

Design of an Efficient Multimodal Image Steganography Framework with Multi-Domain Feature Analysis and Secret Sharing Operations

Ekta^{1*}, Ajit Singh²

Submitted: 18/01/2024 Revised: 27/02/2024 Accepted: 04/03/2024

Abstract: The study introduces an innovative multimodal picture steganography framework addressing data security concerns in digital communication. The framework integrates multi-domain feature analysis and secret-sharing techniques for enhanced security confidentiality. Utilizing resizing and bitwise operations for steganography, along with (n, k) Shamir Secret Sharing for visual cryptography, the model excels in security measures. The algorithmic approaches of the proposed model designed for text, image, audio, and video processing within the multimedia landscape are thoroughly discussed. Comparative analyses demonstrate the superior performance of the proposed model in terms of RMSE, MAE and PSNR across audio, video, picture, and text modalities when compared to existing models. Significant improvements are observed in RMSE values, with reductions of 45%, 36%, and 15%, along with the improved PSNR values in the audio case compared to Chen L, Chen Y and Mo X, respectively. In the image case, the model consistently achieves lower RMSE and MAE values with higher PSNR values, showing improvements of about 48%, 35%, and 13% compared to Chen L, Chen Y and Mo X. Video steganography sees approximately 30% and 21% reductions in RMSE values compared to Chen L and Chen Y, with improved PSNR values. Text steganography displays noteworthy advancements compared to Chen L, including a 13% reduction in delay compared to Mo X. The proposed model outperforms existing models Chen L, Chen Y and Mo X in audio, video, image, and text steganography. The proposed model demonstrates superior performance and reduced processing time and provides an effective solution for securely embedding information. With applications spanning digital media, telecommunications, and information security, it offers a reliable and versatile solution for secure data embedding in diverse scenarios.

Keywords: Multimodal steganography, Visual cryptography, Shamir Secret Sharing, Multi-domain feature analysis, Data security

1. Introduction

In the dynamic landscape of contemporary digital advancements, prioritizing data security and ensuring the confidentiality of communications has become imperative. The extensive exchange of sensitive information across diverse communication channels shows a growing demand for robust methodologies to shield this data from unauthorized access and interception [1,2]. Steganography and the visual cryptography landscape include diverse models that emerge as viable methods to address these concerns effectively.

Steganography achieves concealment by embedding information within multimedia content [3, 4], while Visual Cryptography combines secrets into multiple components [5].

In steganography various models are explored: (a) Least Significant Bit Substitution involving the replacement of the least significant bits (LSB) in the cover data with secret datasets, susceptible to statistical analysis and advanced algorithms [4, 6, 7, 8], (b) Spread Spectrum Approaches

dispersing confidential data across various frequency domains, resistance, yet adding complexity and potential degradation of cover datasets [9,10] and (c) Techniques in the Transform Domain like discrete cosine transform (DCT) and the discrete wavelet transforms (DWT) [11, 12], leverages frequency characteristics of the cover data to integrate secret information, enhances imperceptibility and resistance, though demands computational resources during embedding and extraction processes [13, 14, 15].

There are various models in visual cryptography: (a) $(2,2)$ In the visual cryptography scheme, a binary secret is split into two shares, each represented by a different random pattern. The hidden information is revealed upon superimposing these two shares. Although simple, it is limited to binary secrets. It requires accurate alignment of the shares for successful reconstruction [19,20], (b) (n,n) Visual Cryptography Scheme fragments a share into n shares with different random patterning processes, offering greater flexibility and capability for larger secrets. However, the presence of all n shares is necessary for successful reconstruction [19,20] and (c) Shamir (k,n) Secret Sharing System in which the system divides the secret into n shares, with k shares sufficient for reconstructing the secret. Utilizing both audible and visual components, this system provides enhanced protection and fault tolerance compared to basic visual cryptography [5]. Despite significant contributions, notable limitations

¹PhD Scholar, Bhagat Phool Singh Mahila Vishwavidyalaya, Haryana, India

²Professor, Dept. of CSE, Bhagat Phool Singh Mahila Vishwavidyalaya, Haryana, India

Email: bpsmv.ajit@gmail.com

* Corresponding Author Email ektayadav956@gmail.com

persist, including unimodal focus and a lack of capability to address multimodal scenarios in the existing model.

