FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 1 | Pages 60-65 | e-ISSN: 2347-470X

Design of an Efficient & Secure Steganographic Model using Modified LSB & Encryption Process

Ekta[1], and Ajit Singh[2]

[1]*Department of Computer Science and Engineering, Bhagat Phool Singh Mahila Vidyalaya, India, ektayadav956@gmail.com*
[2]*Department of Computer Science and Engineering, Bhagat Phool Singh Mahila Vidyalaya, India, bpsmv.ajit@gmail.com*

***Correspondence:** ektayadav956@gmail.com

ABSTRACT- This paper introduces a novel steganographic model for robust multimodal data security, seamlessly integrating a modified Least Significant Bit (LSB) technique with encryption, making it applicable to diverse data types such as images, audio, video, and text. Overcoming challenges posed by existing complex models and communication delays, our approach employs a modified LSB technique to encode similar sized data samples, followed by dynamic bioinspired elliptic curve cryptography (BECC) utilizing a Mayfly Optimization (MO) Model. This adaptive strategy optimizes curve types and prime key sets, significantly enhancing data security while minimizing delays and complexities across diverse data sizes. The proposed model achieves an 8.3% reduction in encryption and steganographic process delays, while simultaneously maintaining superior Peak Signal to Noise Ratio (PSNR) and lower Mean Squared Error (MSE) levels compared to existing methods when applied to the same data samples. This highlights its effectiveness in securing dynamic datasets without compromising efficiency.

Keywords: Multimodal, Security, Data, Samples, PSNR (Peak Signal to Noise Ratio), MSE (Mean Squared Error), BECC (bioinspired elliptic curve cryptography), LSB (Least Significant Bit), MO (Mayfly Optimization).

ARTICLE INFORMATION

Author(s): Ekta and Ajit Singh;

Received: 23/09/23; **Accepted**: 02/01/24; **Published**: 05/02/24;
E- ISSN: 2347-470X;
Paper Id: IJEER231015;
Citation: 10.37391/IJEER.120110
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-12/ijeer-120110.html

Publisher's Note: FOREX Publication stays neutral with regard to jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

The essence of steganography lies in three key operations: hiding information, conveying it, and deciphering it accurately. The effectiveness of a steganographic system hinges on its ability to fulfill all these characteristics. Researchers have been proposed numerous distinct approaches including discrete wavelet transforms (DWT), discrete cosine transforms (DCT), and least significant bit (LSB) [1,2], may be used to disguise information sets via Deep Reinforcement Learning (DRL) [3, 4]. Integrating encryption with high-speed communication protocols such as multiple-input multiple-output (MIMO) systems, orthogonal frequency division multiplexing (OFDM), and others enables secure data delivery. Figure 1 depicts the entire steganographic process together with explanations of the primary system components [5, 6]. In this process, the embedded message is transmitted with the input image to the embedding process or cover media, using different modalities such as graphics, text, audio, or video. The cover medium and the information to be hidden are merged using a steganographic key, ensuring synchronous operation between parties [7]. The embedded message retrieval must be error-free, the final image must not reveal any signs of a hidden message, and both the cover media and the embedded message must be appropriately sized for real-time applications. To address these challenges, steganographic images are transmitted over attack-vulnerable mediums like email or instant messaging services, subject to channel models like Rayleigh, Rician, Nakagami M, and additive white Gaussian noise. Binaries of Message Size Encoding (BMSE) introduce random noise to each image component through these channels [8, 9, 10]. It is crucial that the information extraction technique can identify sensitive data amidst background noise or other distortions, as the encrypted message is jumbled. Recovered information undergoes tests to ensure it hasn't been altered before further processing.

