An Analytical Review of Steganography: Traditional Methods, Emerging Hybrids, and Deep Learning Innovations

VARNA O V[1], SARANG C[2], SHREYA SREEKUMAR[3], ALKA SAJEEVAN P[4], SUBHAGA K[5]
[1,2,3,4] *Department of Computer Science and Engineering (Cyber Security) Vimal Jyothi Engineering College, Chemperi, Kannur*
[5]*Assistant Professor Department of Computer Science and Engineering (Cyber Security) Vimal Jyothi Engineering College, Chemperi, Kannur*

***Abstract*—Image steganography is a popular method for hiding information in plain text, but it is still a challenge in digital security due to its high embedding capacity, high fidelity, and robustness against compression. In this paper, we present a novel approach to image hiding that effectively balances three long-standing challenges, namely, embedded capacity and image fidelity. We explore the use of deep convolutional neural networks (DCGANs) to address the dual challenge of maintaining high- capacity hiding and ensuring strong fidelity against modern steganalysis techniques. This paper introduces a hybrid approach that integrates edge detection with Convolutional Generative Adversarial Networks (CNNs), leveraging the strengths of Pixel Value Differencing (PVD) and Least Significant Bit (LSB) substitution with the Histogram of Oriented Gradient (HOG) algorithm. Experimental evaluations across multiple datasets, including DIV2K, COCO, and ImageNet, demonstrate that StegTransX significantly outperforms state-of-the-art methods in single-image and multi-image hiding tasks, achieving higher PSNR, SSIM, and generalization capability while requiring fewer parameters and FLOPs. The results demonstrate that the proposed method achieves competitive PSNR values and better imperceptibility compared to conventional PVD- and LSB-only techniques, demonstrating that edge detection and CNN enhance- ment are a viable direction for concealing data while maintaining visual fidelity while maintaining invisibility. The study explains the mathematical foundation of RSA, particularly its reliance on large prime factorization and modular exponentiation, and demonstrates its effectiveness in ensuring confidentiality and integrity of digital communication.**

***Index Terms*—Steganography, Information Hiding, Least Signifi- can't Bit, Transform-Based Methods, Deep Learning, Generative Adversarial Networks, Robustness and Imperceptibility.**

I. INTRODUCTION

Steganography, derived from the Greek words steganos (covered) and graphein (writing), is the art and science of concealing information in such a way that its very existence remains undetected. Unlike cryptography, which secures the content of a message by transforming it into an unreadable format, steganography ensures that the presence of the mes- sage is invisible to adversaries, thereby providing an additional layer of covert security. This dual role of hiding and protecting makes steganography an increasingly vital research domain in the era of widespread digital communication, where threats to data privacy, unauthorized surveillance, and cyberattacks are rapidly escalating. Traditional approaches such as Least Significant Bit (LSB) substitution served as the foundation of digital steganography, offering simplicity, high capacity, and ease of implementation, yet they were often vulnerable to compression, noise, and steganalysis attacks. To address these limitations, frequency-domain and transform-domain techniques such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Hadamard Transform (DHT) were introduced, improving resilience by embedding information in perceptually less sensitive regions of multime- dia. These innovations laid the groundwork for adaptive meth- ods that exploit image features like edges and textures, and further encouraged the integration of cryptographic algorithms such as RSA and ECC to

strengthen data protection before embedding. Together, these developments reflect the steady evolution of steganography from simple bit-level techniques to sophisticated hybrid frameworks designed to balance capacity, imperceptibility, and robustness.

In recent years, the rapid advancement of artificial intelli- gence and deep learning has transformed the field, bringing a new generation of intelligent steganographic models capable of learning optimal hiding strategies directly from data. Con-

volutional Neural Networks (CNNs), Generative Adversarial Networks (GANs), and attention-based models have been employed to achieve adaptive embedding, high payload capac- ity, and near-perfect imperceptibility, while resisting detection from state-of-the-art steganalysis tools. For example, GAN-based frameworks generate stego-images that are statistically indistinguishable from natural images, while lightweight ar- chitectures such as StegTransX enhance practicality by main- taining high robustness against compression without exces- sive computational cost. At the same time, research into coverless steganography and text-based schemes demonstrates innovative directions that avoid direct modification of content, thereby reducing detectability further. Despite these advances, challenges remain—particularly the inherent trade-offs be- tween invisibility, robustness, and capacity, as well as the demand for computational efficiency in real-world applications such as secure communication, digital forensics, and copyright protection. This literature survey reviews a comprehensive set of models spanning classical, hybrid, and deep learn- ing paradigms, highlighting their key strengths, limitations, and performance characteristics. Through this comparative exploration, the survey seeks to identify trends, unresolved challenges, and promising pathways toward the development of secure, efficient, and future-ready steganographic systems.

II. LITERATURE REVIEW

A. StegTransX: Lightweight Deep Steganography with JPEG Resistance

The paper StegTransX: [1] presents a novel approach to image steganography that effectively balances three long- standing challenges: embedding capacity, image fidelity, and robustness against compression. Unlike traditional techniques such as LSB substitution and QIM, which are limited in both security and capacity, or heavy deep-learning methods like HiNet and DeepMIH that require high computational re- sources, StegTransX introduces a lightweight encoder–decoder network enhanced with TransX blocks and channel–spatial feature fusion. This design allows it to capture both local and global image features while maintaining computational efficiency. The integration of multiscale and restriction loss functions ensures high visual quality of stego images and accurate recovery of hidden content, while the JPEG compres- sion module strengthens resistance to real-world transmission scenarios.

