BIOS: Jurnal Informatika dan Sains
Volume 3 Number 01, 2025, DOI 10.54209/bios.v3i01
E.SSN 2988-6910(Online)
https://seaninstitute.or.id/bersinar/index.php/bios/index

Implementation of Transform Domain Video Steganography (DCT) Method for Embedding Secret Messages in Video Media

Adri Muliadi Pasaribu[1], Ikmat Pengertian Hia[2], Otomosi Gulo[3]
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas

Article Info
Corresponding Author:
Adri Muliadi Pasaribu

ABSTRACT
Steganography is a technique for concealing information by embedding a secret message into a digital medium without causing significant visual changes. In this study, a transform-domain-based video steganography method using the Discrete Cosine Transform (DCT) is implemented to embed secret messages into video media. The embedding process is performed on each video frame by dividing the frame into 8×8 pixel blocks, followed by applying DCT to each block. The secret message is converted into a bitstream and embedded by modifying the mid-frequency coefficients in the DCT domain. After the embedding process, inverse DCT is applied to reconstruct the frame back into the spatial domain, resulting in a stego video. The test results show that the visual differences between the stego video and the original video are not significantly perceptible, thus satisfying the imperceptibility aspect of steganography. In addition, the secret message can be successfully extracted with a high level of accuracy, indicating that the proposed method is capable of maintaining a balance between embedding capacity, visual quality, and extraction reliability. Therefore, the transform-domain-based video steganography method using DCT can be effectively used as a solution for embedding secret messages in video media.

Keywords: Video steganography, Transform domain, Discrete Cosine Transform (DCT), Secret message embedding, Information security.

INTRODUCTION

The rapid development of information technology has increased the exchange of digital data across various media, such as text, images, audio, and video. On the other hand, this growing exchange of information also raises concerns regarding data security and confidentiality. Sensitive information requires protection mechanisms to ensure that it cannot be accessed or misused by unauthorized parties. Therefore, methods are needed to maintain data confidentiality during transmission and storage in digital environments.

Steganography is one of the techniques used to protect information by hiding secret messages within a cover medium without causing significant visual changes. Unlike cryptography, which only encrypts the content of a message, steganography aims to conceal the very existence of the message. Video media has great potential for steganography because it offers a large data capacity and consists of many frames, enabling high imperceptibility and making hidden messages more difficult to detect.

In its implementation, steganography can be applied in either the spatial domain or the transform domain. Spatial domain methods are relatively easy to implement but are more

vulnerable to compression and manipulation. Therefore, transform domain methods such as the Discrete Cosine Transform (DCT) are more widely used because they are more resistant to compression and can better preserve visual quality. Based on this, this project implements a transform-domain-based video steganography method using DCT to embed secret messages into video media, aiming to balance data security, visual quality, and reliable message extraction.

The advancement of multimedia technology and communication networks has increased the need for digital information security. Although cryptographic techniques can secure the content of messages, the existence of encrypted messages can still be detected by unauthorized parties. Therefore, an additional technique is needed that not only secures the message content but also hides its existence, one of which is video steganography.

Based on this, the problem in this project is how to implement a transform-domain-based video steganography method using Discrete Cosine Transform (DCT) to embed secret messages into video media, and how to ensure that the resulting video quality remains good while the hidden message can be correctly extracted. In addition, it is necessary to analyze the extent of changes in DCT coefficients before and after message embedding to determine the impact of the method on stego video quality and security.

METHOD

The workflow in this study is systematically designed to implement video steganography using a transform-domain approach based on the Discrete Cosine Transform (DCT). The stages include data preparation, message embedding, extraction, and result evaluation. This methodology ensures that the secret message is correctly embedded into the video, the visual quality of the video is preserved, and the message can be accurately retrieved.

Data Preparation

At this stage, the video media used as the cover object is prepared. The input video may be in common formats such as MP4 or AVI. The video is read using the OpenCV library to obtain information such as the number of frames, resolution, and frame rate (FPS). In addition, the secret message is prepared in text form and then converted into a binary bitstream to facilitate embedding into DCT coefficients.

