Ruaa Nadhim Younis[1], Jamshid Bagherzadeh Mohasefi[1]

Scrambled Image Embedding Using Wavelet Transform for Secure Data Transmission

Journal of Electrical Systems

Abstract: - This study introduces a method for embedding an image into a video using Discrete Wavelet Transform (DWT) and secure data handling techniques. The process begins by preprocessing the image, where its Red, Green, and Blue (RGB) channels are separated, flattened into one-dimensional streams, and divided into fixed-size blocks. The video frames are processed in parallel, with image data embedded into the high-frequency coefficients (HH2) of a two-level DWT. The embedding process employs scrambling and key encoding to enhance security, resulting in a robust integration of image data into the video stream. For evaluation, the Signal-to-Noise Ratio (SNR) is calculated to measure the quality of the reconstruction. The retrieved image achieves an SNR of **31.9 dB**, demonstrating high fidelity to the original image. Meanwhile, the modified video maintains an SNR per frame ranging from **36.7 dB to 40.5 dB**, indicating minimal perceptual degradation across all embedded frames and preserving video quality. This method demonstrates a secure and efficient approach to image embedding and retrieval, with potential applications in steganography, watermarking, and multimedia security.

Keywords: Image scrambling, Image Embedding , Image Steganography , Discrete Wavelet Transform (DWT) ,Signal-to-Noise Ratio (SNR) ,Multimedia Security, Multi-resolution, High-Frequency Coefficients

1.INTRODUCTION:

Data storage, communication, and security have all been significantly impacted by the recent explosion of digital media. Steganography and secure data embedding have become well-known among the several methods for guaranteeing data security because of their capacity to covertly safeguard private information [1].

The art of hiding data inside a cover media without compromising its perceptual quality is known as steganography. The term "cover-media" refers to digital multimedia data (text, image, audio, and video) that contains secret data, while "stego-media" refers to cover-media that contains hidden data. The capacity to covertly conceal information within text, image, audio, or video data so that recipients are unable to determine which steganography medium holds the concealed data is known as modern digital media steganography[1-6].

Video steganography is used in both the transform-domain and the spatial-domain. In the spatial domain, the pixel values of video frames are directly embedded. The most popular spatial-domain technique, known as least significant bits (LSB), substitutes the most important n bits of the secret data with the n least significant bits of the cover image. For video steganography, numerous studies have employed LSB replacement and LSB matching [16–18].

By altering specific frequency coefficients of the transformed frames, transform-domain concealment is accomplished. DCT (Discrete Cosine Transformation) is one example. [16,20,21] DWT (Discrete Wavelet Transformation).

A signal's frequency components can be compactly represented with excellent spatial support using the Discrete Wavelet Transform. With DWT, a signal can be perfectly recreated by breaking it down into frequency subbands at various scales. Wavelet decomposition filters can be used to deconstruct signals, including pictures. The LL, HL, LH, and HH subbands are the four subbands into which the resulting image is divided. (H=High, L=Low). While the other subbands include the missing features, the LL-subband approximates the original image. It is possible to further decompose

[1]Department of Computer Engineering, University of Urmia, Urmia, Iran
Corresponding author : j.bagherzadeh@urmia.ac.ir

the LL-subband output from any stage [22]. This paper introduces innovative methods for secure data storage and retrieval by leveraging video steganography and image partitioning and scrambling techniques. These methods enhance the robustness and reliability of data embedding and extraction processes, thereby ensuring the integrity and security of the stored data.

2. LITERATURE REVIEW AND PREVIOUS STUDIES

In 2023, Jun Li et al. Proposed three key principles for motion vector-based steganography, introducing innovative distortion functions that enhance resistance to steganalysis while preserving video quality and coding efficiency [19]. But **In 2023, He Yin et al.** Developed a steganographic approach leveraging public videos and multiple keys to boost security. Their method ensures high compression efficiency and robust protection, making it ideal for secure information exchange [20].when **In 2023, Kirtee Panwar et al.** Reviewed deep learning-based encryption techniques, focusing on methods like style transfer and the integration of neural networks with chaotic systems. This work emphasized the potential of deep learning to enhance cryptographic systems and counteract attacks [21].

In 2023, Adel A. Bahaddad et al. Introduced the BESOPS-CE steganography method, combining optimal pixel selection with chaotic encryption to securely embed images. Their approach demonstrated outstanding performance in encryption and steganographic robustness [22]. **When in 2023, Alejandro Martín et al.** Utilized Generative Adversarial Networks (GANs) to optimize steganography in spatial domains, achieving minimal image distortion while evading detection by deep learning-based steganalysis systems [23]. **But 2022, Milad Yousefi Valandar et al.** Proposed a video steganography technique using integer wavelet transforms and a 3D chaotic map. This approach offered strong resilience to noise and enhanced security while maintaining high video quality [24].

