International Journal of Science and Informatics Technology (IJOSIT)
Vol 1, No 1, April 2026, pp. 8-13
https://www.ijosit.org/index.php/ijosit
ISSN: XXXX-XXXX

Implementation of Motion Vector Steganography Method for Secret Message Insertion in Video Media

Ester Manalu, Virzinia Napitupulu, Efrans Surbakti
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas Medan Sumatera Utara, Indonesia

Abstract. Steganography is an information security technique that aims to hide secret messages in digital media so that their existence is not detected by unauthorized parties. Video media is an effective choice because it has large data capacity and high visual complexity. This study aims to implement the Motion Vector Steganography method in video media and simulate the process of inserting and extracting secret messages to understand how it works. The methods used include converting text messages into binary form, inserting message bits into motion vector components resulting from block-based video compression, creating stego videos, and decoding to extract the secret messages. The system was implemented using the Python programming language with the Tkinter graphical interface and video processing using the OpenCV library. The results of the study show that secret messages can be inserted and extracted well without causing significant visual changes to the video. Thus, it can be concluded that the Motion Vector Steganography method is effective and secure in maintaining video quality and message extraction success, making it a potential technique for data security in digital video-based communication systems.
Keywords: Steganography, Motion Vectors, Video Security, Information Hiding, OpenCV.

Corresponding Author:
Ester Manalu
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas Medan Sumatera Utara, Indonesia

1. Introduction

The rapid development of information and communication technology has brought significant transformations in various aspects of human life, especially in the way we communicate and exchange information. Various important activities such as sending confidential documents, business communications, exchanging personal data, storing digital archives, and even financial transactions are now mostly done through computer networks and the internet [1]. Although it provides convenience, efficiency, and flexibility, the use of public networks also increases the risk to digital data security. Information sent over open networks is highly vulnerable to threats such as eavesdropping, data manipulation, information theft, and misuse by unauthorized parties. These threats not only result in material losses, but can also affect users' privacy, reputation, and trust in digital systems. Therefore, information security is a very important issue in the field of information technology. Not only does the protection of message content need to be considered, but also how to conceal the existence of messages so as not to arouse suspicion during the transmission process, especially in open network-based communication systems that have a high level of security vulnerability [2].

Various information security approaches have been developed to address these issues, one of which is cryptography, which aims to protect message content through encryption. Cryptography has proven effective in maintaining data confidentiality, but encrypted messages are generally easily recognizable as confidential information, potentially attracting the attention of parties intent on attacking [2]. This situation has led to the development of other approaches that not only protect the content of messages, but also conceal their existence. Steganography has emerged as an alternative solution, based on the concept of hiding secret messages within carrier media such as text, images, audio, and video, so that the messages appear to be ordinary digital data. However, the application of steganography also faces a number of challenges, including limited insertion capacity, deterioration of the quality of the carrier medium, and the risk of detection due to significant changes to the medium [3]. Simple steganography methods that work directly on pixel values, for example, are often not resistant to compression, retransmission, or data manipulation [4]. In this context, video media offers greater potential as a steganography medium because it has large data sizes, a large number of frames, and a high level of visual complexity. However, the use of video as a steganography medium also requires methods that are able to maintain a balance between visual quality, insertion capacity, and compression efficiency, so there are still challenges and research opportunities that need to be further explored [2].

Based on these issues, this study aims to implement the Motion Vector Steganography method in video media as an effort to improve the security and effectiveness of concealing secret messages in digital communications. This method utilizes

ISSN: XXXX-XXXX

motion vectors generated in the block-based video compression process, where small changes in motion vector values do not cause significant visual differences in the video. The main scientific contribution of this research is the presentation of an implementative and simulative approach that systematically describes the stages of inserting and extracting secret messages through the use of motion vectors. This approach not only emphasizes the final result, but also provides a clearer conceptual understanding of the working mechanism of Motion Vector Steganography. The novelty of this research lies in the presentation of a comprehensive simulation based on implementation that emphasizes the balance between message insertion capacity, video visual quality, and message extraction success [5]. Thus, this research is expected to make a real contribution to the development of secure, effective, and applicable video steganography techniques, as well as serve as a reference for further research in the field of information security and digital communication systems [3].

