Video Steganography

Harshada Pentewar[1], Akansha Netake[2], Yash Sangekar[3], Swapnil Jaybhaye[4], Prof, S.W.Puranik[5]
[1,2,3,4]Undergrad. Student, Dept. of Information Technology SKN Sinhgad Institute of Technology & Science, Lonavala, Maharashtra
[5]Asst Professor, Dept. of Information Tech, SKN Sinhgad Institute of Technology & Science, Lonavala, Maharashtra

Abstract- *Video Steganography is an extension of image steganography where any kind of file in any extension is hidden into the digital video.*

It is art of hiding secret data in a non-secret digital carrier called cover media.

Data exchange occurs with a variety of purpose, ranging from sharing information or just basic communication between people. Data exchanges that occurs every day make data traffic busier. Data theft is made even easier by utilizing the large number of message sender and the busy data traffic.

One popular method used to secure data is steganography method. In this research, End of File steganography method is successfully implemented in the various types of multimedia, namely image, audio, and video. this method provides the effect of increasing the size then it is advisable to use video because generally, video size is always larger than image size because it contains image and audio in one file at a time.

Keywords- Data Exchange; Steganography; Multimedia; Security

I. INTRODUCTION

As the networking and internet technology is growing, illegal copying and editing of multimedia have become a serious issue today.

Steganography is one of the tool for protecting the confidential data inside a multimedia.

It is the process in which watermark information is embedded into the cover video. Videos are predominantly used for hiding confidential data because of Larger hiding space and Hidden data are indiscernible.

In the recent studies of steganography uses a new method, namely the use of expansion and modulus functions with images as media cover. The image file used is subject to calculation of the difference in pixel values which results in +ve and -ve values. That range is used as cover for hiding secret messages. The results shows increase capacity, compared to previous method.

In this research, End of Video steganography method is the most Important and difficult method of Video Steganography is the implemented in multimedia, namely image, audio, and video. The process is done using variety of secret message sizes, then some evaluations carried out. The results will show the various advantages and disadvantages of each type of multimedia used based on the evaluation of human perception.

A further driver towards the self-authentication is the need of storage and analysis of huge amounts of multimedia data, which has propelled companies towards cloud storage for the efficient access. This paper presents a multifaceted solution to the problem of self-authentication and requirements of data protection regulations in respect to storage. The proposed solution works as follows:

- Captured video data is protected by calculating their hash.
- These hashes are stored inside video frames as hidden information.
- Every frame holds the hash of its previous two frames and, therefore, creates a chain-of-evidence.
- All this data are encrypted and stored on the network edge.
- To further enhance security, encryption keys are stored in a hardware wallet, separately from the device holding the actual video.

II. LITERATURE SERVEY

The research of several video steganography techniques is additions of the image-based steganography techniques. The research founds the various works from the various authors.

In Marwa M. Emam & Abdelmg eid A. Aly & Fatma A. Omara: A improved image of steganography method based on LSB technique with random pixel selection: This paper does use spatial and transform domains to hide secret messages into cover files. (2016)

Anamika Saini, Kamaldeep Joshi and Kirti Sharma proposed a robust video steganography by analysis of LSB technique using PSNR and MSE. They presented a review and analysis of the video steganography technique applied to the AVI (Audio Video Interleaved) file using LSB (Least Significant Bit) technique and the frames are compared and analysed using parameters like PSNR and MSE. The most important of these drawback of this work is LSB (Least Significant Bit) technique is easy to decode and thus it is vulnerable to attacks.

In Sumeet Kaur &Savina Bansal & R. K. Bansal: Steganography and classification of image steganography techniques: This paper analyse the various types of the steganography techniques and main concepts and importance of video steganography methods, algorithms were discussed.

In T. Morkel & J.H.P. Eloff & M.S. Olivier: An overview of image steganography: This paper presents the several steganography algorithms and represents the security potential of steganography concepts and also it fallows many methods, techniques and the concerning applications.