Therefore, improvements in imperceptibility, robustness, and data security within established models are needed. Some recent works in cryptography and steganography deal with leveraging network capabilities, private keys, and neural networks. A detailed review of crypto-stego is also given by Jan et al. [21]. A multiscale fusion Extraction Block leveraged with a U-Net network for steganography has been described by Zeng et al. [21]. Multiple-image steganography using private keys has been described by Hyeokjoon et al. [22]. Convolution neural networks have been used for multi-domain learning in steganography by Wang et al. [23]

The present study introduces a novel, advanced, comprehensive architecture for a highly efficient multimodal picture steganography system that integrates multi-domain feature analysis and secret-sharing procedures. The proposed framework includes steganography and visual cryptography operations across four modalities: image, audio, video, and text. For steganography, a meticulous scaling strategy is employed to reduce the size of the data to be concealed to approximately one-third of the size of the input data, ensuring the effective embedding of confidential information. The steganography method involves a sequence of bitwise operations, called bit shifting, to conceal the desired data within the utilized datasets and samples. In addition to steganography, the framework incorporates visual cryptography based on the (n, k) Shamir Secret Sharing method [2] as a complementary procedure to steganography. The synergistic interplay of visual cryptography and steganography further fortifies the security of the encoded confidential information. The details of the algorithmic approaches embedded within the proposed model, crafted explicitly for processing text, image, audio, and video within the expansive multimedia landscape, are systematically discussed in the present study. Extensive testing across diverse multimedia datasets has been done to validate the efficacy and efficiency of this proposed framework.

The proposed framework not only furnishes a dependable and secure approach to conceal sensitive information within multimedia data but also serves as a catalyst for secure communication and safeguarding data privacy across digital media, telecommunications, and information security domains. The paper delves into the intricate details of the proposed framework, spanning the methodology, findings, and analysis. This comprehensive exploration aims to underscore the manifold advantages of the framework and shed light on its potential applications in real-world scenarios.

2. Methodology

A synthesis of multi-domain feature analysis, secret sharing activities, and visual cryptography has been employed to construct the multimodal picture steganography framework. This design intends to enhance the steganography process' security, efficiency, and resilience by integrating multimodal capabilities for embedding secret information into multimedia datasets. The flow diagram of the proposed technique is illustrated in Figure 1.

2.1 Examination of Features Across Modalities

The initial phase of the framework involves multi-domain feature analysis, leveraging the unique characteristics of various modalities, including image, audio, video, and text. The design process includes:

2.1.1 Choosing of Modalities for Analysis: Modalities are selected based on their relevance to the data that needs to be concealed and their potential to yield distinct and complementary qualities.

2.1.2 Feature Extraction: It is performed for each chosen modality, capturing essential qualities such as colour histograms, texture descriptors, and local binary patterns for pictures, spectral energy and Mel-Frequency Cepstral Coefficients (MFCC) for audio, among other modality-specific features, exploitable for embedding confidential information.

2.1.3 Feature Analysis and Fusion: The features collected from various modalities undergo a deep analysis and then merged to provide a comprehensive representation of datasets and samples. Various analyses, such as statistical, correlation, and machine learning methods, are employed to explore links and dependencies between characteristics.

2.1.4 Feature Selection and Dimensionality Reduction: Techniques such as feature ranking, feature significance analysis, and principle component analysis (PCA) are employed to choose discriminative and representative features, intending to reduce the computational complexity and improve the framework's overall performance. Upon completion, the multi-domain feature analysis, evaluated, fused, and appropriately reduced in dimensionality, forms a robust foundation for the subsequent phases of the multimodal picture steganography framework process.

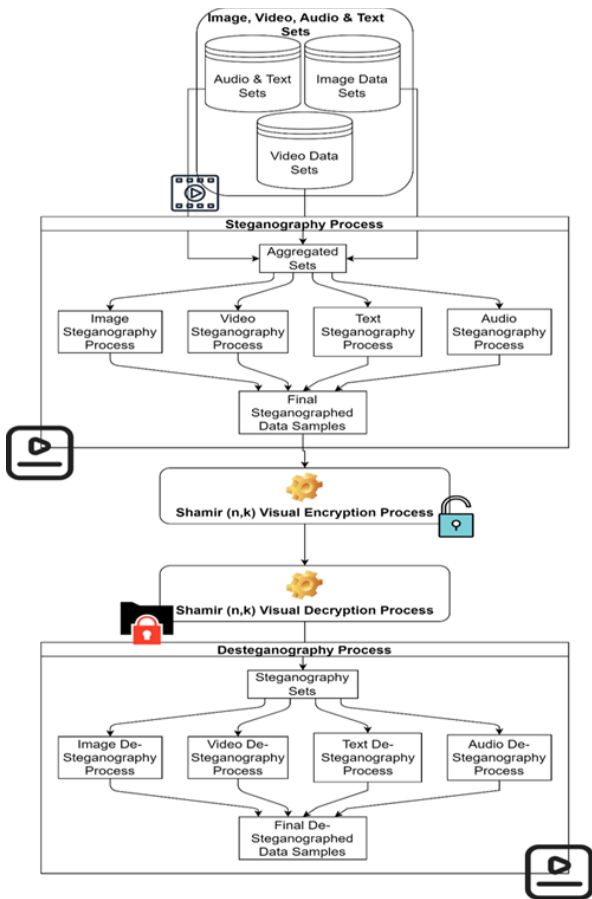


Fig 1. Flow diagram of the proposed technique

2.2 Operations for Sharing Confidential Information

The second element of the proposed architecture focuses on sharing confidential information using the (n, k) Shamir Secret Sharing system. The following procedures were involved in this design process:

2.2.1 Selection of the Shamir Secret Sharing Scheme: After thoroughly evaluating various secret sharing schemes, the (n, k) Shamir Secret Sharing scheme was chosen for its increased security and fault tolerance. This scheme divides secret information into n shares, requiring k shares to reconstruct the original secret. This strategy aligns well with the proposed framework by balancing adaptability and safety.