Video Preprocessing

Each video frame is converted from RGB/BGR color space into YCrCb color space. In this representation, the luminance component (Y) is separated from the chrominance components (Cr and Cb). Message embedding is performed only on the Y channel because it has the greatest influence on visual perception; however, with appropriate coefficient selection, visual distortion can still be minimized. Each frame is then divided into 8×8 pixel blocks according to the standard DCT process.

DCT Transformation

Each 8×8 block in the Y channel is transformed into the frequency domain using the Discrete Cosine Transform (DCT). This transformation produces a matrix of DCT coefficients representing low, mid, and high-frequency components. In this study, mid-frequency coefficients are selected as the embedding location because they provide a balance between robustness and visual imperceptibility.

Message Embedding

Message embedding is performed by modifying selected DCT coefficient values in each block. Each secret bit is embedded by adjusting the sign and/or magnitude of the selected coefficient. If the bit is '1', the coefficient is set to a positive value with a certain magnitude, while if the bit is '0', the coefficient is set to a negative value with a certain magnitude. This technique ensures that the embedded bits can be reliably detected during extraction while remaining resistant to noise and mild compression.

Inverse Transformation (IDCT)

After modifying the DCT coefficients, the Inverse Discrete Cosine Transform (IDCT) is applied to each block to convert the data back into the spatial domain. The result is a pixel block that already contains hidden information. Pixel values are then clipped to the range of 0–255 to ensure valid digital image representation.

Stego Video Reconstruction and Storage

The processed blocks are recombined to form stego video frames. The modified Y channel is merged back with the Cr and Cb channels and converted into BGR/RGB format. Each stego frame is then saved into an output video file using a specific codec. The final result is a stego video that appears visually similar to the original video but contains hidden secret information.

Message Extraction Process

Extraction is performed by reading the stego video and repeating a similar process as embedding, including conversion to YCrCb, division into 8×8 blocks, and DCT transformation. The same DCT coefficients used during embedding are analyzed. The sign or value of the coefficients is used to determine whether each embedded bit is '1' or '0'. These bits are then reconstructed into ASCII characters to recover the original secret message.

Evaluation and Result Analysis

The evaluation stage is conducted to analyze stego video quality and the success of message extraction. This includes visual inspection to ensure no significant color distortion occurs, as well as analysis of DCT coefficient changes before and after embedding. In addition, method effectiveness is assessed based on whether the secret message can be fully and correctly extracted. Thus, this method is expected to demonstrate that DCT-based transform-domain video steganography is effective for secure and imperceptible information hiding.

LITERATURE REVIEW

Steganography

Steganography is a technique for securing information by hiding secret messages within a digital medium so that the existence of the message cannot be detected by unauthorized parties. Unlike cryptography, which obscures the content of a message, steganography focuses on concealing the existence of the message itself. Common media used in steganography include digital images, audio, and video.

The main objective of steganography is to maintain information confidentiality, prevent suspicion from third parties, and ensure secure message transmission. In its implementation, steganography must satisfy several important aspects, namely imperceptibility (undetectability of changes), robustness (resistance to manipulation), and payload capacity (amount of data that can be embedded).

Video-Based Steganography

Video steganography is a technique for embedding secret messages into digital video media. A video consists of a sequence of image frames displayed consecutively to create the illusion of motion. This characteristic makes video a highly potential medium for steganography due to its large data size and relatively high tolerance for visual modifications.

The advantages of video steganography compared to image and audio media include higher embedding capacity, improved security level, and changes that are difficult to detect by human perception. However, video steganography also faces challenges, particularly related to video compression, which may affect the embedded information.

Digital Video and Video Frames

Digital video is a visual representation of motion composed of a sequence of image frames displayed at a specific frame rate (frames per second). Each frame is a static image that can be processed individually. In video steganography, embedding is typically performed on selected frames to minimize visual distortion.

Frame selection and processing techniques significantly influence the quality of the resulting stego video. Therefore, understanding video frame structure is essential in designing a video steganography system.

Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) is a transformation technique that converts a signal from the spatial domain into the frequency domain. DCT is widely used in data compression and steganography due to its ability to concentrate signal energy in low-frequency components.