Experimental evaluations across multiple datasets, including DIV2K, COCO, and ImageNet, demonstrate that StegTransX significantly outperforms state-of-the-art methods in single- image and multi-image hiding tasks, achieving higher PSNR, SSIM, and generalization capability while requiring fewer parameters and FLOPs. Its robustness against advanced ste- ganalyzers shows strong security, with detection rates close to random guessing under normal capacity settings. However, the model's resilience drops under high-intensity noise attacks, and the trade-off between embedding more images and main- taining security remains unresolved. Overall, StegTransX rep- resents a substantial advancement in practical deep steganog- raphy, offering a promising balance of high-capacity hiding, compression resistance, and lightweight design, while high- lighting future research opportunities in noise resilience and capacity security. optimization.

B. CSNTSteg: Text Steganography with Color Spacing Nor- malization

The CSNTSteg model takes a different direction by focusing on text steganography, a domain less explored compared to images. It introduces a novel strategy that combines RGB font color coding, character spacing normalization, and Huffman compression to significantly enhance payload while preserving the invisibility of the cover medium [2]. By normalizing character spacing and leveraging font colors, the model en- sures that the stego text remains visually identical to ordinary text, avoiding suspicion.

Additionally, Huffman compression maximizes the amount of secret data that can be hidden, leading to a substantial increase in capacity up to 98.85% higher than conventional text steganography techniques. The results confirm that this method not only enhances embedding efficiency but also maintains invisibility, proving that structural and formatting-based features of text can be successfully utilized for covert communication.

On the other hand, the scheme is heavily dependent on fonts, color schemes, and platform rendering, which limits its universality across devices and languages. Text as a cover medium is inherently less robust than images or audio, as it can be easily reformatted, stripped of styling, or altered by system conversions, which would destroy the hidden data. More- over, the method's applicability in multilingual or plain-text- only environments remains limited. Nonetheless, CSNTSteg significantly advances the field by showing that text when carefully optimized through spacing normalization and color encoding—can achieve both high invisibility and capacity. Its contribution is important in scenarios where image carriers are not feasible, expanding the scope of steganography research into new modalities, though robustness across platforms re- mains an area for further improvement.

C. High-Capacity Image Steganography Using Discrete Hadamard Transform (DHT)

This study introduces a transform-domain image steganog- raphy method using the Discrete Hadamard Transform (DHT), which is computationally efficient since it relies only on additions and subtractions. The authors aim to overcome the limitations of spatial-domain embedding by using Hadamard coefficients as the embedding space, allowing for higher payload while keeping distortions minimal [3]. Compared to heavier transforms like DWT or DCT, DHT provides a lightweight yet effective platform for embedding. Experiments demonstrate that the method can achieve embedding rates of up to 8 bpp while maintaining strong imperceptibility, as evidenced by high PSNR values. The method thus proves effective in maximizing capacity without significantly com- promising the quality of the cover image, offering a simple yet efficient approach for practical applications requiring fast computation and high hiding ability.

Despite its strengths, the approach suffers from limited robustness under real-world attacks such as lossy compression, additive noise, and format conversions. Since the technique operates mainly in the transform coefficients without adaptive learning or error correction, it cannot withstand aggressive distortions. Furthermore, its adaptability across varied image domains and large-scale datasets is not thoroughly explored, leaving open questions about generalization. In comparison to deep-learning-based methods, the DHT-based scheme is lightweight and easy to implement, but it lacks the adaptive robustness of CNN or Transformer models. Overall, this paper contributes by showing that the Hadamard transform can provide high capacity and efficiency, but further research is needed to integrate robustness and adaptability features to make it suitable for real-world applications.

D. Edge Detection with CNN for Robust Image Steganography

This paper [4] proposes a hybrid approach that integrates edge detection with Convolutional Neural Networks (CNNs) for robust image steganography. The motivation behind the work lies in the fact that edge regions in an image are less sensitive to human visual perception, allowing secret data to be embedded without producing noticeable distortions. By applying edge detection techniques, the method identifies suitable embedding areas, and the CNN is used to adap- tively select features and optimize embedding for improved imperceptibility. This combination enables a balance between payload capacity and visual quality, while also strengthening resistance against steganalysis compared to classical spatial- domain techniques. The results show that the proposed system achieves competitive PSNR and SSIM values, highlighting that edge-aware embedding with CNN enhancement is a viable direction for concealing data while maintaining visual fidelity. However, while the model is effective in images with rich edge structures, it faces challenges with images that are smoother or have fewer high-frequency components, limit- ing embedding opportunities. The robustness evaluation also mainly covers traditional steganalysis techniques, leaving open questions about how the method withstands modern deep- learning-based attacks. Additionally,

while the CNN adds adaptability, it increases computational complexity, which could restrict its use in low-resource environments. Overall, this paper presents an important step in combining tradi- tional edge-based embedding with deep learning, showing improved imperceptibility and security, but still requiring en- hancements in generalization, resilience to diverse distortions, and lightweight deployment.

E. Deep Steganography Using Generative Models for En- hanced Security and Capacity

This paper explores the use of generative deep learning models to address the dual challenge of maintaining high em- bedding capacity and ensuring robustness in image steganog- raphy. Traditional methods like LSB and transform-domain embedding struggle to balance imperceptibility, payload, and security, while earlier deep-learning methods often require heavy computation and remain vulnerable to compression and detection. The proposed approach leverages GAN-based frameworks and adversarial training to generate stego images that are visually indistinguishable from cover images while securely embedding large payloads. By using the generative model's capacity for feature learning and distribution match- ing, the method enhances invisibility, producing stego images that align closely with natural image statistics [5].