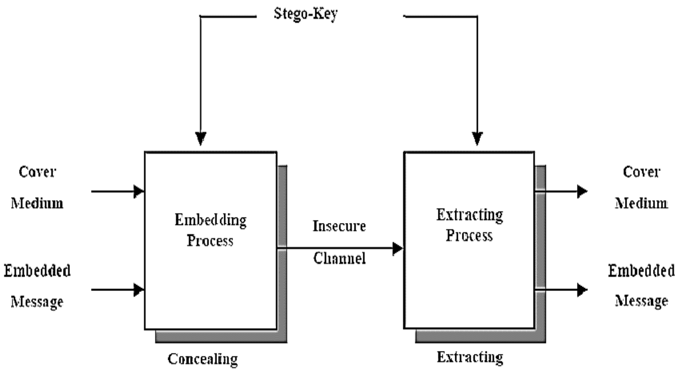

Figure 1. Design of a typical image steganographic process

Before delving into specific works, it is crucial to evaluate the key components such as encryption, integrity, robustness, hiding capacity, authentication, and visual quality metrics like

Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). Figure 1 highlights essential steganographic characteristics. PSNR and MSE provide insights into visual quality [9,11] and deviation between reconstructed and original images, respectively. Stego keys embedded in cover media retrieve secret data, and image steganography algorithms, often incorporating Generative Adversarial Networks (GANs) [11], aim to optimize encryption, integrity, and robustness. Spatial domain bitmap image methods transform pixels visibly, offering high capacity but potentially compromising security. RGB techniques like LSB replacement, pixel indication, optimal pixel adjustment, and secure key-based image realization minimize impact on original pixel values while inserting the message sequentially into the right-most bits of the pixel array [3, 4]. Indicator channels enhance security in pixel indicator and LSB techniques [1]. Frequency domain methods, using DCT or DWT, as demonstrated in JPEG image format algorithms, indicate better security than spatial domain approaches [9,14]. DCT-based methodologies leverage connections between STCs and DCT coefficients [2], [7], [11], with basic DCT techniques. Bit-plane encoding and redundancy evaluation enhance concealment capacity while focus on the Integer Wavelet Transform (IWT) [15]. JPEG cover photographs exhibit superior security, while PNG images offer flexibility through palette or image data additions [12,13]. The research incorporates an efficient bioinspired-based data-driven method for increased flexibility in multiple use cases. Numerous methods for rapidly creating embedding and extractions of building components have been reported. In the following sections, we will discuss the specifics, advantages, and disadvantages of some of these algorithms, followed by the implementation of the recommended paradigm and an assessment of its effectiveness. The study concludes with in-depth observations, evaluations of the proposed paradigm, and recommendations for improvement under multiple use cases.

2. DIFFERENCE BETWEEN ECC & BECC

In this paper, we enhance the efficiency of the steganographic process by introducing a modified Least Significant Bit (LSB) technique for encoding similar-sized data samples. The distinctive feature of this model lies in the subsequent integration of bioinspired elliptic curve cryptography (BECC). This innovative approach infuses bioinspired elements into the well-established elliptic curve cryptography (ECC). The introduced Bioinspired ECC utilizes a Mayfly Optimization (MO) Model, optimizing curve types and prime key sets to enhance data security. Stored parameters ensure the secure handling of dynamic datasets through the application of bioinspired encryption.

A key distinction from conventional ECC is the optimization process; Bioinspired ECC employs biological-inspired techniques like Mayfly Optimization for key generation and encryption. This bioinspired approach not only reinforces encryption security but also maintains lower complexity and delay, as evidenced in our presented results.