In DCT-based steganography, digital media is divided into small blocks, and each block is transformed using DCT. DCT coefficients consist of low, mid, and high-frequency components. Message embedding is typically performed on mid-frequency coefficients because they provide a balance between visual quality and message robustness.

Transform Domain Steganography

Transform domain steganography is a technique in which message embedding is performed after transforming the digital media into a specific domain such as DCT or Discrete Wavelet Transform (DWT). Unlike spatial domain methods, which directly modify pixel values, transform domain techniques offer higher security and robustness against compression and data manipulation. This approach is widely used in video steganography because it aligns well with modern video compression systems, which generally operate in the frequency domain.

Embedding and Extraction Process Using DCT

The embedding process in DCT-based video steganography begins with selecting a video as the cover media. The video is then divided into frames, and DCT is applied to selected frames or blocks.

The secret message is first converted into binary form. The binary data is then embedded by modifying selected DCT coefficients. After embedding, inverse DCT (IDCT) is applied to reconstruct stego frames, which are then combined to form the final stego video. The extraction process is performed by reversing the embedding steps, where DCT coefficients are retrieved from the stego video to reconstruct the hidden message.

Other Steganography Methods for Comparison

In addition to DCT, several other steganography methods are commonly used, such as Least Significant Bit (LSB), End of File (EOF), and Discrete Wavelet Transform (DWT). LSB is

easy to implement but highly vulnerable to attacks and compression. EOF hides data at the end of files but is easily detectable. DWT provides good stego quality but has higher computational complexity.

A comparison of these methods shows that DCT offers advantages in preserving visual quality and message robustness, making it suitable for video steganography.

Stego Video Quality Parameters

Stego video quality can be measured using parameters such as Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). A low MSE indicates a small difference between the original and stego video, while a high PSNR indicates good stego video quality. Additionally, imperceptibility and robustness are also important indicators of steganography performance.

Related Work

Several previous studies have explored DCT-based steganography in various digital media. These studies indicate that DCT can produce stego media with good visual quality and high security levels. However, there is still room for improvement, particularly in optimizing embedding capacity and resistance to video compression.

Based on these prior works, this study is developed to implement a transform-domain video steganography method based on Discrete Cosine Transform (DCT) to securely and efficiently embed secret messages into video media.

RESULTS AND DISCUSSION

In this study, a transform-domain video steganography system using the Discrete Cosine Transform (DCT) method was successfully implemented using an input file named input.mp4 for embedding secret messages into digital video media. The embedding process is carried out by modifying DCT coefficients in 8×8 blocks, particularly in the mid-frequency components, with the aim of maintaining a balance between message robustness and video visual quality. The cover video used can be a standard digital video file such as MP4, which is then processed into a stego video in AVI format as the output of the embedding process.

The test results show that the resulting stego video has a visual quality that is very similar to the original video. Subjectively, no noticeable visual differences can be detected between the stego video and the cover video. This is because the embedding process is performed in the frequency domain rather than directly modifying pixel values, so the changes in the spatial domain after the Inverse DCT (IDCT) process are very minimal. Therefore, the transform-domain method is proven to preserve imperceptibility, meaning the system can hide messages without causing significant visual distortion.

In addition to visual quality, the system was also evaluated in terms of successful message embedding and extraction. The results show that the embedded secret message can be fully and accurately retrieved. This indicates that the embedding mechanism in DCT coefficients, along with the use of message headers and an END marker, effectively supports accurate message detection and extraction. This success demonstrates that the proposed method has a high level of reliability for covert communication.

Changes in DCT coefficient values during the embedding process were also analyzed. The observation shows that mid-frequency DCT coefficients undergo changes in sign and magnitude according to the embedded message bits. However, after applying IDCT, pixel-level changes in video frames remain very small and do not produce noticeable differences in color or intensity. This explains why the stego video still appears normal and visually

unchanged, while the video duration may become shorter in certain cases depending on how frame writing is implemented in the program.

