding to ciphertext segments are transmitted without alteration.

6) IMAGE RETRIEVAL AT THE RECEIVER'S END

This stage is supported by SURF for robust image retrieval to ensure accurate retrieval of transmitted images, even under transformations. For image I, SURF extracts key points K and descriptors D as formed in Eq. 6. Then the receiver compares K and D to identify matching images from the *CID*.

7) DECRYPTION AND MESSAGE RECONSTRUCTION

The first phase of this process is key decryption using *ECC*, where the receiver uses *ECC* to decrypt the *AES* key K_{AES} using the shared secret K_{shared} as formulated in Eq. 12:

$$K_{AES} = ECC_{decrypt}(K_{SHARED}) \tag{12}$$

The second phase is reconstructing the secret message by using the decrypted AES key, the receiver reconstructs the original secret message M_{secret} as in Eq. 13:

$$M_{SECRET} = AES_{decrypt}(C, K_{AES}) \tag{13}$$

IV. PERFORMANCE EVALUATION

A. EXPERIMENTAL CONFIGURATION

All experiments described in this paper were performed on a personal computer equipped with an Intel® Core™ i7 14th generation processor NVIDIA® GeForce RTX™ 4050 Laptop GPU (6 GB GDDR6 dedicated)16 GB memory; 1 TB SSD storage. The image processing tasks, including various types of image attacks such as noise addition and cropping, were implemented using functions from the Image Processing Toolbox in MATLAB R2018a. CIFAR-10 dataset is used as Experimental dataset. This dataset consists of 60,000 images across 10 distinct classes, providing a diverse range of content that is ideal for testing the robustness of our approach. Experimental datasets were carefully curated to evaluate the system's robustness and performance under diverse conditions All images in the dataset were uniformly resized to a fixed resolution of 512 × 512 pixels to ensure consistency and accuracy during the experimental analysis. The selection and resizing procedures in this study were consistent with those used in DWT [22], DCT [23], DCMH-CNN [37], and SURF [55]. While DCT and DWT are advanced generative-based coverless image steganography techniques, DCMH-CNN represents the only mapping-based approach. SURF is the only method that enables both communicating parties to independently generate multiple

coverless image datasets (CIDs) using random seeds. These algorithms were selected as benchmarks to facilitate a thorough comparison. To maintain fairness and consistency, we replicated the experiments of DWT [22], DCT [23], DCMH-CNN [37], and SURF [55] on the same datasets, rather than using their original experimental data. This approach highlights the superiority of the proposed method under uniform and controlled experimental conditions.

B. ANALYSIS OF COVERLESS IMAGE CAPACITY

In coverless image steganography, capacity is typically evaluated based on the number of cover images required to transmit a specific amount of secret information. Below are common approaches for measuring capacity:

- Number of Required Images: Capacity can be measured by determining how many cover images (or sub-images) are needed to encode a given amount of secret data. For example, if each image can encode a certain number of bits, the total number of images required to transmit a secret message of length G can be calculated using the formula (14):

$$N_h = [G/H] \tag{14}$$

  where L is the length of the secret message segment that one image can convey, and N_h is the total number of images needed.
- Bits per Image: Another way to express capacity is in terms of bits per image, which indicates how many bits of secret information can be embedded in each cover image. This value typically depends on the features extracted from the images and the encoding technique used.
- Total Capacity: The overall capacity of a steganographic method can be calculated by multiplying the number of images by the number of bits that can be hidden in each image. This provides a total capacity expressed in bits or bytes.
- Efficiency: The efficiency of the method can be evaluated by analyzing the ratio of the secret message length to the number of images used. This metric reflects how effectively the available cover images are utilized to conceal the secret information.

As illustrated in TABLE 1 The algorithms can be ranked in terms of capacity from highest to lowest as follows: the proposed C-HIDE system offers the highest capacity without requiring additional information or repeated transmission of the same image. DCMH-CNN [37] also achieves high capacity and robustness against various attacks but requires sharing the same feature extraction networks and cluster centers. SURF [29] provides high capacity with moderate robustness but involves sharing the same feature extraction networks and repeated transmission of the same image. DCT [23] has lower capacity and robustness, requiring the transmission of image block positions and repeated image transmission. Finally, DWT [22] has the lowest capacity and robustness, with similar requirements for transmitting image block positions and repeated image transmission.

