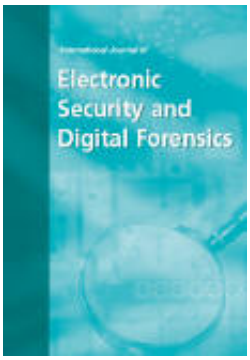


International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

Data hiding using video steganography

C. Ravichandran, Ashok Vajravelu, Sankarsan Panda, Sheshang Dipakkumar Degadwala

DOI: 10.1504/IJESDF.2024.10052934

Article History:
Received: 09 July 2022
Accepted: 05 October 2022
Published online: 12 January 2024

Data hiding using video steganography

C. Ravichandran*

Department of Electronics and Communication Engineering,
GRT Institute of Engineering and Technology,
Tiruttani, Tamilnadu, India
Email: ravisarvajith@gmail.com
*Corresponding author

Ashok Vajravelu

Department of Electronics,
Faculty of Electrical Engineering,
Universiti Tun Hussein Onn Malaysia,
Johor, Malaysia
Email: ashokvajravelu8@gmail.com

Sankarsan Panda

Department of Computer Science,
Acharya Shri Mahapagya Institute of Excellence,
Asind, Bhilwara(Raj.), India
Email: pandasankarsanasind@gmail.com

Sheshang Dipakkumar Degadwala

Department of Computer and Science Engineering,
Sigma Institute of Engineering,
Vadodara, Gujarat, India
Email: sheshang13@gmail.com

Abstract: Video steganography aims to hide the presence of a communication from a hostile third party. One of the techniques recommended in this study is the hash-based least significant bit method for video steganography. The study conducts an in-depth analysis of the numerous enhancements that have been made to the safety of data transmission, as well as the several methods that have been adapted in order to accomplish the same goal. The results of the MATLAB simulation show that the proposed method is superior to other state-of-the-art methods that are currently in use. According to the findings of the comparison, the data-hiding method that has been proposed provides increased safety and reduces distortions for improved video quality. The results of our experiments suggest that our algorithm offers a high level of protection while having just a minimal effect on video quality.

Keywords: cover video; steganography; LSB technique; watermarking; AES; peak signal-to-noise; intra-prediction mode; integer wavelet transform; temporal correlation.

Reference to this paper should be made as follows: Ravichandran, C., Vajravelu, A., Panda, S. and Degadwala, S.D. (2024) 'Data hiding using video steganography', *Int. J. Electronic Security and Digital Forensics*, Vol. 16, No. 1, pp.112–123.

Biographical notes: C. Ravichandran has been working in the Department of Electronics and Communication Engineering at GRT Institute of Engineering and Technology, Tiruttani TamilNadu (India), since 2021. He has a PhD (Video Compression) degree from the Anna University-Chennai (T.N) India; PG course explored ME (Applied Electronics) from the Sathyabama Deemed University – Chennai (T.N) India, and he studied BE (E.C.E) at the Mepco Schlenk Engineering College, Sivakasi (T.N) India. His area of interest is image processing, and he has teaching experience of around 22 years of in both UG and PG courses. He attended 25 workshops and seminars, three patents, publications, and published seven papers in international journals. He organised five workshops and three national-level conferences. He has published *Microwave Component and Circuit Book* in the regional level. He is a life member of ISTE and member of IETE.

Ashok Vajravelu is currently working as a Senior Lecturer in the Department of Electronics, Faculty of Electrical Engineering, Universiti Tun Hussein Onn Malaysia. He received his BE in Electronics and Communication Engineering from the Bharathiar University, India, in 2002 and ME in Process Control and Instrumentation Engineering from the Annamalai University, India, in 2005.He completed his PhD degree from the Anna University, India in 2013 and his area of interest are biomedical signal processing like blood flow, EEG, embedded system design, and neural networks.

