PAPER NAME

Hiding Document Format Files Using Video Steganography Techniques With Least Significant Bit Method.

WORD COUNT	CHARACTER COUNT
4918 Words	**24503 Characters**
PAGE COUNT	FILE SIZE
8 Pages	**810.4KB**
SUBMISSION DATE	REPORT DATE
Jan 31, 2023 12:48 PM GMT+7	**Jan 31, 2023 12:49 PM GMT+7**

● 11% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 7% Internet database
- Crossref database
- 5% Submitted Works database
- 6% Publications database
- Crossref Posted Content database

● Excluded from Similarity Report

- Manually excluded sources
- Manually excluded text blocks

Hiding Document Format Files Using Video Steganography Techniques With Least Significant Bit Method

Tufail Akhmad Satrio
Department of Informatics Engineering
Institut Teknologi Telkom Purwokerto
Purwokerto, Indonesia
tufailas040@gmail.com

Wahyu Adi Prabowo*
Department of Informatics Engineering
Institut Teknologi Telkom Purwokerto
Purwokerto, Indonesia
wahyuadi@ittelkom-pwt.ac.id

Trihastuti Yuniati
Department of Informatics Engineering
Institut Teknologi Telkom Purwokerto
Purwokerto, Indonesia
trihastuti@ittelkom-pwt.ac.id

***Abstract*—Video Steganography is one type that can use to hide secret messages. Video Steganography is a technique to hide messages in video media by inserting messages into one of the video frames. Cryptography can be combined with the Steganography technique to secure hidden messages in video files. This research was conducted to analyze the LSB (Least Significant Bit) steganography test combined with the Fernet cryptographic process. This study investigates the file insertion process, the test extraction process, the speed of system implementation, the visual attack, the Peak Signal Noise Ratio (PSNR) value, and the audio comparison between original video and video with embedded files. The results of this test indicate that the embedding process in the video is directly proportional to the results received. The larger the original video size, the larger the embedded video size will be.**

Keywords*—video steganography, cryptography, Least Significant Bit, LSB, Fernet

I. Introduction

Advances in technology and the internet are currently making various kinds of breakthroughs in the field of data communication. Communication is one of the essential needs in human life to relate to each other [1], [2]. When communicating, there will be an exchange of information between the two parties [3] and often there is essential information that is confidential [4]. Security and confidentiality of data or information are critical in information systems and data communication [5].

The major problem in the digital world, important information or data, is that data is an asset vulnerable to being stolen by others [6] . Recently, there has been renewed interest in data security. One way that is generally used to secure the data is to use a combination of steganography and cryptography [7], [8]. Steganography is one way to hide a message or personal data into data or other messages that appear to contain nothing except for people who know the key [5]. The purpose of steganography is to hide messages and make them invisible to attackers [9] and can even allow someone not to detect a message or data in the file [10]. Cryptography is the art of maintaining the security or confidentiality of data. Cryptography will convert data into specific codes and is only intended for parties with only a key to convert the code back into data [11]. The key is not an object but a secret code known by the party who exchanges information or data and will later be used to encrypt or decrypt data [12]. *Encryption* is a process carried out to secure a message (plaintext) into a hidden message (ciphertext), while decryption is the process of converting ciphertext into plaintext [13].

Studies on steganography and cryptography show the importance of data security. Several researchers have attempted to combine the concepts of steganography and cryptography. Steganography with LSB (Least Significant Hill) method and Hill Chipper cryptography can be combined in securing messages [14]–[16] In some of these studies, image media is used, so the steganography technique can be called Image Steganography. From the results of this study, the process of hiding messages in digital images is safe and unknown to the naked eye because the size of the bitmap resulting from steganography does not change after the process of inserting binary text into a binary bitmap. Using the Least Significant Bit (LSB) method, which replaces the last bit so that the bitmap capacity before and after steganography does not experience significant changes, cryptographic testing can be done encode and decode. Another study combines LSB steganography and RSA cryptography (Rivest-Shamir-Adleman) through video media [17], [18]. The results of this study indicate that this high-level system's performance and methodology have succeeded in performing embedded files compared to other systems using the same methodology [19].

In this study, researchers built an application combining LSB steganography and fernet cryptography on video media. The advantage of this LSB steganography method is that the quality and size of the image after the message is inserted do not look much different[19]. The least significant bit is the part of the binary data sequence (base two) with the most negligible significant/smallest value. It is located on the far right of the bit sequence [20]. In the arrangement of bits in a byte (1 byte = 8 bits), there are the most significant bits (the most significant bit or MSB) and the least significant bit (the least significant bit or LSB) [21]. Fernet is an implementation of symmetric cryptography (also known as “secret key”) authentication [22]. Fernet is a cryptographic method that provides a simple authentication and encryption method using HMAC (Hash-based Message Authentication Code) with SHA256 for authentication and symmetric AES-128 in CBC (Cipher Block Chaining) mode using PKCS7 padding, which offers 128 bits (16 bytes) in lengt [23], [24].

For this reason, in this study, the researchers built an application that was built using the Python language to insert a file that has been encrypted using cryptography into a video

