Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6, 9121-9127
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i6.3948

Enhanced video steganography using genetic algorithms, scrambling techniques, and RSA encryption for secure data embedding

Ruaa Nadhim younis[1], Jamshid Bagherzadeh Mohasefi[2*]
[1,2]Department of Computer Engineering, University of Urmia, Urmia, Iran; j.bagherzadeh@urmia.ac.ir (J.B.M.)

Abstract: This study presents a novel approach for secure data embedding into video frames using a combination of RSA encryption, wavelet transforms, and genetic algorithm-based scrambling techniques. The primary focus of the work is to embed image data securely into video frames while preserving the quality of both the video and the extracted image. The method begins by encrypting critical data parameters (such as frame dimensions, block sizes, and other metadata) using the RSA encryption algorithm. These encrypted parameters are then embedded into the last row of the first frame for secure retrieval. The image data is first divided into blocks, processed using a two-level discrete wavelet transform (DWT), and embedded into the high-frequency sub-bands of the video frames. A genetic algorithm-based scrambling technique is used to increase the security and robustness of the embedding process by scrambling the coefficients before embedding. The embedded data is then spread across multiple video frames, ensuring efficient utilization of frame capacity and maintaining imperceptibility. During extraction, the embedded data is retrieved from the video frames, unscrambled using the best key, and decrypted using RSA to reconstruct the original parameters and image. The performance of the proposed method was evaluated using the Signal-to-Noise Ratio (SNR) metric. The SNR for video frames ranged from 36.7 dB to 39.9 dB, indicating minimal distortion. Furthermore, the reconstructed image achieved an SNR of 31.1 dB, showcasing the method's capability to maintain image quality after the embedding and extraction processes. This method demonstrates a secure and efficient approach for video steganography and data hiding, with potential applications in secure communication, copyright protection, and digital watermarking.

Keywords: *Data hiding, Signal-to-noise ratio (SNR), Digital watermarking, Genetic algorithm, Image reconstruction. RSA encryption, Video embedding, Secure communication, Video steganography, Wavelet transform.*

1. Introduction

In recent years, the rapid growth of digital media has significantly impacted areas such as security, communication, and data storage. Among the various methods for safeguarding sensitive information, steganography and secure data embedding have emerged as effective techniques for discreet data protection [1].

Steganography involves concealing information within a cover medium without compromising its perceptual quality. In this context, digital multimedia data—such as text, images, audio, and video—used to hide the secret information are referred to as cover media, while the resulting media containing the embedded data are known as stego media. Modern digital steganography enables the secret embedding of information within text, images, audio, or video, ensuring that unauthorized users cannot detect which medium contains hidden data [2-6].

Video steganography can be achieved in various domains, including the spatial domain and the transform domain. In the spatial domain, embedding is performed directly on the pixel values of video frames. One of the most widely used methods in this domain is the Least Significant Bit (LSB) technique, which involves replacing the least significant bits of the cover image with the most

* Correspondence: j.bagherzadeh@urmia.ac.ir

significant bits of the secret data. Techniques like LSB replacement and LSB matching have been extensively utilized for video steganography by numerous researchers [7–8].

In contrast, the transform domain involves modifying specific frequency coefficients of transformed frames to hide information. Techniques such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are commonly used in this domain [9,10].

The Discrete Wavelet Transform is particularly effective for providing a compact representation of a signal's frequency components while preserving spatial details. DWT decomposes signals into multiple frequency subbands across different scales, enabling perfect reconstruction of the original signal. For images, DWT splits the data into four subbands: LL, HL, LH, and HH, where 'L' denotes low frequency and 'H' denotes high frequency. The LL subband represents an approximation of the original image, while the other subbands contain detailed information. Additionally, the LL subband from any stage can undergo further decomposition for deeper analysis [11].

This paper presents novel approaches for secure data embedding and retrieval, utilizing video steganography, image partitioning techniques, and genetic algorithms. These methods improve the robustness and reliability of the data storage and extraction processes, ensuring the integrity and confidentiality of the embedded information.