2. Literature Review and Problem Statement

Previous research has shown that Motion Vector Steganography is an effective technique in video steganography because it can insert secret messages with minimal visual distortion. Reported that inserting secret data into motion vectors in the MPEG compression standard produces visual changes that are almost undetectable by the human visual system. H.264 compressed video shows that motion vector-based methods have good resistance to recompression, so that secret messages can still be extracted with a high degree of accuracy [6], [7] . Meanwhile, emphasized that the use of motion vectors can increase message insertion capacity compared to pixel-based steganography methods, because motion information between frames can be modified without significantly changing the visual structure of the video. However, these studies generally focus more on evaluating the performance of the method in terms of visual quality, capacity, and robustness, while the aspects of simulation implementation and understanding of the message insertion and extraction mechanisms are still discussed to a limited extent [3].

Based on a review of previous studies, a research gap can be identified in the lack of studies that emphasize the comprehensive and easy-to-understand implementation and simulation of the Motion Vector Steganography process. Most previous studies have focused on quantitative results without providing a clear picture of the systematic stages of message insertion and extraction. In addition, the complexity of motion vector calculations and the dependence of this method on compression-based video encoding processes remain challenges that have not been fully resolved, especially in maintaining a balance between insertion capacity, video visual quality, and message extraction success [8]. Therefore, the research problem is formulated as how to effectively implement and simulate the Motion Vector Steganography method on video media so that the process of inserting and extracting secret messages can be clearly understood without significantly reducing the visual quality of the video. This research aims to fill this gap by presenting an implementative and simulative approach that confirms the potential of Motion Vector Steganography as a secure, efficient, and applicable video steganography method.

3. Material and Method

The method used in this study is simulation-based Motion Vector Steganography, which is a video steganography approach that utilizes motion vectors as a medium for inserting secret messages [9]. This method was chosen because motion vectors are part of the block-based video compression process, so that small changes in the motion vector values do not cause significant visual differences in the video [10]. This research is experimental in nature and aims to implement and simulate the process of embedding and extracting secret messages in digital video media. The data used consists of digital video as the cover media and secret messages in the form of text as the data to be embedded. The video used is in a compressed format to enable the formation of motion vectors, while text messages are chosen because they are easily converted into binary form [6] [7].

The system was implemented using the Python programming language as the main development tool, with support from the OpenCV library for video processing and simulation of motion vector formation and manipulation, as well as Tkinter for building the graphical user interface [11]. This research does not require special hardware and can be run on computers or laptops with standard specifications, allowing replication by other researchers. The basic principle of the method used is to insert secret message bits into certain components of the motion vector generated in the block-based video compression process. The motion vector represents the movement of objects between frames, so that vector value modifications are carried out minimally and in a controlled manner so as not to affect the visual quality of the video or the efficiency of compression [6].

 ISSN: XXXX-XXXX

The research process begins with data preparation, namely the selection of digital video as the storage medium and the preparation of secret messages in text form. Next, the secret messages are converted into binary representations so that they can be inserted into the motion vector bit by bit. The video is then processed to generate motion vectors between frames simulatively using a block-based compression approach. The embedding process is carried out by modifying certain components of the motion vector according to the secret message bits, while keeping the vector value changes within tolerance limits. After the embedding process is complete, a stego video is formed based on the modified motion vector. The next stage is the extraction process, which involves retrieving the motion vector from the stego video to obtain the secret message bits, then converting them back into text form [6], [8].

Pengujian metode dilakukan dengan membandingkan pesan hasil ekstraksi dengan pesan asli untuk memastikan keberhasilan proses penyisipan dan ekstraksi. Selain itu, dilakukan pengamatan visual secara subjektif terhadap video sebelum dan sesudah penyisipan untuk memastikan bahwa metode yang digunakan tidak menimbulkan perubahan visual yang signifikan. Seluruh tahapan metode disusun secara sistematis dan logis sehingga dapat direplikasi oleh peneliti lain dalam penelitian steganografi video berbasis motion vector.

3.1 Data Preparation

The data preparation stage is the first step in the video steganography process. At this stage, two main data sets are prepared, namely a digital video as the carrier medium (cover video) and a secret message in text form. The digital video is used as the medium for inserting the message by utilizing the motion vector component through a simulation process, while the secret message is chosen in simple text form so that it can be easily converted into a binary representation [7] .

The secret message used in this study is “HALO SEMUA .” The message is converted into ASCII code and then represented in 8-bit binary form. The purpose of this conversion process is so that each character of the message can be inserted into the motion vector bit by bit. All binary bits resulting from the conversion will be inserted sequentially into the motion vector at the insertion stage.

Biner Table 1. Conversion of Secret Messages to ASCII and Binary

Karakter	ASCII	Biner
H	72	01001000
A	65	01000001
L	76	01001100
O	79	01001111
(spasi)	32	00100000
S	83	01010011
E	69	01000101
M	77	01001101
U	85	01010101
A	65	01000001

Table 1 shows the conversion results of each character in the secret message into an 8-bit binary form used as input in the insertion process.

