**An Efficient DCT based Video Steganography using Dual Fisher-Yates Algorithm**

Shanto Chaki

BSC in software Engineering Department of Software Engineering  
Daffodil International UniversityDaffodil Smart City, Dhaka, Bangladesh  
shanto35-2993@diu.edu.bd

Dewan Lamia Sathi  
BSC in software Engineering  
Department of Software Engineering  
Daffodil International UniversityDaffodil Smart City, Dhaka, Bangladesh  
dewan35-3069@diu.edu.bdDr. Marzia Ahmed  
Assistant ProfessorDepartment of Software EngineeringDaffodil International UniversityDaffodil Smart City, Dhaka, Bangladesh  
marzia.swe@diu.edu.bd

*Abstract*— Video steganography has become a vital area in information security, allowing the hiding of confidential information within multimedia files. in this paper, A Dual Fisher-Yates algorithm is proposed to enhance balance between embedding capacity, visual distortion, and increase robustness of stego videos. This proposed technique selectively embeds the secret data into the mid-frequency DCT coefficients of video frames to mitigate the perceptibility. permutation technique ensures the embedding pattern is randomized to enhance enhancing security. The algorithm automatically adjusts the embedding capacity based on frame complexity to ensure flawless stego video content. Our approach provides superior robustness against common video processing attacks along with best embedding capacity and visual quality with an average PSNR exceeding 40 dB which is known for better quality when compared to existing methods. The proposed approach represents a significant improvement in the trade-off between capacity, imperceptibility, and robustness in video steganography.

*Keywords*— *video steganography; compressed domain; imperceptibility; embedding payload; robustness; DCT*

# Introduction

The swift progress of digital communication technologies has increased the demand for secure data transmission techniques. Among different data protection methods, steganography the technique of embedding information within another medium distinguishes itself by its capability to hide not just the message's content but also its mere presence. Video steganography, which conceals data inside video files, has attracted considerable interest because of its ability to store substantial amounts of information without evident effects on visual quality. This trait renders video steganography especially ideal for uses where high security and large capacity are crucial, including military, healthcare, and financial data transfer. (Jayakanth Kunhoth, 2023)

By hiding the existence of private information in innocuous media, such test. images, audio, and video files, steganography offers an alternative way that permits secure communication. This technique aims to embed the data in a cover medium so that it is indistinguishable from the original, so that unwanted users are unaware of its existence. One of the most promising steganographic techniques is video steganography due to its substantial data embedding capacity and resistance to widely used image-based steganalysis tools. Using video as a cover medium allows a steganographic system to distribute hidden data between frames. This enables greater security and makes detection more challenging.

Video steganography techniques are typically divided into spatial domain and transform domain methods. Spatial domain methods, like Least Significant Bit (LSB) (Vivek Kapoor, 2015) replacement, insert data directly into the pixel values of video frames, enabling straightforward implementation, yet frequently rendering them susceptible to steganalysis attacks. Conversely, transform domain methods, especially those employing the Discrete Cosine Transform (DCT) (Babar1, Saurabh, Nagwade4, & Gade5, 2024), provide improved security and invisibility by incorporating data into the frequency coefficients of converted video frames. This technique spreads concealed information in a manner that is less noticeable to the human visual system, achieving a balance between security, quality, and data capacity.

DCT based video steganography uses frequency coefficients (Sahib Khan1, 2019) to hide data within the frequency coefficients, which reduces perceptual artifacts. Adjusting particular DCT coefficients in a way that preserves the video's visual quality can achieve a higher degree of invisibleness than conventional spatial domain strategies. Even techniques based on DCT might be vulnerable to advanced steganalysis tools if adequate randomness is not provided.

besides the benefits of DCT-based video steganography, there are still many obstacles to overcome in order to guarantee the highest level of security, embedding capability, and imperceptibility. The trade-off between data payload and embedding efficiency is one of the main issues. A little payload might not meet application-specific information capacity demands, but embedding a lot of data might make it more detectable because of noticeable distortions. For this reason, embedding efficiency becomes an important consideration for it dictates how precisely and safely data may be hidden inside a video frame without sacrificing quality. An effective video steganography method should strike a careful balance between security, visual quality, and embedding capacity.