2.2.2 Production of Shares: This involves dividing confidential information into n unique shares, ensuring that each share individually revealed no information about the original secret, preserving its integrity. These shares are distributed across various visual components, including pictures, music, video, and text, to maximize protection and resiliency for confidential information. Appropriate embedding methods were applied to conceal each share within multimedia datasets and samples, ensuring their invisibility to the viewer.

2.2.3 Reconstructing the Original Secret: Reconstructing the original secret necessitated collecting at least k shares as the procedures specified by the Shamir Secret Sharing

system to rebuild the original file. This ensures the precise reconstruction without compromising the safety of the information sets. The successful completion of the secret sharing operations component has endowed the developed multimodal picture steganography framework with an effective method of segmenting and distributing secret information across various visual aspects.

3 Steganography Operations

The steganography operations within the proposed framework aim to seamlessly embed secret information into cover data while preserving data integrity and remaining undetectable. The following procedures were involved in this design process:

3.1 Downsizing Operation: A downsizing operation was used to reduce the data to be steganographed (E) to about one-third of the size of the supplied data (I). Image resizing maximizes the efficiency of cover data utilization and minimizes discernible differences introduced by the embedding process.

3.2 Embedding Confidential Information: A sequence of embedding operations was conducted for each value in the array 'E' to conceal confidential information within the read-in data (I). Bitwise manipulations were performed, involving embedding the most significant bit (MSB) of each element in E into the least significant bit (LSB) of the corresponding element in I. Equation 1 was utilized for this embedding process, ensuring the retention of the original data while incorporating confidential information.

$$I_{ij} = (I_{ij} \& 0xFE) | ((E_{ij} \& 0x80) \gg 4) \dots (1)$$

3.3 Storage of Additional Bits: Besides embedding the MSB, the framework stores the following two significant bits in the succeeding byte of the input data using Equation 2. This step ensures data sample integrity and Equation 3 completes encoding the next three bits in the third byte of the message. These processes are applied across all input samples, securely dispersing and concealing confidential information within cover datasets and samples.

$$I_{i+1j} = (I_{i+1j} \& 0xFD) | ((E_{ij} \& 0x60) \gg 4) \dots (2)$$

$$I_{i+2j} = (I_{i+2j} \& 0xF8) | ((E_{ij} \& 0x1D) \gg 4) \dots (3)$$

With the completion of these operations' components, the multimodal image steganography framework successfully implants secret information within cover data, maintaining detectability and preserving data sample integrity. Integrating multi-domain feature analysis, steganography methods, and secret sharing procedures establishes a practical and secure multimodal image steganography framework, providing increased security, resilience, and efficiency in embedding secret information into multimedia datasets and samples.

The workflow of this study can be succinctly outlined as follows:

Input:

- Data (image, audio, video, or text)
- Secret message or data to be hidden (if applicable)

Output:

- Securely encoded data (stego-data)

Process:

1. Select the Data Type:

- Choose the data type (image, audio, video, or text).

For Image Data Type:

- Apply a modified Least Significant Bit (LSB) technique to encode similar-sized data samples into the image.
- Embed the secret message or data into the LSB of the image pixels.

For Audio Data Type:

- Apply a modified LSB technique to encode similar-sized data samples into the audio file.
- Embed the secret message or data into the LSB of the audio samples.

For Video Data Type:

- Apply a modified LSB technique to encode similar-sized data samples into the video frames.
- Embed the secret message or data into the LSB of the video frames.

For Text Data Type:

- Apply a modified LSB technique to encode similar-sized data samples into the text document.
- Embed the secret message or data into the LSB of the text characters.

2. Utilize the Bio-inspired Elliptic Curve Cryptography (BECC) model for enhancing data security:

- Generate an elliptic curve and prime key sets using the Mayfly Optimization (MO) Model.
- Store these optimal curve types and prime key sets for future reference.

3. Encrypt the Stego-Data using the BECC Model:

- Apply the selected elliptic curve and prime key sets for encryption.
- Perform encryption on the stego-data samples.

4. Store Encrypted Data

- Save the encrypted data for future use or transmission.

5. Evaluate Quality:

- Calculate Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) to assess the quality of the encoded data samples.

6. Output:

- Output the securely encoded data (stego-data) and the BECC encryption parameters.