The output results of the secret message embedding project using the video transform domain method:

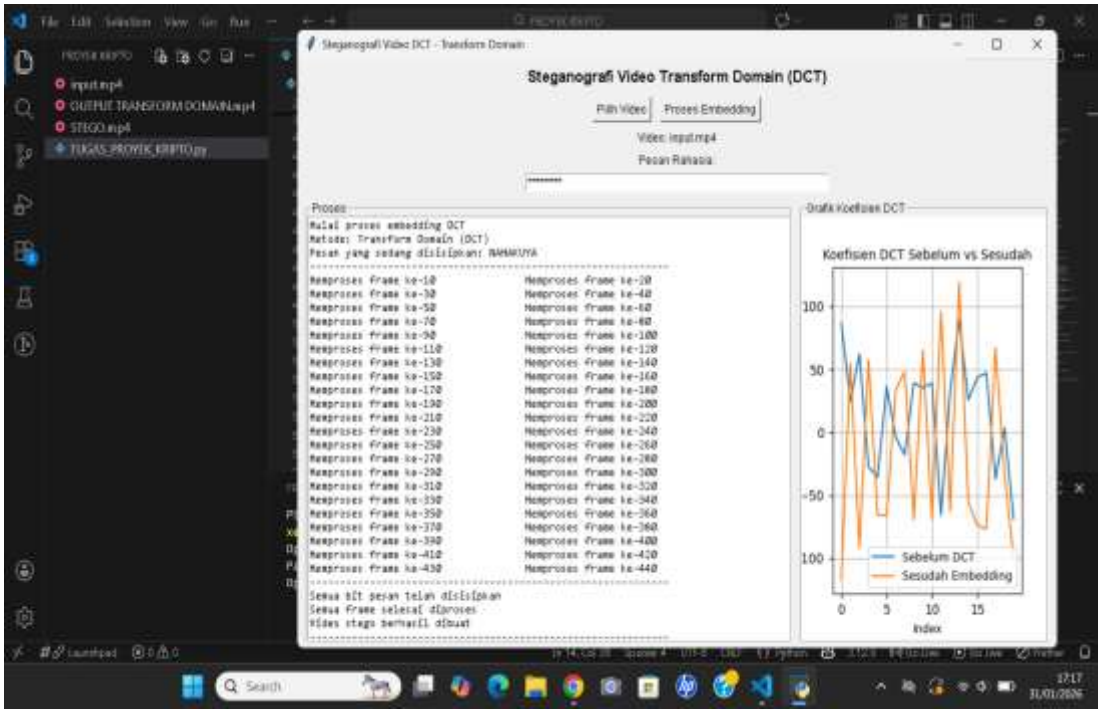

Figure 1. Output Results of the Secret Message Embedding Process Using the Transform Domain (DCT) Method in Video

