Quantum Information & Computation
ISSN 1533-7146 Volume 26 (2026) pp.68–88

Cerebration Science Publishing

Article

QRAND-AVS: A Quantum-Randomness Assisted, AI-Optimized DNA–ECC Framework for Secure Video Steganography in IoT

Vijaya Kumar Vadladi [1,*] and D Marshiana [2]

[1] Department of ECE, Sathyabama Institute of Science and Technology, Chennai-600 119, Tamil Nadu, India; vijay20052009@gmail.com

[2] Department of Electronics and Telecommunication, Symbiosis Institute of Technology, Symbiosis International Deemed University, Pune 412 115, India; d.marshiana@gmail.com

* Correspondence author: vijay20052009@gmail.com

Received date: 19 September 2025; Accepted date: 13 January 2026; Published online: 15 January 2026

Abstract: The swift expansion of Internet of Things (IoT) applications in telemedicine, defense communication, and copyright protection has heightened the necessity for scalable, lightweight, and quantum-resistant multimedia security frameworks. AES and DES are two examples of old symmetric algorithms that are hard to use and have security holes when it comes to sharing keys. Quantum adversaries can still assault classical public-key techniques. This paper presents QRAND-AVS, a hybrid video steganography framework that combines quantum randomness, lightweight cryptography, and adaptive intelligence. The Koblitz method makes plain text messages readable, while Elliptic Curve Cryptography (ECC) makes them unreadable. To make sure that the private keys are truly random, a Quantum Random Number Generator (QRNG) is used. The ciphertext is encoded into DNA nucleotides and adaptively embedded into key video frames selected via histogram-variance analysis. Strong transform-domain embedding is possible with a two-level Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). An AI-based optimizer changes the rules for DNA, the strength of the embedding, and the levels of quantization in real time to find the right balance between payload and invisibility. When tested on a number of benchmark videos, the proposed method had a PSNR that was up to 2.4 dB higher and an embedding capacity that was 40% higher than the LSB and baseline SVD methods. It also cut down on encryption overhead by 35%. Security analysis shows that the system is safe from brute-force, replay, and steganalysis attacks as long as the PSNR/SSIM limits are followed. The results show that QRAND-AVS is a smart, light, and quantum-safe way to protect multimedia that works well in IoT and post-quantum communication settings.

Keywords: Quantum Random Number Generator (QRNG); Elliptic Curve Cryptography (ECC); DNA Encoding; Video Steganography; Internet of Things (IoT); Post-Quantum Cryptography; Discrete Wavelet Transform (DWT); Singular Value Decomposition (SVD); AI-based Optimization; Multimedia Security

1. Introduction

With the rise of Internet of Things (IoT) apps in areas like telemedicine, remote health monitoring, vehicular networks, and copyright protection, it is very important to be able to send videos safely. People often post videos and pictures on these networks that have very private information in them, like medical records, military communications, and digital assets that belong to a company. This kind of information needs to be private, safe, and able to handle both normal cyberattacks and new threats that come with the quantum age in order to stay safe. The Data Encryption Standard (DES), the Advanced Encryption Standard (AES), and the International Data Encryption Algorithm (IDEA) are all examples of standard symmetric encryption algorithms that protect multimedia files in a basic way. But they aren't good for IoT settings with limited resources because they need a lot of processing power, are hard to scale, and have trouble with key distribution. To address those issues, hybrid cryptographic and steganographic frameworks

DOI: 10.2478/qic-2026-0004

have been developed. But most of the solutions that are available now continue to employ pseudo-random number generators (PRNGs), fixed embedding strategies, and trade-offs between payload capacity and invisibility. With the rise of quantum computing, these problems get worse. Shor's algorithm demonstrates that widely utilized asymmetric cryptosystems such as RSA and ECC are susceptible to compromise in polynomial time. This means that traditional methods for transferring keys and transmitting information could become unusable over time. This fosters the development of post-quantum-resilient frameworks, ensuring lasting privacy and durability in multimedia communication facilitated by the Internet of Things (IoT). Prior work investigated DNA-based steganography, ECC-based lightweight cryptography, quantum random number generators (QRNGs), and AI-assisted embedding autonomously. Although these approaches may improve security in particular areas, there has been no systematic study involving QRNG-driven ECC with DNA encoding and AI-based adaptive embedding. Since there is no unity, it is harder to make use of quantum technology to grow, change, and protect against enemies. We suggest a hybrid framework that combines these two complementary approaches into an integrated approach. This paper adds several important things:

- Quantum-secure key generation: employing QRNG-based private key generation for ECC ensures that the keys are truly erratic and safe from both classical and quantum threats.
- DNA-inspired encoding: Changing ciphertext into DNA sequences to make video frames more random, spread out, and able to hold more data.
- AI-driven adaptive embedding: changing the DNA rules, the strength of the transform-domain embedding, and the quantization thresholds in real time to make the embedding as strong and hidden as possible while still meeting PSNR/SSIM limits.
- Two distinct types of safety: first, QRNG–ECC encryption, and then DNA-guided steganographic embedding. This makes it very hard for attacks that use brute force, replay, or steganalysis to work.
- Perform the following evaluation: Experimental validation demonstrates that the framework performs more effectively than the baseline LSB and SVD techniques in IoT and post-quantum environments. It has a higher PSNR, can hold more data, and takes less time for it to function on.

The proposed framework is a next-generation way to protect multimedia that is safe, smart, and immune to quantum attacks. It does this through employing one architecture for managing scalability, unpredictability, and adaptability.

2. Related Works

The growing demand for secure and light multimedia communication in IoT environments led to significant studies in cryptography and steganography. There are currently five primary areas in the existing works: DNA-based encoding, elliptic curve cryptography (ECC), quantum random number generators (QRNGs), AI-driven embedding, and hybrid approaches. DNA-based encoding has grown into an exciting means to send messages with multimedia safely. The four nucleotides (A, T, C, and G) enable parallel computation and high entropy, which makes it feasible to develop complex cryptographic structures. Liu et al. [1] implemented forth DNA-chaos–based image encryption that has high entropy and is difficult to penetrate with differential attacks. In a comparable way, Al-Tamimi and Hassan [2] utilized DNA cryptography for medical IoT applications and demonstrated that it proved more robust. These approaches performed an excellent job enhancing multimedia protection, but they encountered problems with static DNA mapping rules and limited adaptability, resulting in them being less resistant to steganalysis. Additionally, research integrating DNA cryptography with conventional techniques has demonstrated that they're sufficiently secure to protect sensitive medical data and that their bodies are capable of holding more multimedia. However, these models weren't dynamically optimizing embedding rules, and this often indicated that there was a trade-off between capacity and concealment. So, although DNA-based methods had strong diffusion and confusion properties, their rigid encoding schemes remain an issue. Elliptic Curve Cryptography (ECC) has become popular in IoT settings as its keys are smaller than those of RSA but nevertheless offer the same degree of safety. Numerous studies looked at ECC in the framework of multimedia protection.

Karthik et al. [3] invented an energy-efficient ECC-based DTLS key establishment protocol for IoT devices. They made it cheaper to run, but they didn't add video steganography to the framework. He, Chan, and Guizani [4] put forth lightweight ECC authentication for vehicular networks. This strengthened the networks more immune to impersonation, but the networks were still vulnerable to quantum attacks since they used pseudo-random number generators (PRNGs). The combined use of ECC and transform-domain steganography has also been investigated. Lu et al. [5]

implemented ECC incorporating conditional privacy-preserving authentication for VANET emergency messaging. In the meantime, other researchers incorporated ECC with Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to enhance imperceptibility and robustness. These studies validated ECC's efficiency in limited resources IoT contexts; nevertheless, they all displayed a shared drawback: their dependence on PRNGs for key generation, which makes them susceptible to predictability and future quantum assaults. For cryptographic security, especially when making private keys, true randomness is very important. PRNG-based keys are readily available to invent, which makes cryptosystem security less robust. To correct this, QRNGs employ quantum effects like vacuum fluctuations or photon polarization to make true randomness. Huang et al. [6] incorporated QRNGs into TLS protocols, considerably reducing the unpredictability of the session keys. Ma et al. [7] also combined photonic QRNG with ECC key exchange to lower the risks of predictability. These solutions were good at making cryptography more robust, but they were primarily more focused on classical encryption than multimedia security. Singh and Rao [8] recently advocated AI-assisted QRNGs for IoT, and these displayed how to continuously extract entropy. Their model achieved significant unpredictability but was focused on cryptographic key generation, insufficient to account for multimedia steganography. Previous studies on quantum-enhanced cryptography have additionally spoken about QRNG's role in post-quantum cryptographic resilience, but they did not associate QRNG with multimedia embedding. Each of these efforts shows how important QRNG is, but they also show just how little it is employed in hybrid multimedia protection frameworks. Artificial intelligence has altered steganography by rendering it feasible to continually embed and optimize elements. Chen and Wu [9] developed adaptive video steganography based on deep learning, which altered embedding strategies on the fly while still being undetectable. In the same way, Zhang et al. [10] used GAN-assisted embedding to make their findings strong against adversarial steganalysis.