7. Performance Comparison:

- The proposed method reduces the delay needed for encryption and steganographic processes by 8.3% compared to existing methods while maintaining high PSNR and low MSE levels for the same data samples.

A. Algorithms of the proposed model for multimedia

The algorithmic approaches designed for text, image, audio, and video processing within the multimedia landscape are discussed below.

a. LSB Algorithm for Text:

Input:

- Text Message (Message)
- Cover Text (Cover)
- Key for Encryption (Key)

Output:

- Stego Text (Stego_Message)

Algorithm:

1. Divide the Text Message (Message) into smaller chunks if needed, ensuring each can be encoded separately.
2. For each chunk in the Text Message:
 - a. Convert the chunk into a binary representation.
 - b. Apply encryption to the binary chunk using the provided Key.
 - c. Embed the encrypted chunk into the Cover Text (Cover) using a specific method to hide the data within the text.
 - d. Append the resulting text with the embedded chunk to the Stego Text (Stego_Message).
3. Return the Stego Text (Stego_Message) as the output.

b. LSB Algorithm for Image:

Input:

- Secret Image (Secret_Image)
- Cover Image (Cover_Image)

- Key for Encryption (Key)

Output:

- Stego Image (Stego_Image)

Algorithm:

1. Divide the Secret Image (Secret_Image) into smaller blocks or chunks.
2. For each block in the Secret Image:
 - a. Apply encryption to the block using the provided Key.
 - b. Embed the encrypted block into the Cover Image (Cover_Image) using a specific method to hide the data within the image.
3. Return the resulting Cover Image (Cover_Image) with the embedded blocks as the Stego Image (Stego_Image).

c. LSB Algorithm for Audio

Encoding:

- i. Input the text message that is to be embedded.
- ii. Read the audio file and text message in binary.
- iii. The converted binary audio file is sampled into 8-bit equal-size samples.
- iv. Store audio files in a matrix of $a[8][8]$.
- v. Select data reside on the Fibonacci index [j] of the matrix of the audio file.
- vi. Taking this data of the Fibonacci index, select the index value where $a[j] \% 2 == 0$
 Where 'j' is the Fibonacci index of the matrix.
- vii. Embed the data in the reverse order in LSB at the selected position.
- viii. Repeat steps 6 to 8 until the complete text is encoded.

Decoding:

- i. Read the audio file in binary form.
- ii. Select the value at the Fibonacci index [j].
- iii. Retrieve the index value of $a[j] \% 2 == 0$
- iv. Decode the encoded data from the LSB technique.
- v. Store the binary value of the Least Significant Bits.
- vi. Convert the binary values to decimal to get the ASCII values of the secret message.

- vii. From the ASCII value, read the secret message.

d. LSB Algorithm for Video

Encoding:

C:- Carrier Video Stream

Cf:- Set of Frame of Carrier Video Stream
H:-Hidden Image.

Hf:- Set of Images.

HT:- Stego Video Stream

HTf:- Set of Frame of Stego Video Stream
HT:- Reconstructed Video Stream

HTf:- Set of Frames of Reconstructed Stream
K: -Key

Input:- Carrier Video C(W, H, Nc), Hidden Image H(W, H, Nh), Key.

Output:- Stego Video HT(W,H,N)

Algorithm:- Stego Video (C, H, K)

Where C and H are the carrier Video and hidden Image with height H and Width W, Number of Frames Nc and Nh attributes and Symmetric encryption key.

```

{
Extract Frames of carrier video Cf and Secret Image Hf,
respectively.
Cf= Extract_Frames(C)
Hf=Images(H)
1. N= Nc
2. For k=1 to N//Work for each frame of video C and H.
{
i. Read Images Hf[k]//One frame from each
set
Message=Hf(k)
ii. Represent Images Hf(k) in integer.
iii. Prepare a header for the size of Images
and add it to the beginning of the frame.
Header=size(Message)
//In integer, total 8bits 4-4 to each Height and Width.
New_Message=Add(Header,Message)
iv. For each Used Image, Perform
Encryption with Key k
Encrypt_Message = XOR (New_Message,k)
v. Read Frame

```

$C_f(k)Cover=C_f(k)$
)
 vi. Embed the secret frame under the cover frame's LSB using sequential encoding with RGBBGRRGB with a predefined pattern.

//R.G.B means each bit stored in the next pixel's Red, Green, and Blue bands.

Stego_Message = Embed (Cover, Encrypt_Message)

vii. Generate the StegoFrame
 $HT_f(k)=Stego_Message$
 e

}

Add the Stego Frames set HT_k to form video with proper frame rate and compression.

}

Decoding:

Input: - Stego_Video $HT(W, H, N)$, Key.

Output: - Hidden/Secret Images $HT(W, H, N_h)$

Algorithm:- Extract_Video (HT, K)

//Where HT is the Hidden Images with Height H and Width W , Number of Images N attributes

{

Extract frames set HT_f from the Stego video.