3. DESIGN OF AN EFFICIENT & SECURE STEGANOGRAPHIC MODEL USING MODIFIED LSB & ENCRYPTION PROCESS

According to the literature research, it can be shown that current data security models use these strategies to increase the resilience of data against various threats. However, these models either make data transfer activities more difficult or need more delay. This section suggests creating an innovative and secure steganographic model using a modified Least Significant Bit (LSB) and encryption procedure to get around these problems. For the data kinds of images, audio, video, and text, the suggested model is helpful. It first employs a modified LSB approach to encrypt data samples of comparable size, and then it employs a bio-inspired elliptic curve cryptography (BECC) Model to enhance data security while preserving reduced latency & complexity under samples of various sizes. The Mayfly Optimization (MO) Model is used by the BECC to choose the best curve type and prime key sets. In order to use the bioinspired encryption parameter sets to protect dynamic datasets, these parameters are saved for future use. The suggested approach combines an enhanced hash LSB algorithm with AES encryption to enhance the security and QoS performance of steganographic systems. The model makes use of the whole 24-bit (RGB) color space to increase the system's payload capacity. According to Hecht, the human eye cones are only 2% sensitive to blue color, 33% sensitive to green color, and 65% sensitive to red color. By example, the blue (B) color component of the input picture is often used by the enhanced hash LSB model to conceal hidden information. Using the LSB approach, the red (R) and green (G) components of the picture are little changed. The steps provided allow for the better hash LSB model's flow to be followed. *Equation 1,2,3* given below are for shifting bits.

3.1 Match the size of data to be stegano graphed (E) to be 1/3 of the size of input data (I) via resizing operations

3.2 For every value in the array '*E*', perform the following operations,

3.2.1 Find the Most Significant Bit from *E*, and embed this bit to the Least Significant Bit of the I data *via equation 1*,

$$I_{ij} = \left(I_{ij}\&\, 0xFE\right) \mid \left(\left(E_{ij}\&\, 0x80\right) \gg 4\right) \qquad (1)$$

3.2.2 Store the next 2 significant bits in the next byte of the input data samples *via equation 2* as follows:

$$I_{i+1j} = \left(I_{i+1j}\&\, 0xFD\right) \mid \left(\left(E_{ij}\&0x60\right) \gg 4\right) \qquad (2)$$

3.2.3 Next 3 bits are encoded in the 3rd byte *via equation 3*

$$I_{i+2j} = \left(I_{i+2j}\&0xF8\right) \mid \left(\left(E_{ij}\&0x1D\right) \gg 4\right) \qquad (3)$$

3.3 All these operations are repeated for the full length of input samples. As an example, consider the 3 consecutive bytes of scaled input as,

I1 = 00110011

I2 = 01010101

I3 = 10101010

Let the byte value of data to be embedded be,

E = **1 0111**010

After embedding, the output values will be,

I1' = 00110011

I2' = 01010101

I3' = 10101 110

The embedded pixels are encrypted via an efficient bioinspired Mayfly Optimization (MO) Model, which uses Elliptic Curve Cryptography (ECC) that works as per the following operations,

3.4 Setup the Mayfly Optimizer constants as follows,
3.4.1 Initialize a count of Mayflies (NM)
3.4.2 Setup a count of iterations (NI)
3.4.3 Set a learning threshold (L_r)

3.5 To perform Mayfly optimizations, a set of Mayflies are generated as per the following operations,
3.5.1 Select an ECC Curve *via equation 4*,

$$C = STOCH(1, N_c) \qquad (4)$$

Where, N_c represents total number of curves available for encryption operations. These include secp224, secp256, etc.

3.5.2 Based on this curve selection, encrypt the steganographed input via *equation 5 & 6*

$$C1 = P + r * (x_2, y_2) \qquad (5)$$

$$C2 = r * (x_1, y_1) \qquad (6)$$

Where, x & y are set of encryption and decryption points on the selected curves.

3.6 Based on this encryption process, evaluate fitness of Mayflies *via equation 7*,

$$f = \frac{d(encrypt)}{len(C1) + len(C2)} \qquad (7)$$

Where, $d(encrypt)$ represents the delay needed for encryption of the data via selected curves.