TABLE 1. Performance comparison of different algorithms.

Algorithm	Data Size				Capacity
	10 B	50 B	100 B	1KB	
DWT [22]	8	27	57	128	13
DCT [23]	8	26	55	256	15
DCMH-CNN [37]	5	24	50	512	16
SURF [55]	5	20	45	548	17
C-HIDE	**3**	**15**	**39**	**574**	**20**

C. ACCURACY ANALYSIS

In the proposed method, the receiver retrieves the original image from the received one and applies a mapping rule to extract the corresponding secret information. The accuracy of secret information extraction is defined as Eq. 15:

$$\begin{aligned} \text{Acc} &= \frac{\sum_{i=1}^{n} f(El_i)}{n} \times 100\%, \\ f(El_i) &= \begin{cases} 1, & \text{if } El_i = I_i \\ 0, & \text{otherwise} \end{cases} \end{aligned} \tag{15}$$

where I_i represents the original i^{th} secret segment, and EI_i represents the extracted i^{th} secret segment. Since the secret information is divided into n segments, the accuracy depends on how many extracted segments match their original counterparts. This defined accuracy is used to evaluate the robustness of the proposed method against various attacks. High accuracy indicates strong resistance to attacks. To assess the effect of varying image sizes on the accuracy of secret information extraction, we conducted experiments on image databases with different dimensions. In addition to employing the resizing methods used by DWT [22], DCT [23], DCMH-CNN [37], and SURF [55] we resized all images in the database to (128 × 128), (256 × 256), and (512 × 512) and for a comprehensive comparison. The experiments evaluated the average accuracy of secret information extraction following various image attacks, with the results illustrated in FIGURE 5.

The proposed C-HIDE algorithm consistently achieves the highest accuracy, maintaining an accuracy of over 98% for most attacks. Following this, SURF [55] ranks second, and DCMH-CNN [37] ranks third, with slightly lower performance compared to the proposed method. DWT [22] demonstrates moderate accuracy, outperforming DCT [23] but falling behind DCMH-CNN. Among the compared algorithms, DCT shows the lowest accuracy, with significantly weaker performance under various attack scenarios.

1) SECURITY ANALYSIS

Security in steganography can be evaluated using various criteria and methodologies to ensure the reliability and confidentiality of the hidden information. One key measure

TABLE 2. Comparison of security characteristics of coverless image steganography algorithms.

Algorithm	Length of Additional Information (L_a)	Length of Secret Information (L)	Ratio (L/L_a)	Chi-squared Test Results (Hypothetical)
DWT [18]	256 bits (32 bytes)	1024 bits (128 bytes)	0.25	14.8
DCT [19]	256 bits (32 bytes)	1024 bits (128 bytes)	0.25	15.2
DCMH-CNN [28]	512 bits (64 bytes)	1024 bits (128 bytes)	0.5	12.5
SURF [29]	128 bits (16 bytes)	1024 bits (128 bytes)	0.125	10.0
C-HIDE	0 bits (no additional info)	1024 bits (128 bytes)	0.0	5.0

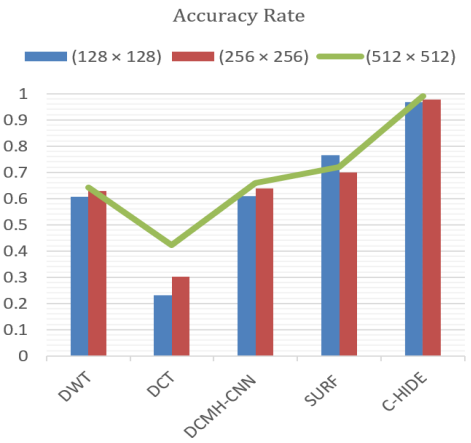

FIGURE 7. Rate of accuracy in the comparison of the proposed system with state-of-the-art algorithms.