To address these challenges, the proposed technique offers a fresh approach to video steganography in order to address these issues. Here we establish a dual layer of randomness To choose embedding places at random, the first Fisher-Yates shuffle is used to cover video frames and for the embedding, the bits of the hidden image are subjected to the second Fisher-Yates shuffle, which randomly arranges them within the chosen frames. Because it is very difficult to find or retrieve the hidden data for an attacker due to the randomized embedding positions between frames, this design greatly balances between security, achieves high payload capacity, and maintains video quality.

# LITERATURE SURVEY

Video steganography, a technique for concealing data or information within video files, has gained significant attention Due to its potential applications in secure communication and data protection, video steganography has gained significant attention due to its potential applications in video steganography. This review gives an understanding of current video steganography techniques that are used in different field focusing on their method of operation and classification of different domain.

*Spatial Domain Techniques\_*

* 1. Least Significant Bit (LSB) Substitution: It is a straightforward method of stego technique, LSB entails swapping the least significant bits of pixel values with the hidden message. Although simple to set up, it can be vulnerable to attacks and might reduce video quality (Vivek Kapoor, 2015).
  2. Pixel Value Differencing (PVD): Pixel Value Differencing (PVD) is a steganographic technique that uses the differences between nearby pixel values in an image to hide sensitive information. By subtly changing these distinctions, secret bits can be added without significantly deteriorating the image's visual quality. PVD is widely accepted for its significant payload capacity and durability to steganalysis attacks.
  3. Histogram Modification: That approach is altering the histogram of the cover video frames to incorporate data. By modifying the pixel value It is possible to conceal information inside the statistical properties of the image by altering the distribution of pixel values

1. *Transform Domain Techniques\_*
   1. Discrete Cosine Transform (DCT): DCT is commonly utilized in video compression standards such as JPEG and MPEG. For embed the data into the DCT coefficients, particularly in the low-frequency, it mitigates the effect on steo-video quality but it compromise the security. (Sahib Khan1, 2019)
   2. Discrete Wavelet Transform (DWT): Through the application of a discrete wavelet transform (DWT), the video is broken down into sub-bands which actually have different frequencies. Because the upper frequency sub bands are harder for humans to perceive, and information can be embedded there. (Elleithy & Abdelfattah, 2017)
   3. Singular Value Decomposition (SVD): To concealed information, SVD separated the video frames into individual parameters that can be changed. This methodological approach offers adaptability in regards to both durability and embedding capacity. (Lingamallu Naga Srinivasu, 2018)
2. *Hybrid Techniques\_*
   1. Combined Spatial and Transform Domain: For the purpose of take advantage each particular technique's and particular benefits, the hybrid approaches combine the characteristics of spatial and transform domains. There author shows that security and robustness may have enhanced in this way. (Rachna Patel, 2021)
   2. Adaptive Embedding: Adaptive embedding methods modify the embedding intensity according to the local features of the video frame, it provide guaranteeing for optimal data to conceal in the videos. (Lingamallu Naga Srinivasu, 2018)concealment while maintaining quality.

*Recent Advancement\_*

* 1. Deep Learning-Based Steganography: To get better result author have been analyzing complex patterns to improve embedding techniques by using machine learning, deep learning techniques such as the CNN method have been applied to video steganography. (Venugopal, Ranganathan, V.Velmurugan, & TadesseHailu, 2020)
  2. Robustness Against Attacks: The academic community are working to create techniques that actually become more unsusceptible to steganalysis attacks along with compression distortions. There have been attempts to create efficient video steganography algorithms that can be used in real-time applications. (Mstafa & Khaled M. Elleithy, 2016)
  3. Real Time Applications: Now a days different aattempts are undertaken to create efficient video steganography algorithms suitable for use in real-time applications. So that there no need to provide any external security

# MATERIALS AND METHODS

The proposed method described in this paper employs a dual Fisher-Yates shuffling approach within a DCT-based video steganography framework to enhance balancing between data-hiding capacity, visual quality, and robustness. By selectively embedding scrambled binary data of a secret image into mid-frequency DCT coefficients across shuffled video frames, this technique ensures imperceptibility and security, effectively balancing robustness and fidelity in converted video communication.