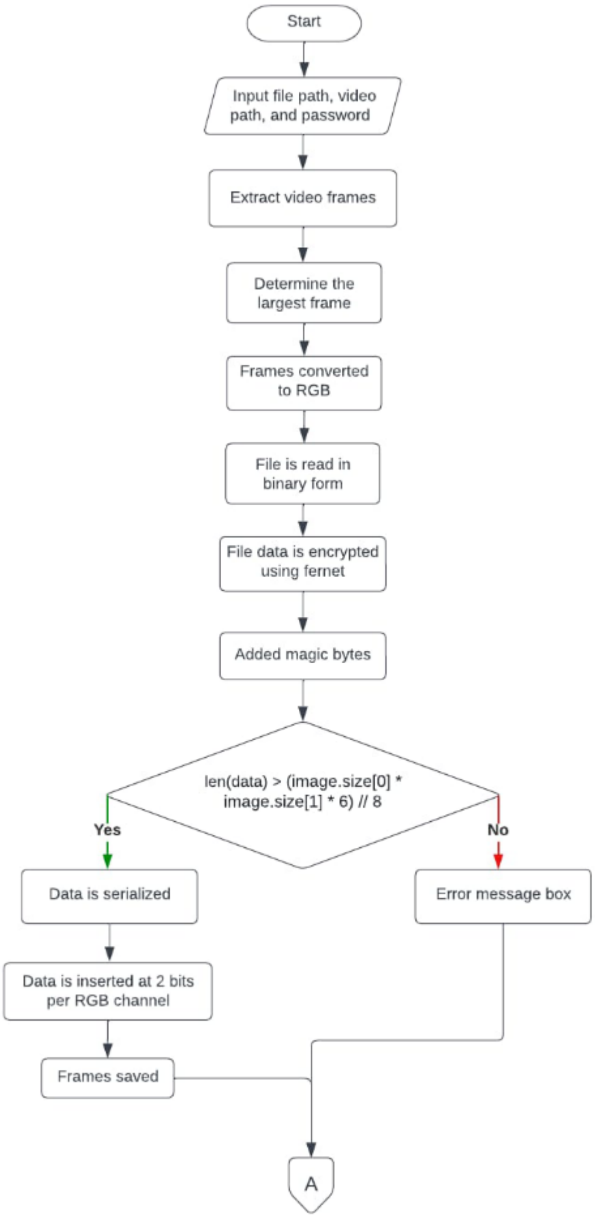
Start
Input file path, video path, and password
Extract video frames
Determine the largest frame
Frames converted to RGB
File is read in binary form
File data is encrypted using fernet
Added magic bytes
len(data) > (image.size[0] * image.size[1] * 6) // 8
Yes
No
Data is serialized
Error message box
Data is inserted at 2 bits per RGB channel
Frames saved
A

Fig. 1. Flowchart encryption process

that has been determined using steganography techniques, better known as Video Steganography. Video steganography is a technique of hiding or inserting data into a video[25]. In a video, some frames can be inserted into secret messages [26], so if someone wants to extract the message, they must check every frame in the video. The video used is a video in MP4 format. This format was chosen because it is often used by many people and is easy to find on the internet [27]. The files used in inserting messages into videos are files with .docx and .pdf formats. The choice of file with this format is because it can accommodate many messages/data compared to the .txt format, which can only be filled with text messages. Test Analysis of the results of steganography and encryption includes investigating the file insertion process, the test extraction process, the speed of system implementation, the visual attack, the Peak Signal Noise Ratio (PSNR) value, and the audio comparison between original video and video with embedded files. The results of this test indicate that the embedding process in the video is directly proportional to the results received. The larger the original video size, the larger the embedded video size will be.

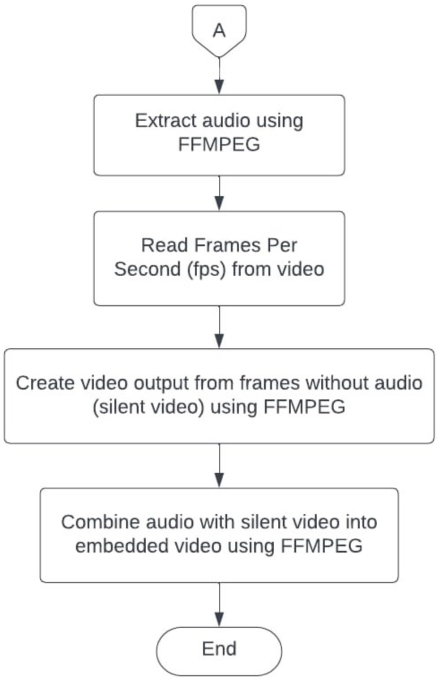
A
Extract audio using FFMPEG
Read Frames Per Second (fps) from video
Create video output from frames without audio (silent video) using FFMPEG
Combine audio with silent video into embedded video using FFMPEG
End

Fig. 2. Flowchart steganography process

II. SYSTEM IMPLEMENTATION

This stage involves applying the methods and techniques used to create application programs. The application implementation uses the python language, which is used to combine LSB steganography and fernet cryptography. The way the first video steganography application works is the insertion of files into the video. This first step aims to enter the file location, video location, and password. Then the inputted video will be extracted frame and audio using FFMPEG, and the frame will be used as a medium for message insertion. The frame selection is based on the largest frame size from a set of extracted frames. The next step is to insert the file into the frame using the LSB method. The file to be inserted is first opened using a binary format, then encrypted using the fernet algorithm to increase the level of data security. Then, the file will be given a unique mark (magic bytes) so that the file is detected in the frame that is the cover object when extracting the video file. After successfully inserting the file, the next step is to unify the frame and audio into a video output containing the secret file. The working process of the video steganography application can be seen in Fig. 1.

Next, the first step in extracting the file is to enter *the path of the Embedded Video* or video that is inserted the message and enter *the password*. Next, the video will be extracted its frames to retrieve hidden file data, this process can be seen in Fig. 2.

The next process is *extract Data File* in Fig. 3, in that process the frames that have been extracted will be selected with the largest size because it contains file data that has been hidden. The frames that have been obtained will be checked for LSB bits, if there are special marks (magic bytes) then the data will be taken from the LSB bits of the frame. Furthermore, the data will be decrypted first to get the original data. Once encrypted, the data will be converted into a *file* again using *binary writing mode*. After *the file* is successfully retrieved, the *extract Data File* completes.