is resistance to attacks, which assesses the method's ability to withstand manipulations such as image compression, cropping, noise addition, and other geometric or non-geometric distortions. Another important factor is steganalysis resistance, which evaluates whether the method can evade detection by techniques designed to uncover hidden information. Additionally, information leakage is a critical consideration, where methods requiring minimal or no extra data transmission are generally more secure, reducing the risk of interception. Key management also plays a vital role, with secure steganography relying on robust, random, and well-managed keys for encoding and decoding secret data. Several metrics used in the measurement of security in steganography. Here are a few key equations and concepts that are commonly applied:

2) RATIO OF ADDITIONAL INFORMATION TO CAPACITY

The ratio helps evaluate the efficiency and security of the transmission. It is defined as Eq. 16:

$$Ratio = (L_a/L) \tag{16}$$

where L_a is the length of the additional information (e.g., parameters or positional data) that needs to be transmitted, and L is the length of the secret information. A lower ratio indicates better security as it implies less additional information is being transmitted as illustrated in TABLE 2.

3) STATISTICAL MEASURES

Various statistical tests can be applied to assess the security of the steganographic method. For example, the Chi-squared test can be used to compare the distribution of pixel values before and after embedding as (17):

$$\chi^2 = \sum \frac{(O_i - E_i)^2}{E_i} \tag{17}$$

where O_i is the observed frequency of pixel values and Ei is the expected frequency. A lower Chi-squared value indicates that the steganographic method has not significantly altered the statistical properties of the cover image.

The proposed C-HIDE algorithm achieves a ratio of 0, meaning no additional information is transmitted, making it optimal for security. In comparison, other algorithms have higher ratios: DWT and DCT are at 0.25, DCMH-CNN at 0.5, and SURF at 0.125. Lower ratios indicate greater efficiency and security, with DCMH-CNN standing out as the best option after C-HIDE. Based on the analysis and performance evaluation, the algorithms are ranked by security as follows: The Proposed C-HIDE offers the highest security, as it does not require transmitting any additional information, minimizing detection risks and enhancing overall security. SURF [55] also demonstrates high security and robustness against attacks but has potential vulnerabilities due to the need to share feature extraction networks and cluster centers. DCMH-CNN [37] provides moderate security but is more susceptible to detection due to repeated transmission of the same image and shared feature extraction networks. DCT [22] and DWT [23] both have lower security, as they require transmitting image block positions, making them more vulnerable to interception and exploitation.

V. CONCLUSION AND FUTURE WORK

The proposed C-HIDE system presents a novel approach to coverless image steganography, combining hybrid encryption techniques with robust image retrieval. By eliminating the need for metadata transmission and leveraging the strengths of Advanced Encryption Standard (AES) for data confidentiality and Elliptic Curve Cryptography (ECC) for secure key exchange, the system addresses key challenges in existing methods, including security vulnerabilities, limited embedding capacity, and susceptibility to image processing attacks. The integration of Speeded-Up Robust Features (SURF) further enhances the system's robustness, enabling

accurate image retrieval even under adversarial conditions such as noise, cropping, and rotation. Experimental results demonstrate that the C-HIDE framework outperforms state-of-the-art approaches in embedding capacity, robustness, and security, providing a scalable and efficient solution for secure communication in real-world applications. Despite these advancements, the proposed system has certain limitations that warrant further investigation. One key challenge lies in optimizing the computational efficiency of the SURF-based retrieval process, which may introduce delays in scenarios requiring real-time communication. Additionally, while the system effectively eliminates metadata transmission, future work could explore alternative methods to further reduce reliance on synchronized datasets, enhancing flexibility in dynamic communication environments. Addressing these aspects could improve the practicality of the C-HIDE framework in scenarios with stringent performance requirements, such as intelligence sharing and emergency communications. Future research could also focus on enhancing the system's resilience against emerging steganalysis techniques and more sophisticated image processing attacks. Integrating advanced machine learning models to improve feature extraction and retrieval accuracy under extreme conditions is a promising direction. Furthermore, expanding the framework to support multimedia data types beyond images, such as video and audio, could broaden its applicability. By addressing these avenues, the C-HIDE system has the potential to further establish itself as a versatile and robust solution for confidential data transmission in an increasingly interconnected digital landscape. We aim to enhance the C-HIDE framework by integrating an adaptive hybrid model that combines transform domain steganography with deep generative adversarial networks (GANs), facilitating dynamic feature extraction and optimizing security while minimizing computational overhead. Incorporating lightweight convolutional neural networks (CNNs) can improve the efficiency of Speeded-Up Robust Features (SURF), reducing computational complexity without sacrificing retrieval accuracy. Additionally, a fuzzy-based synchronization technique for Coverless Image Datasets (CIDs) can replace rigid dataset structures, enhancing scalability and adaptability to dynamic communication environments. Furthermore, embedding an adversarial training mechanism will allow the system to self-improve its resistance to steganalysis tools, ensuring long-term robustness in evolving cybersecurity landscapes.