1. Proposed block diagram for Embedding process
2. *Phases for* *Embedding process*
   * Input Processing Phase
   * First Fisher-Yates Shuffle (Frame Selection)
   * Second Fisher-Yates Shuffle (Bit Scrambling)
   * DCT Transform Process
   * Coefficient Modification
   * Inverse DCT Transform
   * Output Generation
   * Cover Video Processing
3. *Description of Embedding phases:*
   1. ***Input Processing Phase***
      1. *Cover Video Processing:* The first step involves processing the cover video, which is represented as , where denotes the frame sequence. Each frame is extracted as, with and being the spatial coordinates and the frame index. To prepare for data embedding, the color space is converted from RGB to YUV using the formula:  
          (1) (2)  
          (3)  
         Only the Y channel is utilized for embedding to maintain imperceptibility, as highlighted in the proposed method.
      2. *Secret Image Processing:* The secret image, denoted as is processed by converting each pixel into an 8-bit binary sequence. The total number of bits required for embedding is calculated as the product of the image's width, height, and the number of color channels (3 for RGB), resulting in a binary stream representation  
          where .
   2. ***First Fisher-Yates Shuffle (Frame Selection)***
      1. *Algorithm Implementation*: Here to randomly select frames for embedding the first Fisher-Yates shuffle algorithm is employed. The algorithm initializes a random number generator (RNG) with a Shuffle\_Key and iterates through the array of frame indices, then swapping the elements to achieve a random order. This process will enhance the security of data embedding by unpredictable frame selection.
      2. *Frame Selection Process*: After the frame shuffled the input in this phase is an array of frame indices . And the output is a shuffled frame sequence . The selection criteria are based on the total number of secret bits and the number of blocks per frame of the cover video, and here ensures that the sufficient frames are selected for the embedding of confidential data.
   3. ***Second Fisher-Yates Shuffle (Bit Scrambling)***
      1. *Bit Sequence Shuffling:* In this stage, the binary stream B undergoes a second shuffling through the second Fisher-Yates algorithm, initializing a different Shuffle\_Key . This process improves the security by spatially distributing the bits and removing the predictable patterns of bit stream, thereby increasing the resilience of the embedded data against commonly used statistical attacks.
   4. ***DCT Transform Process***
      1. *Block Partitioning:* When the frame is identified for data embedding, frame is divided into non-overlapping 8x8 blocks. This partitioning is crucial as it allows for the calculation of DCT coefficients for each block, which are very essential for the embedding process.
      2. *2D-DCT Transformation:* For each 8x8 block, the DCT coefficients are calculated using the formula:  
          (4)Where is the Y channel of the frame, 𝑁 and 𝑀 are the dimensions of the frame, and are normalization factors. And () represent the frequency indices. This transformation is vital for embedding the data while preserving video quality.
   5. ***Coefficient Modification***
      1. *Selection of Coefficients:* In this 5th phase of embedding process it targeting the mid-frequency DCT coefficients, specifically those in the range of [2,6] for both dimensions. This selection avoids the all DC coefficient and low-frequency coefficients, which actually helps to maintain the quality of the stego video.
      2. *Embedding Formula:* The embedding formula modifies the selected coefficients as follows:  
          (5).  
         Where is the modified coefficient, is the original coefficient, is the embedding strength, and is the secret bit.
      3. *Embedding Conditions:* The conditions for coefficient selection ensure that only appropriate coefficients are modified, and the total capacity for data embedding is calculated based on the number of frames and blocks available.
   6. ***Inverse DCT Transform***
      1. *Block Reconstruction:* After embed the secret image for the purpose of frame reconstruct the IDCT formula is applied to recover pixel values from the modified DCT coefficients, allowing for the reconstruction of the stego video frame by using  
          (6)  
         Where is pixel value at position (x, y) in the spatial domain, is modified DCT coefficient at position () in the frequency domain, which containing the embedded data. is scaling factors define as if otherwise .  
         This process reassembles the embedded frames by converting the altered DCT coefficients back to the spatial domain, ensuring that the embedded data is integrated subtly while preserving the visual quality of the video.
      2. *Frame Reconstruction*: After applying IDCT, the blocks are integrated back into a full frame, and the color space is converted back to RGB to generate the final output video. It uses:   
          (7) (8)  
          (9)
   7. ***Output Generation***
      1. *Video Reconstruction:* The final step involves assembling the frame sequence and ensuring temporal synchronization, which is crucial for maintaining the integrity of the stego video.
4. *Phases for Extracting process*
   * Stego Video Processing
   * Bit Extraction
   * Secret Image Reconstruction
   * Output Generation
   * Quality Consideration
5. Extracting process
6. *Description of Extraction phase*
   1. ***Stego Video Processing***
      1. *Frame Selection*:
      2. The initial stage of the extraction procedure is to pinpoint the frames that hold the hidden secret information. This is accomplished with the identical Fisher-Yates shuffle algorithm employed in the embedding process, but on this occasion, the operation is inverted to retrieve the original frame order. The input to the reverse Fisher-Yates algorithm is the same array of frame indices , and the Shuffle\_Key used during the embedding process.  
         Algorithm steps:  
         step 1. Initialize random number generator with Shuffle\_Key   
         step 2. Loop from the second element down to the first:  
          > Select a random index between 1 and (inclusive)  
          > Swap with