Mehdi Boroumand and Mo Chen proposed their work that deals with Profound Residual Network for Steganalysis of Digital pictures. They planned a profound remaining design to limit the utilization of heuristics and remotely upheld components that are all inclusive as in it gives best in class discovery exactness for both spatialspace and JPEG steganography. Broad tests demonstrate the unrevealed execution of this system with a noteworthy improvement particularly in the JPEG space. (2018)

III. METHODOLOGY

In Video steganography implementation process was successfully carried out using imagery, audio, and video. Various evaluations were carried out to find a comparison of multimedia files before and after the steganography process. In addition, the purpose of the evaluation is find out the comparative advantages between the types of media used (image, audio, and video). Evaluations that done for this research is included changes in size, changes in physical cover file, histogram, and Mean of Score assessment.

3.1 Size Change

After the video steganography process, there is a size change of the media cover that is used both in pictures, audio, and video. The size changes that occur are shown in Table I.

TABLE I. SIZE CHANGE

No	Cover	Cover type	Secret Message Size	Cover size before embedding (byte)	Cover size after embedding (byte)
1	Touch.mp4	Video	10	19813558	19813568
2	Romance.mp4	Video	1000	15338454	15339454
3	Growing.mp4	Video	100000	8570683	670683

Table 1 shows that the change in size follows the number of secret messages added. The greater the secret message added to the file cover, the greater the size changes that occur.

3.2 Physical Changes

In Video Steganography the physical changes to the video are evaluated using a duration benchmark. The results of evaluating the change in the duration of the video cover used are shown in table 4. In table 4 it appears that there is no increase in the duration of the video cover file used. The reason for this is the same as what happened to the image cover file test results, namely the addition of a secret message not accompanied by the addition of frames to the overall structure of the image cover file.

TABLE II. VIDEO COVER’S PHYSYCALLY CHANGED

No	Cover Tittle	Secret Message Size	Duration	
			Before Embedding (seconds)	After Embedding (seconds)
1	Growing.mp4	10	121	121
2		100		121
3		1000		121
4		10000		121
5		100000		121
6	Romance.mp4	10	266	266
7		100		266
8		1000		266
9		10000		266
10		100000		266
11	Touch.mp4	10	212	212
12		100		212
13		1000		212
14		10000		212
15		100000		212

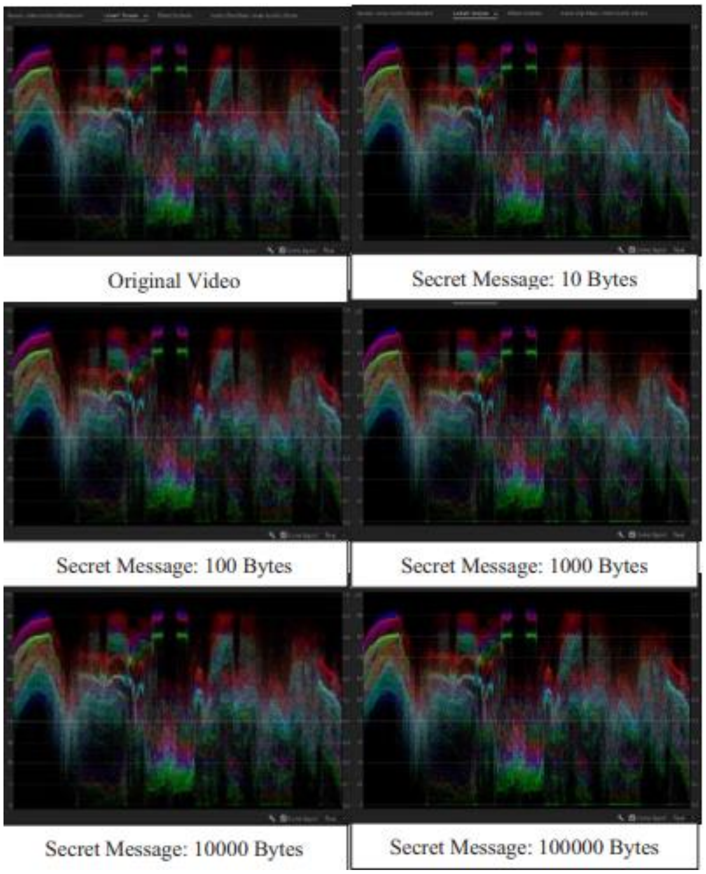
3.3. Histogram

One type of evaluation that can be done to represent the human perception of changes in multimedia cover files used for steganography is a histogram.