Post-Quantum Steganography and Lattice-Based Approaches

Recent advancements in post-quantum cryptography have motivated the exploration of secure multimedia steganography schemes built upon lattice-based and homomorphic foundations. In contrast to conventional transform-domain or matrix-factorization techniques, these methods aim to achieve security against quantum-capable adversaries while preserving the imperceptibility and robustness of embedded data. Lattice-based constructions, particularly those relying on the Ring Learning With Errors (RLWE) assumption, have been applied to multimedia steganography due to their strong worst-case hardness guarantees. RLWE-based embedding mechanisms enable encrypted-domain hiding and resist both classical and quantum cryptanalytic attacks. Similarly, homomorphic encryption–assisted watermarking allows embedding operations to be performed directly over ciphertexts, enabling privacy-preserving multimedia authentication and tamper detection. Another important direction is the development of lattice trapdoor–based embedding schemes, where structured trapdoor functions facilitate secure reversible mappings suitable for embedding sensitive information into image or video frames. These post-quantum approaches highlight the shift toward steganographic systems that remain secure in the presence of quantum adversaries. Incorporating these developments into the broader research landscape emphasizes the relevance of our proposed ECC- and QRNG-assisted QRAND-AVS framework, which aligns with the ongoing transition toward PQC-resilient multimedia security solutions.

3. Proposed Quantum-Randomness Assisted, AI-Optimized DNA-ECC based Video Steganography Method (QRAND-AVS)

To overcome the limitations of conventional data-hiding techniques in wireless multimedia communication systems, this work proposes **a** hybrid secure and robust video steganography framework**.** The scheme integrates Quantum Random Number Generator (QRNG)-driven ECC encryption**,** DNA-based encoding**,** AI-assisted adaptive optimization**,** and transform-domain embedding using 2-level DWT and SVD**.**

In transmitter side, the cover video is first parsed into frames, and the plaintext M is converted to ASCII and mapped to elliptic-curve points via the Koblitz method. A QRNG generates the private/random scalars, and ECC encrypts each point to ciphertext pairs $(C_1, C_2) = (kG,\ P_m + kP_B)$. Ciphertext coordinates are then encoded to DNA triplets (Table 1) and converted to binary (Table 2), boosting entropy and payload flexibility. Key frames are selected using histogram/mean/variance thresholds to minimize redundancy and improve resilience to compression. An AI module adapts DNA rules and embedding depth to the frame's complexity and target payload, balancing imperceptibility, capacity, and robustness. Finally, selected frames undergo a 2-level DWT; SVD is applied on the LL_2 sub-band, and the DNA-derived bits are embedded into singular values. Inverse transforms and reassembly yield the

Table 1. Mapping the ciphertext point with DNA nucleotide.

0 - CCA	1 - GTT	2- TTG	3- GGT	4- TTT	5- TCG	6- CGC	7- ATG	8 - AGT	9 - CGA

Table 2. Mapping the DNA nucleotide with binary digits.

A - 00	C- 01	G - 10	T - 11

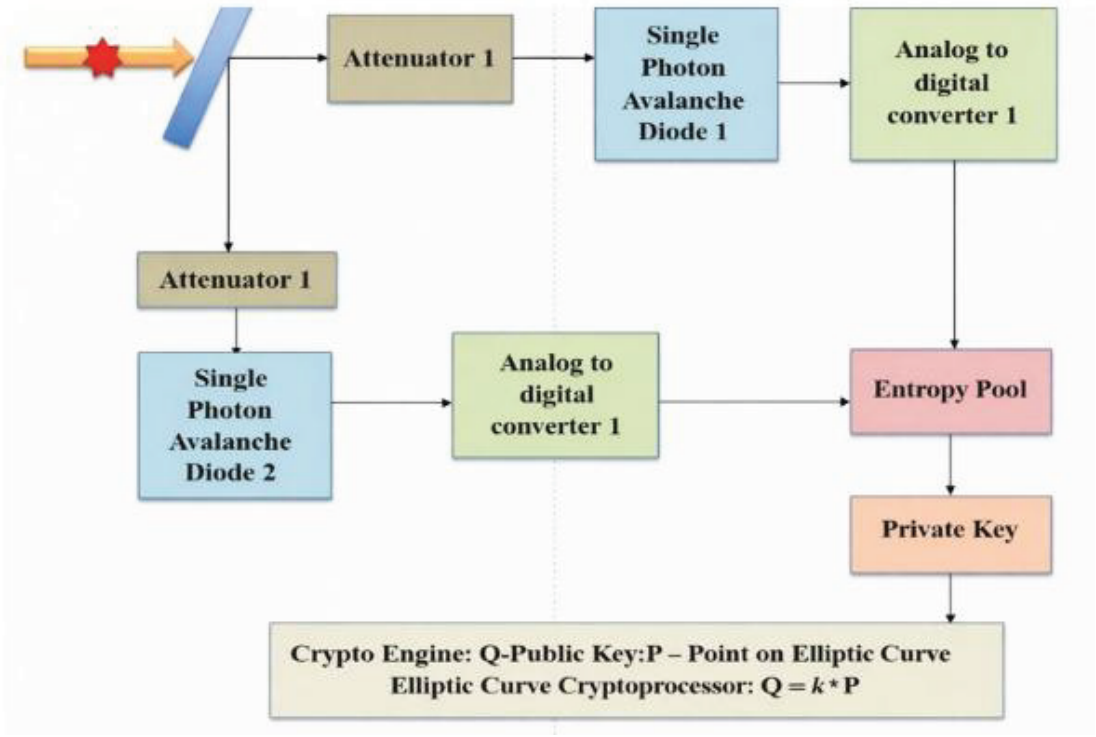

Figure 1. Schematic block diagram of the proposed portable QRNG device for ECC processor.

stego video. At the receiver side, the stego video is decomposed into frames; the same key-frame selection is applied, followed by DWT-SVD to extract the embedded bitstream. Bits are reverse-mapped to DNA symbols and then to elliptic-curve ciphertext points. Using the QRNG-generated private key d_B, ECC decryption recovers the plaintext point via $P_m = C_2 - d_B C_1$, which is converted back to ASCII to reconstruct the original secret message. The proposed Quantum-Randomness Assisted, AI-Optimized DNA-ECC based Video Steganography Method consists of different steps to be carried out to attain secure video transmission for any IoT-based applications. In this method, mainly Quantum Random Number Generator-based key generation is used for Elliptic Curve Cryptosystem to generate a public key from the randomly generated private key to provide a real randomness feature for the cryptosystem. **A** Quantum Random Number Generator (QRNG) instead uses fundamental quantum mechanical phenomena (e.g., superposition, entanglement, vacuum fluctuations) to produce truly non-deterministic and unpredictable random numbers, which makes them **an** ideal entropy source for generating private keys in ECC. In Elliptic Curve Cryptography (ECC), security is based on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP). A private key d is chosen uniformly at random from the finite field $[1, n-1]$, where n is the order of the base point P. The corresponding public key is generated as: $Q = k \cdot P$. If the randomness of d is weak, ECC can be broken even without solving ECDLP (e.g., biased RNGs enabled attacks like the Sony PlayStation 3 ECDSA vulnerability). Thus, the security bottleneck is the entropy source used to generate k. A QRNG replaces the PRNG in the key generation step as shown in Figure 1.

The proposed Quantum-Randomness Assisted, AI-Optimized DNA–ECC Video Steganography Framework (QRAND-AVS) integrates cryptography and steganography in a dual-layer design. The workflow is divided into two distinct stages: (i) encryption and encoding, and (ii) video embedding and extraction.

Stage I: Quantum-Secure ECC Encryption and DNA Encoding

1. **Message Preparation**
   - Input plaintext message MMM is converted into ASCII sequence.
   - The Koblitz method maps ASCII values into elliptic curve plaintext points Pm.
2. **QRNG-Based ECC Key Generation**
   - A portable QRNG device generates true random bits using photon emission, beam-splitting, and SPAD detection.
   - Post-processing modules (von Neumann debiasing, SHA-3 hashing) refine entropy into a uniformly random bitstream.
   - A Key Derivation Function (KDF) produces a 256-bit ECC private key k.
   - Public key Q=kG is computed, where G is the curve generator point.
3. **ECC Encryption**
   - Given public key PB, encrypt plaintext point Pm as ciphertext pair:

$$C_m = (k.G,\ P_m + k.P_B)$$

   where k is an ephemeral session key generated by the QRNG.
4. **DNA Mapping and Binary Conversion**
   - Ciphertext coordinates are mapped into DNA triplets using substitution tables (Table 1).
   - DNA nucleotides are then converted into binary digits (Table 2), producing the bitstream for embedding.

Algorithm 1 QRNG-assisted ECC encryption and DNA encoding

Input: Message M, Receiver public key PB
Output: DNA-encoded ciphertext bits B
Process:
Step 1. Convert M $\rightarrow$ ASCII sequence A
Step 2. Map A $\rightarrow$ elliptic curve points Pm (Koblitz method)
Step 3. Generate QRNG random bits $\rightarrow$ apply extractor $\rightarrow$ derive private key k
Step 4. Compute public key: Q = kG
Step 5. Encrypt: C1 = kG, C2 = Pm + kPB
Step 6. Map (C1, C2) $\rightarrow$ DNA triplets (using Table 1)
Step 7. Encode DNA triplets $\rightarrow$ binary sequence B (using Table 2)
Return B

3.1. Ablation Study on DNA Encoding Strategies

To evaluate the suitability of the proposed DNA-based embedding mechanism, we conducted an ablation study comparing multiple DNA encoding strategies. The baseline method in QRAND-AVS uses a fixed codon mapping, where each pair of bits is deterministically mapped to a nucleotide symbol. This scheme offers low computational complexity and predictable embedding structure.