ACKNOWLEDGMENT

This research project was funded by the Deanship of Scientific Research, Princess Nourah bint Abdulrahman University, through the Program of Research Project Funding After Publication, grant No (44-PRFA-P-114).

REFERENCES

[1] K. Muhammad, J. Ahmad, S. Rho, and S. W. Baik, "Image steganography for authenticity of visual contents in social networks," *Multimedia Tools Appl.*, vol. 76, no. 18, pp. 18985–19004, Sep. 2017.

[2] R. Zhang, S. Dong, and J. Liu, "Invisible steganography via generative adversarial networks," *Multimedia Tools Appl.*, vol. 78, no. 7, pp. 8559–8575, Apr. 2019.

[3] J. Ye, J. Ni, and Y. Yi, "Deep learning hierarchical representations for image steganalysis," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2545–2557, Nov. 2017.

[4] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, "Reversible image steganography scheme based on a U-Net structure," *IEEE Access*, vol. 7, pp. 9314–9323, 2019.

[5] O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Doha, Qatar, Feb. 2020, pp. 131–135.

[6] A. A. Abdelwahab and L. A. Hassaan, "A discrete wavelet transform based technique for image data hiding," in *Proc. Nat. Radio Sci. Conf.*, Mar. 2008, pp. 1–9.

[7] X. Duan, W. Wang, N. Liu, D. Yue, Z. Xie, and C. Qin, "StegoPNet: Image steganography with generalization ability based on pyramid pooling module," *IEEE Access*, vol. 8, pp. 195253–195262, 2020.

[8] W. Tang, S. Tan, B. Li, and J. Huang, "Automatic steganographic distortion learning using a generative adversarial network," *IEEE Signal Process. Lett.*, vol. 24, no. 10, pp. 1547–1551, Oct. 2017.

[9] X. Zhao, C. Yang, and F. Liu, "On the sharing-based model of steganography," in *Proc. 19th Int. Workshop*, Melbourne, VIC, Australia, Nov. 2021, pp. 94–105.

[10] G. Swain, "Very high capacity image steganography technique using quotient value differencing and LSB substitution," *Arabian J. Sci. Eng.*, vol. 44, no. 4, pp. 2995–3004, Apr. 2019.

[11] H.-T. Wu, J.-L. Dugelay, and Y.-M. Cheung, "A data mapping method for steganography and its application to images," in *Proc. 10th Int. Workshop Inf. Hiding*, Santa Barbara, CA, USA. Berlin, Germany: Springer, May 2008, pp. 236–250.

[12] S. Jing-Yu, C. Hong, W. Gang, G. Zi-Bo, and H. Zhang, "FPGA image encryption-steganography using a novel chaotic system with line equilibria," *Digit. Signal Process.*, vol. 134, Apr. 2023, Art. no. 103889.

[13] B. Wei, X. Duan, and H. Nam, "Image steganography with deep learning networks," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Jeju Island, (South) Korea, Oct. 2022, pp. 1371–1374.

[14] L. Liu, L. Tang, and W. Zheng, "Lossless image steganography based on invertible neural networks," *Entropy*, vol. 24, no. 12, p. 1762, Dec. 2022.

[15] P. Chen and W.-E. Wu, "A modified side match scheme for image steganography," *Int. J. Appl. Sci. Eng.*, vol. 7, no. 1, pp. 53–60, Oct. 2009.

[16] N. Subramanian, I. Cheheb, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "End-to-end image steganography using deep convolutional autoencoders," *IEEE Access*, vol. 9, pp. 135585–135593, 2021.

[17] Y. Lan, F. Shang, J. Yang, X. Kang, and E. Li, "Robust image steganography: Hiding messages in frequency coefficients," in *Proc. AAAI Conf. Artif. Intell.*, vol. 37, 2023, pp. 14955–14963.

