Ju-ti : Jurnal Teknik Indonesia
ISSN : 2964-0490 (online)
Vol. 2, No. 01, 2023, pp. 33-38
https://jurnal.seaninstitute.or.id/index.php/juti

Video Based Steganography (Motion Vector Steganography)

Della Patresya Sitohang[1], Purba Lamdippos Hendry Parmadi[2], Vinela Br Sitepu[3], Wilhelmus Wanzerhasratman Gulo[4]
Prodi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas

Article Info

Keywords:
steganography, motion vector, Least Significant Bit, Most Significant Bit, information security.

ABSTRACT

Steganography is a technique for hiding information in digital media so that it cannot be detected by third parties. One effective steganography method is Motion Vector Steganography (MVS), which utilizes motion vectors in video compression to insert secret messages. This study implements the Least Significant Bit (LSB) and Most Significant Bit (MSB) methods on motion vectors in videos to insert messages with minimal changes in visual quality. The results of the analysis show that the LSB method has little impact on video quality, while the MSB method is more resistant to steganalysis detection. However, there are challenges such as changes in file format and video size that need to be considered. This study provides insight into the application of video-based steganography and its potential development in the field of information security.

Corresponding Author:
Della Patresya Sitohang,
Fakultas Ilmu Komputer, Program Study Teknik Informatika, Universitas Katolik Santo Thomas

INTRODUCTION

Steganography is the art and science of hiding messages within other media in such a way that the message's presence is undetectable by a third party. Steganography can be done for various forms of data. Video is one of the most common forms of data used for communication today, so steganography for video is becoming increasingly important.(Nandar Pabokory et al., 2015).

One form of steganography that is widely developed is video-based steganography. Video as a medium has advantages over images or audio because it has a larger storage capacity and changes between frames that make message insertion more difficult to detect. One popular method in video steganography is Motion Vector Steganography (MVS), which utilizes motion vectors in video compression to hide secret information.(Santiko, 2005).

This study uses the EoF algorithm to hide messages in FLV videos. The inserted message is in the form of text that is first encrypted with the Rijndael algorithm. The test results show that this method does not produce visible distortion in the video, with a very high Peak Signal to Noise Ratio (PNSR) value, even reaching infinity, indicating that the video quality is maintained after message insertion.(Riadi et al., 2021).

A study compared the effectiveness of LSB and DCT methods in inserting data into videos. The results showed that the DCT method had a higher success rate (90%) than LSB (38%). In addition, the combination of the two methods also showed good results with higher PSNR than LSB alone.(Yunus & Harjoko, 2014).

Motion vectors are an important component in inter-frame coding-based video compression techniques, such as the H.264, MPEG-4, and HEVC standards.(Hingole, 2015). This technique works by predicting the movement between frames to reduce data redundancy. By carefully modifying the motion vectors, a secret message can be inserted without causing significant visual changes to the video. This makes Motion Vector Steganography an effective technique and difficult to detect by forensic analysis.

Although this technique has great potential in information security applications, there are several challenges that need to be overcome, such as limited embedding capacity, resistance to steganalysis

attacks, and its impact on video quality. Therefore, research in this field continues to grow to improve the efficiency and security of message hiding methods in videos.

METHOD

Least Significant Bits

Least Significant Bit (LSB) is one of the simplest and most popular steganography methods used to hide secret messages in digital media such as images, audio, and video. LSB works by replacing the least significant bit in a data unit of the containing media, such as an image pixel or a sound sample, with bits from the message to be embedded.(Lutfi & Rosihan, 2018).

Matroska Video File

Matroska Video File (MKV) is a multimedia container format that can store various types of data such as video, audio, subtitles, and metadata in a single file. This format was developed as an open-source and non-commercial standard to provide more flexibility than other video formats such as MP4 and AVI. Matroska is designed to store high-quality video with a variety of codecs without losing information or needing to re-convert when playing the files on devices that support them.

Video Based Steganography Algorithm Formula

Video-based steganography is a technique for inserting secret messages into video files by exploiting elements in the video, such as frames, pixels, or bitstream compression. The algorithms used vary depending on the method chosen, but one of the most common methods is

Least Significant Bit (LSB) in Motion Vector Steganography

The LSB (Least Significant Bit) method inserts data by changing the least significant bit of the motion vector value. Since this change is very small, its impact on video quality is almost invisible to the human eye.

Example:

Suppose there is a motion vector with binary values:

10101110 → before insertion

10101111 → after insertion (replacing the last bit with '1')

Most Significant Bit (MSB) in Motion Vector Steganography

The MSB (Most Significant Bit) method replaces the most significant bit of the motion vector. This makes a larger change in the motion vector value, making it harder to detect using simple steganalysis methods.