$HT_f=Extract\ frames(HT)$

3. $N_h=N$

4. Fork=1toN//Work for frameset of video HT

{

i. Read frame $HT_f[k]$ //One frame for each set HT_f .

Stego_Message= $HT_f(k)$

ii. Extract Header from frames which was added at the time of encoding from LSB of stego frame following sequential decoding with RGBBGRRGB predefined pattern

Header=LSB(Stego_Message)//OnlyLSB //of 8 bytes of
 $Steg0_MessageSecret_Message=LSB(Stego_Message)$

//LSBofwholeStego_MessageexceptFirst8bytes.

iii. Perform Decryption of Header and

Secret_Message with Keyk

Header=XOR (Header,k)

Secret_Message=XOR(Secret_Message,k)

iv. Reconstruct the Hidden Images from Secret_Message.

$HT(k)$ Reconstruct(Secret_Message)

}

}

The (n, k) Shamir Secret Sharing scheme, employed post-steganography, enhances security and fault tolerance. Figures 2 (a) and 2 (b) illustrate the secret sharing and recovery phase.

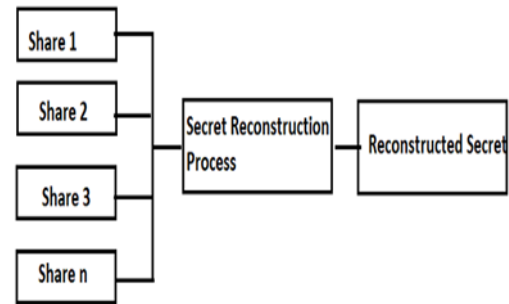


Fig 2 (a): Secret sharing process

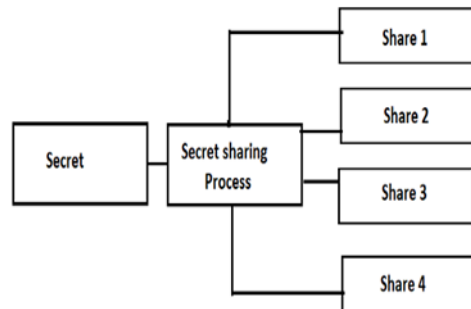


Fig 2 (b): Secret recovery process

3. Results and Discussion

This section presents a comprehensive comparative analysis of the proposed multimodal with three alternative models, focusing on the steganography and cryptography processes applied to audio, video, picture, and text data samples.

3.1 Audio Data Case:

Table 1 illustrates the superior fidelity of our proposed model in preserving original audio material, as indicated by lower RMSE and MAE values compared to [16, 17, and 18]. The RMSE values have improved by 45%, 36%, and

15% from [16, 17, and 18], respectively. Additionally, the higher PSNR value indicates practical signal quality preservation, showing improvements of approximately 13%, 9%, and 6% compared to [16, 17, and 18], respectively. Notably, the proposed model exhibits reduced processing time, facilitating faster embedding and extracting confidential information.

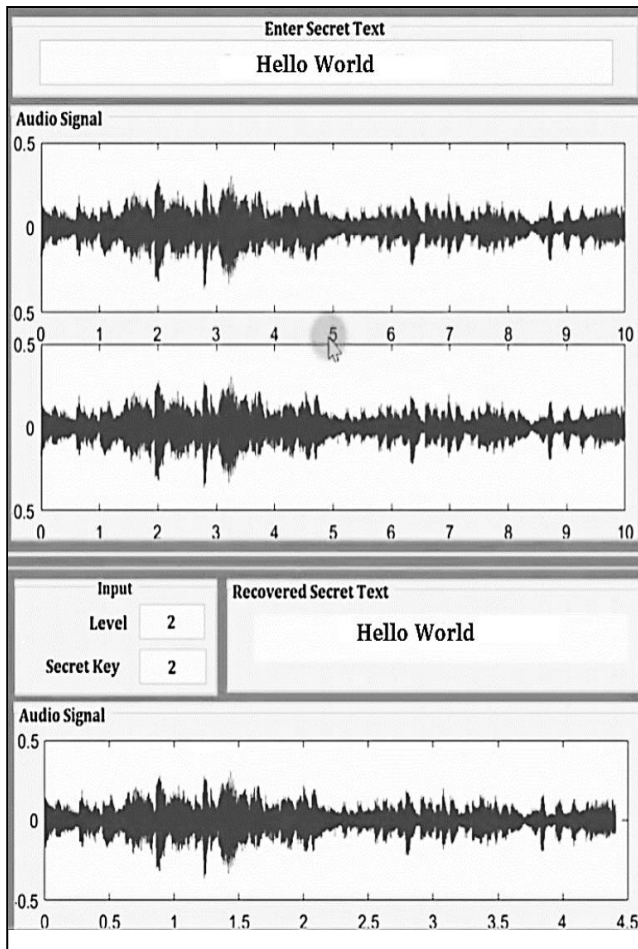


Fig 3: Results of the Audio Steganography Process.