Sankarsan Panda is an Associate Professor at the Acharya Shri Mahapragya Institute of Excellence at Asind and received his PhD from the Sangam University, Bhilwara in Computer Science and Engineering. He is awarded M.C.A. from the Jaipur National University, Jaipur and BTech (CS) from the JRN Rajasthan Vidyapeeth University, Udaipur. He had attended international and national conferences, seminars, workshops, webinars and FDP. He has published four research papers in some reputed journal such as UGC Care, Scopus and IEEE. He is keenly interested in artificial intelligence and machine learning, coding and teaching. He is astonished and influenced from the power of computing. His goal is to combine diverse range of experiences with the ability to be an innovative academician and administrator who will contribute favourably to the concerned institute, society and research communities as well as be caring, energetic, intellectual and creative.

Sheshang Dipakkumar Degadwala is presently working as an Associate Professor and the Head of Computer Engineering Department, Sigma Institute of Engineering, Vadodara. He obtained his BE degree from the Department of Computer Engineering, BITs, Vadodara. Subsequently, he obtained his MTech degree from the Charusat University, Changa and completed his PhD in Computer Engineering from the Madhav University, Abu Road, Sirohi, Rajasthan, India in 2018. He has published 179 research papers in reputed international journals and conferences including IEEE, Elsevier and Springer. His main research work focuses on image processing, computer vision, information security, theory of computation and data mining. He is also a Microsoft Certified in Python Programming and Excel. He has published 18 books and received grant for one patent. He has published 38 Indian patents. He has received 45 awards for academic and research achievement.

1 Introduction

The term 'steganography' originates from the Greek words 'steganos,' which means 'covered', and 'graphia', which means 'writing', respectively. Together, these words form the word 'steganography'. Because of the widespread use of the internet and digital media in today's society, there is a pressing need to improve the safety of data transmission in order to protect sensitive information from falling into the wrong hands. The purpose of steganalysis is to break steganography systems, and this requirement is met if an algorithm can determine whether or not a particular image includes a hidden message. In order to lessen the likelihood of being attacked, it is necessary to keep security a secret, often known as invisible security. There are two distinct types of steganography

1 Linguistic steganography.

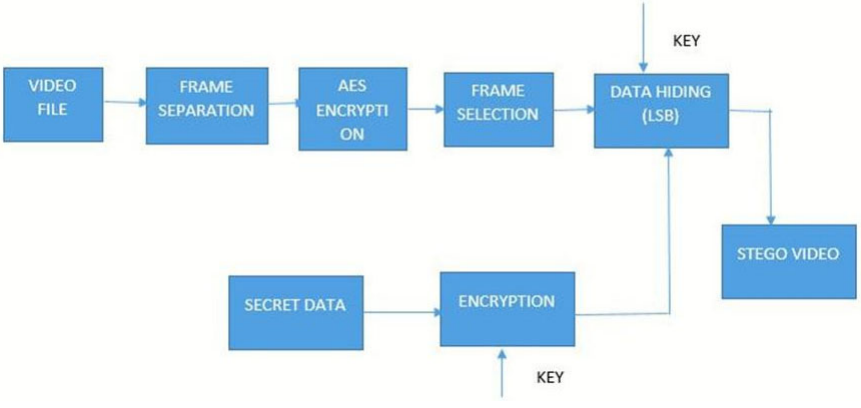
2 One method that is utilised in the data transfer that accomplishes a greater level of confidentiality is known as technical steganography, which also includes watermarking.