This process outputs the sequence of frame indices used for embedding.

* + 1. *DCT Transform*: The selected frames from the stego video are divided into 8×8 non-overlapping blocks, and the 2D-DCT transformation is applied to each block, as described in the embedding process:  
        (10)  
       where for , ; otherwise , = 1. This step separates the spatial domain data into frequency domain coefficients, which are then used to extract the embedded secret bits.
  1. ***Bit Extraction***
     1. *Coefficient Analysis*: Mid-frequency DCT coefficients within the range are analyzed to retrieve the embedded bits. For each selected coefficient , the bit is extracted as:  
        Extracted\_Bit = round

Where (embedding strength). Extracted bits are stored in a binary sequence.

* + 1. *Second Fisher-Yates Shuffle (Reverse):* To undo the bit-level scrambling performed during the embedding process, the extracted binary sequence is subjected to a reverse Fisher-Yates shuffle. The input is the extracted bit sequence, and the Shuffle\_Key used in the embedding process is applied. The output of this step is the recovered and de-scrambled binary sequence representing the original secret data.
  1. ***Secret Image Reconstruction***
     1. *Bit Sequence Reconstruction:* The unsorted binary sequence is utilized to rebuild the original hidden image. The binary stream is split into sets of 8 bits, with each set signifying a pixel value in the RGB color model. The reconstructed pixel values are subsequently organized into a 2D image with the dimensions indicated by the original secret image.
  2. *Color Space Conversion*: Following the bit Sequence reconstruction, the reconstructed image exists in the RGB color space. If needed, a transformation back to the original color space (such as grayscale or CMYK) can be executed to align with the format of the initial secret image.
  3. ***Output Generation:*** The last step is to save the reconstructed secret image into a secret data file, maintaining the original image file format (e.g., .png,.jpeg).
  4. ***Quality Considerations:*** The caliber of the obtained secret image is vital for system effectiveness, evaluated with the subsequent metrics:
     1. *Bit Error Rate (BER):* Evaluates the epact ratio for erroneous bits in the retrieved data, indicating deterioration.
     2. *Structural Similarity Index (SSIM)*: Evaluates the structural resemblance to the initial version, reflecting both the visual quality and the perceptual similarity
     3. *Peak Signal-to-Noise Ratio (PSNR):* Shows the clarity of the signal in relation to the noise, where higher values indicate improved extraction quality.