In 2021, Yuanzhi Yao and Nenghai Yu Developed a motion vector-based video steganography method, introducing a payload allocation strategy to minimize distortion propagation in inter-coded frames. This improved both video quality and computational efficiency [25]. While **In 2021, Osama F. Abdel Wahab et al.** Combined RSA encryption with various steganography techniques, including LSB, Huffman coding, and DWT. Their method provided enhanced security, high imperceptibility, and compact data representation [26].

In 2020, Mritha Ramalingam et al. Devised a steganography method employing affine transformations within integer wavelet transforms. This technique achieved improved PSNR and computational efficiency [27]. But **In 2020, Meenu Suresh and I. Shatheesh Sam** Presented a video steganography approach based on LWT with multi-objective optimization for region selection. Their method excelled in security, embedding capacity, and video quality with minimal distortion [28]. When **In 2019, Ahlem Fatnassi et al.** Proposed a multilayered encryption approach for video transmission over unstable networks. Their method ensured data recovery despite partial network failures, optimizing both security and resource utilization [29].

3. PROPOSED METHODOLOGY

The proposed methodology involves embedding an image into a video using Discrete Wavelet Transform (DWT). The image is first preprocessed by separating its RGB channels, performing scrambling to enhance security, and dividing the scrambled image into fixed-size blocks. The high-frequency DWT coefficients (HH2) of video frames are modified to embed the scrambled image data securely, employing additional scrambling and key encoding for robust data protection. This dual-layer scrambling significantly enhances security and improves the Signal-to-Noise Ratio (SNR) for the video. Finally, the embedded data is retrieved through inverse operations, ensuring high fidelity in both the reconstructed image and the modified video.

3.1 Pseudocode for the Embedding (Hiding) Process

Step 1: Initialization

1. **Define parameters**:
   - Block size for the image (blockSize_image) to determine the number of coefficients for embedding.
   - Block size for the video frame (blockSize_frame) to divide the frame into manageable chunks.
   - Key size (blockSize_key) to securely store scrambling information.
2. **Load the input image**:
   - Read the image file.
   - Extract the dimensions (imageRows, imageCols, numChannels for R, G, B channels).

Step 2: Preprocess the image

1. **Extract and flatten channels**:
   - Extract the R, G, and B channels separately.
   - Flatten each channel into a one-dimensional array (stream).
2. **Calculate required blocks**:
   - Determine the number of blocks required to divide each channel stream into equal-sized blocks of blockSize_image.
3. **Add padding if necessary**:
   - If the channel stream size is not divisible by blockSize_image, append zeros to make it divisible.

Step 3: Reshape image streams

1. **Divide streams into blocks**:
   - Reshape each channel stream into a 2D array, where each row represents a block of size blockSize_image.
2. **Combine R, G, B blocks**:
   - Merge the reshaped arrays for R, G, and B channels into a single 3D array for embedding.

Step 4: Load the video

1. **Read the video file**:
    - Use a video reader to load the video.
    - Retrieve properties such as frame rate, dimensions (frameWidth, frameHeight), and total number of frames.
2. **Calculate embedding requirements**:
    - Determine the number of blocks that can fit into each frame based on blockSize_frame.
    - Calculate the total number of frames needed to embed the image data.

Step 5: Embed the image into video

1. **Loop over the required frames**:
    - For each frame in the video:
        1. Read the current frame.
        2. Divide the frame into blocks of size blockSize_frame.
2. **Process each block**:
    - For each block in the frame:
        1. Perform a 2-level Discrete Wavelet Transform (DWT) to decompose the block.
        2. Embed one block of image data into the HH2 coefficients of the DWT:
            - Scramble the image data using a random key.
            - Encode the scrambling key and append it to the coefficients.
        3. Reconstruct the block using the inverse DWT.
3. **Store the modified frame**:
    - Replace the original frame with the modified frame.
    - Save the modified frame to the output video.

3.2 Pseudocode for the Extraction (Recovery) Process

Step 1: Initialization

1. **Load the video with embedded image**:
    - Use a video reader to load the video containing the embedded image.
2. **Prepare variables**:
    - Initialize arrays to store the reconstructed image blocks.

Step 2: Extract embedded data

1. **Loop over the frames with embedded image**:
    - For each frame in the video:
        1. Read the current frame.