The watermarking can be broken down into two distinct categories, which are:

1 Robust

2 Thus the block diagram of steganography both in the embedding as well as the extraction side is as given in Figure 1.

Figure 1 Embedding (see online version for colours)

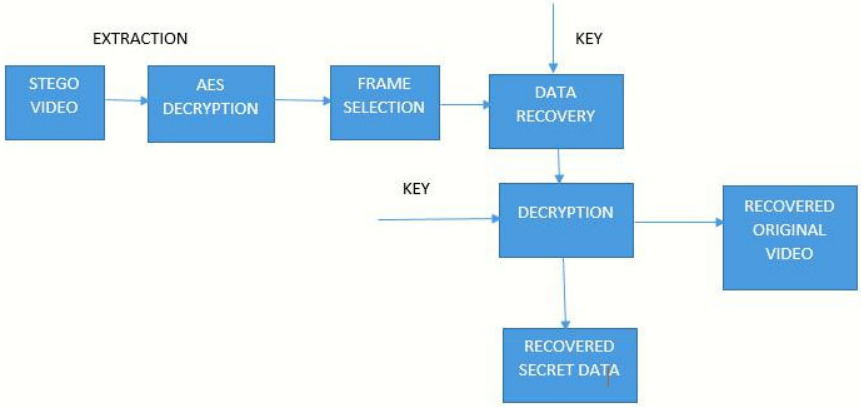


When compared with images and texts, video has a greater number of elements that can be extracted to hide confidential information. The characteristics of the frame pictures, the characteristics of the temporal changes across frames, and the characteristics of the audio are some of these characteristics. In light of this, vulnerable steganography relying on the video is ineffective and require the transmission of an excessively high number of carriers even when additional bits of confidential information need to be concealed, as illustrated in Figure 2.

In order to solve this issue, some information that is not apparent to the naked eye can be encoded within the digital medium in such a way that it cannot be easily recovered

unless a specific method is used (Hrytskiv et al., 1998). These algorithms have the property of being resistant to hacking, but they are not very good at hiding data (Kavitha et al., 2012). Research on information embedding, particularly information hiding techniques, has garnered a significant amount of interest over the course of the past several years due to the fact that it may have potential applications in the fields of multimedia and information security (Shanableh, 2012). The idea of the statistical minimum residual, which lies in comparison to the sub-optimal sum of absolute transformed difference (SATD) and the ideal SATD serves as the foundation for the cost allocation approach, proposed in this article.

Figure 2 Extraction (see online version for colours)



The Syndrome-Trellis code (STC) is then applied to the IPMs that have been deemed qualified for modification. The results of the experiments reveal that this method performs well when competing against the steganalysis algorithm. Nie et al. (2018) suggested an effective adaptive video steganography founded on the intra-prediction mode. In this study, integer wavelet transformations are utilised to take advantage of the spatial and temporal correlation between the video frames in order to decrease, depending on the type of transform, the embedding distortion (1-D, 2-D, or 3-D). Because the suggested approach achieves a bit error rate (BER) of zero when comparing the original data to the recovered data, it is able to embed data such as text, images, or sounds within video frames.

2 Literature survey

In the body of steganographic research, a variety of different approaches have been presented. Because the video file conceals a significant quantity of sensitive data, it is more valuable. The implementation of a protected hash-based LSB approach for image steganography has taken place (Kumar and Sharma, 2013). In this section, we will explain the fundamental requirements for hiding data in a cover file according to Rabah (2004). The art of concealing data within an audio file, video file, or image file is known as steganography. The use of steganography as a method for maintaining the data's confidentiality is an efficient strategy. The method of data hiding for high resolution

video that was proposed by Bhaumik et al. (2009) is described here. It ensures that the data is protected appropriately while it is being transmitted. Paulpandi and Meyyappan (2012) present an introduction to the concept of data obfuscation through the use of the motion vector approach for moving objects.

In order to determine whether or not digital photos are genuine, a number of different forensic techniques have been created. In this paper, a set of digital image forensic techniques is proposed for detecting global and local contrast enhancement, identifying the use of histogram equalisation, and detecting the global addition of noise to a JPEG compressed image. These techniques can be used to determine whether or not an image has been altered. Data concealment was accomplished in this study by Po-Yueh and Hung (2006) by instead of the spatial domain, studying in the frequency response. The frequency-domain approach that was proposed in Po-Yueh and Hung (2006) involved the embedding of secret messages into DWT coefficients with high frequency. To enhance quality, the DWT parameters in the reduced subbands were not altered. Prior to the secret message being implanted, some basic mathematical operations were carried out on it.