Example:

Suppose there is a motion vector with binary values:

10101110 → before insertion

00101110 → after insertion (replacing the first bit with '0')

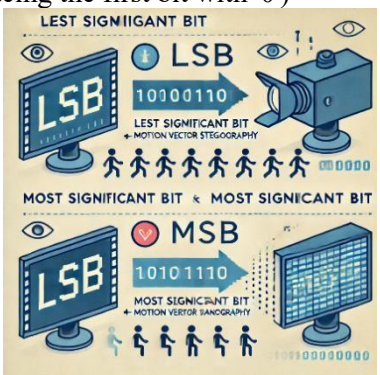

Figure 1. Difference between LSB and MSB methods

Difference between LSB and MSB methods in Motion Vector Steganography.

a. LSB (left): Highlights changes in the last bit, with little impact on video quality.
b. MSB (right): Highlights changes in the first bit, which causes more visible changes in the video.

RESULTS AND DISCUSSION

Calculation Manual

The following is an example of solving Motion Vector Steganography) using the LSB method of manual calculation to insert the character message "K" into the motion vector, using the LSB (Least Significant Bit) method.

a. Converting the Character "K" to Binary
   The character "K" in ASCII is 75. Now we convert this number to 8-bit binary: 75 (decimal) = 01001011 (binary). So, "K" in binary is 01001011.
b. Get Motion Vector (MV)
   Suppose we have a motion vector like the following: mv_x = [[5, 6], [8, 9]]
c. LSB Modification in Motion Vector
   LSB is the rightmost (last) bit of a binary number. We will replace the rightmost bit of each motion vector with the corresponding message bit. The binary message for "K" is 01001011. Now we will replace the LSB of each element of mv_x with the message bits. The message in binary: 01001011 (The first bit is 0, the second bit is 1, the third bit is 0, the fourth bit is 0, etc.)
   LSB modification steps:
   1. mv_x[0][0] = 5
      In binary: 101
      The first bit of the message is 0 → Change the LSB to 0: 101 → 100 (result: 4).
   2. mv_x[0][1] = 6
      In binary: 110
      The second bit of the message is 1 → Change the LSB to 1: 110 → 111 (result: 7).
   3. mv_x[1][0] = 8
      In binary: 1000
      The third bit of the message is 0 → Change the LSB to 0: 1000 → 1000 (result: 8).
   4. mv_x[1][1] = 9
      In binary: 1001
      The fourth bit of the message is 0 → Change the LSB to 0: 1001 → 1000 (result: 8).

   After LSB modification based on the message bits, the result is: mv_x = [[4, 7], [8, 8]]
d. Record LSB and MSB for Each Motion Vector
   Now, let's calculate the LSB and MSB for each value in the modified motion vector.
   mv_x[0][0] = 4, Binary: 100, LSB: 0, MSB: 1 , mv_x[0][1] = 7, Binary: 111, LSB: 1, MSB: 1, mv_x[1][0] = 8, Binary: 1000, LSB: 0, MSB: 1, mv_x[1][1] = 8, Binary: 1000, LSB: 0, MSB: 1.

Table 1. Difference between LSB and MSB for Each Motion Vector

MV	LSB	MSB
4	0 (rightmost bit)	1 (leftmost bit)
7	1	1
8	0	1
8	0	1

Implementation and Comparison

This implementation aims to hide messages in video files using the Motion Vector Steganography method. Messages are inserted into the smallest part of video data, namely the Least Significant Bit (LSB) or Most Significant Bit (MSB). Application Interface:

a. Video Input Selection: Users can select the source video file via the Browse button. The path of the selected video file will appear in the column below.
b. Message Input Column: Users enter the message they want to insert into the video in this column.
c. Video Save Location Options: After inserting a message, users can specify the location where the resulting video will be saved via the Save As column and button.

d. Skip Message Button: This button may be used to skip the message insertion step, or to cancel the operation.
e. LSB and MSB Logs: At the bottom of the application, you can see a log showing the results of the message encoding process. For example: "MV: -10, LSB: 0, MSB: 1" shows the value of a particular Motion Vector and the changes in LSB and MSB due to message insertion.