3.7 Repeat this process for all Mayflies, and then estimate fitness threshold *via equation 8*, where L_r stands for learning rate.

$$f_{th} = \frac{1}{NM} \sum_{i=1}^{NM} f_i * L_r \qquad (8)$$

3.8 Mayflies with f>f_th are discarded and reproduced in the next iteration, while other Mayflies are passed directly to the next set of iterations. This process is repeated for N_i iterations, and at the end of final iteration, curve with minimum fitness levels is selected for the encryption process. The encryption process is accompanied by a decryption process *via equation 9*,

$$Decrypted = C2 - (Encrypted * C1) \quad (9)$$

This decrypted data is de-steganography *via equation 10*, which assists in generation of the original data sets,

$$E' = (I1' \& 0x01) \ll 8 \mid ((I2' \& 0x03) \ll 7) \mid ((I3' \& 0x07) \ll 4) \qquad (10)$$

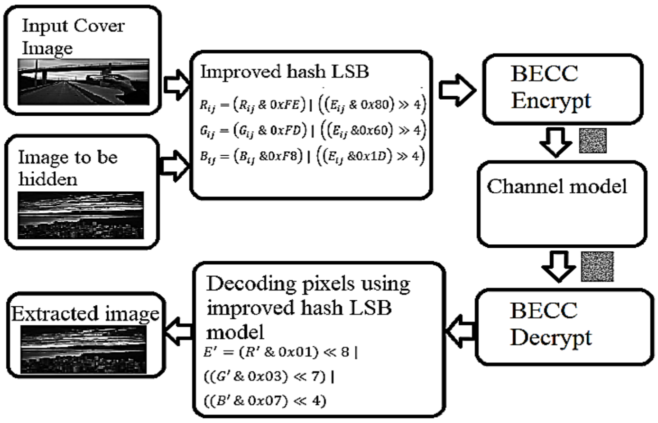
Input Cover Image
Image to be hidden
Improved hash LSB
$R_{ij} = (R_{ij} \& 0xFE) \mid ((E_{ij} \& 0x80) \gg 4)$
$G_{ij} = (G_{ij} \& 0xFD) \mid ((E_{ij} \& 0x60) \gg 4)$
$B_{ij} = (B_{ij} \& 0xF8) \mid ((E_{ij} \& 0x1D) \gg 4)$
BECC Encrypt
Channel model
BECC Decrypt
Decoding pixels using improved hash LSB model
$E' = (R' \& 0x01) \ll 8 \mid ((G' \& 0x03) \ll 7) \mid ((B' \& 0x07) \ll 4)$
Extracted image

Figure 2. Design of the proposed BECC Model for improving security of the steganography process

This process assists in regeneration of the original data with higher security and lower delay levels. RGB channel model is used in *figure 2*. Estimation of these levels and their comparison with other models is discussed in the next section of this text.

4. RESULT AND ANALYSIS

To validate the performance of this model, it was tested on the following data samples.

Visual Question Answering Data Samples (https://visualqa.org/)

Text Amazon Reviews Data Samples (https://www.kaggle.com/datasets/bittlingmayer/amazonreviews)

Audio Speech Emotion Data Samples (http://m3c.web.auth.gr/research/aesdd-speech-emotion-recognition/)

All these sets were combined to form a total of 6k samples, out of which 80% were used for training, while 10% each were used for testing & validation operations. Results of the steganography and encryption process can be observed from *figure 3 & 4*, where different types of images were embedded under real-time scenarios.

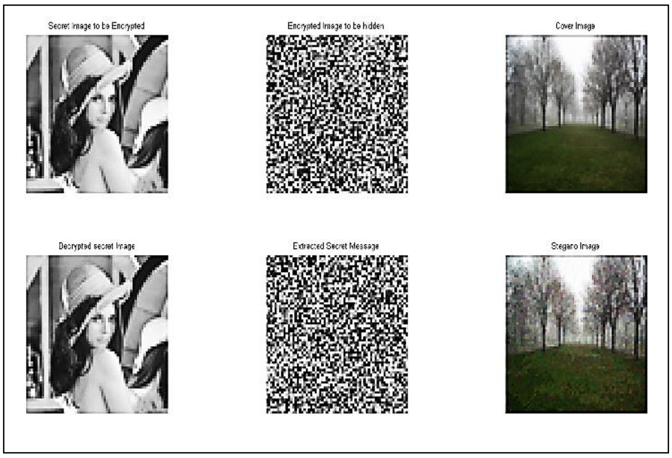

Figure 3. Grey image (2D) embedded into color image (3D)