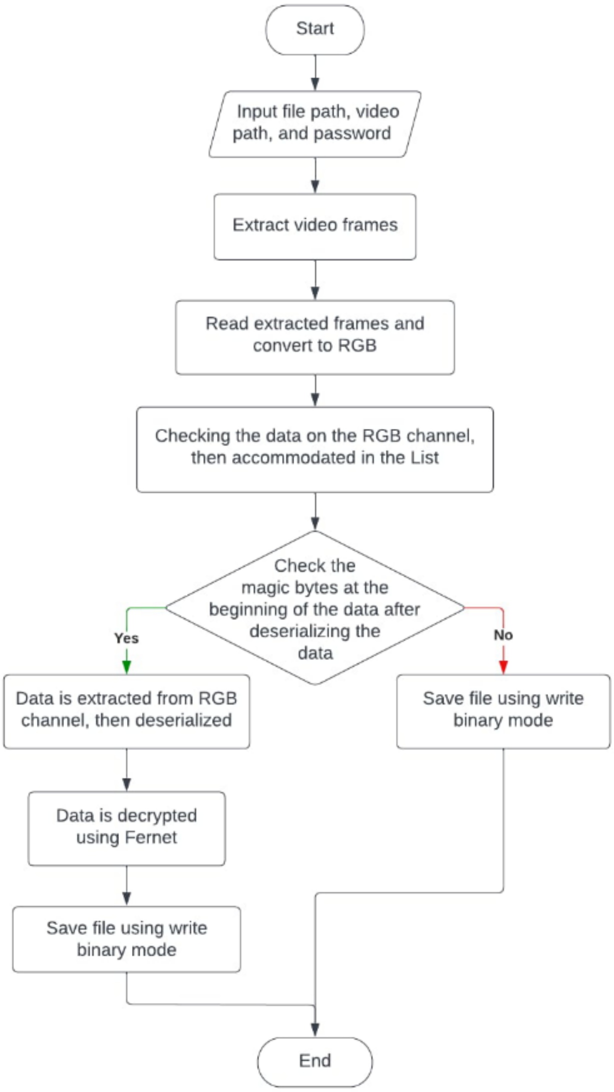
Start
Input file path, video path, and password
Extract video frames
Read extracted frames and convert to RGB
Checking the data on the RGB channel, then accommodated in the List
Check the magic bytes at the beginning of the data after deserializing the data
Yes
No
Data is extracted from RGB channel, then deserialized
Save file using write binary mode
Data is decrypted using Fernet
Save file using write binary mode
End

Fig. 3. Flowchart extraction process

The image below in Fig. 4 is the main window of the application. In the main window, there are two buttons, namely the "Hide File" and "Extract Files." The "Hide File" button inserts files into the video. The "Extract File" button is to retrieve files that have been inserted into the video.

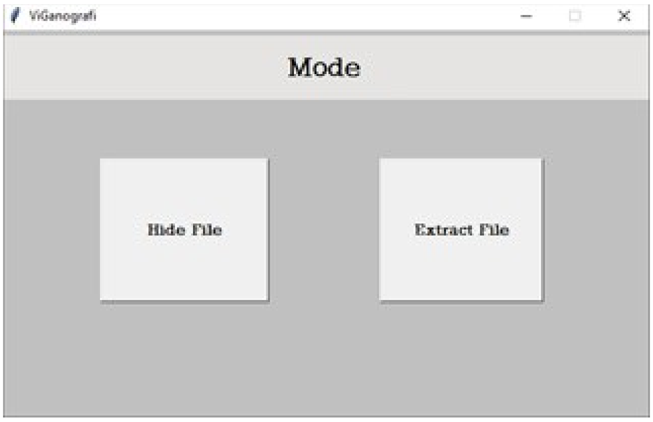

Fig. 4. Main window of the application

When the "Hide File" and "Extract File" button is pressed, then the user will be redirected to a new window as below in Fig. 5.

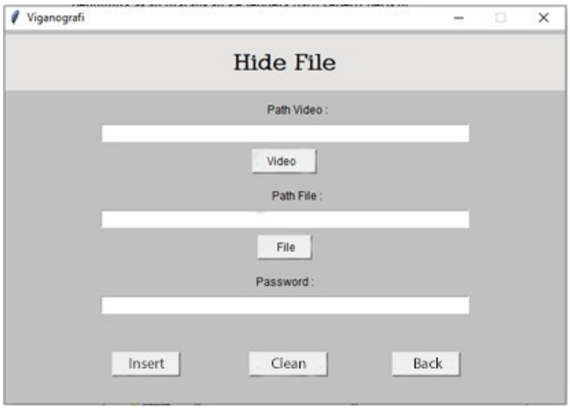

Fig. 5. "Hide File" menu window

In Fig. 5, contains three fields that must be filled in; the three columns are the video path, file path, and password fields. The three columns are inputs or variables used for file insertion into the video. In the "Extract File" menu in Fig. 6, there are two inputs or variables: the video path and password. Both variables must be filled so that the file extraction process runs smoothly.

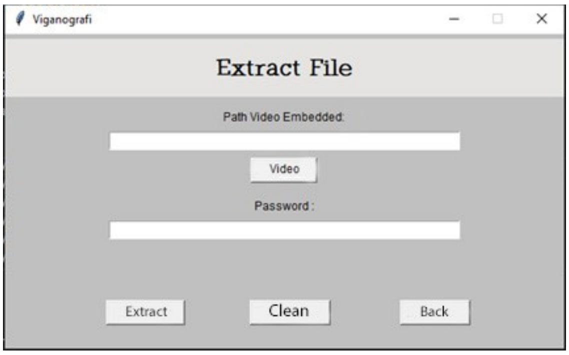

Fig. 6. "Extract File" menu window

III. RESULT AND DISCUSSION

Every process on this system was tested to find out that the system in the application was running well and analyzed the results of the output files received in each running process.

