Review of Enhancing Secure Communication: Unified Study of Cryptographic and Steganographic Techniques in Digital Communication template

Sunit Jana , Rakhi Biswas ,Disha Das, Deepshikha Chatterjee , Nikita Pal , Debasmita Basak ,Koushik Pal

Department of Electronics and Communication Engineering
Guru Nanak Institute of Technology , Kolkata

Abstract - In a time of rising cyber threats and widespread digital communication, protecting sensitive information is crucial. This paper offers a detailed survey and analysis of current methods in secure communication, focusing on the relationship between cryptographic systems and steganographic techniques. We base our work on foundational mathematics, especially commutative algebra, and use modern technologies like Generative Adversarial Networks (GANs), zero-knowledge proofs, and quantum-resistant algorithms. We present a layered approach to information security. We discuss how combining classical and modern cryptography with improved steganographic embedding and signal processing techniques highlights the need for hybrid and adaptable models to protect communication. This study aims to be a reference point for future research and development in secure digital systems.

Key Words: Cryptography : from classical to post-quantum, Steganography and Data hiding Techniques, GAN-Based Steganography in wireless sensor network , Methodology Overview.

1.INTRODUCTION

The 21st century, the rise of digital connectivity has changed how people, organizations, and governments communicate and function. From mobile banking and online education to smart cities and telemedicine, nearly all modern services depend on the safe exchange of information over digital networks. This reliance on digital communication has also increased the risks of cyber threats. Data breaches, unauthorized access, surveillance, identity theft, and espionage are now common problems in cyberspace. As a result, the need for secure communication systems has shifted from a technical issue to a vital global priority. At the core of secure communication are two main goals: protecting the content of messages from unauthorized access and hiding the existence of those messages when needed. Traditionally, steganography and cryptography have been used on their own to reach these goals. Cryptography changes readable text into an unreadable code using mathematical algorithms, ensuring that even if a message is intercepted, it cannot be understood without the correct key. Steganography, on the other hand, hides secret messages within everyday-looking media like images, audio, or video files, which keeps the communication itself hidden. Recent research has shown that emerging technologies play a crucial role in improving secure communication systems. For instance, the theoretical basis for several cryptographic systems, including RSA, ElGamal, and elliptic curve encryption, comes from commutative algebra and number theory. Meanwhile, artificial intelligence, especially Generative Adversarial Networks, is being used to enhance the effectiveness and subtlety of steganographic techniques. Developments like quantum-resistant algorithms, homomorphic encryption, zero-knowledge proofs, and secure multiparty computation have broadened the possibilities for ensuring confidentiality, integrity, authentication, and non repudiation in complex networked settings. Given these changes, studying secure communication systems is more relevant and urgent than ever. The digital threats we face today, along with future risks such as quantum computing and automated cyberweapons, require a proactive and interdisciplinary approach to security. This research paper aims to thoroughly explore the theoretical underpinnings, current practices, and new trends in cryptographic and steganographic systems. By bringing together insights from both traditional and innovative research, this study helps deepen our understanding of how to create multi-layered secure communication systems that can tackle the evolving challenges of the digital age.

2. IMPORTANCE OF SECURE COMMUNICATION

It is impossible to overstate the importance of safe communication in today's digital environment. As cyber threats become more sophisticated and frequent, protecting sensitive information during transmission is essential. Whether it's about personal privacy, military intelligence, or financial and healthcare data, ensuring confidentiality, authenticity, and integrity in communication is key to maintaining trust in digital systems. The combination of cryptographic and steganographic techniques, improved by advances in machine learning and signal processing, provides a strong defense against both passive and active attacks. This topic is not just relevant; it is urgent. It tackles the technological, societal, and ethical challenges of data security in a digital world that is increasingly connected and adversarial.

3. WORKING PRINCIPLE

The main goal of secure communication systems is to keep information safe when it travels over channels that might not be secure. This means ensuring that the data stays private, genuine, unaltered, and sometimes hidden. To achieve this, we use a mix of cryptographic and steganographic methods, along with signal processing and error correction techniques. Below is an overview of

how each key component works and how they fit together.