This primary objective of steganography is to provide for secure communication that is fully undetected (Chandramouli and Memon, 2001), and to prevent the transmission of hidden data from arousing suspicion. It is not to prevent others from discovering the concealed knowledge; rather, it is to prevent people from ever considering the possibility that the information could possibly exist. If someone becomes suspicious that there is confidential information included within a carrier medium as a result of using a steganography method, then the method is considered to be unsuccessful according to Artz (2001). This treatment's goal was to show a histogram that was more tightly packed. This, in turn, may have increased the heights of peak points, which would have enhanced the effectiveness of histogram-based techniques. A new plan was developed by Yang et al. which included Yang and Tsai (2010).

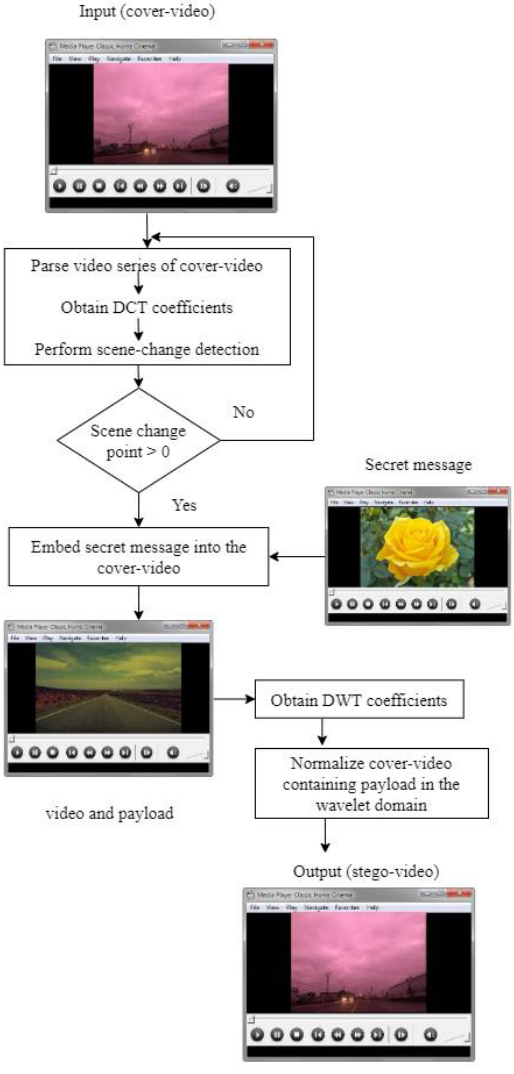
3 Methodology

In wavelet domains, concealing capacity and perceptual transparency can both be improved by the application of a variety of approaches that make use of wavelet coefficients. Ali and Fawzi (2010) used a wavelet transform to expand a steganographic system's capabilities and achieve the highest level of anonymity. This was done by hiding the data in the cover image's this double discrete wavelet transform (DWT) domain. Despite having reached acceptable levels of imperceptibility and visual distortion, the method involves a significant amount of processing overhead. Alternatively, a statistics method for H.264 video streams utilising scene-change detecting was given in Kapotas and Skodas (2008). During inter-prediction phase, the H.264 encoder employs blocks of video that are various sizes to conceal the coded sequence represent data.

In the research conducted by Li et al. (2006) a method for identifying scene changes in MPEG films was established. During the process of video parsing, Eq is used to identify when there is a change in the scene (3). The video's colour, spatial correlation, motion vectors, and DCT coefficients are some of the pieces of information that are saved by the parser. Whenever the SCDH technique is used, these coefficients are modified to reflect the secret message's pixel values. When a scene transitions from one scene to the next in a video sequence, the colouring and intensities of the picture typically

differ from those of the prior scene sequence. The method for recognising scene changes does so by successively measuring the interframe differences in order to identify any changes that have taken place in the scene. In most cases, the first thing that needs to be done is to cut the video into a series of temporal snapshots, or 'shots', each of which depicts an individual event or an ongoing series of activities. A sequence of still images obtained from a single, unbroken recording made by a camera is referred to as a shot. To break up a video sequence into shots, you will need to establish a measure of the degree to which two frames differ from one another. Only in the case where two continuous frames are separated by different video shots will this metric produce a high result. The DCT coefficients are gathered during the parsing of video series in order to identify the point in the video frame where the scene shifts.