2. Literature Review and Previous Studies

In (2023) Jun Li et al.: Proposed three principles for motion vector-based steganography, leading to innovative distortion functions that improve resilience against steganalysis while maintaining video quality and efficient coding [26]. But He Yin et al. (2023): Developed a steganography method using public videos and multiple keys to enhance security. The technique offers high compression efficiency and robust security, making it suitable for information security applications [28]. While Kirtee Panwar et al. (2023): Reviewed deep learning-based encryption techniques, discussing methods like style transfer and neural networks combined with chaotic systems. The work highlights the potential of deep learning for cryptographic attacks and encryption system improvements [12].

Adel A. Bahaddad et al. (2023): Introduced a steganography method (BESOPS-CE) using optimal pixel selection and chaotic encryption to securely conceal images, showing superior performance in terms of encryption and steganographic robustness [13]. And Alejandro Martín et al. (2023): Used Generative Adversarial Networks (GANs) to optimize steganography in spatial domains, ensuring minimal image distortion while successfully avoiding detection by deep learning-based steganalysis methods [14].

In (2022) Milad Yousefi Valandar et al.: Proposed a video steganography method using integer wavelet transforms and a 3D chaotic map. The approach offers strong resilience to noise and improved security while maintaining video quality [15]. But Yuanzhi Yao, Nenghai Yu (2021): Focused on motion vector-based video steganography, proposing a payload allocation strategy to reduce distortion propagation in inter-coded frames, enhancing both video quality and computational efficiency [29]. While Osama F. Abdel Wahab et al. (2021): Combined RSA encryption with various steganography techniques like LSB, Huffman coding, and DWT to securely hide data, providing enhanced security with high invisibility and compact data representation [16].

Mritha Ramalingam et al. (2020): Developed a steganography technique using affine transformations within integer wavelet transforms, achieving better performance in terms of PSNR and computational cost [30]. whilst Meenu Suresh, I. Shatheesh Sam (2020): Presented an LWT-based video steganography approach with multi-objective optimization for region selection, achieving high security, embedding capacity, and video quality with minimal distortion [3]. and Ahlem Fatnassi et al. (2019)**:** Proposed a multilayered encryption method for video transmission over unstable networks, ensuring data recovery even with partial network failures, optimizing both security and resource usage [17].

3. Proposed Methodology

The proposed method integrates RSA encryption, genetic algorithm-based scrambling, and Discrete Wavelet Transform (DWT) for secure data embedding in video frames. Sensitive data is encrypted

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 9121-9127, 2024
DOI: 10.55214/25768484.v8i6.3948

using RSA and scrambled for added security. The scrambled data is embedded into the HH subbands of video frame blocks using DWT. After embedding, the frames are reconstructed and saved into a new video. During extraction, the embedded data is descrambled, decrypted, and verified for accuracy. The methodology ensures high security, minimal perceptual quality loss, and effective data recovery[18].

3.1. Pseudocode for Hiding the Image in the Video

Step 1: Load the image.
- Read the image file.
- Split the image into three color channels (R, G, B).
- Flatten each channel into a 1D array (image stream).

Step 2: Load the video.
- Read the video file.
- Extract video properties such as the number of frames, frame rate, and frame dimensions.

Step 3: Initialize variables.
- Define block size, key size, and storage size for embedding.
- Create variables to store the modified video frames (stego frames).

Step 4: Encrypt metadata using RSA.
- Create a metadata array (a) containing video dimensions, block sizes, and other parameters.
- Use RSA encryption to encrypt the metadata array.
- Display the encrypted metadata.

Step 5: Loop through each frame in the video.
- For each frame:
  - Extract the R, G, and B channels.
  - Apply a 2-level Discrete Wavelet Transform (DWT) to each channel.
  - Obtain sub-bands: LL2, LH2, HL2, HH2.