Experiments demonstrate improved payload capacity, re- silience to steganalysis, and fidelity compared to existing CNN-based hiding schemes, showing the potential of gen- erative models as a transformative approach in this do- main. Despite its strengths, the method also faces limitations. Generative models, particularly GANs, are computationally expensive to train, requiring large datasets and fine-tuned optimization for stability. While the approach shows resilience against traditional steganalysis, its robustness against mod- ern deep-learning-based detectors remains an open question. Furthermore, like many GAN-based solutions, issues such as mode collapse and training instability can affect consistency in performance. Compared to lightweight approaches such as StegTransX or transform-based methods like DHT, this framework offers higher flexibility and realism but at the cost of increased computational complexity and training resources. Overall, this paper significantly contributes to the advancement of steganography by showing that generative modeling can bridge the gap between capacity and invisibility, though further work is needed to enhance efficiency, stability, and universal robustness.

F. Research and Implementation of RSA Algorithm for En- cryption and Decryption

This paper focuses on the design and implementation of the RSA algorithm, one of the most widely used public-key cryptosystems for secure communication. The study explains the mathematical foundation of RSA, particularly its reliance on large prime factorization and modular exponentiation, and demonstrates its effectiveness in ensuring confidentiality and integrity of digital communication. The implementation showcases how RSA can be practically applied in encrypting and decrypting sensitive information, while also highlight- ing key trade-offs in speed and computational complexity. Compared to symmetric key methods, RSA offers higher security since it does not require sharing a secret key, making it well-suited for authentication and digital signatures [6]. However, the paper also acknowledges certain limitations. RSA is computationally heavy, especially when dealing with large datasets or when implemented in resource-constrained environments. Its security depends on the hardness of integer factorization, which might be threatened by advancements in quantum computing. Compared to steganographic approaches, RSA provides cryptographic protection but does not hide the existence of the message, potentially drawing suspicion. Thus, while RSA remains foundational in cybersecurity, combining it with steganography or hybrid cryptographic models may offer enhanced secrecy and robustness for future applications.

G. Information Hiding: A Survey

This survey provides an extensive overview of the three main approaches to information hiding: steganography, cryp- tography, and watermarking, and how they complement one another in digital security [7]. It introduces steganography as the art of concealing the existence of a message, cryp- tography as securing message content through encryption, and watermarking as embedding ownership or authentication marks. The paper

systematically classifies existing techniques, focusing on spatial-domain and transform-domain methods, and explains their typical strengths, weaknesses, and use cases. For example, spatial-domain methods offer high capacity and simplicity but are less robust, whereas transform-domain methods are more resistant to compression and attacks at the cost of reduced embedding efficiency. By framing these categories, the survey not only explains technical foundations but also highlights the broad application areas of information hiding, including copyright protection, authentication, covert communications, and secure digital watermarking. The authors also discuss the key challenges in information hiding, most notably the trade-off between capacity, imperceptibility, and robustness. Increasing one factor often decreases the others, making it difficult to achieve an ideal solution. They also identify vulnerabilities to statistical and machine-learning-based steganalysis, which can reveal hidden information de- spite careful embedding. While the survey does not present new algorithms or experimental results, it makes a strong contribution by offering a theoretical framework and classification scheme that later works have continued to refine. Compared to practical analyses such as tool-based reviews, this survey sets the stage for future innovation, including deep- learning-based steganography, which attempts to dynamically balance capacity and robustness. Overall, the paper remains a significant contribution in providing a structured understanding of the field, serving as a reference point for both early researchers and advanced work.

H. Exploring Steganography: Seeing the Unseen

[8] This foundational paper introduces steganography in an accessible, practical way, positioning it as the art of "covered writing" and contrasting it with cryptography. It explains the motivation for steganography hiding the very existence of communication to avoid suspicion and discusses various techniques, from simple Least Significant Bit (LSB) insertion to masking, filtering, and transform-domain methods. Impor- tantly, it analyzes how different image formats, such as GIF and JPEG, influence the embedding process, especially under lossy compression. The paper also explores practical software implementations like EzStego and S-Tools, demonstrating how steganographic concepts translate into real-world applications. Its clarity and inclusion of examples make it a crucial early reference that shaped the way digital steganography was introduced to researchers and practitioners alike.

However, as an early contribution (1998), the paper is lim- ited by its time. The methods it reviews are primarily simple spatial-domain approaches, which modern steganalysis tech- niques can easily detect through statistical or deep-learning- based analysis. It does not address contemporary challenges such as compression robustness, adaptive embedding, or the use of neural networks for improved security. Nonetheless, its value lies in its pedagogical strength and historical sig- nificance. By offering practical insight into early tools and techniques, it remains a cornerstone reference that shows how steganography evolved from basic LSB approaches into today's sophisticated deep-learning-driven methods. While dated, its role as a foundational text makes it indispensable in any comprehensive literature survey.

I. Analysis of Current Steganography Tools: Classifications & Features

This paper provides a comprehensive evaluation of steganography tools available at the time of its publication, offering a bridge between theoretical research and practical applications. The authors categorize over 200 tools into five classes: spatial-domain, transform-domain, document-based, file-structure-based, and spread-spectrum methods. Each cat- egory is explained with representative examples such as S- Tools, JSteg, OutGuess, and F5, alongside their strengths and vulnerabilities. For instance, spatial-domain tools are praised for their simplicity and high embedding capacity but are prone to detection by statistical steganalysis. Transform-domain tools like F5 are highlighted as more robust, particularly against compression, though they embed less data and are computa- tionally heavier. By systematically documenting the features, capacities, and weaknesses of these tools, the paper provides a taxonomy that is invaluable for both researchers and practi- tioners.

The strength of the paper lies in its comparative framework, which allows readers to evaluate tools based on impercepti- bility, capacity, robustness, and detectability [9]. This level of categorization provides

a practical reference point for selecting tools depending on the application, whether the goal is covert communication, digital watermarking, or copyright protec- tion. However, being published in 2006, the work does not account for advances in deep-learning-based steganography or adversarial approaches, which dominate the modern field. Still, it remains an important milestone in documenting the evolution of steganographic tools, marking the transition from simple LSB-based systems to more complex transform-domain methods. Its enduring contribution lies in offering a benchmark for tool evaluation that continues to inform research, even as new AI-driven methods redefine the landscape.