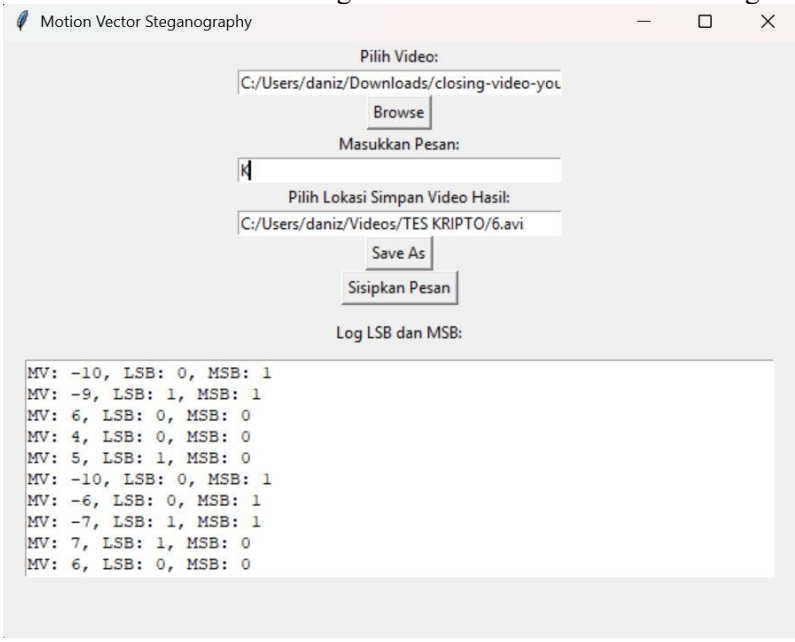

Figure 2. Application Interface

Implementation Process

a. Video Input: The user selects a video file as the message carrier.
b. Message Input: The message to be inserted is entered into the text field.
c. Encoding Process: The message is converted into digital bits, then inserted into the video frame using LSB/MSB manipulation techniques on the motion vector.
d. Video Output: Video with hidden message is saved to a user-specified location.

The log section records how the message bits are changed and inserted into the motion vector. This information is useful for debugging and ensuring that the message insertion is going according to plan. Here is a comparison between the video before and after inserting the message into the video.

Comparison before and after the steganography process is carried out.

Before Steganography Process File Name: closing-video-youtube-keren-no-copyright-youtubers-pemula.mp4. File Format: MP4 (MPEG-4 Video). File Location: Saved in C:\Users\daniz\Downloads. File Size: Size on disk: 220 KB (225,280 bytes). Size: 218 KB (223,856 bytes)

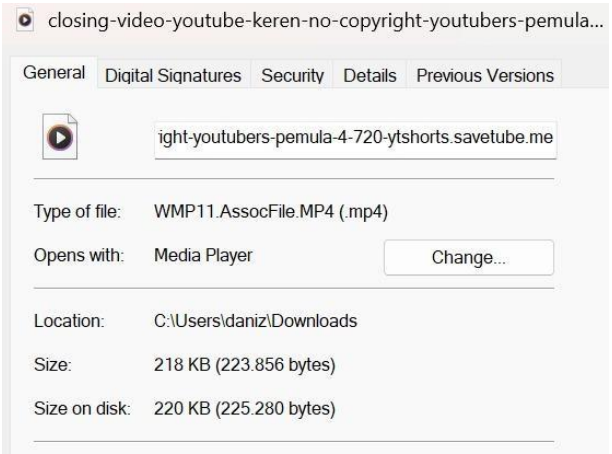

Figure 3.steganography process

After Steganography Process File Name: 6 (file name changed). File Format: AVI (Audio Video Interleave). File Location: Saved in C:\Users\daniz\Videos\TES KRIPTO. File Size: Size on disk: 164 KB (167,936 bytes). Size: 163 KB (167,430 bytes).