2. Divide the frame into blocks of size blockSize_frame.

2. **Process each block**:
    - For each block in the frame:
        1. Perform a 2-level Discrete Wavelet Transform (DWT) to extract HH2 coefficients.
        2. Decode the key stored in the coefficients.
        3. Descramble the coefficients using the decoded key to recover the original image block.
        4. Append the recovered block to the output image array.

Step 3: Reconstruct the image

1. **Combine the extracted blocks**:
    - Assemble the blocks for R, G, and B channels.
    - Reshape the combined blocks to match the original image dimensions.
2. **Post-processing**:
    - Remove any padding added during the embedding process.

Step 4: Verify the results

1. **Compare original and reconstructed images**:
    - Calculate the Signal-to-Noise Ratio (SNR) to measure the similarity between the original and reconstructed images.
2. **Display results**:
    - Show the reconstructed image and report the SNR value.

4. RESULTS

The implementation of the image embedding and retrieval process, shown in figure 1. yields promising results. First, the image reconstruction quality is impressive, achieving a Signal-to-Noise Ratio (SNR) of 31.9 dB. This indicates that the embedded image is reconstructed with high fidelity and minimal distortion. In terms of video quality preservation, the modified video maintains an SNR per frame ranging from 36.7 dB to 40.5 dB. As shown in figure 2. This ensures that the embedding process introduces negligible perceptual degradation to the video frames. Additionally, the embedding process incorporates secure techniques, including scrambling and key encoding, to protect the embedded image data, making it robust against unauthorized extraction. Furthermore, the methodology efficiently embeds the image into the high-frequency coefficients of the video frames without exceeding the video's capacity, demonstrating the effectiveness of block-based embedding techniques.