Video is a compilation of images made in a certain period or duration [10]. If the histogram image can be displayed with only one graphic, it is different from the histogram on the video. The histogram evaluation of videos are shown in Figure 1.

The number of histogram graphics on a video depends on the number of frames owned by the video which is also affected by the duration of the video itself. Because the video is a collection of images that are made to move continuously, the video histogram is a collection of histograms of the images forming the video itself. In this research, histogram evaluation on video using Adobe Premiere application. Because a video can have an unlimited number of image histograms, this paper only shows a few samples of a video histogram at a predetermined duration.

Some of these samples that shown in Figure 1 where the video used is the same cover file with a variety of secret message sizes. Based on the evaluation results of 30 frame sampling times on 30 video cover files with 5 variations in the number of secret messages, no differences were found in the histogram frequency. Evaluation of the difference in the histogram chart is done by looking at the maximum value, minimum value, and overall graph plot for each sampling.



Original Video

Secret Message: 10 Bytes

Secret Message: 100 Bytes

Secret Message: 1000 Bytes

Secret Message: 10000 Bytes

Secret Message: 100000 Bytes

Fig. 6. Histogram sample on the 30th second from 121 seconds total duration

The quality of the cover file that is used as a cover file for steganography is also evaluated subjectively by test respondents using one technique that is quite popular in the scope of digital signal processing, namely MOS (Mean Opinion Score) [12], using 30 respondents and 30 test files. Respondents were first shown and played the original cover file, then played and displayed the steganography cover file again without being notified of the addition of a secret message and an additional duration of the audio file. Respondent were asked to provide the qualitative rating based on their sensory catches. The qualitative values given are then transformed into quantitative values using the MOS Rate table in table 5. Several samples of respondents' assessment results are presented in Table 3.

TABLE III. Mean Opinion Score Explanation

MOS Value	Opinion Score	Explanation
1	Excellent	The quality of the stego file is much better than the quality of the original file
2	Good	Stego file quality is better than the original file quality
3	Fair	The quality of the stego file is the same as the quality of the original file
4	Poor	Stego file quality is worse than the original file quality
5	Bad	The quality of the stego file is much worse than the quality of the original file

TABLE IV. QUALITATIVE SCORING OF THE RESPONDENTS

Steganography File	Type of File	Size of Secret message	Total of Opinion Score	MOS Value
Woman1.jpeg	image	10	90	3
Woman2.jpeg	Image	100	90	3
Woman3.jpeg	Image	1000	90	3
Woman4.jpeg	Image	10000	90	3
Woman5.jpeg	Image	100000	90	3
Intuisi1.mp3	Audio	10	90	3
Intuisi2.mp3	Audio	100	90	3
Intuisi3.mp3	Audio	1000	90	3
Intuisi4.mp3	Audio	10000	90	3
Intuisi5.mp3	Audio	100000	89	2.967
Growing1.mp4	Video	10	90	3
Growing2.mp4	Video	100	90	3
Growing3.mp4	Video	1000	90	3
Growing4.mp4	Video	10000	90	3
Growing5.mp4	Video	100000	90	3

In table 3, the average respondent assessed that there was no difference in quality between the original cover file and the cover file of the results of steganography. There was only one respondent who assessed that the cover file of the results of steganography had a worse quality than the cover file of the result of steganography, namely the 5.mp3 intuition test file with the number of secret messages of 100000 bytes.