J. Implementation of LSB Steganography and Its Evaluation for Various Bits

This paper explores the classical Least Significant Bit (LSB) technique in image steganography, focusing on its ability to conceal data while maintaining imperceptibility. The authors provide a comprehensive explanation of how LSB embedding works and apply it to different image formats such as BMP, PNG, and GIF. They emphasize that images, due to their large storage and redundancy, are well-suited for information hiding, and demonstrate that modifying the least significant bits of pixel values introduces only minimal distortions that are imperceptible to the human eye. By experimenting with embedding across 2, 4, and 6 LSBs, the paper shows how varying the number of bits directly affects the balance be- tween payload capacity and visual quality. Standard evaluation metrics like MSE (Mean Squared Error), PSNR (Peak Signal- to-Noise Ratio), and histogram analysis are used to assess the quality of stego images, providing a systematic understanding of LSB performance across different conditions [10].

However, the study also underscores the limitations of basic LSB steganography, particularly its vulnerability to common image-processing operations such as cropping, compression, and filtering, as well as its susceptibility to steganalysis techniques that can detect hidden patterns. While the approach is simple, efficient, and capable of hiding substantial data, its lack of robustness reduces its applicability in secure real- world communication. The paper concludes that although LSB substitution is foundational to image steganography, its direct application is best suited for scenarios where high capacity is prioritized over strong resistance to attacks. This work contributes significantly by offering a structured evaluation of LSB variations and acts as a baseline reference for researchers developing more advanced, secure techniques.

K. A New Approach for LSB Based Image Steganography Using Secret Key

[11] This paper advances the LSB technique by introduc- ing a secret key-based embedding mechanism that improves the security and confidentiality of hidden data. Instead of directly embedding the secret bits into fixed pixel positions, the proposed approach incorporates a secret key and XOR operations to dynamically decide whether to embed data in the green or blue channel of each pixel. This randomization increases the difficulty for attackers to retrieve the hidden message without knowledge of the key, thereby addressing one of the major weaknesses of conventional LSB methods. The authors emphasize that by adding this layer of unpredictability, the approach not only hides the data but also strengthens its protection against unauthorized access. The experimental evaluation reports very high PSNR values (above 53 dB), confirming that the stego images are visually indistinguishable from the cover images, even after embedding.

The strength of this method lies in its ability to maintain a strong balance between imperceptibility, payload capacity, and enhanced security compared to traditional LSB embedding. By incorporating the secret key, the system mitigates straight- forward statistical detection methods that exploit predictable embedding patterns in standard LSB approaches. However, the study also notes that robustness against advanced steganalysis tools and aggressive image-processing attacks remains a chal- lenge, as the technique still operates in the spatial domain. Nonetheless, the paper represents a valuable progression in LSB steganography research by demonstrating how simple cryptographic principles can be combined with data hiding techniques to create a more secure and practical system. This work not only strengthens traditional LSB embedding but also paves the way for further hybrid approaches that integrate steganography with cryptographic security

mechanisms.

L. A Novel Image Steganography Method via Deep Convolu- tional Generative Adversarial Networks

This paper presents a modern approach to image steganogra- phy by leveraging the power of Deep Convolutional Generative Adversarial Networks (DCGANs). The authors emphasize the limitations of traditional techniques, such as LSB or transform domain approaches, which often suffer from low embedding capacity, detectability by steganalysis, or degradation in image quality. By employing GANs, the proposed model learns the distribution of natural images and generates stego images that are visually indistinguishable from authentic cover images, thereby enhancing both imperceptibility and security [12]. The architecture integrates a generator–discriminator framework, where the generator embeds secret data into images, and the discriminator evaluates the authenticity of the output, creating a robust adversarial training loop that continually improves the embedding strategy.

The experimental results demonstrate that this GAN based model outperforms traditional methods in terms of payload capacity, robustness, and resistance against modern steganaly- sis techniques. The produced stego images exhibit high visual fidelity with minimal distortion, as quantified by image quality metrics. However, while the method achieves significant im- provements, it faces challenges such as the computational cost of training deep networks, dependency on large datasets, and difficulties in maintaining consistent extraction accuracy under heavy distortions or attacks. Overall, this study highlights the potential of GANs in revolutionizing steganography, though it also signals the need for further optimization to make such approaches practical for large scale or real time applications.

M. A Coverless Plain Text Steganography Based on Character Features

This paper addresses the unique problem of hiding infor- mation in plain text, focusing on a "coverless" steganography approach that avoids modifying existing text. Instead, it maps secret information to naturallooking character features and constructs stego texts that appear completely benign. Unlike image and video- based steganography, text- based methods are constrained by low redundancy and higher detectability, since minor changes in text are easily noticeable. To overcome this, the authors propose exploiting the structural and stylistic variations of characters, such as different fonts, symbols, and orthographic properties, which can represent binary or coded data without altering the readability of the text.

The method demonstrates that coverless text steganography can achieve a balance between imperceptibility and embedding capacity while reducing the risk of exposure to linguistic steganalysis [13]. The results show an improvement in security since there is no direct modification of pre existing content, making detection more difficult. However, the approach is still limited by language dependency, constrained payload capacity, and potential issues with standardization across platforms and encodings. This study broadens the scope of steganography research by focusing on text, a domain often overlooked compared to images or audio, and it lays a foundation for future work in coverless and semantic based techniques that could further improve stealthiness and applicability in real- world secure communications.