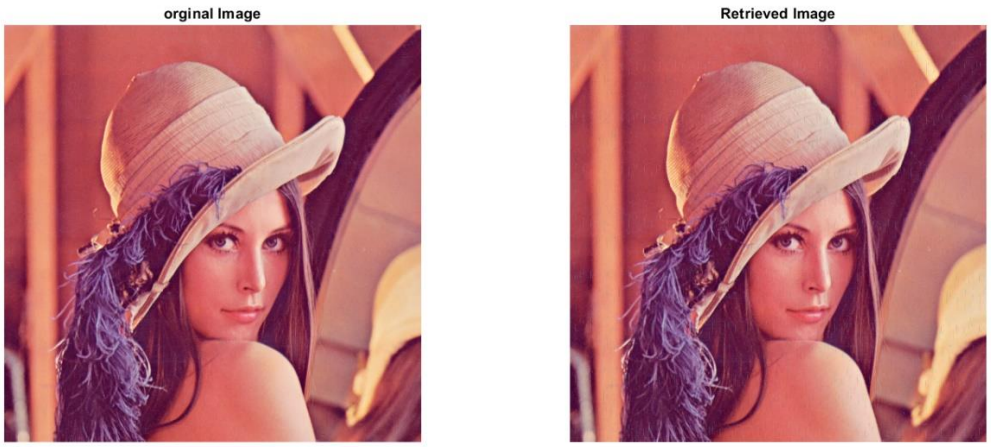

Figure1: original and retrieved image

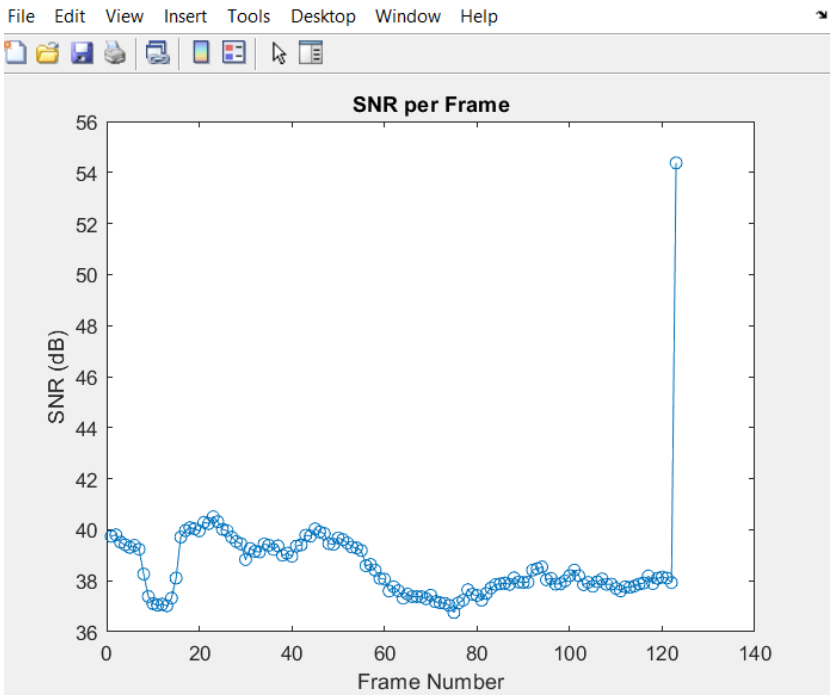

Figure2: SNR for video frame from 36.7 to 40.5

5. EXPLANATION

The provided code illustrates a robust method for embedding an image into a video and retrieving it with minimal distortion. The image preprocessing stage involves dividing the input image into its RGB channels, which are processed separately for precise embedding. Each channel is flattened into a 1D stream and divided into fixed-size blocks, with zero padding added to ensure block size compatibility. During the embedding process, the video is processed frame by frame, and each frame is divided into blocks. A two-level Discrete Wavelet Transform (DWT) is applied to these blocks to extract high-frequency coefficients

(HH2) where the image data is embedded. Scrambling and key encoding are used to secure the data, ensuring that it cannot be extracted without the correct key. The blocks are then reconstructed using an inverse DWT, and the modified frames are saved in a new video file.

The retrieval process involves extracting the HH2 coefficients from each block of the modified video and decoding the scrambling key to descramble the embedded data. The original image blocks are reconstructed and reshaped to recover the image. Quality metrics are computed to evaluate the effectiveness of the process. The retrieved image achieves an SNR of 31.9 dB, reflecting high-quality reconstruction, as illustrated in Figure 1. Similarly, the video maintains an SNR per frame ranging from 36.7 dB to 40.5 dB, with minimal perceptual changes post-embedding

This approach effectively balances embedding capacity, security, and data quality, making it ideal for secure multimedia applications like digital watermarking and steganography.

6. CONCLUSION

This study successfully demonstrates a secure and efficient method for embedding an image into a video using Discrete Wavelet Transform (DWT). By leveraging high-frequency coefficients (HH2) and employing scrambling with key encoding, the proposed method ensures robust image concealment with minimal distortion. The retrieved image achieves a high Signal-to-Noise Ratio (SNR) of **31.9 dB**, indicating excellent reconstruction quality. Meanwhile, the modified video maintains an SNR per frame ranging from **36.7 dB to 40.5 dB**, ensuring negligible perceptual impact on the video's visual quality. These results validate the effectiveness of the method in balancing security, quality, and embedding capacity, making it highly suitable for applications in digital watermarking, steganography, and multimedia content protection.

REFERENCES:

[1] A. S. Anaz, M. Y. Al-Ridha, and R. R. O. Al-Nima, "Signal multiple encodings by using autoencoder deep learning," Bulletin of Electrical Engineering and Informatics, vol. 12, no. 1, pp. 435–440, 2023.

[2] Q. Li, X.Y. Wang, X.Y. Wang, B. Ma, C.P. Wang, Y.Q. Shi, An encrypted coverless information hiding method based on generative models, Inform. Sci. 553 (3) (2020).

[3] Qi Li, Xingyuan Wang, Bin Ma, Xiaoyu Wang, Chunpeng Wang , Zhiqiu Xia, Yunqing Shi, Image steganography based on style transfer and quaternion exponent moments, Applied Soft Computing, Volume 110, October 2021, 107618.

[4] Zhou, S., Wei, Z., Wang, B., Zheng, X., Zhou, C., & Zhang, Q. (2016). "Encryption method based on a new secret key algorithm for color images". AEUInternational Journal of Electronics and Communications, 70(1), 1-7.

[5] Saha, B., & Sharma, S. (2012). “Steganographic techniques of data hiding using digital images”. Defence Science Journal, 62(1), 11.

[6] Ziellnska, E., Mazurczyk, W., & Szczypiorski, K. (2014). “Trends in Steganography”. Communications of the ACM, 57(3), 86-95.

[7] Zhang, W., & Li, S. (2004). “Security measurements of steganographic systems”. International Conference on Applied Cryptography and Network Security. 194-204. Springer, Berlin, Heidelberg.

[8] Thanikaiselvan, V, Bansal T, Jain P & Shastri S (2016). “9/7 IWT Domain data hiding in image using adaptive and non-adaptive methods”. Indian Journal of Science and Technology, 9(5).