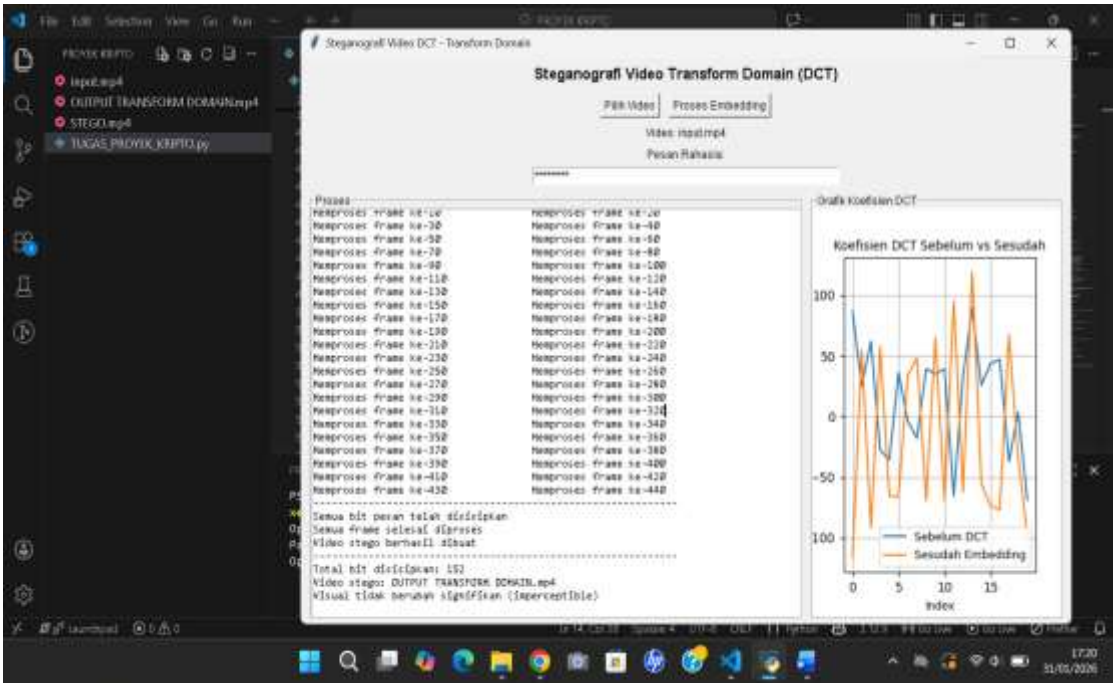

Figure 3. Comparison Graph of DCT Coefficients Before and After the Embedding Process

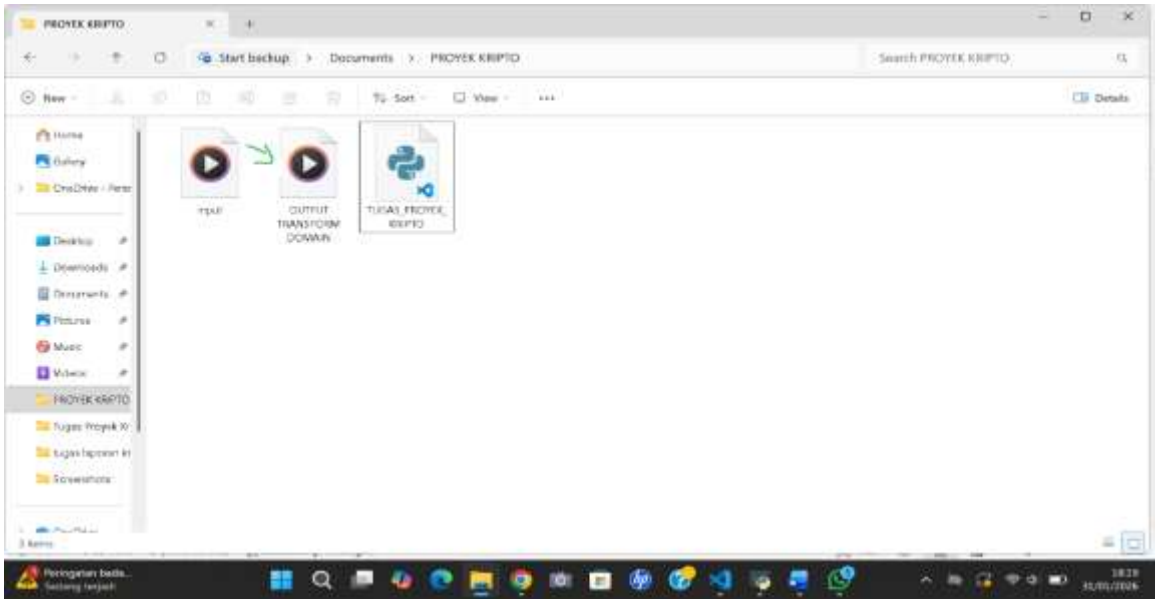

Figure 2. Stego Video Result of Secret Message Embedding Using the Discrete Cosine Transform (DCT) Method

Based on the testing results conducted using the Video Steganography Transform Domain (DCT) method, the following results were obtained: The process of embedding a secret message into the video was successfully carried out using the Discrete Cosine Transform (DCT) method. The secret message embedded was “NAMAKUYA”. The video steganography process using the Transform Domain (DCT) method was successfully implemented by inserting the secret message into the input.mp4 video file, which served as the original (cover) video before the embedding process. The secret message was converted into binary form and gradually embedded into several selected video frames at specific intervals. The total amount of secret data successfully embedded was 152 bits, and the entire embedding process ran smoothly without any failures.

The resulting stego video was successfully generated with the filename OUTPUT TRANSFORM DOMAIN.mp4. Based on visual observations and analysis of DCT coefficients before and after embedding, no significant visual differences were found between the original video and the stego video. This indicates that the DCT method is capable of hiding secret messages imperceptibly, thereby maintaining video visual quality and making it difficult to distinguish from the original video.