N. An Adaptive Image Steganography Method Based on His- togram of Oriented Gradient and PVD-LSB Techniques

[14] This paper proposes an adaptive image steganography technique that combines the strengths of Pixel Value Differ- encing (PVD) and Least Significant Bit (LSB) substitution with the Histogram of Oriented Gradient (HOG) algorithm. The motivation stems from the observation that conventional PVD and LSB methods often ignore image content variations, leading to vulnerabilities in smooth regions and increased susceptibility to steganalysis. To address this, the authors introduce a method where the HOG descriptor analyzes edge directions in 2×2 blocks of the cover image, and secret data is embedded adaptively: the dominant edge pixels use PVD em- bedding, while non-dominant pixels employ LSB substitution. This hybrid embedding strategy leverages edge structures to conceal more data in complex regions while preserving visual quality in smoother areas.

Experimental evaluations on standard image datasets reveal that the proposed method achieves higher

embedding capacity and better imperceptibility compared to conventional PVD- and LSB-only techniques. Moreover, it demonstrates strong re-sistance to steganalysis methods such as RS analysis and pixel difference histogram attacks. The study's critical contribution lies in its adaptive embedding mechanism, which intelligently tailors the hiding strategy to local image features. Nonetheless, the method may face scalability challenges for color images or real-time applications, and performance could degrade under heavy compression or noise attacks. This paper reinforces the value of hybrid and adaptive strategies in image steganography and provides an important step toward secure, high-capacity embedding schemes.

O. An ECC/DCT-Based Robust Video Steganography Algo- rithm for Secure Data Communication

This paper introduces a video steganography approach that combines Discrete Cosine Transform (DCT) domain embed- ding with Error Correcting Codes (ECC), such as Ham- ming and BCH codes, to enhance robustness, embedding efficiency, and security [15]. The motivation comes from the shortcomings of existing video steganography schemes, which often struggle with low payload capacity, poor visual quality, or vulnerability to steganalysis. In the proposed framework, secret messages are first encrypted and error-corrected, then embedded into the DCT coefficients of video frames across Y, U, and V channels while excluding DC coefficients to min- imize perceptual distortion. By integrating ECC, the scheme ensures that even if some embedded bits are lost or altered due to compression, noise, or attacks, the original message can still be recovered accurately.

Experimental results demonstrate that the method achieves a high hiding ratio of around 27.53% while preserving good visual quality of stego videos. The system also shows re- silience against common attacks such as compression, filtering, and geometric transformations, outperforming several existing algorithms in robustness and payload capacity. However, the use of ECC introduces extra computational complexity, and the tradeoff between embedding rate and video quality still requires careful balancing. Furthermore, real-time deployment might be constrained by the encoding/decoding overhead. Despite these limitations, this paper provides a significant advancement in video steganography by showing how ECC and transform-domain techniques can work synergistically to achieve secure, high-capacity, and robust hidden communica- tion.

III. PROPOSED MODEL

The first set of works focuses on classical LSB-based steganography. In [10], the proposed model is a basic LSB substitution framework that evaluates embedding with 2, 4, and 6 bits per pixel. The model systematically studies the trade-off between capacity and imperceptibility, showing that increasing embedded bits enhances payload but reduces image quality and robustness against attacks. Similarly, LSB Based Image Steganography Using Secret Key [11] advances this by introducing a secret-key controlled LSB scheme that random- izes embedding between green and blue channels using XOR operations. This enhances security and unpredictability while retaining imperceptibility, though it still inherits vulnerabilities of spatial-domain embedding under compression or noise.

A second stream of research moves into survey and classifi- cation frameworks. Information Hiding: A Survey [7] proposes a taxonomy model classifying cryptography, watermarking, and steganography into a unified information-hiding frame- work, mapping trade-offs among robustness, capacity, and invisibility. Similarly, in Exploring Steganography: Seeing the Unseen [8] develops a general conceptual model of embedding and extraction processes, highlighting spatial, transform, and statistical approaches. These models are conceptual rather than algorithmic, serving as foundations for understanding steganographic workflows. In [9] they further develops a tool classification model, comparing existing software based on domains, file formats, capacity, robustness, and usability. While these works do not propose new hiding algorithms, they provide structured evaluation frameworks critical for identifying weaknesses in existing methods.

A related paper [6], steps slightly aside from steganog- raphy to propose an RSA encryption model. It implements asymmetric encryption using public and private keys, modular exponentiation, and large primes to secure the content of communication.

While not a steganographic system itself, it highlights the importance of cryptography in complementing steganography for stronger security. Its limitation lies in com- putational cost and vulnerability to quantum cryptanalysis, motivating hybrid encryption–steganography approaches.

The transform and hybrid-domain approaches attempt to overcome LSB's limitations. [14] proposes a hybrid adaptive embedding framework combining HOG-based edge analysis, PVD embedding in edge-rich regions, and LSB in smoother areas. This achieves higher imperceptibility and robustness against steganalysis but still struggles with lossy compression.

[15] extends to video, embedding data in DCT coefficients of YUV channels while applying Error-Correcting Codes (ECC) to ensure resilience against noise and compression. This model balances robustness, payload, and error tolerance, though with higher computational complexity. Similarly, [3] proposes a Hadamard transform-based embedding model that achieves up to 8 bits per pixel capacity while being computationally lightweight, though at the cost of robustness under compres- sion or noise.

In the text steganography domain, [13] proposes a coverless mapping model, where binary information is represented by character features (fonts, Unicode variations) without modi- fying existing text. This makes detection difficult but limits capacity and platform portability. Likewise, [2] introduces a color and spacing-based embedding model that uses RGB font color coding and spacing normalization, enhanced with Huffman compression for efficiency. It achieves high capacity and invisibility but is dependent on consistent rendering across platforms, limiting robustness.