1.1 Cryptography

Cryptography protects the message content. The basic idea is to turn plaintext into ciphertext using an encryption algorithm and a secret key. Only authorized people with the right decryption key can change the ciphertext back into its original form.

Core Steps:

1.Encryption: The sender uses an algorithm (like AES, RSA, or ECC) on the plaintext with a key to create ciphertext.

2. Transmission: The encrypted message is sent over the communication channel.

3. Decryption: The receiver uses the matching key and decryption algorithm to retrieve the original message.

4. Types of Cryptography: Symmetric: The same key is used for both encryption and decryption, such as in AES. Asymmetric (like RSA or ECC): A public key is used for encryption, and a private key for decryption.

Cryptography ensures confidentiality, authentication, and integrity, but it does not hide the fact that communication is happening.

1.2 Steganography

Steganography hides the existence of a message. It does this by embedding the secret message (whether plaintext or ciphertext) into a cover medium, such as an image, audio, or video file. The result is a stego-object that looks normal to anyone who might see it.

Core Steps:

1.Embedding: The secret message is encoded into the cover medium using methods like Least Significant Bit (LSB), Discrete Wavelet Transform (DWT), or Generative Adversarial Networks (GANs).

2. Transmission: The stego-object looks like a regular file while it is sent through the channel.

3. Extraction: The recipient uses a stego-key or decoding method to retrieve the hidden message from the stego-object. Steganography allows for secret communication by hiding not just the message content but also the fact that any communication is taking place.

1.3 Integrated Approach:

Crypto-Steganography For better security, cryptography and steganography are often used together in a two-layer security model:

Encryption Phase: The plaintext is first encrypted with a cryptographic algorithm to create ciphertext. Embedding Phase: Next, a steganographic method is used to hide the ciphertext within a cover medium. Transmission Phase: The stego-object is sent through a public or insecure channel. Extraction and Decryption Phase: The receiver extracts the ciphertext from the stego-object and then decrypts it to get the original message.

The combination of encryption to secure data and steganographic embedding to hide the data's presence creates a complete security system. This system can stop both passive eavesdropping and active detection. This integrated approach is central to modern secure communication strategies, especially in settings where confidentiality and stealth are equally important.

4. CRYPTOGRAPHY : FROM CLASSICAL TO POST-QUANTUM

1.1 Cryptography:

From Classical to Post-Quantum Cryptography, the practice of securing information, has changed a lot over the years. It started with simple hand written ciphers in ancient times and has evolved into complex algorithms used in today's digital systems. The transition from classical methods to post-quantum cryptography shows how security needs and technology have developed over time. Each phase has addressed specific threats, computing power, and ways people communicate.

1.1.1 Classical Cryptography

Classical cryptography includes early encryption systems that were used before modern computing. These techniques relied on straightforward character transformations and were suitable for manual encoding and decoding. Common examples are:

Caesar Cipher: A substitution cipher that shifts characters in the alphabet a set number of places.

Vigenère Cipher: A polyalphabetic substitution cipher that uses a keyword to vary the shift for each character.

Transposition Ciphers: These rearrange characters in the plaintext based on a defined system.

While they were innovative for their time, classical ciphers lacked the complexity needed for security. They were eventually broken using frequency analysis and other cryptanalytic methods. Their main weakness was poor key management and limited resistance to brute-force attacks, making them inadequate for today's data protection needs.

1.1.2 Modern Cryptography

The introduction of digital computing in the mid-20th century marked the start of modern cryptography. This relies on solid mathematical principles and the difficulty of certain

computations. Modern cryptographic systems mainly fall into two categories:

1. Symmetric Key Cryptography (e.g., AES, DES): Uses one key for both encryption and decryption. It is efficient and commonly used to protect large amounts of data, such as in disk encryption or VPNs.

2. Asymmetric Key Cryptography (e.g., RSA, Elliptic Curve Cryptography - ECC): Employs two keys—one public for encryption and one private for decryption. Asymmetric systems address the key distribution issue and allow for digital signatures and public key infrastructure (PKI).

These systems depend on mathematical problems that are easy to calculate one way but hard to reverse without specific information (like factoring large numbers in RSA or solving discrete logarithms in ECC). They provide strong security under current computing power and are deeply embedded in protocols such as HTTPS, TLS, SSH, and blockchain technologies.