[18] Z. Yang, K. Chen, K. Zeng, W. Zhang, and N. Yu, "Provably secure robust image steganography," *IEEE Trans. Multimedia*, vol. 26, pp. 5040–5053, 2024.

[19] K. Karampidis, E. Kavallieratou, and G. Papadourakis, "A review of image steganalysis techniques for digital forensics," *J. Inf. Secur. Appl.*, vol. 40, pp. 217–235, Jun. 2018.

[20] D. Megías and D. Lerch-Hostalot, "Subsequent embedding in targeted image steganalysis: Theoretical framework and practical applications," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 2, pp. 1403–1421, Mar. 2023.

[21] Z. Lin, Y. Huang, and J. Wang, "RNN-SM: Fast steganalysis of VoIP streams using recurrent neural network," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1854–1868, Jul. 2018.

[22] Z. Zhou, H. Sun, R. Harit, X. Chen, and X. Sun, "Coverless image steganography without embedding," in *Proc. 1st Int. Conf. Cloud Comput. Secur. (ICCCS)*, vol. 1. Nanjing, China: Springer, Aug. 2015, pp. 123–132.

[23] Q. Liu, X. Xiang, J. Qin, Y. Tan, J. Tan, and Y. Luo, "Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping," *Knowl.-Based Syst.*, vol. 192, Mar. 2020, Art. no. 105375.

[24] V. Kumar and D. Kumar, "Digital image steganography based on combination of DCT and DWT," in *Proc. Int. Conf.*, Kochi, India. Berlin, Germany: Springer, Sep. 2010, pp. 596–601.

[25] X. Zhang, F. Peng, and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," *IEEE Trans. Multimedia*, vol. 20, no. 12, pp. 3223–3238, Dec. 2018.

[26] S. Zheng, L. Wang, B. Ling, and D. Hu, "Coverless information hiding based on robust image hashing," in *Intelligent Computing Methodologies*, vol. 13. Cham, Switzerland: Springer, 2017, pp. 536–547.

[27] C. Yuan, Z. Xia, and X. Sun, "Coverless image steganography based on SIFT and BOF," *J. Internet Technol.*, vol. 18, no. 2, pp. 435–442, Mar. 2017.

[28] Y. Luo, J. Qin, X. Xiang, and Y. Tan, "Coverless image steganography based on multi-object recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 7, pp. 2779–2791, Jul. 2021.

[29] X. Hu, S. Li, Q. Ying, W. Peng, X. Zhang, and Z. Qian, "Establishing robust generative image steganography via popular stable diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 8094–8108, 2024.

[30] M. Gabr, A. Diab, H. T. Elshoush, Y.-L. Chen, L. Y. Por, C. S. Ku, and W. Alexan, "Data security utilizing a memristive coupled neural network in 3D models," *IEEE Access*, vol. 12, pp. 116457–116477, 2024.

[31] F. Li, Y. Sheng, K. Wu, C. Qin, and X. Zhang, "LiDiNet: A lightweight deep invertible network for image-in-image steganography," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 8817–8831, 2024.

[32] W. Alexan, E. Mamdouh, A. Aboshousha, Y. S. Alsahafi, M. Gabr, and K. M. Hosny, "Stegocrypt: A robust tri-stage spatial steganography algorithm using TLM encryption and DNA coding for securing digital images," *IET Image Process.*, vol. 18, no. 13, pp. 4189–4206, Nov. 2024.

[33] Q. Liu, X. Xiang, J. Qin, Y. Tan, and Q. Zhang, "A robust coverless steganography scheme using camouflage image," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 6, pp. 4038–4051, Jun. 2022.

[34] Y. Luo, J. Qin, X. Xiang, Y. Tan, Q. Liu, and L. Xiang, "Coverless real-time image information hiding based on image block matching and dense convolutional network," *J. Real-Time Image Process.*, vol. 17, no. 1, pp. 125–135, Feb. 2020.

[35] X. Chen, Z. Zhang, A. Qiu, Z. Xia, and N. N. Xiong, "Novel coverless steganography method based on image selection and StarGAN," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 219–230, Jan. 2022.