The deep learning approaches push steganography forward.

[5] proposes a DCGAN-based model where a generator embeds data into images and a discriminator enforces im- perceptibility through adversarial training. This distribution- based approach reduces statistical anomalies and enhances robustness. [12] takes this further by embedding data during the image generation process itself, rather than modifying existing images, which significantly reduces detection risk. Both models outperform CNN-only methods but require large datasets and high computational resources.

Other hybrid deep models also emerge. [4] integrates edge detection with CNN-based adaptive embedding, exploiting human insensitivity to edge distortions. While it improves quality and robustness, it is less effective in smooth im- ages. [4] follows a similar principle, using edge regions for embedding with CNN refinement, ensuring balance between invisibility and robustness. Finally, [1] introduces a lightweight encoder–decoder network using TransX blocks (convolution + attention), Channel–Spatial Collaborative Fusion (CSCF), and multiscale losses. A key innovation is the inclusion of a JPEG compression simulation module during training, making it explicitly robust against compression. This model surpasses prior deep steganography systems like HiNet and StegFormer in both efficiency and robustness while remaining lightweight. Across these works, we observe an evolution from simple LSB-based spatial methods to hybrid transform methods, and finally to deep-learning–driven adaptive models. The classical methods basic LSB, key-based LSB, Hadamard transform pro- vide simplicity and high capacity but lack robustness. Survey and classification papers contribute valuable frameworks but do not propose operational hiding systems. Hybrid approaches HOG-PVD-LSB, ECC-DCT video balance imperceptibility and robustness but introduce computational costs. Text-based approaches coverless, CSNTSteg provide innovative alterna- tives for linguistic domains but remain constrained by payload and rendering issues. The deep-learning models GAN-based, generative, CNN–edge, robust CNN hybrid bring adaptability, improved security, and higher imperceptibility, though often with training overhead.

Among all, the StegTransX model stands out as the most advanced and practical [1]. It combines lightweight architec- ture, attention-enhanced feature fusion, adversarial robustness, and explicit resistance to JPEG compression—one of the most common real-world challenges. Compared to traditional and hybrid models, it offers a better balance of capacity, imperceptibility, and robustness, while being computationally efficient. Thus, StegTransX is the top model, representing the current best direction in steganography research among the surveyed works.

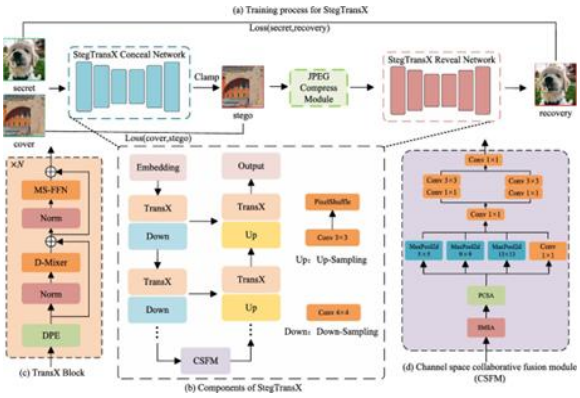

Fig. 1. Core Components of StegTransX [1]

IV. PERFORMANCE ANALYSIS AND COMPARISONS

The earliest works, such as in [10], demonstrated that classical LSB substitution can achieve high payloads with minimal complexity. However, performance analysis shows that its PSNR quickly drops as more bits are embedded, making it highly detectable. This confirms existing knowledge that spatial-domain methods offer capacity at the cost of robustness. Similarly, in the paper [11] enhanced security with secret-key randomization, but while it improved resistance to simple attacks, its overall robustness against compression and statistical steganalysis remained low. These works highlight that while LSB forms the foundation of image steganography, it is insufficient against modern detection techniques. Survey- based contributions do not propose algorithms but instead provide frameworks for performance comparison. Their key insight is that no single approach simultaneously maximizes capacity, robustness, and invisibility.

TABLE I COMPARISON TABLE

Ref.	Model	Key Strengths	Limitations
[1]	StegTransX Deep Learn- ing Steganography	Combines convolution and attention for better feature modeling. JPEG simulation during training ensures strong compression resilience. Lightweight compared to heavy models while retaining accuracy.	- Requires deep learning expertise. - Resilience beyond JPEG not tested. - Training still resource-intensive.
[2]	CSNTSteg Text Steganog- raphy	Huffman compression increases payload by nearly 99 percent. Maintains text invisibility across normal view- ing. - Simple to apply on structured documents.	- Depends on rendering consistency. - Vulnerable to formatting changes. - Lacks robustness across platforms.
[3]	Hadamard Transfor m Steganography	Provides extremely high payload capacity (up to 8 bpp). Lightweight computation using additions and subtractions only. - Easy to implement in practice.	Poor robustness against compression and noise. - No error correction applied. - Vulnerable to format conversions.
[4]	Edge Detection and CNN Steganography	Embeds data in edge areas to reduce visual artifacts. CNN adaptively optimizes embedding posi- tions. Improves invisibility compared to plain LSB.	- Performs poorly on smooth images. - Limited robustness under compression. Outperformed by advanced deep learning methods.
[5]	Privacy-Preserving Biometric Steganography	- Integrates biometric authentication with steganography for secure cloud access. Enhances privacy by ensuring that biometric templates are hidden during transmission and storage. Provides dual-layer security: biometric identity + steganographic concealment.	Model is tightly coupled to biometric systems, limiting broader applicability. Performance depends on both biometric recog- nition accuracy and steganographic robustness. Vulnerable to advanced biometric spoofing or if cloud security is compromised.