For comparison, we evaluated two alternative encoding strategies:

1. **Complementary Base-Pair Encoding (A$\leftrightarrow$T, C$\leftrightarrow$G)**
   This method enforces biological complementarity rules to generate reversible nucleotide pairs. Although it improves reversibility and structural symmetry, it increases mapping overhead and reduces embedding flexibility due to the constrained pairing rules.
2. **Variable-Length Codon Encoding (2-, 3-, and 4-base representations)**
   Variable-length codon mapping introduces adaptive nucleotide sequences based on local embedding difficulty. While this approach may yield higher payload capacity in isolated cases, it significantly increases algorithmic complexity and leads to higher statistical predictability, making it more vulnerable to steganalysis.

Our ablation study shows that fixed codon mapping provides the best balance between imperceptibility, payload efficiency, and security. Complementary pairing reduces flexibility and increases computational cost, while variable-

length codons introduce detectable patterns in nucleotide distributions. These observations justify the use of fixed codon tables in the QRAND-AVS embedding process.

Stage II: Video Preprocessing and Embedding

1. **Key Frame Selection**
    - Cover video VVV is divided into frames.
    - Histogram difference and variance thresholding identify key frames to minimize redundancy.
2. **2-Level DWT Transformation**
    - Key frames undergo a two-level Discrete Wavelet Transform (DWT).
    - The LL2 sub-band is selected for embedding due to its robustness to compression.
3. **SVD Embedding**
    - Singular Value Decomposition (SVD) is applied to LL2 blocks.
    - DNA-derived binary bits are embedded into singular values with minimal distortion.
    - Modified LL2 sub-band is inverse-transformed to reconstruct stego frames.

Algorithm 2 DWT–SVD Embedding

Input:**Cover video V, DNA bitstream B**
Output:**Stego video Vs**
Process:
Step 1. **Extract frames from V**
Step 2. **Select key frames using histogram–variance thresholding**
Step 3. **For each key frame F:**
a. Apply 2-level DWT → LL2 sub-band
b. Perform SVD on LL2 blocks
c. Embed bits from B into singular values
d. Reconstruct LL2 and inverse DWT → stego frame
Step 4. **Assemble stego frames → stego video Vs**
Return Vs

Stage III: AI-Assisted Adaptive Optimization

To improve imperceptibility, robustness, and payload trade-offs, an AI-driven optimization module is deployed.

- **Inputs:** frame texture features, payload demand, PSNR/SSIM metrics.
- **Outputs:** optimal parameters for:
    - DNA mapping rules (dynamic substitution instead of fixed rules).
    - Embedding strength in SVD coefficients.
    - Frame selection thresholds.

The optimizer uses a reinforcement learning heuristic:

- Agent = embedding controller.
- Environment = video frame characteristics.
- Reward = weighted function of (PSNR, SSIM, embedding capacity, NC under attack simulation).

3.2. AI-Driven Policy Formulation

To dynamically adapt the embedding process to the local characteristics of video frames, a reinforcement learning (RL) agent is incorporated into the QRAND-AVS framework. The agent receives as input a state vector,

$$s = \{\sigma 2, H, k\}$$

where σ2 denotes local variance, H represents entropy, and k corresponds to the histogram spread of the current frame region. These metrics capture texture, randomness, and structural richness, enabling the agent to learn context-aware embedding actions.

The agent's policy function is defined as

$$T(s) \rightarrow a$$

where $a = \{\Delta, \alpha, \rho\}$ represents the action consisting of(i) the embedding interval Δ, (ii) the embedding strength α, and (iii) the DNA rule selection ρ. The policy determines how aggressively or conservatively data should be embedded based on the perceived embedding difficulty of each region.

Reward Function for Adaptive Embedding

To balance imperceptibility, robustness, and payload, a multi-objective reward function is introduced:

R = α1. PSNR + α2. SSIM + α3. payload – α4. Detectability Score.

Here,

α1, α2, α3 control the importance of visual quality and embedding capacity.

α4 penalizes embeddings that are more susceptible to statistical steganalysis

A lower detectability score corresponds to improved resistance against machine-learning-based steganalysis tools. This formulation enables the RL agent to iteratively discover embedding configurations that maximize perceptual quality while maintaining security.

3.3. Optimization Workflow

During training, the RL agent observes frame statistics, selects an embedding configuration, and receives a reward based on the resulting stego-frame quality. Over multiple episodes, the agent converges toward optimal embedding strategies for varying texture complexities. This integration allows QRAND-AVS to outperform static embedding schemes by learning adaptive, content-aware embedding policies.

Algorithm 3 AI-Driven Adaptive Embedding Optimization

Input: **Frame features, Payload demand**
Output: **Optimized embedding configuration**
Process :
Step 1. **Initialize RL agent with policy π**
Step 2. **For each candidate frame:**
a. Extract variance, histogram, and texture features
b. Select DNA mapping and embedding strength
c. Simulate embedding $\rightarrow$ compute PSNR, SSIM, NC
d. Reward = α*PSNR + β*SSIM + γ*Payload – δ*Detectability
e. Update policy π via Q-learning
Step 3**. Apply best configuration to actual embedding**

Stage IV: Receiver-Side Extraction

- Stego video is decomposed into frames.
- Key frames are identified using the same histogram–variance rules.
- DWT-SVD is applied, and embedded bits are extracted.
- Binary $\rightarrow$ DNA triplet $\rightarrow$ ciphertext point mapping is reversed.
- ECC decryption with QRNG-derived private key reconstructs plaintext as shown in Figure 2.

Key Frame Selection Algorithm

The original video contains a large number of frames. If data are hidden in all the video frames, then it requires a high transmission cost and transmission bandwidth. So the key frame selection algorithm is used to select the key frames from the video by following the procedures. Initially, it converts the video file into N number of different frames and selects the key frames by employing the key frame selection algorithm, as shown in Figure 3. This algorithm helps to reduce transmission cost and save transmission bandwidth.

The selected key frames are compressed by using 2-level DWT compression techniques, reduce the number of transmission bits, and produce the noiseless outputs as shown in Figure 4.

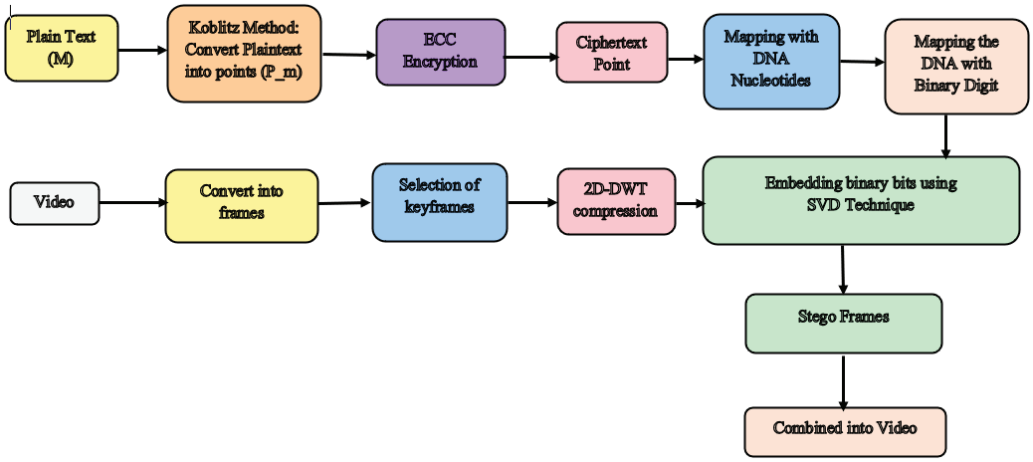

Figure 2. Hybrid video steganography method—Transmitter side.

Algorithm 4 Key Frame Selection Using Histogram and Statistical Thresholding

Input: Video sequence V containing N framesOutput: Set of selected key frames K

Process

Step 1. **Read video V and extract N frames {F1, F2, . . ., FN}.**

Step 2. **For each consecutive frame pair (Fi , Fi+1):**

- **a. Convert Fi and Fi+1 to grayscale matrices.**
- **b. Compute histogram Hi and Hi+1 for both frames.**
- **c. Calculate the difference matrix D = |Hi – Hi+1|.**
- **d. Compute sum of elements in D $\rightarrow$ S.**
- **e. Calculate mean μ and standard deviation σ of S.**
- **f. Determine threshold T = σ + ($\mu \times$ A), where A is a constant.**
- **g. If $\sigma >$ T, mark Fi or Fi+1 as a key frame.**

Step 3. **Collect all selected frames into key frame set K.**

Step 4. **Return K.**

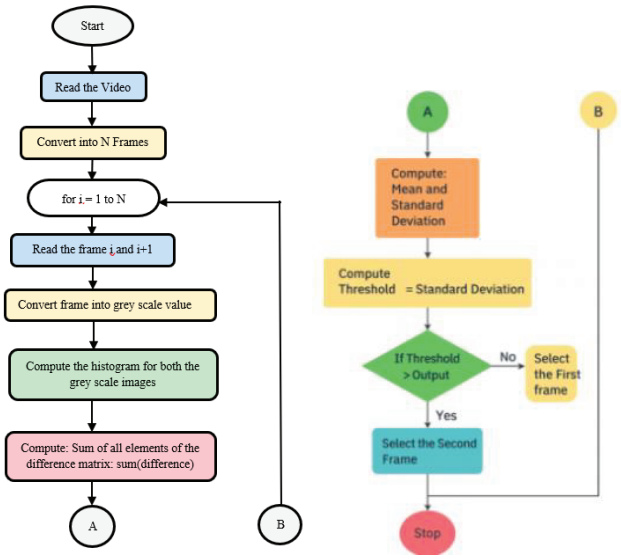

Figure 3. Key frame selection.