A. Process of Hiding Files Into Videos

In this hiding testing process, four videos and three files are used. The first three videos are similar with a duration of 29 seconds. The first three videos have differences in quality, namely 144p, 360p, and 720p. The video tests the success of the file-hiding process on a 2-bit data frame. Then the last video is used to test the visual attack on the given results. In the last video, the bits used in file hiding are 2 bits, 4 bits, and 6 bits. Then the three files used, both "docx" and "pdf" formats, have different sizes. The difference is applied to find out how big the maximum size of the data file that can be inserted into the video frame.

TABLE 1. FILE HIDING TEST RESULT

No	Original Video Name	Original Video Size	File Name	File Size	Password	Embedded Video Name	Embedded Video Size	Average Hiding Time (s)	Success or Failed
1.	144. mp4	633 KB	file. docx	20 KB	doc123	Embedded_Video_ 144p.mp4	45.933 KB	6,113	Success
2			file1. docx	112 KB		-	-	-	Failed
3			file2. docx	379 KB		-	-	-	Failed
4			file. pdf	13 KB	pdf123	Embedded_Video_ 144p1.mp4	45.927 KB	6,295	Success
5			file1. pdf	105 KB		-	-	-	Failed
6			file2. pdf	350 KB		-	-	-	Failed
7	360p.mp4	1.575 KB	file. docx	20 KB	doc123	Embedded_Video_ 360p.mp4	209.286 KB	16,620	Success
8			file1. docx	112 KB		Embedded_Video_ 360p1.mp4	209.378 KB	18,533	Success
9			file2. docx	379 KB		-	-	-	Failed
10			file. pdf	13 KB	pdf123	Embedded_Video_ 360p2.mp4	209.279 KB	16,319	Success
11			file. pdf	105 KB		Embedded_Video_ 360p3.mp4	209.370 KB	17,738	Success
12			file2. pdf	350 KB		-	-	-	Failed
13	720p.mp4	4.401 KB	file. docx	20 KB	doc123	Embedded_Video_ 720p.mp4	585.612 KB	43,403	Success
14			file1. docx	112 KB		Embedded_Video_ 720p1.mp4	585.729 KB	48,954	Success
15			file2. docx	379 KB		Embedded_Video_ 720p2.mp4	586.060 KB	46,912	Success
16			file. pdf	13 KB	pdf123	Embedded_Video_ 720p3.mp4	585.604 KB	43,622	Success
17			file1. pdf	105 KB		Embedded_Video_ 720p4.mp4	585.720 KB	42,001	Success
18			file2. pdf	350 KB		Embedded_Video_ 720p5.mp4	586.024 KB	45,805	Success

Based on Table 1. above, it can be seen that hiding files in videos with low-quality 144p can only be inserted with files with the smallest size, both "docx" and "pdf" files. The other four files cannot be inserted because they exceed the size limit that a 144p.mp4 video frame can store. Then the video with 360p quality can be inserted into two "docx" files and two "pdf" files because the frame is larger than the 144p quality video. Then on the video with the highest quality, which is 720p, all files can be inserted; this is because the video frame has a larger size than the two previous videos, so the maximum limit of the data size that can be inserted is getting bigger.

In the Table 1, it can be seen that there is an apparent difference between the original video and the embedded video, which lies in its size. Embedded video has a considerable size, and this is because the process of making video after file insertion does not use an encoding. Encoding serves to compress the video so that it can reduce its size of the video. However, in video steganography using this LSB method, the encoding process can cause the loss of file data inserted into the frame so that when the file extraction process is run, the file data is not found. In addition, the size of the embedded video is also affected by Frame Per Second (FPS). FPS will determine the number of frames contained in a video. The greater the number of FPS of a video, the larger the size of the embedded video produced.

Videos with the same content but different video quality, namely 144p, 360p, and 720p, significantly differ in file hiding time. The higher the video quality, the longer the file hiding time will be. From these results it can be seen that the large number of FPS and the larger frame size will affect the process of extracting frames and making embedded videos, thus making the file insertion time longer.

B. Testing the Process of Extracting Files From Embedded Video

This test determines the smooth process of extracting files from embedded video. This test has a frame extraction process and file data decryption. The frame extraction process takes the frames contained in the embedded video and then checks each frame to determine whether there is a secret data file in it. If the data file is found, the data will be decrypted using Fernet; after successfully decrypting, the data will be made into a file according to the extension.

TABLE 2. FILE EXTRACTING TEST RESULT

No.	Embedded Video Name	Embedded Video Size	Extraction File Name	Extraction File Size	Average Extraction Time	Success or Failed
1	Embedded_Video_cat144p.mp4	45.933 KB	extracted_data.docx	20 KB	4,493	Success
2	Embedded_Video_cat144p1.mp4	45.927 KB	extracted_data.pdf	13 KB	4,354	Success
3	Embedded_Video_cat360p.mp4	209.286 KB	extracted_data1.docx	20 KB	11,451	Success
4	Embedded_Video_cat360p1.mp4	209.378 KB	extracted_data2.docx	112 KB	11,579	Success
5	Embedded_Video_cat360p2.mp4	209.279 KB	extracted_data1.pdf	13 KB	11,136	Success
6	Embedded_Video_cat360p3.mp4	209.370 KB	extracted_data2.pdf	105 KB	11,628	Success
7	Embedded_Video_cat720p.mp4	585.612 KB	extracted_data3.docx	20 KB	29,080	Success
8	Embedded_Video_cat720p1.mp4	585.729 KB	extracted_data4.docx	112 KB	27,376	Success
9	Embedded_Video_cat720p2.mp4	586.060 KB	extracted_data5.docx	379 KB	28,752	Success
10	Embedded_Video_cat720p3.mp4	585.604 KB	extracted_data3.pdf	13 KB	26,928	Success
11	Embedded_Video_cat720p4.mp4	585.720 KB	extracted_data4.pdf	105 KB	30,145	Success
12	Embedded_Video_cat720p5.mp4	586.024 KB	extracted_data5.pdf	350 KB	29,816	Success
13	Embedded_Video_cam2bit.mp4	28.162 KB	extracted_data6.docx	112 KB	3,130	Success
14	Embedded_Video_cam4bit.mp4	28.131 KB	extracted_data7.docx		3,097	Success
15	Embedded_Video_cam6bit.mp4	28.110 KB	extracted_data8.docx		3,135	Success

Based on Table 2. above, it can be seen that the file extraction process from all embedded videos was successfully carried out. All files inserted in both "docx" and "pdf" formats have been successfully extracted into a complete file. Files on insertion with different bits were also recovered. File extraction speed is affected by FPS; the higher the quality of a video, the longer the file hiding time will be.