Figure 3 Proposed technique for video steganography data concealment (see online version for colours)



A secret message is added to the video and utilised to detect the changes within scene using the frame difference. By hiding the concealed message at a succession of frames in a moving video sequence, this embedding technique considerably raises the security level of the SCDH technique and makes it more difficult for someone to decipher. This is because the secret message is obscured as the streaming video sequence changes scenes. To improve the overall quality of the stego-video sequence, the cover video and the payload are first placed through a normalisation process that takes benefit of the wavelet sub-bands of the DWT coefficients. The stages that are involved in the approach that is proposed further below and is represented in Figure 3 are explained in the following subsections.

3.1 Embedding of a secret message

Once a modification in the situation has been noted, one of the most important tasks in the data-hiding method that has been presented is embedding the hidden message. When the scene-change point is larger than zero, the cover-hidden video's message will be shown in a variety of distinct scenes. When coding a cover-video frame, the DCT picture that has the proportionate average of the pixels is what is ultimately obtained. After that, The DCT algorithm produces an image that the next frames of the movie use as a reference point. The moment at which the scene changes is referred to as the scene-change point, and it is used to refer Whenever the changeover of unbroken pictures is detected from the video, pay attention towards the changes that happen in the scene.

3.2 Video embedded message

Following the completion of the detection of the scene transitions inside the video frames, the algorithm shown in Figure 4 is used to embed the secret message. Even relatively subtle shifts within a scene can be picked up by the algorithm that monitors for scene changes. After that, the scene-change point variable is set to the value 1. If there is not a discernible shift in the scenes that make up the video sequences, the scene-change point that is being identified will be left at 0. If the scene change point is larger than 0, a hidden message will be inserted into it at that time. After the payload-containing video sequence that has been created has been normalised and DWT has been applied to it, the generated intermediate video is considered complete. In conclusion, a stego-video sequence like the one displayed in Figure 4 is obtained.

Figure 4 The secret statement's embedding algorithm

Input: Secret message; cover-video frame
1: with the detected scene change 2: While secret message to embed do 3: get next DCT coefficient from parser 4: if DCT ≠ 0 and DCT ≠ 1 then 5: Calculate LSB of each coefficient 6: replace DCT LSB with message bit 7: end if 8: Write steganographic frame using DCT 9: end while
Output: Steganographic frame containing the secret message

3.3 Segmenting a video and choosing specific frames' pixels

After the segmentation of the cover-video clip into individual frames has been completed, the next step in the data hiding process is to get the average histogram values for those frames using Figure 5.

Figure 5 RGB values spectrum in a single frame of a video file (see online version for colours)