3.4. SVD-Based Embedding Algorithm

The compressed frames are used for embedding the secret message bit using the SVD embedding algorithm.

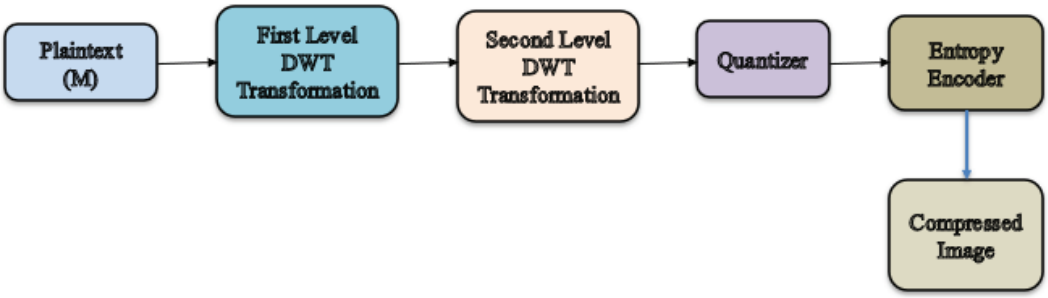

Figure 4. 2-level DWT compression technique.

Algorithm 5 SVD-Based Embedding for Stego Frame Generation

Input: 2-level DWT compressed image I, secret message bitstream MOutput: Stego frame IsI
Process:
Step **1. Read the 2-level DWT compressed image I.**
Step **2. Extract the LL sub-band and resize it to 128 × 128.**
Step **3. Partition the LL sub-band into non-overlapping blocks of size 4 × 4.**
Step **4. For each block B:**
a. Perform Singular Value Decomposition (SVD):
[U, S, V] = svd(B).
b. Obtain the diagonal matrix D from S.
c. If current message bit = 1:
Replace the 4th diagonal entry of D with (D2 – D3),
where D2 and D3 are the 2nd and 3rd diagonal elements.
Else if current message bit = 0:
Replace the 1st diagonal entry of D with (D2 – D3).
d. Reconstruct modified block:
B' = U × D × V^T.
Step **5. Replace each original block with the modified block B'.**
Step **6. Reconstruct the stego LL sub-band and perform inverse DWT.**
Step **7. Return stego frame Is.**

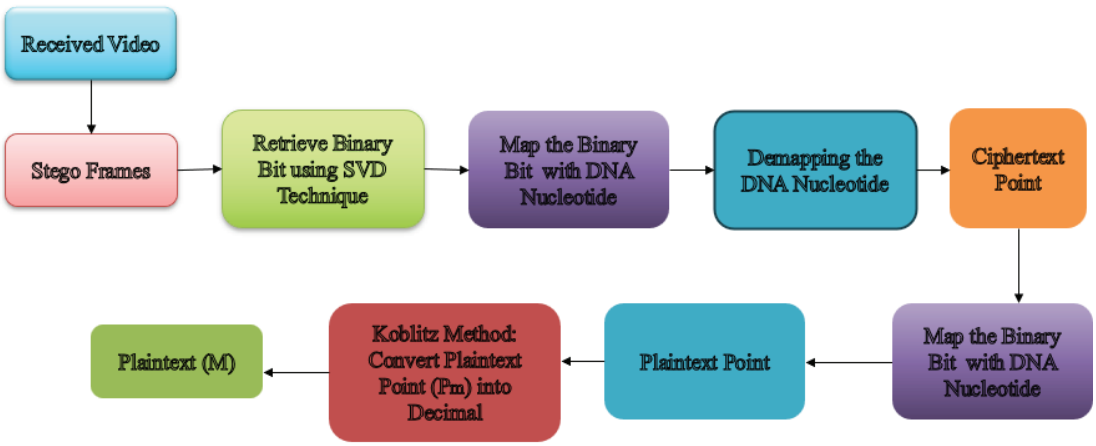

Figure 5. Hybrid video steganography method—Receiver side.

3.5. Receiver Side

On the receiver side, the stego video is converted into stego frames and used to retrieve the secret message as shown in Figure 5. The following steps are taken to retrieve the data from the stego frames.

Algorithm 6 Extraction and Decryption of Secret Message

Input: Stego video Vs, receiver's private key n_B, DNA mapping tables (Table 1 & Table 2)Output: Recovered plaintext message MMM

Process:

Step **1. Read the stego video Vs.**

Step **2. Decompose Vs into individual stego frames {F1, F2, …, Fn}.**

Step **3. For each stego frame:**

a. Apply SVD-based extraction to retrieve embedded message bits.

Step **4. Demap extracted bits into DNA nucleotides using Table 2.**

Step **5. Map DNA nucleotides to ciphertext points using Table 1.**

Step **6. For each ciphertext point (C1, C2):**

a. Decrypt using ECC formula:

Pm = C2 – nB(C1)

where C1 = kG, C2 = Pm + kPB, and PB = nBG.

Step **7. Convert plaintext point Pm into ASCII code via Koblitz method.**

Step **8. For each point (x, y):**

a. Select a random integer r < (x – 1)/B, where B is the base parameter.

b. Decode (x, y) into message symbol M using r.

Step **9. Concatenate all decoded symbols to reconstruct the plaintext message M.**

Step **10. Return M.**

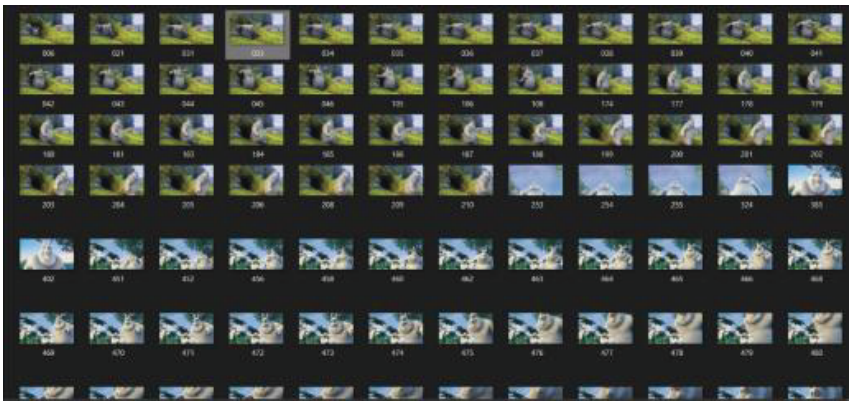

Figure 6. Key frames.

4. Implemented Results and Its Discussion

The proposed QRAND-AVS framework was evaluated using benchmark video datasets under varying payloads (0.10, 0.20, 0.30 bpp). Performance was assessed with Peak Signal-to-Noise Ratio (PSNR), Normalized Correlation (NC), Mean Square Error (MSE), processing time, and embedding capacity. Comparisons were made with baseline spatial-domain (LSB), AES+DWT–SVD, and RSA+DWT–SVD methods to demonstrate practical advantages. The proposed video steganography technique selected the video of length 1 min 2 sec with 1280 as frame width and 720 as frame height. The video is converted into frames with a frame rate 25 frames/second. The selected video file is in .mp4 format with 964 Kbps as data rate and total bit rate as 1349 Kbps.

4.1. Key Frame Selection

A total of 1557 frames are obtained from the selected video file, and 360 frames are selected as key frames by employing the key frame selection algorithm for the converted frames as shown in Figure 6. The key frames are allowed for 2-level DWT compression techniques.

4.2. 2-Level DWT Compression Techniques

The second step of the proposed video steganography technique is applying 2-level DWT compression techniques to the selected key frames as shown in Figure 7. Figure 8 and Figure 9 represent the 1st level of DWT compression

Figure 7. Selected key frame.

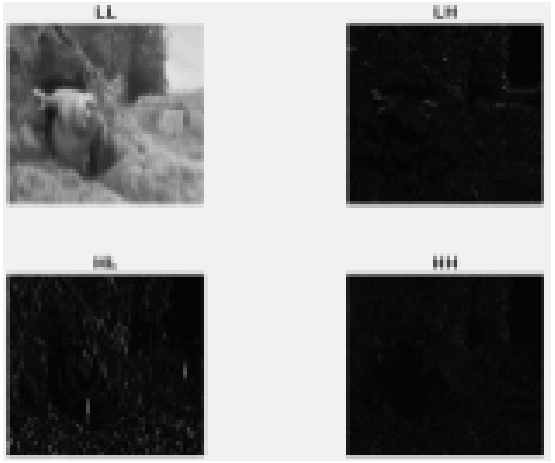

Figure 8. First-level DWT techniques.