C. Visual Attack Test

Visual attack testing is a test that is carried out by looking for visible differences in the embedded video with the naked eye. If a difference is visible to the naked eye when the embedded video is played, then it indicates that the frame inserted by the message is not of decent quality. Because the purpose of steganography is to keep the data secret so that others do not readily know it, the results of this study can be seen in the Fig 7 and 8.

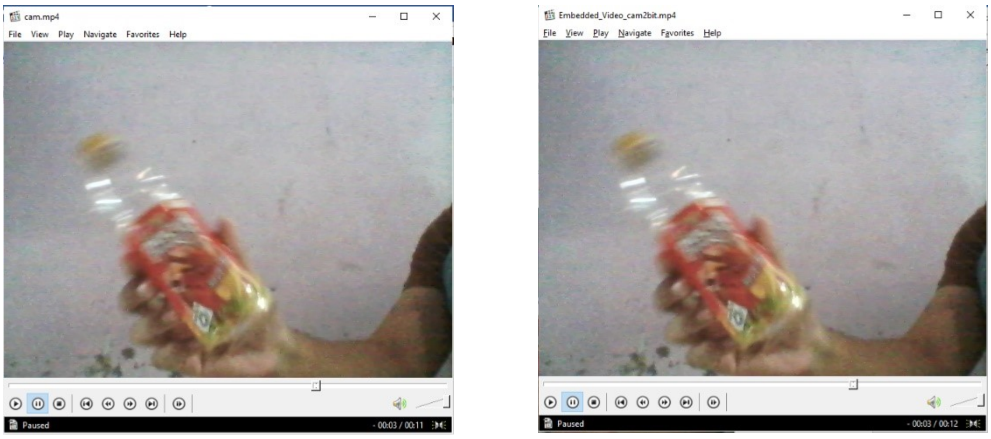
cam.mp4
File View Play Navigate Favorites Help
Paused
00:03 / 00:11
Embedded_Video_cam2bit.mp4
File View Play Navigate Favorites Help
Paused
00:03 / 00:12

Fig. 7. Before & after video 2bit embedded video footage at 8th seconds

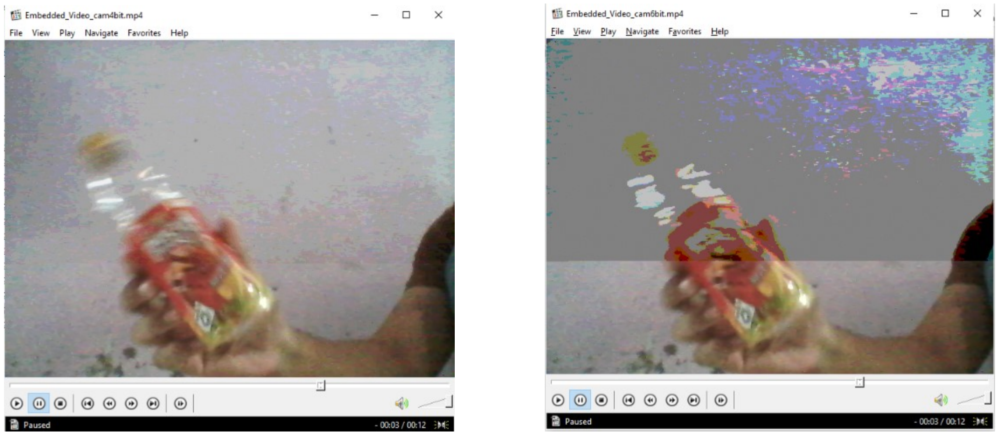
Embedded_Video_cam4bit.mp4
File View Play Navigate Favorites Help
Paused
00:03 / 00:12
Embedded_Video_cam6bit.mp4
File View Play Navigate Favorites Help
Paused
00:03 / 00:12

Fig. 8. Before & after video 6bit embedded video footage at 8th seconds

Based on the results above, it can be concluded that the frame inserted by the file at 2 bits of data does not show any visible difference compared to the hidden file at 4 bits and 6 bits of data. Therefore, in this video steganography application, 2 bits of data are used in hiding files.

D. Peak Signal Noise Ratio (PSNR) Test

PSNR testing is carried out to determine the difference in the quality of the frame, which is the object of hiding the secret file after the process is carried out. If the resulting PSNR value is more than 30 decibels (> 30 dB), then the image quality after hiding can be said to be good, whereas if the PSNR value is less than 30 decibels (< 30 dB), then the image quality can be said to be poor [28].

TABLE 3. PSNR VALUE TEST RESULTS

No.	Original Video Name	File Name	File Size	Order Of Frames (.png)	Frame Size Before Hiding	Frame Size After Hiding	PSNR Value(dB)
1.	144p. mp4	*file*. docx	20 KB	101	67,8 KB	92,7 KB	44,661
2.		*file*. Pdf	13 KB			83,9 KB	46,471
3.	360p. mp4	*file*. docx	20 KB	235	315 KB	351 KB	52,623
4.		*file*1. docx	112 KB			517 KB	44,984
5.		*file*. pdf	13 KB			339 KB	54,478
6.		*file*1. pdf	105 KB			504 KB	45,301
7.	720. mp4	*file*. docx	20 KB	237	907 KB	952 KB	58,751
8.		*file*1. docx	112 KB			1.169 KB	51,016
9.		*file*2. docx	379 KB			1.774 KB	45,732
10.		*file*. pdf	13 KB			938 KB	60,607
11.		*file*1. pdf	105 KB			1.150 KB	51,329
12.		*file*2. pdf	350 KB			1.710 KB	46,080

Based on table 3. above, it can be concluded that the frame inserted in the data file changes significantly in size. If the inserted file is getting more significant (up to the specified frame size limit), then the frame inserted by the file will be more oversized. This is inversely proportional to the resulting PSNR value. The larger the file inserted into the frame, the smaller the PSNR value will be. A smaller PSNR value indicates a decrease in the resulting image quality.