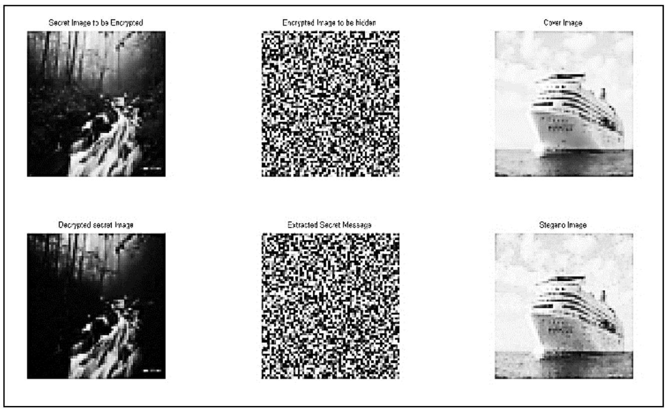

Figure 4. Color image hidden into color image sets

Based on these sample sets, the Minimum Mean Squared Error (MMSE), Peak Signal to Noise Ratio (PSNR), and delay were estimated as per *equations 11, 12 & 13* as follows,

$$MMSE = \frac{1}{N}\sum_{i=1}^{N} I_{orig_i} - I_{decoded_i} \dots (11)$$

$$PSNR = 20 * \log_{10}\left(\frac{1}{MMSE}\right) \dots (12)$$

$$Delay = t_{complete} - t_{start} \dots (13)$$

Where, I_{orig}&$I_{decoded}$ represents original and decoded inputs, while $t_{complete}$&t_{start} represents completion and start timestamps for the steganographic operations with N number of values per input sets. As per these evaluations, the MMSE was compared with DRL [4], BMSE [9], and GAN [11] w.r.t. Test Data Samples (TDS) in *table 1* as shown.

Based on this analysis it can be observed that the proposed model is 6% more effective than DRL [4], 4.5% more effective than BMSE [9], and 9% more effective than GAN [11] under different test data set, which can also be observed from figure 5, wherein accuracy values are visualized. The results of PSNR are shown in figure 6, wherein PSNR of the proposed model is compared with other reference models.

Table. 1: **Comparison of the MMSE was compared with DRL [4], BMSE [9], and GAN [11] w.r.t. Test Data Samples (TDS)**

TDS	MMSE DRL [4]	MMSE BMSE [9]	MMSE GAN [11]	MMSE HSM LE [Present]
1000	0.098	0.119	0.131	0.064
1125	0.098	0.120	0.132	0.064
1250	0.098	0.120	0.132	0.064
1375	0.099	0.121	0.133	0.064
1500	0.099	0.121	0.133	0.064
1625	0.099	0.122	0.133	0.065
1750	0.099	0.122	0.134	0.065
1875	0.099	0.122	0.134	0.065
2000	0.099	0.123	0.134	0.065
2125	0.099	0.123	0.135	0.065
2250	0.100	0.124	0.135	0.065
2375	0.100	0.124	0.135	0.066
2500	0.100	0.125	0.136	0.066
2750	0.100	0.125	0.136	0.066
3000	0.100	0.126	0.137	0.066
3250	0.100	0.126	0.137	0.066
3500	0.101	0.127	0.137	0.067
3750	0.101	0.127	0.138	0.067
4000	0.101	0.128	0.138	0.067
4250	0.101	0.128	0.138	0.067
4500	0.101	0.128	0.139	0.067
5000	0.101	0.129	0.139	0.067
5500	0.102	0.129	0.140	0.068
6000	0.102	0.130	0.140	0.068