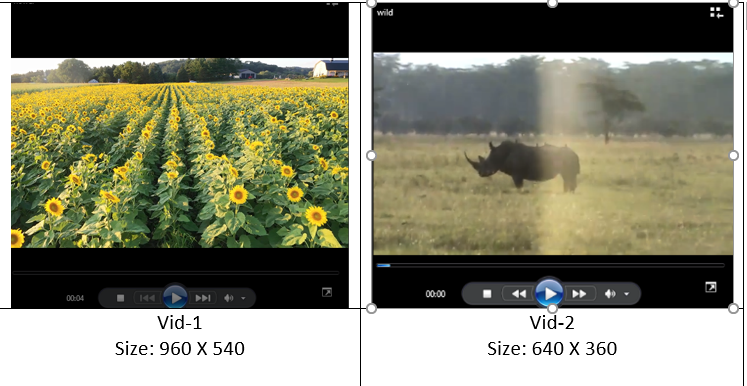
These matrices will be more discuss on result and discussion part.

# Results and Discussions

The suggested method for video steganography was executed and evaluated with MATLAB. Three distinct concealed images were embedded to evaluate the effectiveness of the system. Lena, Barbara and 1971, in two separate cover videos. The system's performance was assessed by concealing these images within the cover video and analyzing the results through three essential metrics. The distortion rate in the stego-image was initially assessed using Mean Square Error (MSE), which measures the differences between the original and stego images. Secondly, to assess the preservation of image quality following embedding, the embedding quality of the stego-image was evaluated in decibels (dB) through the Peak Signal-to-Noise Ratio (PSNR). Data Capacity was ultimately investigated to determine the extent of private information that could be hidden in each video frame in each Cover Video Files.

## Secret Image files

The figure (3) below displays two input cover video files intended for secure transfer the secret image from one location to another.



1. Sample Cover Videos

## Secret Image files

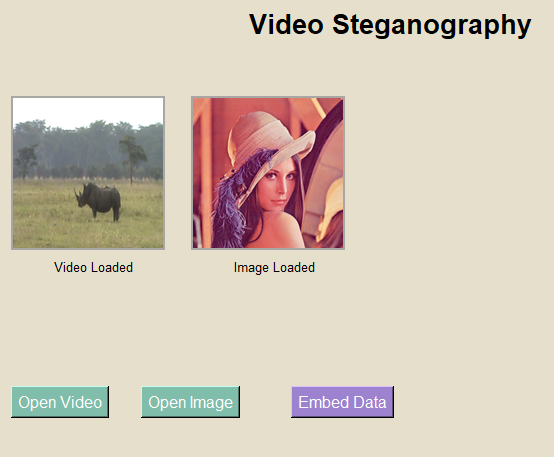
The TableI below illustrates various secret images embedded within the proposed steganography system for secure concealment and transfer

1. Input Images

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Barbara  Size: 512 X 512 | 1971  Size: 740 X 500 | Lena  Size: 512 X 512 |

## GUI to get Embedded video

In this video steganography process shown in the figure (4) below, a video and an image file are used as inputs for encoding. This allows secret image or information to be securely transferred from one user to another while it ensures the safeguard from unauthorized access.



1. User interface to embed secret image into cover video file

## GUI to Extract the stego video

To extract the embedded image, Click the "Open Video" option in figure (5) to choose the stego video, which is the first step in extracting the embedded image. After choosing the stego video, all you have to do is click the "Extract" button, and the secret image will be immediately extracted.



1. User interface to extract secret image from stego video file

To calculate the data capacity and visual quality after embedding and extraction the used equations are:

(11)  
Where MAX is the maximum pixel value (255 for 8-bit grayscale or RGB images)

(12)  
Where is pixel value in the original frame. is Pixel value in the stego frame, is the number of frames. is Frame height and is Frame with.

(13)  
Where is for number of frames used for embedding,   
is for number of blocks per frame and is for number of coefficients per block used for embedding (in your case, 16 coefficients from the 2nd to 6th row and column)

To start the evaluation process, we will use the two selected cover videos along with three hidden images to calculate the Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and data capacity for each combination of video and image. These metrics will provide an extensive assessment of the system's performance by analyzing the distortion rate, embedding quality, and data capacity achieved when every image is integrated into each video. The results will aid in evaluating the effectiveness of the suggested steganography model concerning image quality maintenance and data hiding efficiency.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Cover Video** | **Secret image** | **MSE** | **PSNR**  **(dB)** | **Capacity to hide**  **(bits)** |
| Vid-1 | Barbara | 0.80421 | 45.84 | 6,291,456 |
| 1971 | 0.65999 | 40.01 | 8,880,000 |
| Lena | 0.74315 | 42.56 | 6,291,456 |
| Vid-2 | Barbara | 0.80421 | 45.33 | 6,291,456 |
| 1971 | 0.65999 | 40.36 | 8,880,000 |
| Lena | 0.74615 | 42.14 | 6,291,456 |