In this study, the frame inserted by the file can still be categorized as decent quality because the resulting PSNR value is above 30 dB. However, when inserting files into different bit frames (2 bits, 4 bits, and 6 bits), apart from changing the size, there is also a decrease in frame quality which can be seen from the smaller PSNR value. Based on Table 3, it can be seen that the insertion of a 2-bit frame produces a larger frame size than the insertion of a 4-bit and 6-bit frame. Insertion of 4-bit and 6-bit frames results in a smaller frame size than the original. So it can be concluded that the insertion of files in 4-bit and 6-bit frames is not recommended because the quality of the resulting frame is not feasible to use.

E. Audio Comparison Test

In this study, the audio Bit Rate value and the audio Sample Rate value in the embedded video are the same as the original audio. Therefore, it can be concluded that the audio quality of the embedded video does not change even though the video has been regenerated through frames, one of which contains a secret data file. So in this insertion, the audio quality is maintained, and the audio playback timing follows the original video.

F. Comparison Of The Original File With The Extracted File

Based on the tests that have been carried out, the original file with the extracted file has the same contents, the exact details, and also the same size. So it can be concluded that every file inserted into the video can be entirely recovered without any difference. The following is a table and some pictures that contain a comparison between the original file and the extracted file, all files used in this study can be hidden in the video.

TABLE 4. FILE EXTRACTING TEST RESULT

No.	Original File Name	Original File Size	Extraction File Name	Extraction File Size
1.	*file*.docx	20 KB	*extracted*_data3.docx	20 KB
2.	*file*1.docx	112 KB	*extracted*_data4.docx	112 KB
3.	*file*2.docx	379 KB	*extracted*_data5.docx	379 KB
4.	*file*.pdf	13 KB	*extracted*_data3.pdf	13 KB
5.	*file*1.pdf	105 KB	*extracted*_data4.pdf	105 KB
6.	*file*2.pdf	350 KB	*extracted*_data5.pdf	350 KB

Based on Table 4 above, it can be concluded that the size of the file that has been hidden into the video and then extracted again, both files in .docx or .pdf formats have the same size as the original file without any changes.

IV. CONCLUSSION

The results found that the embedded video's size was huge due to the .png format and the process of merging frames into video without encoding. The use of encoding during video creation will lead to the loss of file data that has been inserted. Files extracted from embedded videos have not changed, either in the content or in size. Factors that affect embedded video size are the frame format, video quality, Frame Per Second (FPS), file size, and data bits used for file insertion. Hiding files at 2 bits of data results in better frame quality, and there is no visible difference with the original frame, compared to inserting files at 4 bits of data and 6 bits of data which produces steganography frames with noise that is visible to the naked eye. Hiding files at 2 bits of data results in better frame quality, no visible difference with the original frame, and has a PSNR value between 40 dB to 61 dB so that it can be categorized as a decent frame. Hiding files at 4 bits of data and 6 bits of data produces steganography frames with visible noise and have a PSNR value below 40 dB, so it is not feasible to use.

REFERENCES

[1] N. Roztocki, P. Soja, and H. R. Weistroffer, “The role of information and communication technologies in socioeconomic development: towards a multi-dimensional framework*,” *Information Technology for Development*, vol. 25, no. 2. 2019, pp.171–183.

[2] M. A. Ruben, M. D. Stosic, J. Correale, and D. Blanch-Hartigan, “Is Technology Enhancing or Hindering Interpersonal Communication? A Framework and Preliminary Results to Examine the Relationship Between Technology Use and Nonverbal Decoding Skill,” *Front Psychol*, vol. 11, 2021, pp.1-10.

[3] J. Li *et al.*, “Semantic multi-agent system to assist business integration: An application on supplier selection for shipbuilding yards,” *Comput Ind*, vol. 96, 2018, pp.10-26.

[4] [illegible] Rauh, “Secret sharing and shared information,” *Entropy*, vol. 19, no. 11, 2017, pp.2-12.

[5] N. Sohrabi Safa, R. von Solms, and S. Furnell, “Information security policy compliance model in organizations,” *Comput Secur*, vol. 56, pp. 70–82, Feb. 2016, pp.70-82.

[6] “Steganographic Method of Data Hiding using JPEG Images,” *International Journal of Science and Research (IJSR)*, vol. 4, no. 11, pp. 1175–1178, Nov. 2015, doi: 10.21275/v4i11.nov151370.

[7] S. Basuki and R. Anugrah, “Transaction Document Security Protection In The Form Of Image File, Jpg or Tif Interbank Transfer Using Steganography And Cryptography,” *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 1, no. 1, 2021, pp.[illegible]48.

[8] . K., “Image Security using Steganography and Cryptography,” *Int J Res Appl Sci Eng Technol*, vol. 9, no. VII, 2021, pp.366-371.

[9] V. Varuikhin and A. Levina, “Continuous Wavelet Transform Applications in Steganography,” in *Procedia Computer Science*, 2021, vol. 186, pp. 580–587. doi: 10.1016/j.procs.2021.04.179.

[10] A. H. S. Saad, M. S. Mohamed, and E. H. Hafez, “Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning,” *IEEE Access*, vol. 9, 2021, pp.16522-16531.