[36] S. Biswas, S. Debnath, and R. K. Mohapatra, "Coverless image steganography based on DWT approximation and pixel intensity averaging," in *Proc. 7th Int. Conf. Trends Electron. Informat. (ICOEI)*, Tirunelveli, India, Apr. 2023, pp. 1554–1561.

[37] Q. Li, X. Wang, X. Wang, B. Ma, C. Wang, and Y. Shi, "An encrypted coverless information hiding method based on generative models," *Inf. Sci.*, vol. 553, pp. 19–30, Apr. 2021.

[38] F. Li, C. Liu, Z. Dong, Z. Sun, and W. Qian, "A robust coverless image steganography algorithm based on image retrieval with SURF features," *Secur. Commun. Netw.*, vol. 2024, pp. 1–22, May 2024.

[39] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless image steganography: A survey," *IEEE Access*, vol. 7, pp. 171372–171394, 2019.

[40] J. Hemalatha, M. Sekar, C. Kumar, A. Gutub, and A. K. Sahu, "Towards improving the performance of blind image steganalyzer using third-order SPAM features and ensemble classifier," *J. Inf. Secur. Appl.*, vol. 76, Aug. 2023, Art. no. 103541.

[41] A. Dwaik and Y. Belkhouche, "Enhancing the performance of convolutional neural network image-based steganalysis in spatial domain using spatial rich model and 2D Gabor filters," *J. Inf. Secur. Appl.*, vol. 85, Sep. 2024, Art. no. 103864.

[42] M. Keizer, Z. Geradts, and M. Kombrink, "Forensic video steganalysis in spatial domain by noise residual convolutional neural network," 2023, *arXiv:2305.18070*.

[43] T. Denemark, V. Sedighi, V. Holub, R. Cogranne, and J. Fridrich, "Selection-channel-aware rich model for steganalysis of digital images," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2014, pp. 48–53.

[44] Y. Qian, J. Dong, W. Wang, and T. Tan, "Deep learning for steganalysis via convolutional neural networks," *Proc. SPIE*, vol. 9409, Mar. 2015, Art. no. 94090J.

[45] P. Bas, T. Filler, and T. Pevnỳ, "'Break our steganographic system': The ins and outs of organizing BOSS," in *Proc. Int. Workshop Inf. Hiding*. Berlin, Germany: Springer, 2011, pp. 59–70.

[46] A. Team. (2019). *Anonymized Labeled Alaska Stego Algorithm Database*. Accessed: Jan. 7, 2025. [Online]. Available: https://alaska.utt.fr/

[47] G. Schaefer and M. Stich, "UCID: An uncompressed color image database," *Proc. SPIE*, vol. 5307, pp. 472–480, Dec. 2003, Accessed: Jan. 7, 2025. [Online]. Available: https://www.sites.google.com/site/uciddataset/

[48] T.-Y. Lin, M. Maire, and S. Belongie. (2014). *Microsoft Common Objects in Context (MS-COCO)*. Accessed: Jan. 7, 2025. [Online]. Available: https://cocodataset.org/

[49] G. Griffin, A. Holub, and P. Perona. (2007). *The Caltech-256 Object Category Dataset*. Accessed: Jan. 7, 2025. [Online]. Available: http://www.vision.caltech.edu/Image_Datasets/Caltech256/

[50] T. Gloe and R. Böhme. (2010). *The Dresden Image Database for Benchmarking Digital Image Forensics*. Accessed: Jan. 7, 2025. [Online]. Available: https://www.kaggle.com/datasets/micscodes/dresden-image-database

[51] H. Jegou, M. Douze, and C. Schmid, "Inria holidays dataset: A database for image retrieval benchmarking," *J. Image Retr.*, 2008, Accessed: Jan. 7, 2025. [Online]. Available: https://lear.inrialpes.fr/people/jegou/data.php.html

[52] J. Deng, W. Dong, and R. Socher. (2009). *Imagenet: A Large-Scale Hierarchical Image Database*. Accessed: Jan. 7, 2025. [Online]. Available: https://www.image-net.org/

[53] A. Kuznetsova, H. Rom, and N. Alldrin. (2020). *Open Images Dataset: A Large Collection of Annotated Images*. Accessed: Jan. 7, 2025. [Online]. Available: https://storage.googleapis.com/openimages/web/index.html