[9] Jian Zhang, Jifeng Guo, Donglei Lu, An efficient image encryption algorithm based on S-box and DNA code Measurement: Sensors Volume 29, October 2023, 100894.2

[10] Mandeep Kaur, Surender Singh, and Manjit Kaur, Computational Image Encryption Techniques: A Comprehensive Review. 2021, Mathematical Problems in Engineering Volume 2021, Article ID 5012496, 17 pages.

[11] Ye Ma, Research and application of Big data encryption technology based on quantum lightweight image encryption. Results in Physics, Volume 54, November 2023, 107057.

[12] Sajitha A.S., A. Shobha Rekh, Review on various image encryption schemes. Materials Today: Proceedings Volume 58, Part 1, 2022, Pages 529-534.

[13] Taylor, Onate E. Emmah, Victor T. Comparative Analysis of Cryptographic Algorithms in Securing Data. International Journal of Engineering Trends and Technology (IJETT) – Volume 58 Issue 3 – April 2018 ISSN: 2231-5381. Page 118.

[14] Manzoor Ahmad Lone, Shaima Qureshi, RGB image encryption based on symmetric keys using Arnold transform, 3D chaotic map and affine hill cipher, Optik, Volume 260, June 2022, 168880.

[15] M. Essaid, I. Akharraz, A. Saaidi, et A. Mouhib, Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps, Journal of Information Security and Applications, Volume 47, August 2019, Pages 173-187.

[16] Chong Mou, Youmin Xu , Jiechong Song, Chen Zhao, Bernard Ghanem, Jian Zhang, Large-capacity and Flexible Video Steganography via Invertible Neural Network, (2023).arXiv:2304.12300v1.

[17] Meng, R., Zhou, Z., Cui, Q., Sun, X. and Yuan, C., 2019. A novel steganography scheme combining coverless information hiding and steganography. Journal of Information Hiding and Privacy Protection, 1(1), p.43.

[18] N. Subramanian, O. Elharrouss, S. Al-Maadeed and A. Bouridane, "Image Steganography: A Review of the Recent Advances," in IEEE Access, vol. 9, pp. 23409-23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[19] J. Li, M. Zhang, K. Niu, and X. Yang, "Investigation on principles for cost assignment in motion vector-based video steganography," J. Inf. Secur. Appl., vol. 73, p. 103439, Mar. 2023.

[20] H. Yin, X. Zhou, N. Xin, J. Hong, Q. Li, and X. Zhang, "Optical steganography with sign-based keys and video as vessel medium," Opt. Commun., vol. 526, p. 128829, Jan. 2023.

[21] K. Panwar, S. Kukreja, A. Singha, and K. K. Singh, "Towards deep learning for efficient image encryption," Procedia Comput. Sci., vol. 218, pp. 644–650, 2023.

[22] A. A. Bahaddad, K. A. Almarhabi, and S. Abdel-Khalek, "Image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption," Alexandria Eng. J., vol. 75, pp. 41–54, 2023.

[23] A. Martín, A. Hernández, M. Alaza, J. Jung, and D. Camacho, "Evolving generative adversarial networks to improve image steganography," Expert Syst. Appl., vol. 222, p. 119841, 2023.

[24] M. Y. Valandar, P. Ayubi, M. J. Barani, and B. Yosefnezhad, "A chaotic video steganography technique for carrying different types of secret messages," J. Inf. Secur. Appl., vol. 66, p. 103160, May 2022.

[25] Y. Yao and N. Yu, "Motion vector modification distortion analysis-based payload allocation for video steganography," J. Vis. Commun. Image Represent., vol. 74, p. 102986, Jan. 2021.

[26] O. F. A. Wahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, and A. A. M. Khalaf, "Efficient combination of RSA cryptography, lossy, and lossless compression steganography techniques to hide data," in 17th Int. Learn. Technol. Conf., Procedia Comput. Sci., vol. 182, pp. 5–12, 2021.

[27] M. Ramalingam, N. A. M. Isa, and R. Puviarasi, "A secured data hiding using affine transformation in video steganography," in 3rd Int. Conf. Comput. Netw. Commun. (CoCoNet'19), Procedia Comput. Sci., vol. 171, pp. 1147–1156, 2020.

[28] M. Suresh and I. S. Sam, "Optimized interesting region identification for video steganography using fractional grey wolf optimization along with multi-objective cost function," J. King Saud Univ. – Comput. Inf. Sci., vol. 34, pp. 3489–3469, 2022.

[29] A. Fatnassi, H. Gharsellaoui, and S. Bouamama, "Towards novel video steganography approach for information security," Procedia Comput. Sci., vol. 159, pp. 953–962, 2019.