1.1.3 Challenges from Quantum Computing

The rise of quantum computing poses a serious threat to traditional public-key cryptography. Quantum algorithms, like Shor's Algorithm, can efficiently solve the integer factorization and discrete logarithm problems that secure RSA, ECC, and Diffie-Hellman key exchange. Once practical quantum computers are available, these systems might become vulnerable to decryption by those with enough quantum resources. Symmetric algorithms (such as AES) are somewhat more resilient, but Grover's Algorithm can effectively reduce their key length in half. This means longer key sizes will be necessary to maintain the same level of security (e.g., AES-256 instead of AES-128).

The impending quantum threat is driving the development of post-quantum cryptography (PQC), which consists of algorithms designed to remain secure against both classical and quantum attacks.

1.1.4 Post-Quantum Cryptography

Post-quantum cryptography focuses on schemes based on mathematical problems that are believed to be hard for quantum computers. The National Institute of Standards and Technology (NIST) is leading a global effort to standardize PQC algorithms. Key categories include:

1.Lattice-Based Cryptography: Based on the difficulty of problems like Learning With Errors (LWE) and the Shortest Vector Problem (SVP). Examples: Kyber, NTRU.

2.Code-Based Cryptography: Built on the challenge of decoding random linear codes. Example: McEliece.

3.Multivariate Quadratic Cryptography: Uses systems of multivariate polynomial equations. Example: Rainbow.

4.Hash-Based Cryptography: Relies on the security of cryptographic hash functions and is especially suitable for digital signatures. Example: XMSS. Performance, scalability, and resistance to conventional and quantum attacks are the primary focuses for post-quantum cryptography methods. These will eventually replace vulnerable algorithms in applications like secure messaging, digital signatures, blockchain, and virtual private networks.

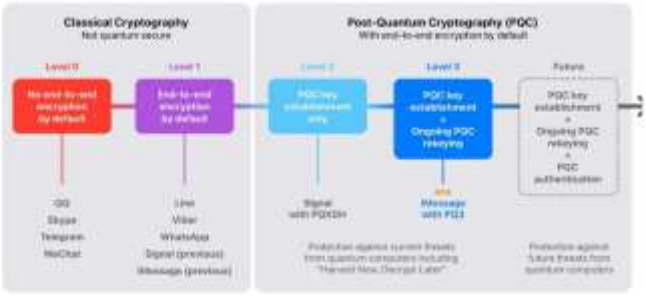

Fig1: Quantum Secure Cryptography in Messaging apps

1.1.5 The Transition and Future Outlook

Transitioning to post-quantum encryption presents some challenges: Performance Trade-offs: Some PQC algorithms require larger keys or take longer to process.

Backward Compatibility: Updating existing systems without causing disruptions.

Public and Private Sector Adoption: Promoting industry-wide migration while balancing costs and security needs.

Despite these challenges, the shift is inevitable. Organizations and governments need to start adopting quantum-resistant strategies. This should include hybrid models that combine classical and post-quantum algorithms during the transition period. Research in quantum-safe cryptography is not only relevant academically but also crucial for national security, privacy, and digital trust in the coming years.

Cryptography has transformed from simple ciphers to complex systems built on strong mathematical foundations and is now entering a new phase due to quantum threats. This development reflects the field's main goal: to protect information against ever-changing attacks and computing models. Understanding this evolution—from classical methods to

quantum resistance—is essential for creating secure communication systems for the future.

5. STEGANOGRAPHY AND DATA HIDING TECNIQUES

While cryptography aims to make information unreadable to unauthorized users, steganography takes a different but related approach by hiding the existence of the communication. Steganography comes from the Greek words steganos (covered) and graphia (writing). It is the practice of embedding secret messages within ordinary digital files, like images, audio, video, or even text. The main goal of steganography is to allow hidden communication, which is particularly useful in situations where surveillance, censorship, or interception may occur.