[6]	RSA Cryptographic Algo- rithm	Strong mathematical security model through public and private key operations. Widely adopted and trusted in modern secure communication protocols. Ensures confidentiality when used with steganography for dual protection.	Computationally heavy for large inputs and real-time data. Not a steganographic method, limited to encryption only. Vulnerable to attacks from quantum computing advancements.
[7]	Information Hiding Tax- onomy	Comprehensive overview of steganography, cryptography, and watermarking within information-hiding. Explains trade-offs and complementarity between different methods. Identifies research gaps and opportunities for improvement.	Entirely descriptive, without introducing an algorithm or framework. Lacks performance validation through experimental evaluation. Minimal direct contribution to practical implementation.
[8]	Exploring Steganography: Seeing the Unseen	Provides one of the earliest structured explanations of steganography concepts and methods. Introduces practical examples across image, text, and audio domains. Serves as a foundational tutorial reference for both researchers and practitioners.	Outdated relative to modern adaptive and deep learning techniques. Primarily descriptive — does not introduce a novel embedding algorithm. Limited scope compared to more comprehensive surveys such as Petitcolas et al. (2002).

TABLE II COMPARISON TABLE

Ref.	Model	Key Strengths	Limitations
[9]	Steganography Tool Classification	- Provides structured comparison of existing steganography tools, highlighting capacity, invisibility, and usability features. - Helps practitioners select appropriate tools for various real-world applications and environ- ments. Identifies missing features and trends in exist- ing tools, guiding future development.	- Does not propose or evaluate a new embedding algorithm, remaining analytical only. - Can quickly become outdated as new tools and frameworks emerge. - Limited practical contribution without experimental validation or case studies.
[10]	Basic LSB Steganography	- Very simple substitution method, easy to implement and useful as a baseline model for steganography analysis. - Flexible payload capacity achieved by altering number of least significant bits used for embedding information. Requires minimal computational resources, suitable for lightweight applications and teach- ing basic steganography concepts.	- Highly vulnerable to compression and noise, leading to rapid degradation of embedded data in real-world conditions. Increasing payload size reduces invisibility, making the stego-image more detectable by human eye or algorithms. Easily detected by statistical steganalysis tools due to predictable pixel modifications.
[11]	Key-Based LSB Steganography	Embedding positions randomized with secret key, significantly improving security compared to basic LSB substitution. Maintains high imperceptibility, often achiev- ing PSNR values above 53 dB with moderate payload. Lightweight implementation, offering an efficient extension over standard LSB without heavy computation.	Inherits spatial-domain weaknesses, fragile under compression, scaling, and filtering opera- tions. Security depends entirely on secrecy of the key, which if compromised exposes hidden data. Limited robustness against advanced steganal- ysis and hostile communication channels.
[12]	GAN-Based Image Steganography	GANs generate highly realistic stego-images close to natural distributions. Allows high payload without noticeable arti- facts. - Minimizes anomalies common in traditional substitution methods.	- Requires large training datasets. - GAN instability challenges training. Computationally demanding to train and de- ploy.

[13]	Coverless Text Steganography	• Avoids modifying text, preventing statistical detection. • Resistant to simple steganalysis tools and attacks. • Produces natural-looking stego-text with no visible anomalies.	Payload capacity remains very low compared to images. • Strongly dependent on platform-specific text rendering. • Poor cross-platform portability.
[14]	Adaptive HOG-PVD-LSB Steganography	• Content-aware embedding in edges increases invisibility. • Balances high payload with quality of stego-image. More secure compared to plain LSB embed- ding.	• Vulnerable to lossy compression such as JPEG. • Requires higher computational processing. • Less efficient for lightweight devices.
[15]	ECC/DCT Video Steganography	• Robust against compression and transmission errors using error correction codes. Maintains effective balance of imperceptibility and capacity. • Suitable for secure video communication applications.	• Computationally expensive due to ECC integration. • Video embedding increases processing complexity. • Challenging for real-time applications.

This matches long-standing steganography theory that these three parameters are in constant trade-off. These surveys also highlight that while many tools exist, most fail under practical hostile environments (compression, cropping, noise), aligning with established weaknesses in spatial and transform- only schemes. The cryptographic paper [6] does not directly contribute to hiding, but its performance shows reliable confi- dentiality without imperceptibility. It reminds us of the well- known concept that cryptography secures content, steganog- raphy secures existence, and the best performance comes from hybrid systems combining both. In transform-based and hybrid approaches, paper [14] and [15] represent attempts to balance trade-offs. The former improves imperceptibility by embedding adaptively in edge regions, and experimental results showed improved PSNR compared to plain LSB. The latter uses error correction in the DCT domain, providing ro- bustness to compression and transmission errors, aligning with existing knowledge that frequency-domain methods generally outperform spatial-domain ones in hostile conditions. Simi- larly, in the paper [3] it achieved exceptional payload capacity (up to 8 bpp), but its weakness under compression echoes the long-known limitation that lightweight transforms without redundancy are unsuitable for practical secure communication. In the text domain, [13] and [2] push the boundaries of non-image steganography. Their performance lies in high imperceptibility since changes are nearly invisible to readers. CSNTSteg in particular demonstrated almost 99% improved payload capacity with Huffman compression. However, both approaches confirm the known limitation that text steganog-raphy suffers from portability and platform-dependence, as font rendering and encoding vary across devices. The deep learning–based models demonstrate the most significant leap in performance compared to traditional methods. [12] lever- age GANs to align stego-images with natural data distribu- tions. Their performance analysis showed superior invisibility and robustness, outperforming traditional CNN embedding methods. This confirms the recent shift in literature where distribution-based generative hiding surpasses deterministic pixel modifications. Similarly, Robust Image Steganography Based on Edge Detection and CNN and Robust Image Steganography Approach Based on Edge Detection Combined With CNN Algorithm show hybrid CNN-edge schemes that improve imperceptibility, especially in edge-dense images, though they underperform on smooth ones consistent with prior knowledge that content-aware embedding boosts invisi-

bility but remains context-dependent.