  Step 6: Use genetic algorithm to scramble the image data.
- For each pixel in the image streams:
  - Scramble the pixel data using a genetic algorithm to find the best key for embedding.
  - Encode the scrambling key into the HH2 coefficients.
  - Replace the HH2 coefficients with the scrambled data.

Step 7: Embed encrypted metadata into the video.
- Store the encrypted metadata in the last row of the first frame.

Step 8: Reconstruct the video frame.
- Apply inverse DWT to each channel to reconstruct the modified frame.
- Store the modified frame in the stego frame array.

Step 9: Write the stego frames to a new video file.
- Combine all modified frames and save them as a new video file.

Step 10: End the process.
- Print a success message and display the modified video file path.

3.2 Pseudocode for Retrieving the Image from the Video

Step 1: Load the modified video.
- Read the modified video file.
- Extract video properties such as the number of frames, frame rate, and frame dimensions.

Step 2: Extract and decrypt the metadata.
- Retrieve the encrypted metadata from the last row of the first frame.
- Use RSA decryption to recover the original metadata.

Step 3: Initialize variables.
- Create variables to store the extracted image parts for the R, G, and B channels.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 9121-9127, 2024
DOI: 10.55214/25768484.v8i6.3948

- Initialize arrays for storing extracted image streams.

Step 4: Loop through each frame in the video.

- For each frame:
  - Extract the R, G, and B channels.
  - Apply a 2-level DWT to each channel.
  - Obtain sub-bands: LL2, LH2, HL2, HH2.

Step 5: Extract the image using genetic algorithm and descrambling.

- For each pixel in the HH2 sub-band:
  - Decode the scrambling key stored in the coefficients.
  - Unscramble the data using the extracted key and genetic algorithm.
  - Reconstruct the image stream.

Step 6: Continue extracting for all frames.

- Append the retrieved image parts from all frames until all image data is retrieved.

Step 7: Reshape the extracted parts to form the original image.

- Reshape the R, G, and B image streams into 2D arrays.

Step 8: Combine the R, G, and B channels.

- Reconstruct the full image by combining the reshaped R, G, and B channels into an RGB image.

Step 9: Display or save the retrieved image.

- Save the retrieved image to a file or display it.

Step 10: End the process.

- Print a success message and display the retrieved image.

4. Results for Image Hiding and Retrieval

The proposed method leverages a combination of advanced techniques, including RSA encryption**,** genetic algorithm-based scrambling, and discrete wavelet transformation (DWT)**,** to achieve robust and secure video steganography. The embedding process begins with the extraction and partitioning of image data into color channels (R, G, B), which are then embedded into the high-frequency HH2 sub-band of video frames using DWT. The data embedding is enhanced by a genetic algorithm that selects optimal scrambling keys, ensuring reduced correlations and increased security. Metadata related to embedding, such as frame dimensions and block sizes, is encrypted using RSA, providing an additional layer of protection. The modified video maintains high visual quality, with an average SNR of 36.7–39.9 dB for the frames as shown in figure 1 , while the extracted image achieves a high fidelity with an SNR of 31.1 Db the original and reconstructed image shown in figure 2 .

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 9121-9127, 2024
DOI: 10.55214/25768484.v8i6.3948