[11] F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, “A new lightweight cryptographic algorithm for enhancing data security in cloud computing,” *Global Transitions Proceedings*, vol. 2, no. 1, pp. 91–99, 2021, doi: 10.1016/j.gltp.2021.01.013.

[12] V. B. Kirubanad and M. Kumari, “Data encryption and decryption using graph plotting,” *International Journal of Civil Engineering and Technology*, vol. 9, no. 2, 2018, pp.36-46.

[13] N. M. Zamri, S. M. H. Asraf, and S. Z. S. Idrus, “Two Level Security in Delivering Message Using Encryption and Steganography Techniques,” in *Journal of Physics: Conference Series*, 2020, vol. 1529, no. 3. pp.1-9.

[14] Win junaidi, “Algoritma Hill Cipher untuk Enkripsi Data Teks yang digunakan untuk Steganografi gambar dengan Metode LSB (Least Significant Bit),” *Pelita Informatika Budi Darma*, vol. 9, no. 3, 2015. pp.92-99.

[15] W. Junaidi, “ALGORITMA HILL CHIPER UNTUK ENKRIPSI DATA TEKS YANG DIGUNAKAN UNTUK STEGANOGRAFI GAMBAR DENGAN METODE LSB (LEAST SIGNIFICANT BIT),” *Pelita Informatika Budi Darma*, no. 3, 2015. pp.92-99.

[16] D. Laoli, B. Sinaga, and A. S. R. M. Sinaga, “Penerapan Algoritma Hill Cipher Dan Least Significant Bit (LSB) Untuk Pengamanan Pesan Pada Citra Digital,” *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 4, no. 3, 2020, pp.138-148.

[17] S. G. Supratman, “STEGANOGRAFI DENGAN MENGGUNAKAN METODE LSB DAN ALGORITMA HILL CIPHER,” *Buffer Informatika*, vol. 1, no. 1, 2017, pp.38-48.

[18] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, “Hiding data using efficient combination of RSA cryptography, and compression steganography techniques,” *IEEE Access*, vol. 9, 2021, pp.31805-31815

[19] M. Kaur and A. Kaur, “Improved Security Mechanism of Text in Video using Steganographic Technique: A Review,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7782, no. 5, 2014. Pp.44-51.

[20] K. Vyas and B. L. Pal, “a Proposed Method in Image Steganography To Improve Image Quality With Lsb Technique,” *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 1, 2014. pp.5246-5251.

[21] T. Barhoom and W. Saqer, “Steganography algorithm within 2-LSBs with indicators-based randomness,” *International Journal of Computing and Digital Systems*, vol. 6, no. 5, 2017, pp.272.276.

[22] D. Rawat and V. Bhandari, “A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image,” *Int J Comput Appl*, vol. 64, no. 20, 2013, pp.1-4.

[23] S. Tripathi, R. K. Tiwari, R. Nigam, N. K. Gupta, and B. Verma, “The hybrid cryptography for enhancing the data security in fog computing,” in *Proceedings - 2021 IEEE 10th International Conference on Communication Systems and Network Technologies, CSNT 2021*, 2021. pp. 766-771.

[24] Pronika and S. S. Tyagi, “Enhancing security of cloud data through encryption with AES and fernet algorithm through Convolutional-Neural-Networks (CNN),” *International Journal of Computer Networks and Applications*, vol. 8, no. 4, 2021, pp.288-299.

[25] D. P., S. S. Babu, and Y. Vijayalakshmi, “Enhancement of e-commerce security through asymmetric key algorithm,” *Comput Commun*, vol. 153, 2020, pp.125-134.

[26] E. J. Baker *et al.*, “Video steganography using 3D distance calculator based on YCbCr color components,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 24, no. 2, 2021, doi: 10.11591/ijeecs.v24.i2.pp831-842.

[27] J. Vivek and B. Gadgay, “Video Steganography Using Chaos Encryption Algorithm with High Efficiency Video Coding for Data Hiding,” *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 5, 2021, pp.15-24.

[28] R. L. Oxford and C. Y. Lin, “Autonomous learners in digital realms: Exploring strategies for effective digital language learning,” in *Independent Language Learning: Building on Experience, Seeking New Perspectives*, Hong Kong University Press, 2011. pp.157-172.

[29] Hemanth, *Intelligent Data Analysis for Biomedical Applications*. Elsevier, 2019.

● 11% Overall Similarity

Top sources found in the following databases:

- 7% Internet database
- Crossref database
- 5% Submitted Works database
- 6% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	ejournal.raharja.ac.id Internet	2%
2	semanticscholar.org Internet	1%
3	"Program Schedule", 2022 IEEE International Conference on Communic... Crossref	<1%
4	dergipark.org.tr Internet	<1%
5	I Wayan Mustika, Fauza Khair, Anggun Fitrian Isnawati, Annisa Nur Aini... Crossref	<1%
6	tnsroindia.org.in Internet	<1%
7	ijitee.org Internet	<1%
8	CSU Office of the Chancellor on 2022-04-26 Submitted works	<1%

9	Amrita Vishwa Vidyapeetham on 2022-06-29 Submitted works	<1%
10	link.springer.com Internet	<1%
11	ijcaonline.org Internet	<1%
12	Edge Hill University on 2019-03-26 Submitted works	<1%
13	Islamic University of Gaza on 2019-03-02 Submitted works	<1%
14	researchgate.net Internet	<1%
15	ABV-Indian Institute of Information Technology and Management Gwal... Submitted works	<1%
16	De Rosal Ignatius Moses Setiadi, Supriadi Rustad, Pulung Nurtantio An... Crossref	<1%
17	Napier University on 2017-04-23 Submitted works	<1%
18	Elly Matul Imah, Ivan Kurnia Laksono, Karisma Karisma, Atik Wintarti. "... Crossref	<1%
19	Khalid A. Al-Afandy, Osama S. Faragallah, Ahmed Elmhalawy, El-Sayed ... Crossref	<1%
20	Methaq Talib Gaata, Mustafa Dhiaa Al-Hassani. "Underwater image co... Crossref	<1%