1.2.1 Data Hiding:
Concept and Classifications Data hiding involves adding extra information to digital signals without greatly compromising their quality or function. It is essential for: 1. Covert communication 2. Copyright protection (digital watermarking) 3. Integrity verification 4. Secure authentication systems .
Data hiding can be grouped into:
Steganography: Focused on keeping information secret and undetectable.
Digital watermarking: Mainly used for copyright protection and content authentication.
Covert Channels: Paths not meant for communication that are used to send hidden information.
Anonymity Techniques: Hide the identity of the sender or receiver along with the message.

1.2.2Types of Steganography Techniques
Steganography techniques are typically grouped based on the type of carrier and how the information is embedded. The main categories are:

A. Text Steganography
This includes methods to hide information within text: 1. Format-based hiding: Changing font styles, spacing, or line breaks. 2. Random and statistical generation: Creating grammatically correct but meaningless sentences that carry data. 3.Syntactic and semantic modification: Using synonyms, rephrasing, or making intentional typos.
Text steganography has limits because text data has low redundancy, making it generally easier to detect than other forms.

B. Image Steganography
This is the most common method because digital images have a lot of redundancy and the human eye can handle small changes. Common techniques include:
Least Significant Bit (LSB) insertion: This modifies the least significant bits of pixel values.
Transform domain techniques: This method embeds data in frequency coefficients, like DCT or DWT.
Edge-based and region-based embedding: This targets visually complex areas to avoid detection.
New methods, like GAN-based steganography, use AI to create entirely new images (stego-images) that naturally include hidden information without changing an existing cover image.

C. Audio Steganography
This method embeds secret data into digital audio files using:
Phase coding: This alters phase components that people cannot hear.
Echo hiding: This embeds information in the delay between echoes.
Spread spectrum: This spreads the message across a wide frequency band, similar to radio signals. Audio steganography takes advantage of how people perceive sound but needs solid synchronization to decode accurately.

D. Video Steganography
This combines image and audio steganography by using video frames and soundtracks to hide information. Techniques include: Frame-based LSB modification Motion vector manipulation in video compression Embedding in I-frames or macroblocks Video steganography offers a large capacity but requires more computing power and is more complex to implement securely.

E. Network Steganography
This method uses network protocols and transmission patterns, like packet timing and sequence numbers, to hide information. While effective for covert channels, it can be affected by network conditions or firewalls

1.2.3 Steganography without Embedding (SWE)
Steganography Without Embedding (SWE) is a modern technique that bypasses the traditional data embedding process. Instead, it creates images that naturally encode the message. GANs or other machine learning models are trained to generate a stego-object directly from the secret data. This method has two main benefits; It reduces the risks of steganalysis since there is no change to the original image and It allows messages to be mapped to unique synthetic images. Although SWE shows promise, it still faces issues with decoder leakage, key management, and error correction in environments where data loss is possible.

1.2.4 Performance Metrics in Data Hiding
To evaluate the quality and security of steganographic methods, we commonly use the following metrics:
1.Peak Signal-to-Noise Ratio (PSNR): This measures the distortion caused by embedding.

2.Structural Similarity Index Metric (SSIM): This assesses the perceptual quality of the stego-object. 3.Bit Error Rate (BER): This indicates the accuracy of message extraction
. 4.Embedding Capacity: This defines the maximum amount of data that can be hidden without sacrificing invisibility.
5.Steganalysis Resistance: This refers to the ability to avoid detection by automated tools.
An ideal steganographic system finds a balance between security, invisibility, capacity, and robustness. Steganography and data hiding techniques are powerful tools for secure communication, especially when combined with encryption for added protection. As detection tools and adversary technologies become more sophisticated, the field is evolving by incorporating AI, statistical modeling, and signal processing to keep pace. Grasping the various methods and their basic principles is crucial for creating strong systems that can protect sensitive information in a more monitored and hostile digital landscape.

6. GAN-BASED STEGANOGRAPHY IN WIRELESS SENSOR NETWORK

The rise of Wireless Sensor Networks (WSNs) has changed how we monitor and control physical environments in many fields. These include military surveillance, industrial automation, smart agriculture, healthcare, and disaster management. WSNs consist of sensor nodes that are spread out, have limited resources, and collect, process, and send sensitive information over potentially unsafe wireless channels. Because these networks operate in critical and often dangerous situations, secure and hidden communication in WSNs is essential and technically challenging. Traditional cryptographic methods offer strong protection for data content, but they can draw attention to the communication itself. This makes them vulnerable to traffic analysis and denial-of-service (DoS) attacks. In contrast, steganography hides the fact that communication is taking place, making it a promising option for covert data transmission in WSNs.