3.2 Video Data Case:

In video steganography (Table 2), our model consistently outperforms our counterparts [16, 17, and 18], achieving lower RMSE and MAE values and higher PSNR values, signifying the faithful preservation of original video content. Improvements of approximately 30% and 21% in

RMSE values, 28% and 20% in MSE values, and 14% and 8% in PSNR values are observed compared to [16 and 17], respectively. However, the outcomes are slightly improved compared to [18].

3.3 Image Data Case:

Table 3 presents data demonstrating that our proposed model consistently achieves lower RMSE and MAE values while higher PSNR values than [16, 17, and 18], highlighting superior fidelity in preserving original image content. RMSE values have improved by 48%, 35%, and approximately 13% compared to [16, 17 and 18], respectively. About 45%, 25%, and 14% improvements are observed for MAE values. The higher PSNR values show notable improvements of approximately 12%, 6.5%, and 2% compared to [16, 17, and 18], respectively. Like audio, the proposed model exhibits reduced processing time for faster embedding and extracting confidential information

3.4 Text Data Case:

Table 4 shows that the proposed model demonstrates significant improvements in all analyzed parameters compared to [16]. Results are comparable to [17 and 18], except for delay, which shows an improvement of approximately 13% compared to [18].

Steganographed Text Example

Input Text: "I love to read books."

Steganographed Text: "I love to get new books and read books."

Output: "I love to SECRET read books."

Here, "get new books and" is the encoded message, while "SECRET" is the decoded message obtained by the proposed model process.

In summary, the proposed model consistently outperforms previous models regarding fidelity and efficiency across various modalities, including audio, video, picture, and text steganography. It consistently achieves lower RMSE and MAE values, higher PSNR values, and reduced processing delays across diverse datasets and samples.

Table 1. Audio Steganography Results and Comparisons

Parameters	Proposed Model	Ref [16]	Rel. change		Rel. change		Rel. change	
			w.r.t	[16]Ref [17]	w.r.t	[17]Ref [18]	w.r.t	[18]
			(%)		(%)		(%)	
RMSE	0.023	0.042	45.24	0.036	36.11	0.027	14.81	
MAE	0.012	0.021	42.86	0.018	33.33	0.015	20.00	
PSNR	56.7	50.2	12.95	52.1	8.83	53.6	5.78	
Delays (ms)	2.9	4.5	35.56	3.9	25.64	3.4	14.71	

4. Conclusion and Future Scope

This study presents an advanced, novel multimodal picture steganography framework, integrating multi-domain feature analysis and secret sharing techniques. Operating seamlessly across diverse data modalities—audio, video, pictures, and text—the model exhibits unparalleled fidelity, efficiency, and concealing capabilities compared to existing models. The algorithmic core relies on sophisticated multi-domain feature analysis, significantly reducing RMSE and MAE values alongside higher PSNR values. Integrating the (n, k) Shamir Secret sharing method enhances resilience, elevating the overall robustness of the proposed model. Consistent comparisons with existing models underscore superior fidelity, which is evident through lower RMSE and MAE values and higher PSNR values. Beyond fidelity, the model demonstrates accelerated information processing, minimal delays, and an enhanced concealment capacity across digital media formats.

Comparative analyses demonstrate the superior performance of the proposed model across various modalities, including audio, video, picture, and text. In audio steganography, our model excels with RMSE values improving by 45%, 36%, and 15% compared to existing models [16, 17, and 18]. For video steganography, the framework achieves substantial reductions in RMSE values (approximately 30% and 21%) compared to [16 and 17], accompanied by improvements in PSNR values. The model consistently outperforms counterparts in image steganography, showing reductions of about 48%, 35%, and 13% in RMSE values compared to [16, 17, and 18]. Text steganography reveals significant improvements compared to [16], with a 13% reduction in delay compared to [18].

The developed framework stands as a testament to superior performance and lays the foundation for ongoing research. Addressing emerging challenges and enhancing capabilities contribute to the evolution of steganography methodologies, ensuring efficacy in an ever-evolving digital landscape. While the proposed model advances multimodal steganography, future research directions include exploring advanced feature analysis, adaptive capacity allocation, resilience against sophisticated attacks, and real-time implementation considerations. Such trajectories aim to optimize further concealing capacity, enhance security, and improve practical usability, ensuring the model's continued evolution. Additionally, it is crucial to investigate the model's resilience against advanced attacks and evaluate its performance in real-world scenarios. Further exploration of novel cryptographic techniques and integration with emerging technologies like blockchain could fortify data security.