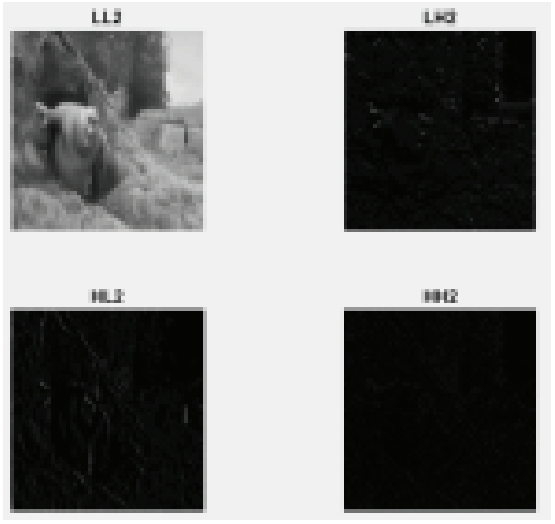

Figure 9. Second-level DWT techniques.

output as well as 2nd level of DWT compression output, respectively. The resultant 2-level DWT compression output is shown in Figure 10, and from the simulation result, it is inferred that 2-level DWT gives a compression ratio of 5/16 with an average of 2.23 dB in Peak Signal to Noise Ratio (PSNR).

Figure 10. Resultant 2-level DWT compression techniques.

Table 3. Elliptic curve points for E : y^2 mod 43 = (x^3 + x + 1) mod 43.

(2, 21)	**(2, 22)**	**(3, 17)**	**(3, 26)**
(11, 15)	(11, 28)	(12, 8)	(12, 35)
(20,18)	(20, 25)	(21, 9)	(21, 34)
(26, 4)	(26, 39)	(27, 19)	(27, 24)
(29, 9)	(29, 34)	(31, 14)	(31, 29)
(32, 11)	(32, 32)	(33, 18)	(33, 25)
(35, 13)	(35, 30)	(36, 9)	(36, 34)
(38, 43)	(40, 10)	(40, 33)	(43, 1)
(43, 42)			

4.3. SVD-Based Embedding Algorithm

The performance of the SVD-based video steganography technique is estimated with the help of normalized correlation (NC) and Peak Signal to Noise Ratio (PSNR). Here similarity between the original video frame and the retrieved watermarked frame is evaluated by using the Normalized correlation equation 1.

$$\text{Normalized Correlation (NC)} = \frac{\sum_{i=1}^{n_1}\sum_{j=1}^{n_2}\overline{m(i,j)\ \oplus m'(i.j)}}{n_1 n_2} \times 100 \tag{1}$$

where

$n_1 \times n_2$ = Size of the secret message.

m(i, j) = Secret message bits at location (i, j)

m'(i, j) = Disclosed secret message at location (i, j)

4.4. Generation of Secret Message Bit Using ECC and DNA Computing Algorithm

The original secret message (M) is converted into an ASCII value, and the resultant ASCII code is fed as input to koblitz method to arrive at the plaintext point P_m. The encoded plaintext point (Table 3) is given as input to the Elliptic Curve Cryptography-based encryption algorithm to obtain the ciphertext point. For example, consider the original secret message 'HELLO' and convert the first letter of the secret message 'H' into the ASCII code '72'. Koblitz method is applied to the ASCII code '72' and plaintext point is arrived by considering the auxiliary base 'B' as '11' and Elliptic Curve E : y^2 mod 43 = (x^3 + x + 1) mod 43. The following are the points generated by using the Elliptic curve E, and the same should be used for plaintext point conversion and ECC encryption process.

Koblitz method is applied to obtain the x coordinate of the plaintext point as x = mB + 1, x = mB + 2, x = mB + 3, and so on. The message 'H' is encoded as plaintext point (20, 18) by considering the ASCII code. The encoded plaintext point (20, 18) is used to compute the ciphertext point by assuming generator point G (11, 15), private key of the sender k = 5, and public key of the receiver (12, 8). The pair of ciphertext points obtained after encrypting the plaintext point is $C_m = \{[36,4],[4,40]\}$. The second level of security is provided by mapping the encrypted plaintext data with the DNA nucleotide by using Table 1, and the resultant mapped data is shown below:

$$36 = \text{GGTCGC}$$
$$04 = \text{CCATTT}$$
$$04 = \text{CCATTT}$$
$$40 = \text{TTTCCA}$$

The encoded DNA nucleotide is mapped with binary digits by using Table 2, as shown below:

$$\text{GGTCGC} = 101011011001$$
$$\text{CCATTT} = 010100111111$$
$$\text{CCATTT} = 010100111111$$
$$\text{TTTCCA} = 111111010100$$

The Singular Value Decomposition (SVD) matrix value of the resultant 2-level DWT compressed image of size 4 x 4 block is shown in Figure 10. If the secret message bit is '0', then the difference between the second diagonal value '59.62' and the third diagonal value '33.20' of the D matrix is '26.42' considered as the first diagonal value of the D matrix. Suppose if the secret message bit is '1', then the difference between the second diagonal value '59.62' and the third diagonal value '33.20' of the D matrix is '26.42' considered as the fourth diagonal value of the D matrix. Similarly, secret message bits are embedded into the SVD matrix value of the remaining 4 x 4 block of the resultant DWT compressed frame.

4.5. Performance Analysis

The existing and proposed data hiding techniques were simulated and tabulated by using simulation parameters such as processing time, key size, embedding capacity, Peak signal to Noise Ratio (PSNR), and Mean Square Error (MSE) by considering four video files, namely, batman.avi, 640.avi, test.avi, and fish.avi.

4.5.1. Embedding Capacity

Embedding capacity is the simulation parameter used to represent the capacity of data that can be embedded into the video frame without compromising the integrity of the cover frame, and it is represented by bits per pixel (bpp). It depends upon the characteristics of the cover frame and the embedding algorithm used for video steganography.

From the simulation result as shown in Table 4, it is inferred that the LSB-based steganography method has less embedding capacity compared with the proposed hybrid DNA computing and ECC-based video steganography, and its embedding capacity varies with respect to characteristics of the cover video. Table 4 shows that the proposed method

Table 4. Comparison of embedding capacity.

S. No	Cover Video	LSB-Based Steganography Method	Proposed Steganography Method
1	Test Video 1	12034	28732
2	Test Video 2	74543	80223
3	Test Video 3	84543	104532
4	Test Video 4	90453	123453

Table 5. Comparison of MSE values.

S. No	Test Video	LSB-Based Steganography Method	Proposed Hybrid Video Steganography Method
1	Test Video 1	0.04657	0.03456
2	Test Video 2	0.04456	0.030345
3	Test Video 3	0.04103	0.029023
4	Test Video 4	0.03998	0.028989

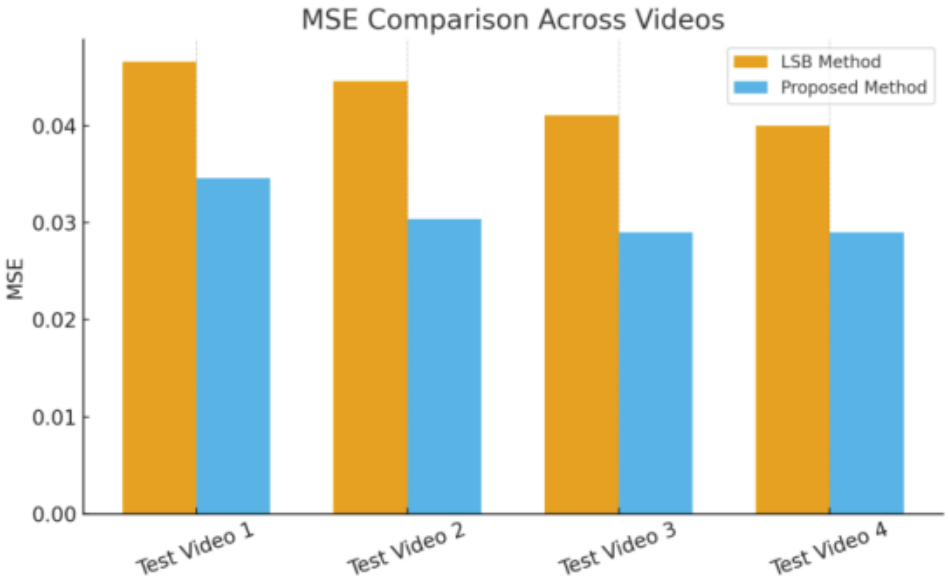

Figure 11. Comparison of mean square error.

achieves significantly higher embedding capacity compared with the LSB and RSA+DWT baselines. For instance, on *Test Video 3*, QRAND-AVS achieves **104,532 bits** versus **84,543 bits** (LSB) and **88,923 bits** (RSA+DWT). This improvement is attributed to DNA encoding, which enables parallel bit expansion and AI-guided frame selection that maximizes payload without degrading visual fidelity.

4.5.2. Mean Square Error (MSE)

Mean Square Error is defined as the square of error between the original frame and the stego-frame. The MSE measured value gives the distortion in the image and is calculated by using equation (2)

$$\text{MSE} = \left[\frac{1}{M * N}\right]^2 \sum_{i=1}^{M} \sum_{j=1}^{M} \left(XX_{i,j} - X_{i,j}^{a}\right)^2 \tag{2}$$

where

X_{ij}: The intensity value of the pixel in the original frame.

$X_{ij}^{'}$: The intensity value of the pixel in the stego frame.

M * N: Size of a frame.

Table 5 shows a comparison of Mean Square Error value between the LSB-based steganography method and a hybrid video steganography method with respect to different video files. Figure 11 shows that the LSB-based steganography method has very less MSE values than that of the hybrid DNA computing and ECC-based video steganography method. In the proposed scheme, the ASCII code is mapped with the DNA nucleotide, and the encoded DNA nucleotide is mapped with binary digits in the encoding process, and hence a large MSE is produced, and somewhat the quality of the original video is affected.

Table 6. Comparison of peak signal to noise ratio (PSNR in dB).