21	**Universiti Tenaga Nasional on 2021-05-10** Submitted works	<1%
22	**University of Stirling on 2022-01-14** Submitted works	<1%
23	**ijece.iaescore.com** Internet	<1%
24	**Aditya Kotkar, Shreyas Khadapkar, Aniket Gupta, Smita Jangale. "Multi...** Crossref	<1%
25	**Coventry University on 2022-08-12** Submitted works	<1%
26	**Mustafa Munther Mashkour, Lahieb Mohammed Jawad. "Compressed ...** Crossref	<1%
27	**University Tun Hussein Onn Malaysia on 2017-06-06** Submitted works	<1%
28	**University of Durham on 2019-09-05** Submitted works	<1%
29	**Xue-Hang Qian, Guang-Bao Xu, Hua-Kun Wang, Dong-Huan Jiang. "Thr...** Crossref	<1%
30	**scholar.archive.org** Internet	<1%
31	**neliti.com** Internet	<1%
32	**"Proceedings of International Conference on Communication and Netw...** Crossref	<1%

33	emerald.com Internet	<1%

● Excluded from Similarity Report

- Manually excluded sources
- Manually excluded text blocks

EXCLUDED SOURCES

Tufail Akhmad Satrio, Wahyu Adi Prabowo, Trihastuti Yuniati. "Hiding Docume... 78%

Crossref

EXCLUDED TEXT BLOCKS

2022 IEEE International Conference on Communication, Networks and Satellite (C...

I Wayan Mustika, Fauza Khair, Anggun Fitrian Isnawati, Annisa Nur Aini Maryadi, Dwi Edi Setyawan, Arrizky A...

Hiding Document Format Files Using VideoSteganography Techniques With Least ...

www.semanticscholar.org

EngineeringInstitut Teknologi Telkom PurwokertoPurwokerto, Indonesia

Ghina Fahira, Alfin Hikmaturokhman, Achamd Rizal Danisya. "5G NR Planning at mmWave Frequency : Study...

EngineeringInstitut Teknologi Telkom PurwokertoPurwokerto, Indonesia

I Wayan Mustika, Fauza Khair, Anggun Fitrian Isnawati, Annisa Nur Aini Maryadi, Dwi Edi Setyawan, Arrizky A...

2022 IEEE International Conference on Communication, Networks and Satellite (C...

I Wayan Mustika, Fauza Khair, Anggun Fitrian Isnawati, Annisa Nur Aini Maryadi, Dwi Edi Setyawan, Arrizky A...

2022 IEEE International Conference on Communication, Networks and Satellite (C...

I Wayan Mustika, Fauza Khair, Anggun Fitrian Isnawati, Annisa Nur Aini Maryadi, Dwi Edi Setyawan, Arrizky A...

Algoritma Hill

widuri.raharja.info

ALGORITMA HILL CHIPER UNTUK ENKRIPSIDATA TEKS YANG DIGUNAKAN UNTU...

widuri.raharja.info

REFERENCES[1]N. Roztocki, P. Soja, and H. R. Weistroffer, “The role of information...

Niranjan Rao Deevela, Farheen Chishti, Bhim Singh, Tara C. Kandpal. "NGK-LMS Control for Grid Connected ...

M. A. Ruben, M. D. Stosic, J. Correale, and D. Blanch-Hartigan, “IsTechnology Enha...

lersse-dl.ece.ubc.ca

J. Li et al., “Semantic multi-agent system to assist businessintegration: An applica...

ijstr.org

N. Sohrabi Safa, R. von Solms, and S. Furnell, “Information securitypolicy complian...

pdfs.semanticscholar.org

Basuki and R. Anugrah, “Transaction Document SecurityProtection In The Form Of ...

media.neliti.com

V. Varuikhin and A. Levina, “Continuous Wavelet TransformApplications in Stegan...

journal.unipdu.ac.id

A. H. S. Saad, M. S. Mohamed, and E. H. Hafez, “Coverless ImageSteganography B...

Lalit Negi, Lokesh Negi. "Hybrid approach for Data Security using Coverless Image Steganography with AES"...

11]F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap,“A new lightw...

downloads.hindawi.com

N. M

University of Northumbria at Newcastle on 2021-01-04

B. Sinaga, and A. S. R. M. Sinaga, “Penerapan AlgoritmaHill Cipher Dan Least Signi...

ejournal.uin-suka.ac.id

STEGANOGRAFI DENGAN MENGGUNAKANMETODE LSB DAN ALGORITMA HILL C...

Yati Nurhayati, Siti Maesyaroh, Sherly Gina Supartman, Erlan Darmawan, Elin Herlina. "Implementation of the...

18]O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed,“Hiding data u...

Estabraq Hussein Jasim Halboos, Abbas M. Albakry. "Improve steganography system using agents softwar...

Kaur, “Improved Security Mechanism of Text inVideo using Steganographic Techni...

www.ijaerd.com

Vyas and B. L. Pal, “a Proposed Method in Image SteganographyTo Improve Image...

www.jatit.org

Tyagi, “Enhancing security of cloud data throughencryption with AES and fernet al...

ijettjournal.org

E. J. Baker et al., “Video steganography using 3D distance calculatorbased on YCb...

Methaq Talib Gaata, Mustafa Dhiaa Al-Hassani. "Underwater image copyright protection using robust water...

J. Vivek and B. Gadgay, “Video Steganography Using ChaosEncryption Algorithm ...

inass.org

R. L. Oxford

Cheng, Gary, and Juliana Chau. "Exploring the relationship between students' self-regulated learning ability a...

D. P., S. S. Babu, and Y. Vijayalakshmi, “Enhancement of e-commerce security thro...

Qixin Zhang. "An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption an...