Finally, StegTransX provides the strongest performance gains. Compared to existing knowledge, where most deep models (HiNet, StegFormer) were heavy and not robust to real- world compression,

StegTransX innovates by adding TransX blocks for efficient feature extraction, Channel-Spatial Collaborative Fusion (CSCF) for feature mixing, and a JPEG attack module during training. This makes it explicitly re- sistant to one of the most common distortions JPEG com- pression—while remaining lightweight. It balances the three steganographic goals (capacity, imperceptibility, robustness) better than any previous approach.

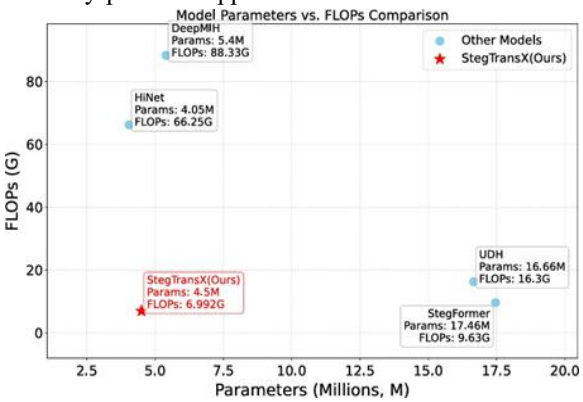

Fig. 2. StegTransX vs. recent SOTA: parameters and computational cost [1]

V. CONCLUSION

From the collective review of classical, hybrid, and deep learning–based steganography methods, it is clear that the field has evolved significantly, moving from simple substitution- based approaches like LSB to highly sophisticated deep gen- erative frameworks. Early models established the foundation by demonstrating how digital media could conceal information with minimal perceptual distortion, yet they struggled with robustness under compression, noise, and steganalysis. Hybrid and transform-domain methods extended this foundation by embedding data in more resilient frequency components and incorporating adaptive schemes, which improved performance but added computational cost and design complexity. Text- based approaches provided creative alternatives for non-image hiding, achieving high invisibility, yet their applicability was constrained by platform dependencies and limited payload. The real leap forward has come from deep learning, where CNNs, GANs, and attention-based architectures have enabled adaptive, context-aware embedding that minimizes detectable artifacts and maximizes robustness. Among these, lightweight models such as StegTransX represent a turning point by explicitly training against real-world distortions like JPEG compression, offering a more practical and scalable balance between imperceptibility, robustness, and capacity. Overall, the progression of these works confirms that while no single method fully resolves the inherent trade-offs of steganography, the integration of deep learning with efficiency and real- world resilience points toward the future of secure and covert communication.

REFERENCES

[1] X. Duan, Z. Wang, S. Li, and C. Qin, “Stegtransx: A lightweight deep steganography method for high-capacity hiding and jpeg compression resistance,” Information Sciences, p. 122264, 2025.

[2] R. Thabit, N. I. Udzir, S. M. Yasin, A. Asmawi, and A. A.-A. Gutub, “Csntsteg: Color spacing normalization text steganography model to improve capacity and invisibility of hidden data,” IEEE Access, vol. 10, pp. 65439–65458, 2022.

[3] Y.-Q. Zhang, K. Zhong, and X.-Y. Wang, “High-capacity image steganography based on discrete hadamard transform,” IEEE Access, vol. 10, pp. 65141–65155, 2022.

[4] R. Al-Rawashdeh, M. M. Rahman, and M. Niazi, “Robust image steganography approach based on edge detection combined with cnn algorithm,” IEEE Access, 2025.

[5] D. Prabhu, S. V. Bhanu, and S. Suthir, “Privacy preserving steganog- raphy based biometric authentication system for cloud computing environment,” Measurement: Sensors, vol. 24, p. 100511, 2022.

[6] X. Zhou and X. Tang, “Research and implementation of rsa algorithm for encryption and decryption,” in Proceedings of 2011 6th international forum on strategic technology, vol. 2, pp. 1118–1121, IEEE, 2011.

[7] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding-a survey,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1062–1078, 2002.

[8] N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” computer, vol. 31, no. 2, pp. 26–34, 2008.

[9] M. Chen, R. Zhang, X. Niu, and Y. Yang, "Analysis of current steganog- raphy tools: classifications & features," in 2006 International Conference on Intelligent Information Hiding and Multimedia, pp. 384–387, IEEE, 2006.

[10] D. Neeta, K. Snehal, and D. Jacobs, "Implementation of lsb steganog- raphy and its evaluation for various bits," in 2006 1st international conference on digital information management, pp. 173–178, IEEE, 2006.

[11] S. M. Karim, M. S. Rahman, and M. I. Hossain, "A new approach for lsb based image steganography using secret key," in 14th international conference on computer and information technology (ICCIT 2011), pp. 286–291, IEEE, 2011.

[12] D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, "A novel image steganography method via deep convolutional generative adversarial networks," IEEE access, vol. 6, pp. 38303–38314, 2018.

[13] K. Wang and Q. Gao, "A coverless plain text steganography based on character features," IEEE Access, vol. 7, pp. 95665–95676, 2019.

[14] M. A. Hameed, M. Hassaballah, S. Aly, and A. I. Awad, "An adaptive image steganography method based on histogram of oriented gradient and pvd-lsb techniques," IEEE Access, vol. 7, pp. 185189–185204, 2019.

[15] R. J. Mstafa and K. M. Elleithy, "An ecc/dct-based robust video steganography algorithm for secure data communication," Journal of Cyber Security and Mobility, vol. 5, no. 3, pp. 167–194, 2016.