1. calculation results
2. compare with simple DCT approach

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name of image | Simple DCT approach | | | Proposed approach | | |
| PSNR | MSE | number of Frame | PSNR | MSE | number of Frame |
| Barbara | 34.8262 | 1.3642 | 40 | 44.38 | 0.80421 | 49 |
| 1971 | 38.51 | 2.425 | 88 | 42.83 | 0.65999 | 69 |
| Lena | 34.8310 | 1.2148 | 64 | 46.06 | 0.74615 | 49 |

# Conclution

This paper presents an efficient video steganography technique based on the Discrete Cosine Transform (DCT) and the Dual Fisher-Yates algorithm. Where the secret image or data embedding in mid-frequency coefficients and Fisher-Yates shuffling approaches, the proposed model provides significant improvements in data concealing capacity, video quality preservation, and robustness. The dual shuffling technique ensures that the embedded data is securely hidden and recoverable even in the presence of noise or compression. Experiments' results demonstrate how successfully the model embeds a lot of data while maintaining high visual quality.

# References

1. Ajmera, A., Divecha, M., Ghosh, S. S., Raval, I., & Chaturvedi, R. (2019). Video Steganography: Using Scrambling- AES Encryption and DCT, DST Steganography. *Pune Section International Conference (PuneCon.* Pune, India: IEEE.
2. Babar1, B. N., S. J., Nagwade4, P., & Gade5, A. (2024). Video Steganography Using DCT Algorithm. (pp. 300-303). INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY.
3. Elleithy, K. M., & Abdelfattah, E. (2017). A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC. (pp. 5354 - 5365). IEEE.
4. Jayakanth Kunhoth, N. S.-M. (2023). Video steganography: recent advances and challenges. 41943–41985.
5. Laxmi Gulappagol\*1, 2. a. (2020). Application of Fisher Yates Data Shuffling and RSA Encryption in Transform Domain Video Steganography. *A Society of Science and Nature Publication*, (pp. 52-57). Bhopal India.
6. Lingamallu Naga Srinivasu, K. S. (2018). Video Steganography Using Two-Level SWT and SVD.
7. Meenu Suresh1, D. I. (2018). High Secure Video Steganography Based on Shuffling of Data on Least significant DCT Coefficients. *ICICCS.* IEEE.
8. Mstafa, R. J., & Khaled M. Elleithy, I. (2016). A Novel Video Steganography Algorithm in DCT Domain Based on Hamming and BCH Codes . *37th IEEE Sarnoff Symposium.* Newark, NJ.
9. Rachna Patel, K. L. (2021). Study and investigation of video steganography over uncompressed and compressed domain: a comprehensive review. (pp. 985–1024). Springer.
10. Sahib Khan1, M. A. (2019). On Hiding Secret Information in Medium Frequency DCT Components Using Least Significant Bits Steganography., (pp. .529-546).
11. Shivani Gupta1, G. K. (2019). Video Steganography Using Discrete Wavelet Transform and Artificial Intelligence. *International Journal of Trend in Scientific Research and Development*, (pp. 1210 - 1215).
12. Tanveer J. Siddiqui, A. K. ( 2020). CHAOS-BASED VIDEO STEGANOGRAPHY METHOD IN DISCRETE COSINE TRANSFORM DOMAIN. *International Journal of Image and Graphics.* World Scientific.
13. Venugopal, E., Ranganathan, S., V.Velmurugan, & TadesseHailu. (2020). Design and implementation of video steganography using Modified CNN algorithm . *hird iternational Conference on Advances in Electronics, Computers and Communications (.* IEEE.
14. Vivek Kapoor, A. M. (2015). An Enhanced LSB based Video Steganographic System for Secure and Efficient Data Transmission. (pp. 38-42). International Journal of Computer Applications.