IV. CONCLUSION

The End of File steganography method was successfully implemented in the various types of multimedia, namely image, audio, and video. The trials use the most common formats of each file type, namely JPEG for images, MP3 for audio, and MP4 for video. Various analyses and tests have been carried out after the implementation of steganography, namely changes in size, changes in physical cover files, histograms, and Mean Opinion Score. Of all the tests conducted, audio media experienced the most significant changes. Audio media changes in terms of size and physical changes

MOS value collection test also shows the value of audio media has decreased quality, although not significantly. But the audio media did not change in terms of the histogram. While the image and audio-only change in terms of size, but do not change in terms of histograms and physical changes. The MOS value collection test also showed that the quality of the image and video cover media after cryptographic implementation remained stable. From all of the above reviews, it can be concluded that the most suitable multimedia files to be used as the steganography media for End of File method are the image and video media. However, this method provides the effect of increasing size, so it is advisable to use video because generally, the video size is always larger than image size because it contains the image and audio in one file at a time.

V. REFRENCE

A. Brunetti, D. Buongiorno, G. F. Trotta, and V. Bevilacqua, “Computer vision and the deep learning techniques for the pedestrian detection and tracking: A survey,” Neurocomputing, vol. 300, pp. 17–33, 2018.

Y.-H. Chen and V. Sze, “A deeply pipelined CABAC decoder for HEVC supporting level 6.2 the high-tier applications,” IEEE Trans. Circuits System.Video Technol., vol. 25, no. 5, pp. 856–868, May 2015.

K. Sitara and B M. Mehtre, “Digital video tampering the detection: An overview of the passive technique,” Digital Investigation, vol. 18, pp. 8–22, 2016.

R. Zhang, V. Sachnev, M. B. Botnan, H. Joong Kim, and J. Heo, “An efficient embedder for BCH coding for steganography,” IEEE Trans. Inf. Theory, vol. 58, no. 12, pp. 7272–7279, Dec. 2012.

Krishnaveni, N. (2018). IMAGE STEGANOGRAPHY USING LSB EMBEDDING WITH CHAOS. International Journal of Pure and Applied Mathematics, 118(8), 505-509.

Ramadhan J. Mstafa and Khaled M. Elleithy & Eman Abdelfattah (2017). “Video Steganography Technique: Taxonomy, Challenge and Future Directions. 2017 IEEE

H.-C. Huang and F.-C. Chang, “Hierarchy-based reversible data hiding,” Expert Systems with the Applications, vol. 40, no. 1, pp. 34–43, Jan. 2013, doi: 10.1016/j.eswa.2012.07.010.

S. Imaculate Rosaline and M. Ashok Raj, “Adaptive Pixel Pair Matching Based Steganography for Audio Files,” in 2013 International Conference on Emerging Trends in the Vlsi, Embedded System, Nano Electronics and Telecommunication System (Icevent), 2013, Pp. 1–5.

A. K. Singh, M. Dave, and A. Mohan, “Hybrid technique for robust and imperceptible multiple watermarking using the medical images,” Multimedia Tools Appl., vol. 75, no. 14, pp. 8381–8401, Jul. 2016.

P.-C. Chang, K.-L. Chung, J.-J. Chen, C.-H. Lin, and T.-J. Lin, “An error propagation free data hiding algorithm in HEVC intra-coded frames,” in Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf.,Kaohsiung, Taiwan, Oct./Nov. 2013, pp. 1–9.

Jessica Fridrich, Holub and Vojtech. “Designing the video steganography distortion using the directional filters.” In the Information Forensics and Security (WIFS), 2012 IEEE International Workshop on, pp. 234-239. IEEE, 2012.

Z. Qian, X. Zhang, and S. Wang, “Reversible data hiding in encrypted JPEG bitstream,” IEEE Trans. Multimedia, vol. 16, no. 5, pp. 1486–1491, Aug. 2014.

I. J. Kadhim, P. Premaratne, and P. J. Vial, “High Capacity of Adaptive Image Steganography with Cover Region Selection using Dual-Tree Complex Wavelet Transform,” Cogn. Syst. Res., 2019.

Karanjit Kaur & Baldip Kaur (2018). “DWT-LSB Approach for the Video Steganography using Artificial Neural Network”. In International Advanced Research Journal in the Science, Engineering and Technology, IARJSET.