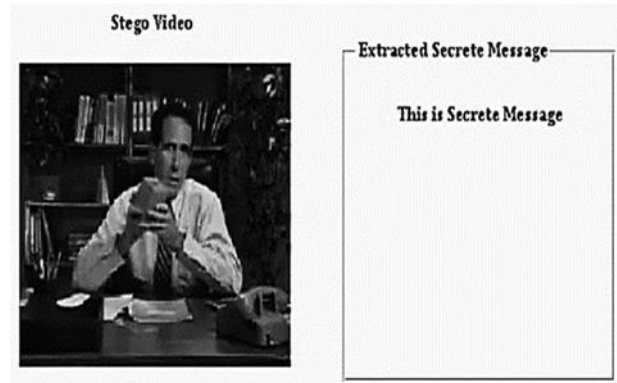


Fig 4. Results of the Video Steganography Process

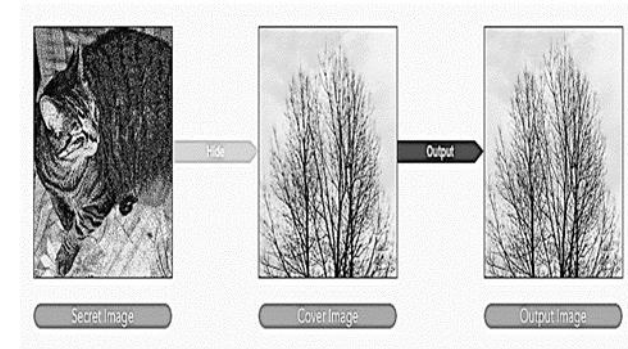


Fig 5: Results of the Image Steganography Process

Table 3: Image Steganography Results and Comparisons

Parameters	Proposed Model	Ref [16]	Rel. Change w.r.t [16] (%)	Ref [17]	Rel. Change w.r.t [17] (%)	Ref [18]	Rel. Change w.r.t [18] (%)
RMSE	0.013	0.025	48	0.02	35	0.015	13.33
MAE	0.006	0.011	45.45	0.008	25	0.007	14.29
PSNR	68.5	61.2	11.93	64.3	6.53	67.2	1.93
Delays (ms)	1.3	2.9	55.17	2.2	40.91	1.8	27.78

Table 4: Text Steganography Results and Comparisons

Parameters	Proposed Model	Ref [16]	Rel. Change w.r.t [16] (%)	Ref [17]	Rel. Change w.r.t [17] (%)	Ref [18]	Rel. Change w.r.t [18] (%)
RMSE	0.002	0.003	33.33	0.002	0	0.002	0
MAE	0.001	0.0012	16.67	0.001	0	0.001	0
PSNR	78.2	75.4	3.71	77.1	1.43	77.8	0.51
Delays (ms)	0.4	0.6	33.33	0.4	0	0.46	13.04