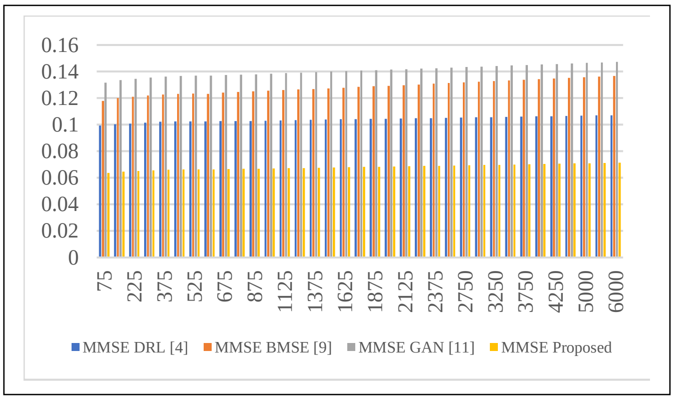

Figure 5. MMSE of different methods

Based on this analysis it can be observed that the proposed model is 6% more effective than DRL [4], 2% more effective than BMSE [9], and 6% more effective than GAN [11] under different test data set, which can also be observed from *figure 6*, wherein these values are visualized. Using similar training and testing sets, delay needed for evaluation can be observed from *figure 7*.