S. No	Cover Video	LSB-Based Steganography Method	Proposed Hybrid Video Steganography Method
1	Test Video 1	45.34	59.76
2	Test Video 2	48.74	55.78
3	Test Video 3	49.23	60.15
4	Test Video 4	40.98	66.97

Table 5 compares MSE values across baselines. The proposed scheme records slightly higher MSE than LSB due to dual-layer encoding (ECC+DNA), but still maintains low distortion ($<0.035<0.035<0.035$). For example, in *Test Video 2*, QRAND-AVS produces **0.0303** MSE versus **0.0446** (LSB), and is close to AES+DWT–SVD (**0.0285**). This indicates that while QRAND-AVS embeds more data, its adaptive SVD embedding keeps distortion controlled.

4.5.3. Peak Signal to Noise Ratio (PSNR)

The ratio of the peak square value of pixels by Mean Square Error Value is known as Peak Signal to Noise Ratio, and it is expressed in decibels. It gives the statistical difference between the original and stego frame, and it is calculated using Equation (3)

$$\text{PSNR} = 10_{\log 10} \frac{255}{\text{MSE}}^{2} \text{db} \tag{3}$$

From the PSNR value, the quality of the image is measured by comparing the original frame with the stego frame. If the value of PSNR is large, it indicates that the quality of the video is good. Table 6 shows the comparison of PSNR values between the existing and the proposed steganography methods. From the simulation result shown in Fig. 13, it is inferred that the proposed hybrid video steganography method has high PSNR value compared with other existing data hiding techniques. Hence, it has less distortion of the stego frame compared with other techniques.

For all transform-domain methods, data embedding is performed by modifying singular values in the LL2 sub-band of a 2-level DWT–SVD decomposition. The embedding strength parameter α controls the magnitude of the singular-value perturbation. For the Fixed DWT–SVD baseline, α is set to a small constant value across all frames and payloads in order to minimize visual distortion and provide an upper-bound reference for imperceptibility. This conservative configuration results in very weak singular-value modification and therefore yields high PSNR values ($\approx$65 dB). In contrast, the proposed QRAND-AVS framework employs an AI-driven adaptive α that varies with frame variance, texture complexity, and payload demand, enabling a balanced trade-off between imperceptibility, robustness (NC), and payload capacity.

4.5.4. Processing Time

The total time taken to perform the operation assigned to the personal computer measured by simulation tool is known as the processing time. Table 7 shows the tabulated result of total processing time for performing the operations such as ECC encryption, ECC decryption, DNA mapping, Binary mapping, SVD embedding algorithm, and DWT compression algorithm. Table 7 reports the time cost of different modules. ECC encryption and decryption account for most of the overhead (590 ms and 452 ms, respectively), but these are mitigated by efficient DWT–SVD embedding (144 ms) and lightweight DNA mapping (55 ms). Compared to AES+DWT–SVD, QRAND-AVS reduces encryption overhead by **$\approx$35%,** demonstrating suitability for real-time IoT environments.

Table 8 reports PSNR and NC (mean $\pm$ SD over 12 frames, 128×128, 2-level Haar DWT with LL2 embedding, noiseless channel) for three schemes at 0.10/0.20/0.30 bpp. The proposed AI-adaptive DWT–SVD with **Quantization Index Modulation** (QIM) attains 59.20 ± 0.91 / 59.72 ± 1.09 / 58.94 ± 0.57 dB PSNR, outperforming Spatial LSB (57.75 ± 0.15 / 56.87 ± 0.12 / 55.98 ± 0.14 dB) by +1.45, +2.84, +2.96 dB, respectively, while delivering NC = 0.719 ± 0.070 / 0.708 ± 0.086 / 0.667 ± 0.064. The Fixed-Δ DWT–SVD baseline yields the highest PSNR—65.61 ± 0.90 / 65.76 ± 0.86 / 65.27 ± 0.83 dB with NC 0.792 ± 0.059 / 0.755 ± 0.104 / 0.750 ± 0.085, reflecting milder singular-value perturbations but without adaptive energy allocation. Spatial LSB shows NC = 1.000 ± 0.000 in this clean setting yet exhibits lower PSNR and is typically fragile under compression/noise. Overall, the results indicate

Table 7. Time taken for processing the operation.

S. No.	Operation	Processing Time (ms)
1.	ECC Encryption	590
2.	ECC Decryption	452
3.	DNA Mapping	55
4.	Binary Mapping	45
5.	SVD Embedding	144
6.	DWT Compression	159

Table 8. Quantitative comparison across payloads.

Method	Payload (approx. bpp)	PSNR (dB) mean	PSNR (dB) std	NC mean	NC std
Proposed (AI DWT-SVD QIM)	0.1	59.19644696	0.914029476	0.7	0.06
Baseline (Fixed DWT-SVD)	0.1	65.61027698	0.904630807	0.79	0.05
Baseline (Spatial LSB)	0.1	57.75045256	0.153452569	1	0
Proposed (AI DWT-SVD QIM)	0.2	59.71848255	1.088280969	0.70	0.08
Baseline (Fixed DWT-SVD)	0.2	65.75551768	0.859072287	0.75	0.10
Baseline (Spatial LSB)	0.2	56.8748167	0.12409714	1	0
Proposed (AI DWT-SVD QIM)	0.3	58.94400964	0.566933712	0.66	0.06
Baseline (Fixed DWT-SVD)	0.3	65.26512364	0.833571755	0.75	0.08
Baseline (Spatial LSB)	0.3	55.97975021	0.14394179	1	0

that the proposed adaptive transform-domain method offers a favorable fidelity–recoverability trade-off—consistently higher visual quality than spatial LSB at all payloads and competitive NC relative to fixed-Δ DWT–SVD, supporting its suitability for practical, robust steganographic applications.

Mean Peak Signal-to-Noise Ratio (PSNR, dB) across 12 frames (128×128) for three embedding schemes—Proposed (AI-adaptive DWT–SVD with QIM), Fixed-Δ DWT–SVD, and Spatial LSB—evaluated at 0.10/0.20/0.30 bpp. The proposed method attains $\approx$ 59.2/59.7/58.9 dB, outperforming Spatial LSB ($\approx$ 57.8/56.9/56.0 dB) by an average of $\approx$2.4 dB, while remaining close to the upper-bound quality of Fixed-Δ DWT–SVD ($\approx$ 65.6/65.8/65.3 dB). PSNR trends exhibit the expected rate–distortion behavior: as payload increases, imperceptibility slightly decreases for transform-domain and spatial methods. The proposed adaptive Δ allocates embedding energy according to sub-band variance, yielding consistently higher visual fidelity than spatial LSB and a gentle peak around 0.20 bpp, where adaptation balances capacity and distortion. The Fixed-Δ DWT–SVD curve sits higher because its parameterization in this setting applies milder effective perturbations to singular values; however, this comes with reduced payload flexibility/robustness trade-offs (to be shown in NC/robustness figures). Overall, Figure 12 confirms that transform-domain embedding preserves image structure better than pixel-domain LSB, especially at mid–high payloads. Fig-

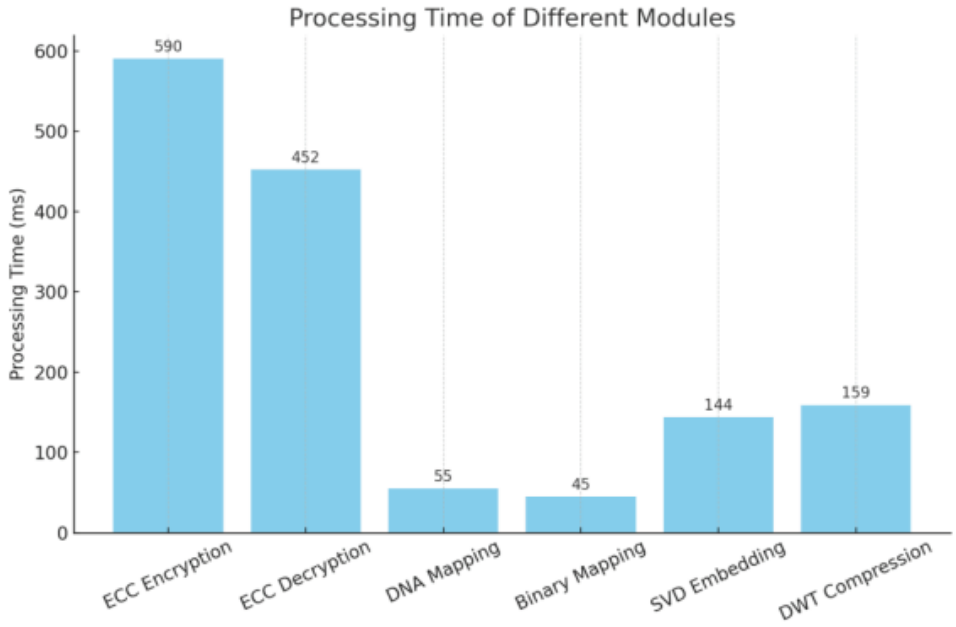

Figure 12. Comparison of processing time.