References

- [1] Su W, Ni J, Hu X, Fridrich J. Image Steganography with Symmetric Embedding Using Gaussian Markov Random Field Model. *IEEE Transactions on Circuits and Systems for Video Technology*. 2021 Mar;31(3):1001–15. doi: 10.1109/TCSVT.2020.3001122.
- [2] Hu, Y., Yang, Z., Cao, H., Huang, Y. (2021). Multimodal Steganography Based on Semantic Relevancy. In: Zhao, X., Shi, YQ., Piva, A., Kim, H.J. (eds) *Digital Forensics and Watermarking. IWDW 2020. Lecture Notes in Computer Science()*, vol 12617. Springer, Cham. https://doi.org/10.1007/978-3-030-69449-4_1
- [3] Tan J, Liao X, Liu J, Cao Y, Jiang H. Channel Attention Image Steganography With Generative Adversarial Networks. *IEEE Transactions on Network Science and Engineering*. 2022 Mar 1;9(2):888–903. doi: 10.1109/TNSE.2021.3139671.
- [4] Zhou H, Zhang W, Chen K, Li W, Yu N. Three-Dimensional Mesh Steganography and Steganalysis: A Review. *IEEE Transactions on Visualization and Computer Graphics*. 2022 Dec 1;28(12):5006–25. doi: 10.1109/TVCG.2021.3075136.
- [5] Ibrahim DR, Teh JS, Abdullah R. An overview of visual cryptography techniques. *Multimedia Tools and Applications*. 2021 Jul 21;80(21-23):31927–52. DOI: 10.1007/s11042-021-11229-9.
- [6] Xie Jia-liang, Wang H, Wu D. Adaptive Image Steganography Using Fuzzy Enhancement and Grey Wolf Optimizer. *IEEE Transactions on Fuzzy Systems*. 2022 Nov 1;30(11):4953–64. doi: 10.1109/TFUZZ.2022.3164791.
- [7] Butora J, Bas P. Side-Informed Steganography for JPEG Images by Modeling Decompressed Images. *IEEE Transactions on Information Forensics and Security*. 2023 Jan 1;18:2683–95. doi: 10.1109/TIFS.2023.3268884.
- [8] Qin X, Li B, Tan S, Tang W, Huang J. Gradually Enhanced Adversarial Perturbations on Color Pixel Vectors for Image Steganography. *IEEE Transactions on Circuits and Systems for Video Technology*. 2022 Aug 1;32(8):5110–23. doi: 10.1109/TCSVT.2022.3148406.
- [9] Li Z, Jiang X, Dong Y, Meng L, Sun T. An anti-steganalysis HEVC video steganography with high performance based on CNN and PU partition modes. *IEEE Transactions on Dependable and Secure Computing*. 2022;1–1. doi: 10.1109/TDSC.2022.3140899.
- [10] Wang W, Li Q. An Image Steganography Algorithm Based on PSO and IWT for Underwater Acoustic Communication. *IEEE Access*. 2022;10:107376–85. doi: 10.1109/ACCESS.2022.3212691.
- [11] Chen Y, Salcic Z, Wang H, Choo KKR, Zhang X. NACA: A Joint Distortion-Based Non-Additive Cost Assignment Method for Video Steganography. *IEEE Transactions on Dependable and Secure Computing*. 2022;1–16. doi: 10.1109/TDSC.2022.3182148.
- [12] Gurunath R, Alahmadi AH, Samanta D, Khan MZ, Alahmadi A. A Novel Approach for Linguistic Steganography Evaluation Based on Artificial Neural Networks. *IEEE Access*. 2021;9:120869–79. doi: 10.1109/ACCESS.2021.3108183.
- [13] Peng F, Chen G, Long M. A Robust Coverless Steganography Based on Generative Adversarial Networks and Gradient Descent Approximation. *IEEE Transactions on Circuits and Systems for Video Technology*. 2022 Sep;32(9):5817–29. doi: 10.1109/TCSVT.2022.3161419.
- [14] Farhad Sadmand, Medvedev I, Nuno Gonçalves. CodeFace: A Deep Learning Printer-Proof Steganography for Face Portraits. *IEEE Access*. 2021 Jan 1;9:167282–91. doi: 10.1109/ACCESS.2021.3132581.
- [15] Dhawan S, Chakraborty C, Frnda J, Gupta R, Rana AK, Pani SK. SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT. *IEEE Access*. 2021;9:87563–78. doi: 10.1109/ACCESS.2021.3089357.
- [16] Chen L, Wang R, Yan D, Wang J. Learning to Generate Steganographic Cover for Audio Steganography Using GAN. *IEEE Access*. 2021;9:88098–107. Available from: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&number=9459771>. doi: 10.1109/ACCESS.2021.3090445.
- [17] Chen Y, Wang H, Li W, Luo J. Cost Reassignment for Improving Security of Adaptive Steganography Using an Artificial Immune System. *IEEE Signal Processing Letters*. 2022 Jan 1;29:1564–8. doi: 10.1109/LSP.2022.3188174.
- [18] Mo X, Tan S, Tang W, Li B, Huang J. ReLOAD: Using Reinforcement Learning to Optimize Asymmetric Distortion for Additive Steganography. *IEEE Transactions on Information Forensics and Security*. 2023;18:1524–38. doi: 10.1109/TIFS.2023.3244094.
- [19] Karolin M, Meyyappan T. Visual Cryptography Secret Share Creation Techniques with Multiple Image Encryption and Decryption Using Elliptic

Curve Cryptography. IETE Journal of Research. 2022 Nov 22;1–8. doi: <https://doi.org/10.1080/03772063.2022.2142684>

- [20] Bhosale AG, Patil V. A (2, 2) Visual Cryptography Technique to Share Two Secrets. 2020 Feb 1. doi: 10.1109/ICICT48043.2020.9112420
- [21] Jan, A., Parah, S.A., Hussan, M. et al. Double layer security using crypto-stego techniques: a comprehensive review. Health Technol. 12, 9–31 (2022). <https://doi.org/10.1007/s12553-021-00602-1>
- [22] Zeng, Lu, Ning Yang, Xiang Li, Aidong Chen, Hongyuan Jing, and Jiancheng Zhang. (2023). "Advanced Image Steganography Using a U-Net-Based Architecture with Multiscale Fusion and Perceptual Loss" Electronics 12.18: 3808. <https://doi.org/10.3390/electronics12183808>
- [23] Kweon, Hyeokjoon, Jinsun Park, Sanghyun Woo, and Donghyeon Cho. (2021). Deep Multi-Image Steganography with Private Keys. Electronics. 10.16: 1906. <https://doi.org/10.3390/electronics10161906>
- [24] Wang, Z., Chen, M., Yang, Y. et al. (2020). Joint multi-domain feature learning for image steganalysis based on CNN. EURASIP Journal on Image and Video Processing. 2020. 28. <https://doi.org/10.1186/s13640-020-00513-7>