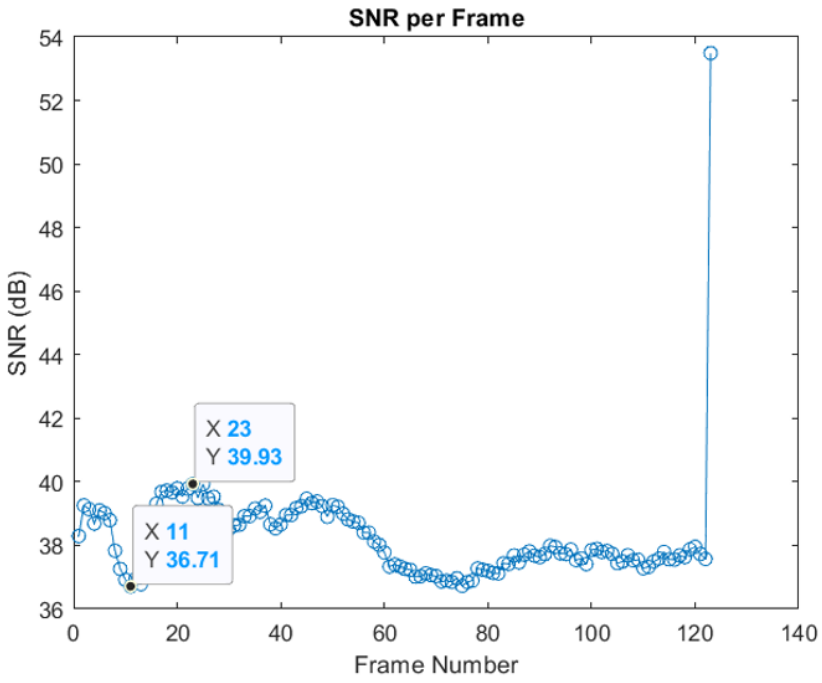

Figure 1:
SNR for video frames.

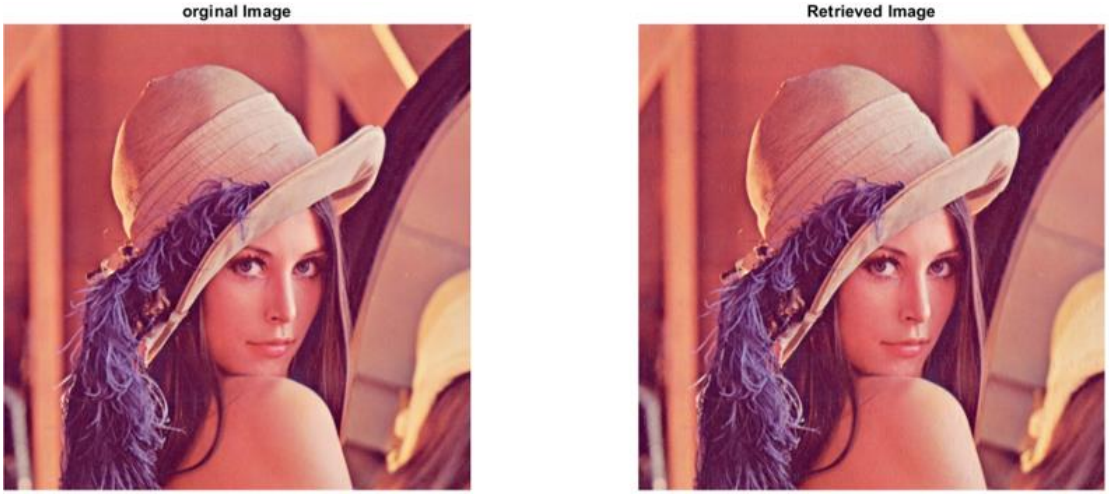

Figure 2:
Original and retrieved image.

5. Explanation

The proposed method combines RSA encryption, genetic algorithms, and discrete wavelet transform (DWT) to achieve secure and imperceptible image embedding into video frames. Initially, metadata such as frame dimensions and block sizes are encrypted using RSA, ensuring secure storage. The genetic algorithm is employed to scramble the image data, enhancing security by randomizing the embedding process. The algorithm identifies the optimal scrambling key by minimizing correlations, using evolutionary operations like selection, mutation, and crossover. The DWT is applied to decompose each video frame into sub-bands, with the high-frequency HH2 sub-band chosen for embedding as it is less perceptible to human vision. During embedding, the scrambled image data, along

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 9121-9127, 2024
DOI: 10.55214/25768484.v8i6.3948

with the encoded key and metadata, are stored in the HH2 coefficients of the video frames. The modified frames are reconstructed using inverse DWT (IDWT) and saved as the stego-video. For extraction, the HH2 coefficients from the stego-video are analyzed to retrieve the embedded key and descramble the data. The extracted image streams are reshaped and combined to reconstruct the original image. This method maintains high visual quality for the video (frame SNR: 36.7–39.9 dB) and achieves accurate image extraction (SNR: 31.1 dB), demonstrating its robustness and effectiveness in secure data embedding.