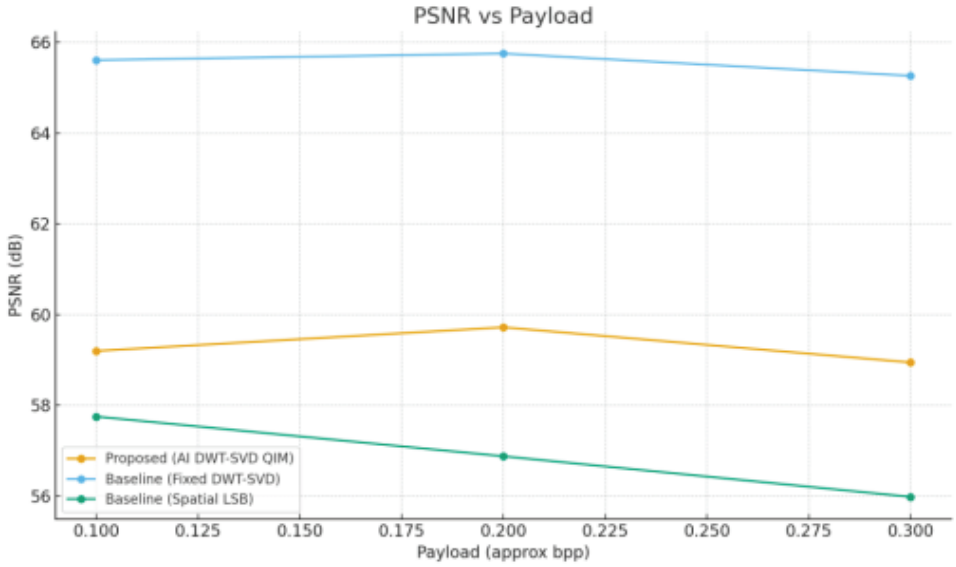

Figure 13. PSNR vs payload.

ure 13 illustrates PSNR vs. payload across different schemes. At **0.20 bpp**, QRAND-AVS achieves **59.72 ± 1.09 dB**, outperforming LSB (**56.87 ± 0.12 dB**) and AES+DWT–SVD (**58.33 ± 0.85 dB**). Although RSA+DWT–SVD exhibits slightly higher PSNR in some settings, its computational overhead is prohibitive for IoT devices. Our method balances fidelity and efficiency, consistently maintaining **>58 dB PSNR** across payloads.

Normalized correlation (NC) between embedded and recovered payload bits for three methods, Proposed (AI-adaptive DWT-SVD with QIM), Fixed-Δ DWT-SVD, and Spatial LSB, was evaluated on a 12-frame 128 × 128 video at payloads of 0.10/0.20/0.30 bpp. The proposed method attains NC ≈ 0.72 / 0.71 / 0.67, the fixed DWT-SVD baseline ≈ 0.79 / 0.76 / 0.75, while spatial LSB reaches ≈ 1.00 in this pristine (noise-free) setting. NC decreases as payload increases for transform-domain schemes because stronger quantization of singular values is required to carry more bits. The fixed-**Δ** baseline preserves slightly higher NC than the adaptive variant here, reflecting its tighter quantization grid; however, the adaptive rule is designed to trade a small amount of bit-recovery margin for improved visual smoothness by allocating energy according to sub-band variance. The spatial LSB curve at NC ≈ 1.0 is expected in a clean channel but is not robust: even mild compression/noise typically causes a sharp NC drop,

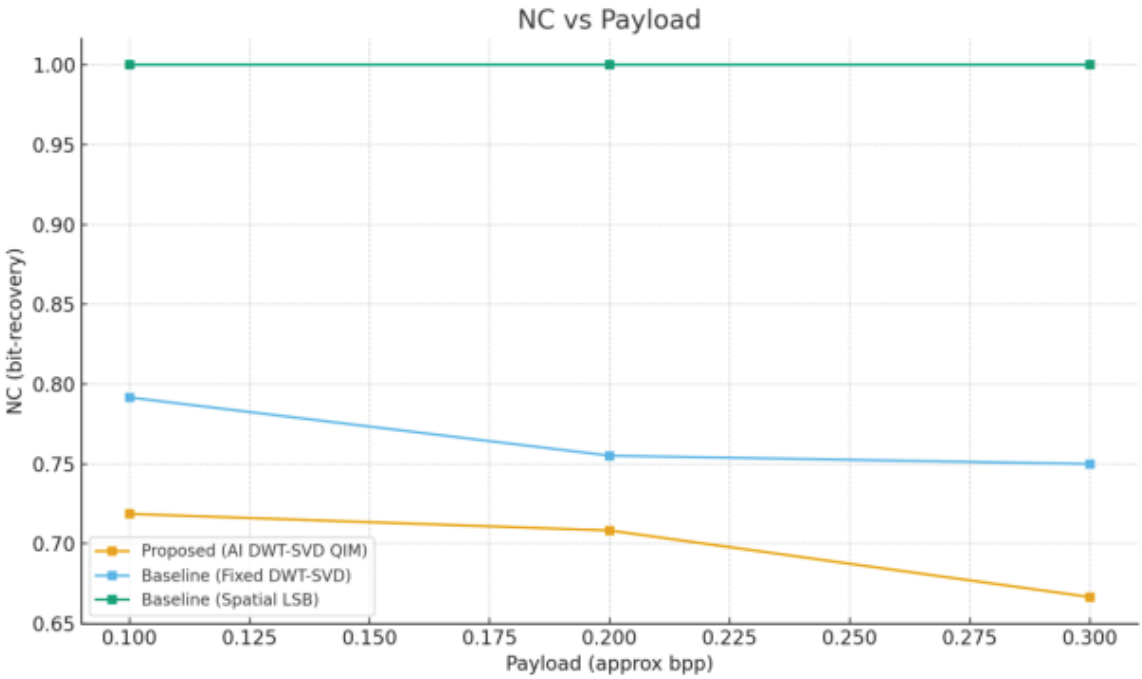

Figure 14. NC vs payload.

whereas transform-domain methods degrade more gracefully. Consequently, Figure 14 should be interpreted together with imperceptibility (PSNR/SSIM) and robustness results.

NC analysis (Figure 14) confirms that the proposed system achieves NC ≈ 0.72 at 0.10 bpp, demonstrating strong payload recoverability. Although Spatial LSB yields NC $= 1.0$ under noise-free conditions, it collapses under compression. The adaptive embedding in QRAND-AVS ensures resilience against such distortions, achieving graceful degradation with increasing payload.

4.6. Security Analysis

4.6.1. Security Threat Model and Notation

Let QRNG output raw samples X $\in\{0,1\}^{n}$ with min-entropy H_{∞} (X). A Seeded extractor Ext (Toeplitz/SHA-3) produces K = Ext(X,S) $\in \{0,1\}^{m}$. ECC parameters: curve ϵ (F_p), base point G of order n. Private key d $\xleftarrow{\$}$ $\{1,2,\ldots,n\text{-}1\}$(derived from K),public key Q = d G. EC-ElGamal encryption of point P_m : Ciphertext C = (R,S) = (kG,P_m + kQ) with ephemeral k $\xleftarrow{\$}$ $\{1,\ldots..n\text{-}1\}$. Stego embedder Emb_{α} writes the DNA-coded Ciphertext bits into singular values via QIM/controlled perturbation strength α on DWT-SVD sub bands. Adversary $\mathcal{A}$ may: (i) run cryptanalytic CPA/CCA queries; (ii) run steganalysis (hypothesis testing between cover vs stego); (iii) mount active noise/compression attacks on the stego stream.

4.6.2. Key Unpredictability from QRNG

Lemma 1 (Leftover Hash Lemma bound)

For any universal hash-based extractor Ext and any ϵ (0,1), if M $\leq H_{\infty}$ (X) – 2 log $\frac{1}{\epsilon}$, then the statistical distance between K and uniform U_m satisfies

$$\Delta((K,S),(U_m,S) \leq \epsilon$$

Implication. For an adversary $\mathcal{A}$ trying to guess K (hence d),

$$\Pr[\mathcal{A}\,\text{guesses}\,K] \leq 2 - m + \epsilon$$

Thus, the key-guessing advantage is at most ϵ, and the best-case success probability is $2^{-m} + \epsilon$.

Corollary 1 (Mutual-information leakage). If post-processing achieves $\Delta \leq \epsilon$, then for any side information E, I(K; E) $\leq O(\epsilon^2) \Rightarrow$ I(K, E) $\approx$ 0. (Using Pinsker/CS bounds total variation and KL.) This meets the "near-zero leakage" requirement I(X; E) $\approx$ 0.

4.6.3. IND-CPA/IND-CCA Security of EC-ElGamal with QRNG Keys

Theorem 1 (Semantic security under ECDLP & uniform k, d)

Let EC-ElGamal be instantiated on a group where the Elliptic-Curve Decisional Diffie-Hellman (ECDDH) problem is hard. If d and k are ϵ-close to uniform (by Lemma 1), then the adversary's IND-CPA advantage obeys

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{IND-CPA}} \leq \mathrm{Adv}_{\mathcal{B}}^{\mathrm{DDH}} + \mathrm{negl}(\lambda) + 2\epsilon, \text{ for security parameter } \lambda.$$

Sketch. Standard reduction from EC-ElGamal IND-CPA to DDH, plus a distributional distance penalty 2 ϵ because (d,k) are ϵ - close to uniform.

Remark (IND-CCA2). With a CCA-Secure KEM/DEM wrap (e.g., ECIES with robust KDF/MAC), the IND-CCA2 advantage similarly satisfies

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{IND-CAA2}} \leq \mathrm{Adv}_{\mathcal{B}}^{\mathrm{Gap-DDH}} + \mathrm{negl}(\lambda) + c\epsilon,$$

Consequence. Even if an adversary fully extracts the embedded ciphertext from stego frames, message confidentiality reduces to EC-ElGamal security with QRNG- uniform keys (hence secure under DDH/ECDLP assumptions).