In addition, the comparison graph of DCT coefficients before and after the embedding process shows changes in some mid-frequency coefficients. These changes are relatively small and controlled, so they do not affect the overall visual quality of the video. These results demonstrate that the selection of the mid-frequency domain in the DCT method is effective in maintaining a balance between embedding capacity and stego video quality.

CONCLUSION

Based on the design, implementation, and testing conducted, it can be concluded that the video steganography system based on the transform domain using the Discrete Cosine Transform (DCT) method has been successfully implemented. The system is capable of performing both the embedding and extraction of secret messages in digital video media by modifying DCT coefficients in 8×8 blocks, particularly in the mid-frequency components. The test results show that the resulting stego video has a visual quality very similar to the original

video. The changes occurring after the Inverse DCT (IDCT) process produce extremely small pixel differences, resulting in no significant visual distortion. This demonstrates that the imperceptibility aspect of the steganography system has been successfully achieved. In addition, the system is also able to successfully extract the embedded secret message from the video. Although in some cases character distortion occurs due to lossy video compression and changes in DCT coefficient values, in general the system remains capable of detecting and extracting the hidden message. This indicates that the transform domain steganography method has a good level of reliability, although it is still affected by compression processes and video quality. Therefore, it can be concluded that the video steganography method based on the transform domain using DCT is suitable for use as a solution for hiding confidential information in digital video media. The developed system has fulfilled the main characteristics of steganography, namely imperceptibility and message extraction capability, and is in accordance with the research objectives that have been set.

REFERENCES

1. Ansor, A. (2016). Penerapan Steganografi Video Dengan Metode Discrete Cosine Transform. *Media Informasi Analisa dan Sistem*, *1*(2), 25-32.
2. Ratnasari, A. P., & Dwiyanto, F. A. (2020). Metode steganografi citra digital. *Sains, Apl. Komputasi dan Teknol. Inf*, *2*(2), 52.
3. Herlinawati, H. (2016). Steganografi Video H263 dengan Metode Discrete Cosine Transform. *Electrician: Jurnal Rekayasa dan Teknologi Elektro*, *10*(1), 11-20.
4. Apriani, P., Hasugian, A. H., & Rusydi, I. (2024). TEKNIK STEGANOGRAFI DISCRETE COSINE TRANSFORM DAN ALGORITMA RSA UNTUK MENYISIPKAN PESAN PADA AUDIO. *JSR: Jaringan Sistem Informasi Robotik*, *8*(1), 1-9.
5. Rianti, M. (2022). *Perbandingan Metode Steganografi DCT Dan DWT Pada Berkas Video Mp4* (Doctoral dissertation, Universitas Islam Riau).
6. Pratama, A. S., & Suartana, I. M. (2021). Analisis Kualitas Stego Video dalam Penyisipan Data Memanfaatkan Metode DCT-DWT. *Journal Information Engineering and Educational Technology) ISSN*, *2549*, 869X.
7. Anti, U. A., Kridalaksana, A. H., & Khairina, D. M. (2017). Steganografi Pada Video Menggunakan Metode Least Significant Bit (LSB) Dan End Of File (EOF). *Jurnal Informatika Mulawarman*, *12*(2), 104-111.
8. Saifuddin, S., Mido, A. R., & Ujianto, E. I. H. (2020). Perancangan Aplikasi Steganografi Menggunakan Metode Discrete Cosine Transformation berbasis Android. *Progresif: Jurnal Ilmiah Komputer*, *16*(1), 25-36.
9. Widyawati, L. (2019). *Implementasi Metode Steganografi SLT-DCT pada Citra untuk Meningkatkan Kualitas Citra Steganografi* (Master's thesis, Universitas Islam Indonesia).
10. Ardhimasetyo, S., Tritoasmoro, I. I., & Ibrahim, N. (2019). Steganografi Video Dengan Penyisipan Pesan Rahasia Menggunakan Teks Pada Frame Video Berbasis Ssb-4 Dan Discrete Cosine Transform (dct). *eProceedings of Engineering*, *6*(2).