[54] J. Z. Wang, J. Li, and G. Wiederhold, "SIMPLIcity: Semantics-sensitive integrated matching for picture libraries," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 23, no. 9, pp. 947–963, Sep. 2001. Accessed: Jan. 7, 2025. [Online]. Available: https://wang.ist.psu.edu/docs/related/

[55] L. Zou, J. Li, W. Wan, Q. M. J. Wu, and J. Sun, "Robust coverless image steganography based on neglected coverless image dataset construction," *IEEE Trans. Multimedia*, vol. 25, pp. 5552–5564, 2023.

SAHAR A. EL-RAHMAN (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees from Benha University, Cairo, Egypt, in 1997, 2003, and 2008, respectively. She is currently an Associate Professor with the Electrical Engineering Department-Computer Systems Program, Faculty of Engineering-Shoubra, Benha University. She has been recognized as one of the Top 2% of Scientists Worldwide in 2024 by Stanford University's ranking. Her research interests include artificial intelligence, machine learning, information security, distributed systems, computer vision, human–computer interaction, big data, and cloud computing.

AHMED E. MANSOUR received the B.Sc. degree from Alexandria University, Alexandria, Egypt, in 1999, the master's Diploma degree in computer science from the Faculty of Graduate Studies of Statistical Research, Cairo University, Egypt, in 2012, and the M.Sc. degree in electrical communication and the Ph.D. degree in computer vision applications from the Faculty of Engineering, Ain Shams University, Cairo, Egypt, in 2016 and 2022, respectively. With a distinguished career in research and academia, served as the Chief Research Officer (CRO) in governmental research and development, leading various innovative projects and advancing the field of defense technology. Currently, he is an Assistant Professor with the Faculty of Computer Science, Misr International University.

LEILA JAMEL received the Engineering degree in computer sciences and the Ph.D. degree in computer sciences and information systems. She was the Program Leader of the IS Program and the ABET and NCAAA Accreditation Committees, CCIS, Princess Nourah bint Abdulrahman University (PNU), Saudi Arabia. She was the Head of the Department of Information Systems Security of the Premier Ministry of Tunisia. She is currently an Associate Professor with the College of Computer and Information Sciences, PNU. She is also a Researcher with the RIADI Laboratory, Tunisia. Her research interests include business process modeling, business process management/re-engineering and quality, context-awareness in business models, data sciences, ML, process mining, e-learning, and software engineering. She was a member of the Steering and Scientific Committees of the IEEE International Conference on Cloud Computing. She is a reviewer of many international journals and conferences.

MANAL ABDULLAH ALOHALI received the Ph.D. degree in computer science from the University of Plymouth, U.K. She is currently an Assistant Professor with the Information Systems Department, College of Computer and Information Sciences (CCIS), Princess Nourah bint Abdulrahman University (PNU), Saudi Arabia. She is also the Dean of CCIS. Her research interests include information systems, machine learning, and cyber security. She received the PNU Research Excellence Award.

MOHAMED SEIFELDIN received the B.S. degree in electrical engineering from Alexandria University, Alexandria, Egypt, in 2007, the M.S. degree in electronics and electrical communication engineering from Ain Shams University, Cairo, Egypt, in 2016, and the Ph.D. degree in cybersecurity from the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada. His M.S. research was in the field of modern cryptography. In addition, he is a Certified Higher Education Lecturer in Canada and the USA, since he received the Learning and Teaching in Higher Education (LATHE) Diploma from the University of Victoria, BC, Canada. LATHE Diploma is an accredited certificate in learning and teaching in North America (the USA and Canada). He is also a Certified Ethical Hacker (CIEH), Certified Penetration Tester Professional (CIPENT), and EC-Council Certified Instructor (CIEI) for teaching the cybersecurity professional courses provided by EC-Council.

YASMIN ALKADY received the B.Sc. degree in computer and control engineering from Suez Canal University, in 2007, and the M.Sc. and Ph.D. degrees in computer and control engineering from Port Said University, in 2014 and 2020, respectively. He is currently an Assistant Professor with the Faculty of Computer Science, Misr International University, Egypt.