6. Conclusion

This work presents a novel approach to secure image embedding in video frames by integrating RSA encryption, genetic algorithms, and discrete wavelet transform (DWT). The proposed method ensures high security by employing RSA to encrypt critical metadata and using genetic algorithms to scramble image data, making unauthorized extraction extremely challenging. By leveraging the HH2 sub-band in DWT, the embedding process remains imperceptible, preserving the visual quality of the stego-video. Experimental results demonstrate the effectiveness of the method, with high frame SNR values (36.7–39.9 dB) indicating minimal distortion in the video and an image SNR of 31.1 dB confirming accurate extraction of the embedded image. This approach combines robust encryption, advanced optimization, and efficient data embedding, making it a promising solution for secure multimedia applications. Future work can focus on enhancing computational efficiency and extending the method to real-time video processing scenarios.

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] De Rosal Ignatius Moses Setiadi, Improved payload capacity in LSB image steganography uses dilated hybrid edge detection. Journal of King Saud University - Computer and Information Sciences. Volume 34, Issue 2, February 2022, Pages 104-114

[8] Jun Li , Minqing Zhang , Ke Niu , Xiaoyuan Yang, Investigation on principles for cost assignment in motion vector-based video steganography Journal of Information Security and Applications, Volume 73, March 2023, 103439.

[9] He Yin, Xi Zhou, Nian Xin, Jiaying Hong, Qin Li, Xiao Zhang, Optical steganography with sign-based keys and video as vessel medium. Optics Communications, Volume 526, 1 January 2023, 128829.

[10] Kirtee Panwar, Sonal Kukreja, Akansha Singha, Krishna Kant Singh, Towards Deep Learning for Efficient Image Encryption. Procedia Computer Science 218 (2023) 644–650.

[11] Adel A. Bahaddad, Khalid Ali Almarhabi, Sayed Abdel-Khalek, Image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption. Alexandria Engineering Journal, 2023, 75, 41-54.

[12] Alejandro Martín, Alfonso Hernández, Moutaz Alaza, Jason Jung, David Camacho, Evolving Generative Adversarial Networks to improve image steganography. Expert Systems With Applications 222(2022) 119841.

[13] Milad Yousefi Valandar , Peyman Ayubi , Milad Jafari Barani , Behzad Yosefnezhad, A chaotic video steganography technique for carrying different types of secret messages, Journal of Information Security and Applications, Volume 66, May 2022, 103160.

[14] Yuanzhi Yao, Nenghai Yu, Motion vector modification distortion analysis-based payload allocation for video steganography. Journal of Visual Communication and Image Representation, Volume 74, January 2021, 102986.

[15] Osama F. AbdelWahab, Aziza I. Hussein , Hesham F. A. Hamed , Hamdy M. Kelash , Ashraf A.M.Khalaf, Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data. 17th International Learning & Technology Conference 2020 (17th L&T Conference), Procedia Computer Science 182 (2021) 5–12.

[16] Mritha Ramalingama, Nor Ashidi Mat Isab, R.Puviarasic, A secured data hiding using affine transformation in video steganography. Third International Conference on Computing and Network Communications (CoCoNet'19) Procedia Computer Science 171 (2020) 1147–1156.

[17] Meenu Suresh, I. Shatheesh Sam, Optimized interesting region identification for video steganography using Fractional Grey Wolf Optimization along with multi-objective cost function. Journal of King Saud University – Computer and Information Sciences, 34, 2022, 3489-3469.

[18] Ahlem Fatnassia, Hamza Gharsellaouic, Sadok Bouamama, Towards Novel Video Steganography Approach for Information Security. Procedia Computer Science 159 (2019) 953–962.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 9121-9127, 2024
DOI: 10.55214/25768484.v8i6.3948