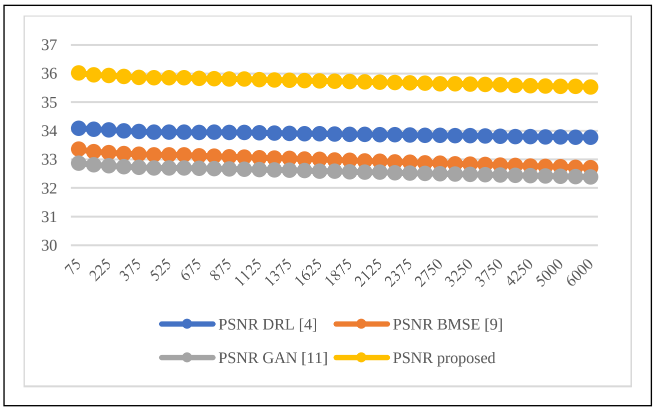

Figure 6. PSNR of recognition for different test image sets

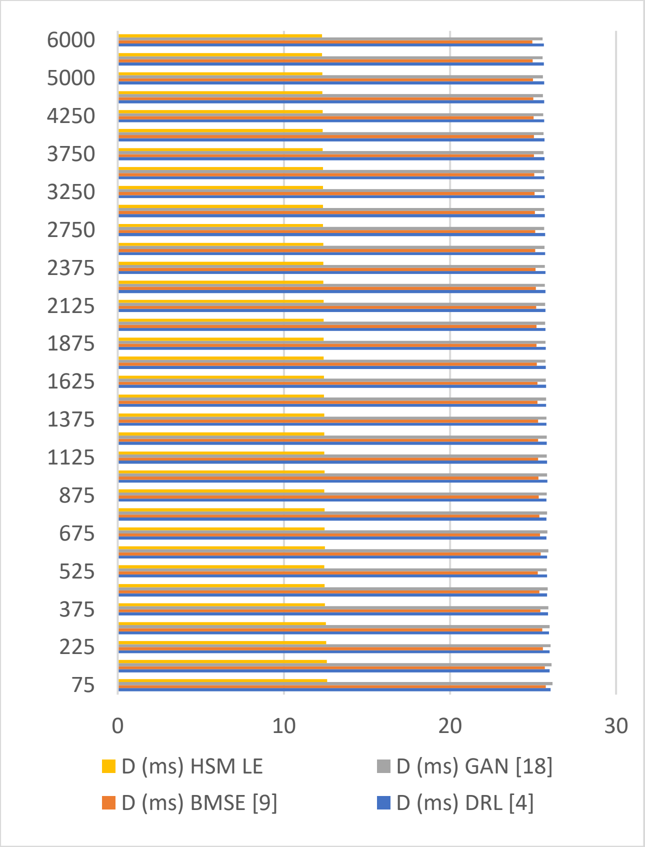

Figure 7. Delay needed for analysis of different models

Based on this analysis and *figure 7*, it can be observed that the proposed model is 19% more effective than DRL [4], 8% more effective than BMSE [9], and 18% more effective than GAN [11] under different test sets.

5. DISCUSSIONS ON ATTACK AND SECURITY ANALYSIS

The proposed method combines modified LSB steganography and Bioinspired Elliptic Curve Cryptography (BECC) to enhance data security. Evaluating its effectiveness against existing methods involves considering potential attacks and the method's response to these challenges.

5.1 LSB Steganography Resilience: Traditional LSB steganography is vulnerable to visual and statistical analysis attacks. The modified LSB technique in this model addresses these weaknesses by introducing alterations that enhance resistance against detection.

5.2 Encryption Strength: Encryption methods, including ECC, face vulnerabilities such as brute force attacks or cryptanalysis. The integration of Bioinspired ECC, utilizing the Mayfly Optimization (MO) Model, enhances encryption security by selecting optimal curve types and prime key sets, making it more resistant to conventional attacks on ECC-based encryption.

5.3 Data Communication Security: The proposed method reduces encryption and steganography delays by 8.3%, maintaining high security levels. This faster processing ensures robust security, minimizing opportunities for attackers to intercept or compromise data during transmission.

5.4 Multimodal Data Versatility: The proposed model is versatile and applicable to various data types (images, audio, video, and text). This adaptability ensures a consistently high level of security across different data modalities, reducing vulnerabilities associated with specialized methods for each data type.

In summary, the proposed method effectively addresses vulnerabilities in traditional LSB steganography, strengthens encryption, and minimizes processing delays which compelling choice for enhancing real-world data security.

6. CONCLUSION AND FUTURE SCOPE

The proposed model demonstrates versatility across various data types, including images, audio, video, and text. It employs a refined LSB technique for encrypting comparable-sized data samples, followed by the innovative integration of bio-inspired elliptic curve cryptography (BECC) Model. This not only enhances data security but also maintains lower delay and complexity across samples of diverse sizes. The effectiveness of the proposed model is evident in its 9% improvement over GAN [18], 4.5% over BMSE [9], and 6% over DRL [4] in terms of MMSE when applied to various test image sets. Similar advantages are observed in PSNR, where the proposed model outperforms DRL [4] by 6%, BMSE [9] by 2%, and GAN [11] by 6%. The delay analysis reveals the superior performance of the proposed model, surpassing DRL [4] by 19%, BMSE [9] by 8%, and GAN [11] by 18% across diverse test image sets.

This model's efficacy extends to a broad spectrum of real-time steganographic applications, making it a valuable asset for future research. Researchers can validate the model under different real-time scenarios, enhancing its performance through secret sharing mechanisms. Additionally, the integration of deep learning for identifying steganographic patterns and selecting optimal indices to conceal samples promises improved PSNR, even under elevated noise levels in real-time scenarios. The proposed model, with its robust optimizations, sets the stage for further exploration and advancements in real-time steganography applications.

REFERENCES

[1] R. Meng, Q. Cui, Z. Zhou, Z. Li, Q. M. J. Wu and X. Sun, "High-Capacity Steganography Using Object Addition-Based Cover Enhancement for Secure Communication in Networks," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 2, pp. 848-862, 1 March-April 2022, doi: 10.1109/TNSE.2021.3137829.

[2] M. Sharifzadeh, M. Aloraini and D. Schonfeld, "Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image Steganography," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 867-879, 2020, doi: 10.1109/TIFS.2019.2929441.