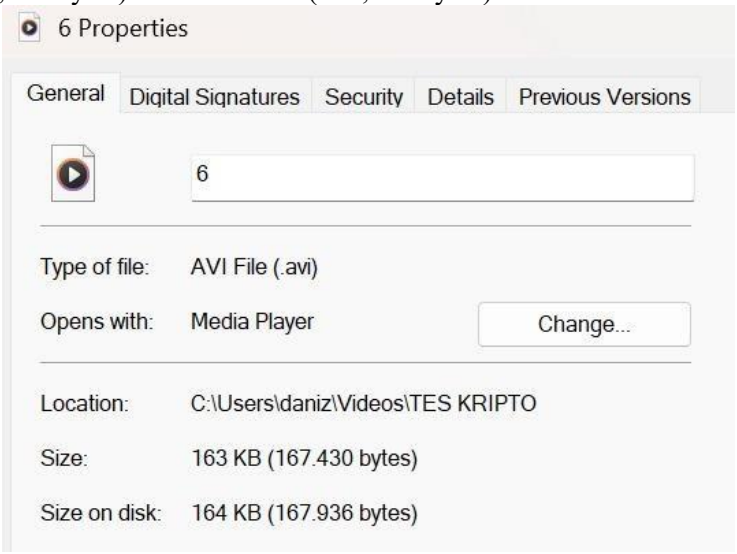

Figure 4. Storage Location Process

Comparative Analysis

File Format Change The file format changes from MP4 to AVI. This may be because the steganography algorithm uses a library or encoding method that produces a different output format. File Size ChangeSize: Reduced from 218 KB to 163 KB. Size on DiskReduced from 220 KB to 164 KB. The decrease in file size indicates that the encoding process may have also involved recompression or removal of unnecessary metadata from the original file.Change of LocationStorageThe resulting files are saved in a different directory, namely in the folderCRYPTO TEST. This showsstepexplicitly in the application to specify the location of the output file.

Effect on Quality Although not shown here, changing the format and file size may affect the visual quality of the video. AVI usually has different encoding than MP4.The change in file size and format indicates that the application successfully inserted the message, although there were side effects in the form of file size reduction and format changes. This is important to note if the application is used on a production scale, especially if video quality or format compatibility is a priority.

CONCLUSION

Video-based steganography using Motion Vector Steganography has the main advantages of large message storage capacity, high security because it is difficult to detect, and flexibility in the embedding method. However, this technique also has disadvantages, such as high complexity in implementation, vulnerability to compression or editing, and the need for large computing resources. The use of methods such as Least Significant Bit (LSB) provides a simple way to embed data, but challenges remain in maintaining media quality and avoiding detection by forensic analysis.

REFERENCES

Hingole, D. (2015). *MavMatrix MavMatrix H.265 (HEVC) BITSTREAM TO H.264 (MPEG 4 AVC) BITSTREAM H.265 (HEVC) BITSTREAM TO H.264 (MPEG 4 AVC) BITSTREAM TRANSCODER TRANSCODER*. https://mavmatrix.uta.edu/electricaleng_theseshttps://mavmatrix.uta.edu/electricaleng_theses/374

Lutfi, S., & Rosihan, R. (2018). PERBANDINGAN METODE STEGANOGRAFI LSB (LEAST SIGNIFICANT BIT) DAN MSB (MOST SIGNIFICANT BIT) UNTUK MENYEMBUNYIKAN INFORMASI RAHASIA KEDALAM CITRA DIGITAL. *JIKO (Jurnal Informatika Dan Komputer)*, *1*(1), 34–42. https://doi.org/10.33387/jiko.v1i1.1169

Nandar Pabokory, F., Fitri Astuti, I., & Harsa Kridalaksana, A. (2015). IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD. In *Jurnal Informatika Mulawarman* (Vol. 10, Issue 1).

Riadi, I., Sunardi, S., & Aryanto, D. (2021). Algoritma End of File dan Rijndael pada Steganografi Video. *JRST (Jurnal Riset Sains Dan Teknologi)*, *5*(1), 17. https://doi.org/10.30595/jrst.v5i1.9187

Santiko, I. (n.d.). *Conference on Information Technology, Information System and Electrical Engineering 44 Implementasi Model Steganografi Dalam Mengelola Kerahasiaan Informasi Dengan Metode LSB (Least Significant Bit)*. http://repository.usu.ac.id

Yunus, M., & Harjoko, D. A. (2014). Penyembunyian Data pada File Video Menggunakan Metode LSB dan DCT. *IJCCS*, *8*(1), 81–90.

Wang, K., Zhao, H., & Wang, H. (2014). Video steganalysis against motion vector-based steganography by adding or subtracting one motion vector value. *IEEE Transactions on Information Forensics and Security*, *9*(5), 741-751.

Su, Y., Zhang, C., & Zhang, C. (2011). A video steganalytic algorithm against motion-vector-based steganography. *Signal Processing*, *91*(8), 1901-1909.

Yao, Y., Zhang, W., Yu, N., & Zhao, X. (2015). Defining embedding distortion for motion vector-based video steganography. *Multimedia tools and Applications*, *74*, 11163-11186.

Rezagholipour, K., & Eshghi, M. (2016, September). Video steganography algorithm based on motion vector of moving object. In *2016 Eighth international conference on information and knowledge technology (IKT)* (pp. 183-187). IEEE.

Cao, Y., Zhao, X., & Feng, D. (2011). Video steganalysis exploiting motion vector reversion-based features. *IEEE signal processing letters*, *19*(1), 35-38.

Zhang, H., Cao, Y., & Zhao, X. (2016). Motion vector-based video steganography with preserved local optimality. *Multimedia Tools and Applications*, *75*, 13503-13519.