1.3.1 Overview of GANs in Steganography

Generative Adversarial Networks (GANs) are a type of deep learning model made up of two neural networks, the generator and the discriminator, that train together in a competitive environment. The discriminator tries to tell the difference between real data and the fake data created by the generator, which aims to look like real data, such as images. Through repeated training, the generator learns to produce highly realistic outputs. In steganography, GANs can be used in two main ways: Cover Image Synthesis: Instead of changing an existing image, the generator creates a new image that naturally encodes the secret message. Stego Image Refinement: GANs can improve the embedding process by making it less noticeable and reducing distortion. This method allows for Steganography Without Embedding (SWE), where the secret information is included in the generation process itself, rather than through later modifications.

1.3.2 Application in Wireless Sensor Networks

1.Wireless Sensor Networks have unique challenges: Limited processing power and memory, Restricted energy budgets,Vulnerability to interception in open environments. GAN-based steganography works well for WSNs because it allows for hidden and energy-efficient communication. It also minimizes the transfer of sensitive plaintext or ciphertext and lowers the risk of traffic analysis.
2.Key Mechanisms in GAN-Based Steganography for WSNs: Before entering a trained GAN generator, the secret message is transformed into a noise vector, The generator creates a synthetic image that hides the message within its visual features. This stego-image is sent over the wireless network. At the receiving end, the image goes through the GAN decoder, which rebuilds the noise vector, allowing for the extraction of the original message. This method effectively conceals the communication and eliminates the need to embed data within existing media, greatly lowering the chance of detection through steganalysis.

1.3.3 Enhanced Security Features

While GAN-based steganography shows high imperceptibility, it has vulnerabilities. One major concern is that any person with access to the trained GAN model (decoder) could extract the hidden message, posing risks of insider threats or decoder leakage. Recent studies suggest enhanced security measures, including: Key-Based Decoding: Only receivers with the correct cryptographic key can access the noise vector and recreate the message. Error Correction Layers: Fix image distortion caused by lossy wireless channels by correcting noise in the recovered data. Authentication Layers: Confirm that only authorized sensor nodes can create or decode stego-images. These features elevate the system from a simple covert channel to a secure, verified, and resilient communication protocol.

1.3.4 Evaluation Metrics and Performance

The effectiveness of GAN-based steganography in WSNs is measured using several standard metrics: 1.PSNR (Peak Signal-to-Noise Ratio): Compares the quality of the stego-image to the expected image .. 2.MSE (Mean Squared Error): Measures the distortion caused during the generation and transmission steps. 3.The Structural Similarity Index Metric, or SSIM, evaluates the similarity between stego and cover images as perceived by the human eye. 4.Bit Recovery Rate: Measures how accurately the hidden data is recreated after transmission. Experiments have shown that the GAN-based approach excels over traditional embedding

methods in both security and image quality, making it suitable for real-world WSN applications.

1.3.5 Challenges and Future Directions

Despite its potential, GAN-based steganography in WSNs faces challenges: Model Size and Training: GANs need substantial computational resources for training, which may not be available in WSN settings. Model Distribution: Ensuring secure deployment of generator and decoder models across sensor nodes. Adversarial Attacks: GANs are also susceptible to adversarial interference, which could compromise message recovery reliability. Future research directions include: Lightweight GAN structures designed for embedded systems. Federated training of GANs across distributed sensor networks. Integration with blockchain for verified and tamper-proof transmission records. Hybrid models that combine cryptography, GANs, and biometric keys for enhanced security.

GAN-based steganography presents an innovative method for secure communication in wireless sensor networks. It combines the strengths of artificial intelligence and data hiding. Its ability to create natural-looking cover images that discreetly encode sensitive information, along with improved imperceptibility, robustness, and key-based access control, makes it a strong candidate for deployment in environments with limited resources and high threats. As WSNs expand in scale and application, GAN-powered secure communication is set to become a fundamental part of next generation cybersecurity architectures.