3.2 Secret Message Insertion

The message insertion stage begins with block-based video encoding to generate motion vectors that represent the movement of pixel blocks between video frames. Motion vectors are chosen as the medium for insertion because small changes in their values do not cause significant visual differences in the video [12]. In this study, the encoding process and motion vector formation are carried out simulatively to facilitate understanding of the message insertion mechanism. Message insertion is performed by taking the secret message bits one by one from the binary conversion result, then inserting them into the Least Significant Bit (LSB) of the motion vector [6]. The insertion formula used is:

$$MV' = MV - (MV \, mod 2) + b$$

Information:

MV is the initial motion vector,

b is the message bit, and

MV' is the motion vector after insertion.

As an illustration, Table 2 shows an example of manual insertion steps for the first 8 bits of the binary message 01001000 with an initial motion vector value of 32 (10101010).

Table 2. Example of Message Bit Insertion in Motion Vector

Step	Bit Pesan	Sebelum	Sesudah
1	0	10101010	10101010
2	1	10101010	10101011
3	0	10101010	10101010
4	0	10101010	10101010
5	1	10101010	10101011
6	0	10101010	10101010
7	0	10101010	10101010
8	0	10101010	10101010

Table 2. Example of Message Bit Insertion in Motion Vector Table 2 illustrates the process of modifying the LSB motion vector according to the inserted secret message bits. The insertion process is repeated until all secret message bits have been inserted. The modified motion vector is then reused in the encoding process to form the stego video. Visually, the stego video appears identical to the original video because the changes to the motion vector are minimal and controlled.

3.3 Secret Message Extraction

At the extraction stage, the stego video is reanalyzed to obtain the motion vector resulting from the insertion. The message bits are extracted by reading the LSB from the motion vector. Extraction Formula:

$$b = MV' mod \, 2$$

Example of Manual Extraction Steps

Motion vector stego:

10101011

Bit extraction:

$$10101011_2 \, mod \, 2 = 1$$

This process is repeated until all bits of the message are obtained.

The binary bits are then grouped in sets of 8 bits and converted back to ASCII to obtain the original text message.

4. Result And Discussion

The results of the implementation and discussion of the video steganography system using the Motion Vector Steganography method developed based on the Python programming language. The results are presented systematically based on the stages of implementation and system testing, while the discussion focuses on the scientific interpretation of the results obtained without repeating the detailed explanation of the method.

4.1 Test Results and System Discussion

Based on the test results, the video steganography system using the Motion Vector Steganography method is capable of effectively embedding secret messages into video media. The use of motion vectors as an insertion medium produces stego videos that can still be played normally and do not show significant visual differences compared to the original videos. This shows that the method used is able to fulfill the aspect of imperceptibility, namely that the existence of secret messages is not easily recognizable visually.

In addition, all secret message bits were successfully inserted into the motion vector according to the designed scheme. During the extraction stage, the system was able to read back the message bits and generate a message identical to the original inserted message. No data loss or information changes were found during the insertion and extraction processes. These results show that the system has a good level of consistency and synchronization between the encoding and decoding processes.

The success of inserting and extracting secret messages shows that motion vectors can be effectively used as a medium for hiding information in digital videos. By taking advantage of natural changes between video frames, the existence of secret messages becomes more difficult to detect, both visually and simply.

4.2 System Performance Evaluation

System performance evaluation was conducted by observing the success of the secret message insertion and extraction processes and their impact on video visual quality. The test results showed that the stego video retained good visual quality and did not experience significant interference after the message insertion process. This indicates that the Motion Vector Steganography method has a low visibility level and does not interfere with the user's visual comfort.

In terms of reliability, the system demonstrated stable performance in the message extraction process. Secret messages could be extracted in their entirety and matched the original messages that had been inserted, indicating that the system was able to maintain data integrity during the steganography process. This reliability indicates that the method used is effective enough to be applied in secret communication scenarios based on video media. Overall, the evaluation results show that the developed video steganography system performs well in terms of visual quality and data integrity. This indicates that the Motion Vector Steganography method is suitable for use as an approach to hiding information in digital videos.

4.3 Limitations and Further Discussion

Although the developed system shows good results, there are still some limitations that need to be considered. System testing was conducted on specific types and characteristics of videos, so the results obtained do not fully represent all types of videos. In addition, the evaluation of system performance is still qualitative and does not involve quantitative metrics such as PSNR or SSIM.