[3] R. Cogranne, Q. Giboulot and P. Bas, "Efficient Steganography in JPEG Images by Minimizing Performance of Optimal Detector," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1328-1343, 2022, doi: 10.1109/TIFS.2021.3111713.

[4] W. Pan, Y. Yin, X. Wang, Y. Jing and M. Song, "Seek-and-Hide: Adversarial Steganography via Deep Reinforcement Learning," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 11, pp. 7871-7884, 1 Nov. 2022, doi: 10.1109/TPAMI.2021.3114555.

[5] J. Zhang, X. Zhao, X. He and H. Zhang, "Improving the Robustness of JPEG Steganography with Robustness Cost," in IEEE Signal Processing Letters, vol. 29, pp. 164-168, 2022, doi: 10.1109/LSP.2021.3129419.

[6] A. A. Lopez-Hernandez, R. F. Martinez-Gonzalez, J. A. Hernandez-Reyes, L. Palacios-Luengas and R. Vazquez-Medina, "A Steganography Method Using Neural Networks," in IEEE Latin America Transactions, vol. 18, no. 03, pp. 495-506, March 2020, doi: 10.1109/TLA.2020.9082720.

[7] S. Banerjee and G. K. Singh, "A Robust Bio-Signal Steganography with Lost-Data Recovery Architecture Using Deep Learning," in IEEE Transactions on Instrumentation and Measurement, vol. 71, pp. 1-10, 2022, Art no. 4007410, doi: 10.1109/TIM.2022.3197781.

[8] M. Aloraini, M. Sharifzadeh and D. Schonfeld, "Quantized Gaussian JPEG Steganography and Pool Steganalysis," in IEEE Access, vol. 10, pp. 38031-38044, 2022, doi: 10.1109/ACCESS.2022.3165031.

[9] M. M. Mahmoud and H. T. Elshoush, "Enhancing LSB Using Binary Message Size Encoding for High Capacity, Transparent and Secure Audio Steganography–An Innovative Approach," in IEEE Access, vol. 10, pp. 29954-29971, 2022, doi: 10.1109/ACCESS.2022.3155146.

[10] R. Gurunath, M. F. J. Klaib, D. Samanta and M. Z. Khan, "Social Media and Steganography: Use, Risks and Current Status," in IEEE Access, vol. 9, pp. 153656-153665, 2021, doi: 10.1109/ACCESS.2021.3125128.

[11] J. Tan, X. Liao, J. Liu, Y. Cao and H. Jiang, "Channel Attention Image Steganography with Generative Adversarial Networks," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 2, pp. 888-903, 1 March-April 2022, doi: 10.1109/TNSE.2021.3139671.

[12] Y. -Q. Zhang, K. Zhong and X. -Y. Wang, "High-Capacity Image Steganography Based on Discrete Hadamard Transform," in IEEE Access, vol. 10, pp. 65141-65155, 2022, doi: 10.1109/ACCESS.2022.3181179.

[13] Z. Zhang, G. Fu, R. Ni, J. Liu and X. Yang, "A generative method for steganography by cover synthesis with auxiliary semantics," in Tsinghua Science and Technology, vol. 25, no. 4, pp. 516-527, Aug. 2020, doi: 10.26599/TST.2019.9010027.

[14] Z. Zhang, G. Fu, R. Ni, J. Liu and X. Yang, "A generative method for steganography by cover synthesis with auxiliary semantics," in Tsinghua Science and Technology, vol. 25, no. 4, pp. 516-527, Aug. 2020, doi: 10.26599/TST.2019.9010027.

[15] H. Tian, J. Wu, H. Quan and C. -C. Chang, "Detecting Multiple Steganography Methods in Speech Streams Using Multi-Encoder Network," in IEEE Signal Processing Letters, vol. 29, pp. 2462-2466, 2022, doi: 10.1109/LSP.2022.3226126.