7. METHODOLOGY OVERVIEW

The methodology presented in this research integrates cryptographic, steganographic, and artificial intelligence-based techniques into a multi-layered framework for secure communication. This hybrid approach is designed to simultaneously address data confidentiality, concealment, integrity, and robustness—key pillars of modern information security. The proposed methodology can be conceptually broken down into five core stages: data preprocessing, encryption, steganographic embedding using GANs, transmission, and extraction and decryption. Each stage contributes uniquely to the overall system's effectiveness and resistance to both passive and active cyber threats.

Stage 1: Data Preprocessing Before the encryption and embedding process begins, the raw message (e.g., sensor data, personal information, or command signals) undergoes preprocessing to ensure it is optimally formatted and free from errors. Encoding: The message is converted into a binary format suitable for encryption. Compression (optional): Data may be compressed to reduce its size and increase embedding capacity. Error Correction Coding (ECC): Techniques such as Hamming codes or Reed-Solomon codes are applied to ensure message resilience against noise and transmission loss—especially critical in wireless sensor networks.

Stage 2: Encryption Layer To ensure confidentiality and authentication, the preprocessed data is encrypted using a secure cryptographic algorithm. Depending on the application context and performance constraints, either symmetric or asymmetric cryptography may be used.Symmetric encryption (e.g., AES) is chosen for real-time, low-latency systems like WSNs due to its computational efficiency.Asymmetric encryption (e.g., RSA, ECC) is used in scenarios requiring public-key distribution and digital signatures.Post-quantum algorithms (e.g., lattice-based encryption) are employed for forward secrecy against quantum attacks.The result is a ciphertext that cannot be interpreted without the appropriate decryption key.

Stage 3: Steganographic Embedding Using GANs The encrypted message is then passed into the GAN-based steganographic system, the core innovation in this methodology.

This multi-stage methodology leverages the combined strengths of cryptography, steganography, and GAN-based generation to create a holistic and forward-looking model for secure communication. Each stage is modular, allowing the system to be adapted for specific application domains—from wireless sensor networks and military communications to private messaging and cloud storage. The integration of AI and cryptographic theory not only increases the resilience of the system but also represents a major advancement in how sensitive information can be protected in the digital age.

8. CONCLUSIONS

The combination of strong cryptography, subtle steganography, and AI-driven innovation marks a new chapter in secure communication systems. This paper has examined a method for improving secure communication by merging these fields into a layered framework that can tackle today's biggest digital security challenges. The suggested system works well in situations where both confidentiality and invisibility matter. By encrypting sensitive information and hiding it within media created by GANs, the communication is not only unreadable to unauthorized users but also almost impossible to detect. This twofold protection makes it much harder for attackers to intercept, examine, or sabotage transmitted data.

Key contributions of this research include:

A thorough look at the evolution of cryptography, from classical to post-quantum methods. An assessment of data hiding techniques, including advanced GAN-based steganography. A strong hybrid communication model that strikes a balance between security, stealth, and performance. A flexible method that can be applied across a range of real-world scenarios, from IoT to military intelligence.

Nevertheless, challenges exist. We need to carefully manage computational complexity, ethical issues, and the risk of model leakage through continued research and responsible implementation. Future work will aim to develop lightweight, understandable, and quantum-resistant steganographic systems. It will also look into the use of blockchain for traceability and federated learning for decentralized model training.

REFERENCES

1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.

2. A foundational textbook that covers classical and modern cryptographic techniques, protocols, and algorithms.

3. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd ed.). CRC Press.

4. Johnson, N. F., Duric, Z., & Jajodia, S. (2001). Information Hiding: Steganography and Watermarking, Attacks and Countermeasures. Springer.
5. Shah, A., & Thakkar, P. (2021). Survey on Cryptographic Algorithms for Secure Communication in IoT.
6. Zhang, Y., & Qin, Y. (2022). Quantum-Safe Cryptography: State-of-the-Art and Future Directions.
7. Dey, S., & Chowdhury, T. R. (2023). Improving secure communication: Implementation and optimization of a new algorithm for steganography with better security and efficiency.
8. Hameed, S. A., & Garcia, F. D. (2022). Security in Wireless Sensor Networks Using Hybrid Cryptography and Steganography.