Another limitation is the message insertion capacity, which depends on the number of motion vectors available in the video. Videos with low motion potentially have a smaller insertion capacity than videos with high motion. Therefore, video selection is an important factor in applying this method.

As a further development, subsequent research could be directed toward testing the system using various types and resolutions of video, as well as applying more comprehensive evaluation metrics. In addition, testing the system's resistance to recompression and steganalysis attacks could also be conducted to improve the security and reliability of the proposed method.

5. Conclusion

Based on the results of the study, the Motion Vector Steganography method has been proven to be capable of effectively embedding and extracting secret messages in video media without causing significant visual changes. The use of motion vectors allows for effective message concealment and addresses data security issues in video-based communication systems. The implementation of encoding and decoding simulations shows a high and consistent level of message extraction success with the original message. The contribution of this research lies in the presentation of structured simulations that clarify the working mechanism of the method, while the novelty is demonstrated through the visualization

of the insertion process based on a graphical interface that supports further understanding and development of video steganography.

6. References

[1] S. Quach, P. Thaichon, K. D. Martin, S. Weaven, and R. W. Palmatier, "Digital technologies: tensions in privacy and data," J. Acad. Mark. Sci., vol. 50, no. 6, pp. 1299–1323, Nov. 2022, doi: 10.1007/s11747-022-00845-y.

[2] M. E. Danlami, L. L. Raymond, and T. Solomon, "Hybridization of Cryptography and Steganography to Achieve Secret Communication," International Journal of Advances in Engineering and Management (IJAEM), vol. 5, p. 428, 2023, doi: 10.35629/5252-0508428437.

[3] H. Alshamrani, Dr. S. H. Alajmani, Dr. R. Y. Alyami, and Dr. Ben Soh, "Comprehensive Comparison of Image Steganography Techniques with Security Enhancement," International Journal of Recent Technology and Engineering (IJRTE), vol. 14, no. 2, pp. 7–19, Jul. 2025, doi: 10.35940/ijrte.A8249.14020725.

[4] M. A. Ali, A. Mahmoud, and A. A. Jabbar, "Steganography Encryption Secret Message in Video Raster Using DNA and Chaotic Map," Iraqi Journal of Science, pp. 5534–5548, Dec. 2022, doi: 10.24996/ijs.2022.63.12.38.

[5] Muhammad Agus Septiawan, Fiky Anggara, Zidan Alvie Nugroho, and Zaldy Irhas Addiyat, "Optimasi Steganografi Video Berbasis LSB Multi-Faktor dengan Penyesuaian Bit Adaptif Berdasarkan Kecerahan, Tekstur, dan Stabilitas Gerakan Antar-Frame," Modem : Jurnal Informatika dan Sains Teknologi., vol. 4, no. 1, pp. 98–108, Jan. 2026, doi: 10.62951/modem.v4i1.738.

[6] B. Cornelius, "Makalah IF4020 Kriptografi-Teknik Informatika ITB-Semester I Tahun," 2025.

[7] M. ud Din et al., "Randomized Frame Selection Based Video Steganography Method for Secure Embedding of Secret Data", doi: 10.56979/802/2025.

[8] D. P. Sitohang, P. Lamdippos, H. Parmadi, V. B. Sitepu, and W. Gulo, "Video Based Steganography (Motion Vector Steganography)," 2023. [Online]. Available: https://jurnal.seaninstitute.or.id/index.php/jutiρ33

[9] J. Petrus, "Implementasi Steganografi pada Citra dengan Metode Bit-Plane Complexity Segmentation Untuk Transformasi Data".

[10] R. N. Al-Mallah and M. H. Al-Jammas, "Adaptive steganography based on motion vectors for H.264/AVC," Cyber Security and Applications, vol. 3, Dec. 2025, doi: 10.1016/j.csa.2025.100109.

[11] Supiyandi Supiyandi, Andriani Sitorus, Nurul Fitriah, Havni Virul, and Syawaliah Putri Rangkuti, "Pendeteksi Gerakan Pada Vidio Menggunakan Pyton dan OpenCV," Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika, vol. 2, no. 6, pp. 334–343, Nov. 2024, doi: 10.61132/merkurius.v2i6.522.

[12] J. Kunhoth, N. Subramanian, S. Al-Maadeed, and A. Bouridane, "Video steganography: recent advances and challenges," Multimed. Tools Appl., vol. 82, no. 27, pp. 41943–41985, Nov. 2023, doi: 10.1007/s11042-023-14844-w.