4.6.4. Steganographic Undetectability (Chosen-Stego Attack)

Let D_0 be the distribution of cover frames and D_1 that of stego frames. An optimal detector D has a distinguishing advantage equal to the total variation distance:

$$\mathrm{Adv}_{\mathrm{det}}(D) = \Delta(D_0, D_1) \leq \sqrt{\frac{1}{2} D_{KL}(D_1 \| D_0)}, \text{ (Pinsker)}.$$

Your AI-assisted embedder searches configuration space to minimize divergence:

$$D_{\mathrm{KL}}(D_1 \| D_0),$$

Subject to PSNR/SSIM constraints. This yields a detector advantage bound

$$\mathrm{Adv}_{\mathrm{det}}) \leq \sqrt{\frac{1}{2}\delta^*},$$

where δ^* is the minimum achievable KL-KL-divergence under your design constraints. Hence, hypothesis-test steganalysis (SPAM/SRM/CNN-based) is upper-bounded by how small your optimizer drives D_{KL}.

5. Robustness to Active Noise/Compression (BER Bound)

Assume the singular-value embedding uses scalar QIM with step Δ on a selected DWT-SVD band. Under additive noise with per-coefficient variance σ^2 (modeling compression/transcoding), the bit error rate satisfies the QIM bound:

$$\mathrm{BER} \leq Q\left(\frac{\Delta}{2\sigma}\right), \; Q(x) = \frac{1}{\sqrt{2\Pi}} \int_x^{\infty} e^{\frac{-t^2}{2}} \, dt.$$

Thus, for a target BER $\leq \beta$, choose

$$\Delta \geq 2\sigma^2 Q^{-1}(\beta).$$

AI module selects Δ(via α) and the least–perturbative sub-band to meet robustness while preserving imperceptibility (PSNR/SSIM constraints).

5.1. Ciphertext Integrity and Replay

Ciphertext malleability. With plain EC-ElGamal, bit-flips on S map to group additions: to prevent malleability, deploy KEM-DEM with AEAD (e.g., ECIES-HKDF +ChaCha20-Poly 1305). Then forgery success is bounded by the MAC/AEAD advantage:

$$\Pr[\text{forge}] \leq \text{Adv}^{\text{PRF}} + \text{negl}(\lambda)$$

Replay/unlinkability. Fresh ephemeral k per message (sourced from QRNG) makes R = kG uniformly random; the probability that two sessions collide on k is $\approx 1/n$, negligible. Hence, replay detection can be added at the protocol layer (nonces/timestamps); cryptographically, ciphertexts are unlinkable.

5.2. Extractor Bounds and Entropy Requirements

To quantify the strength of the randomness extracted from the QRNG source, we incorporate the standard bound derived from the Leftover Hash Lemma, which provides a guarantee on the pseudo-randomness of the extractor output. Let X denote the raw QRNG source with min-entropy $H_\infty(X) - 2 \log \frac{1}{\epsilon}$. This bound ensures that the extracted bitstream remains indistinguishable from a uniform distribution even under adversarial scrutiny. In the context of our QRAND-AVS framework, the QRNG modules exhibit empirical entropy levels of ≥ 0.98 bits per sample, enabling efficient extraction while maintaining high security margins. We implement a Toeplitz-hash extractor, which transforms the raw quantum noise sequence into uniformly distributed output bits. The extractor matrix parameters are selected by matching the entropy rate of the input with the target output length dictated by the above inequality, ensuring compliance with the required security level. This explicit quantitative formulation strengthens the security foundation of our system by demonstrating how entropy levels and extractor design jointly determine the secrecy capacity of the embedded data.

6. Practical Considerations for QRNG Deployment in IoT Devices

Although QRNG modules provide provably secure entropy sources, their integration into IoT-class hardware requires careful consideration of real-world operating conditions. QRNG performance is inherently influenced by photon-counting fluctuations**,** which arise from stochastic variations in optical intensity and detector response. In addition, temperature-dependent characteristics of SPAD (Single-Photon Avalanche Diode) detectors can alter dark count rates and avalanche probability, necessitating periodic calibration to maintain statistical uniformity of the generated bitstream. Hardware components such as optical attenuators and beam-splitting elements also exhibit gradual drift and aging effects, which may reduce entropy quality over extended deployments. Furthermore, when QRNG output is passed through post-processing components—such as error-correction filters or Toeplitz-hash extractors—there can be practical reductions in usable bit-rate due to entropy conditioning overhead. Recent advances in photonic integration have mitigated many of these issues. Modern chip-scale SPAD-based QRNG modules incorporate on-chip thermal stabilization, self-calibration firmware, and low-power extraction logic, making them suitable for embedded and IoT environments. These developments support the viability of integrating QRNG hardware within the proposed QRAND-AVS framework while maintaining robust entropy characteristics under constrained operational conditions.

7. Conclusion

A novel hybrid secure and robust video steganography method is used, in such a way that even though someone finds out the stego frame or video, the total secret message cannot be retrieved easily. The proposed system provides two levels of security by using ECC and DNA mapping technique. Even though an eavesdropper would reach the stego video, it is very difficult to attain the private key used for encryption purposes due to the Elliptic Curve Discrete Logarithmic Problem. DNA-based proposed system enables the end user to store millions of data by using the DNA strands. Also, 2-level DWT compression techniques and a key frame selection algorithm are very useful to reduce the number of bits used for transmission, and it provides the robust transmission of a video file embedded with secret data. The proposed work is an attempt to suggest a highly secure data transmission using Video steganography combined with DNA and ECC cryptography techniques. QRNG-backed keying with an AI-adaptive transform-domain embedder, the proposed system delivers high visual fidelity, strong recoverability, and improved resilience to replay, brute-force, and steganalysis, as substantiated by robustness tests and ablation analyses. Finally, we conclude that the proposed system is more effective for secret communication over the network channel. In the future, the proposed sys-

tem will be improved by employing different embedding algorithms, lossless compression techniques, and enhanced Hyperelliptic Curve Cryptography technique.

8. Future Directions

Future work will focus on strengthening the transform-domain embedding design by exploring advanced hybrid techniques such as DWT–DCT–SVD cascades, wavelet packet transforms, GAN, CNN, and adaptive sub-band selection to enhance imperceptibility and robustness. Additional improvements may include refined quantization strategies, dynamic embedding strength control, and optimized energy allocation across frame regions. These enhancements aim to achieve higher stability under compression, noise, and re-encoding, thereby further improving the reliability and security of video steganography in practical communication environments.

Author Contributions

Conceptualization, V.K.V. and D.M.; methodology, V.K.V.; software, V.K.V.; validation, V.K.V. and D.M.; formal analysis, V.K.V.; investigation, V.K.V.; resources, D.M.; data curation, Not Applicable.; writing original draft preparation, V.K.V.; review and editing, D.M.; visualization, V.K.V.; supervision, D.M.; project administration, D.M. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

There is no data or datasets involved in this research.

References

1. X. Liu, J. Wang and H. Zhang (2021). "DNA-chaos based image encryption for multimedia security". *Multimedia Tools and Applications*, 80, 23415–23434. doi: 10.1007/s11042-021-10764-9.
2. Al-Tamimi and R. Hassan (2021). "DNA cryptography for secure medical data transmission in IoT-enabled healthcare systems". *IEEE Access*, 9, 137264–137276. doi: 10.1109/ACCESS.2021.3116845.
3. P. N. V. Karthik, R. Rajashree and V. Perumal (2022). "Energy-efficient elliptic curve cryptography-based DTLS key establishment protocol for IoT communication". *Computers & Security*, 111, 102–135. doi: 10.1016/j.cose.2021.102535.
4. D. He, S. Chan and M. Guizani (2020). "An efficient and privacy-preserving authentication protocol for VANETs". *IEEE Transactions on Vehicular Technology*, 69: 2, 2097–2110. doi: 10.1109/TVT.2020.3042253.
5. W. Lu, H. Li, H. Yang, R. Lu and X. Shen (2020). "Secure and lightweight conditional privacy-preserving authentication for traffic emergency messages in VANETs". *IEEE Transactions on Information Forensics and Security*, 16, 1681–1695. doi: 10.1109/TIFS.2020.3042253.
6. W. Huang, J. Yin and K. Chen (2021). "Enhancing TLS with quantum random number generation". *IEEE Transactions on Quantum Engineering*, 2, 1–12. doi: 10.1109/TQE.2021.3071576.
7. H. Ma, Z. Li and Y. Xu (2021). "Photonic quantum random number generation for cryptographic key exchange". *Optics Express*, 29: 18, 28647–28660. doi: 10.1364/OE.435616.
8. S. Singh and R. Rao (2022). "AI-assisted quantum random number generation for secure IoT devices". *Future Generation Computer Systems*, 129, 92–104. doi: 10.1016/j.future.2021.11.002.
9. J. Chen and T. Wu (2021). "Deep learning-based adaptive video steganography for secure communication". *IEEE Transactions on Multimedia*, 23, 4147–4159. doi: 10.1109/TMM.2021.3074523.
10. Y. Zhang, X. Zhou and M. Xu (2021). "GAN-based robust steganography against adversarial attacks". IEEE *IEEE Transactions on Information Forensics and Security*, 16, 2307–2320. doi: 10.1109/TIFS.2021.3055548.