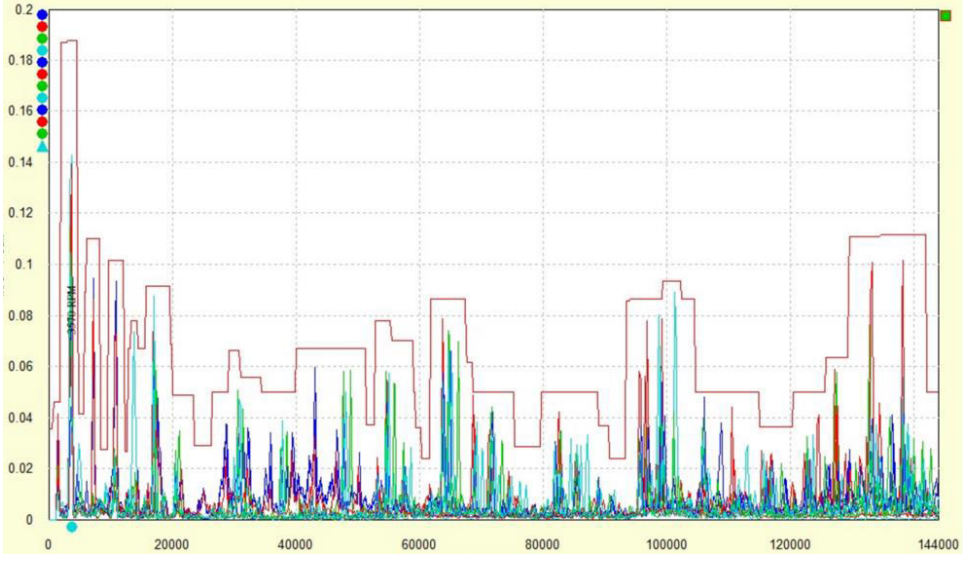
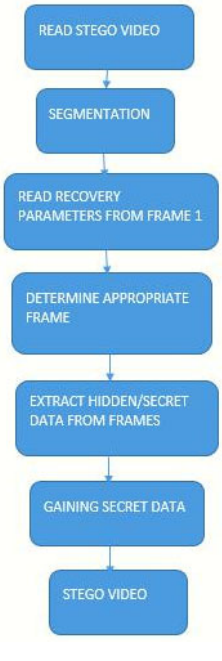


Figure 6 Flowchart of extracting algorithm (see online version for colours)



In addition, suitable frames are selected with consideration given to the HCV parameter. Figure 6 illustrates the flowchart of our recommended plan for the project.

4 Result and discussion

The steganography technique is primarily distinguished by its capability and its lack of perceptibility. To be imperceptible, the embedded data must be completely unnoticeable to the person performing the observation. The effectiveness of the suggested method is assessed by analysing the performance of five distinct video streams (Road.avi, India.avi, Birds.avi, and Paint.avi) and one hidden text (msg.txt), as shown in Table 1 and Table 2.

Table 1 Cover video information

Video file	*Resolution W × H*	*No. of frames*	*Size*
Road.avi	360 × 240	337	83.4 MB
lndia.avi	640 × 360	126	83.I MB
Birds.avi	540 × 360	248	l38 MB
Paint.avi	520 × 293	169	73.7 MB

We were able to conclude from the data in Table 1 that the hash-based least significant bit method for video steganography, which uses the MATLAB programme as the steganographic tool, produces a greater PSNR. Given that video has a significant hiding capacity as well, we also discovered that a larger hiding capacity resulted in a higher PSNR and a lower MSE.

Table 2 Obtained result information

Video files	*No. of character in text file*	*Hiding capacity*	*PSNR*	*MSE*
Road.avi	623	259,200	55.1217	0.1999
lndia.avi	623	691,200	58.7526	0.0866
Birds.avi	623	583,200	60.3847	0.0594
Paint.avi	623	457,080	57.4613	0.1166

According to our best knowledge, the first method of coverless video steganography was proposed in the year 2020 by Pan et al. Because of this, we will undertake performance comparison tests utilising Pan's technique on the same collection of data, which will contain some openly available movies that we downloaded from the internet using crawler technology. These experiments will be conducted on the same data set. The mean squared error (MSE) and the peak signal to noise ratio (PSNR) are two objective measurements that can be used to evaluate the quality of this characteristic. The main video as well as the stego-video is contrasted in terms of these dimensions. The term 'MSE' is used. It is the measurement that is used to quantify the change that occurred between the original video and the video that was distorted or noisy.

By comparing the original video to the stegovideo and obtaining the PSNR, which we can extract from the MSE, we can assess the video's quality (MSE). The equations for the both MSE and PSNR are as follows.

$$\mathrm{MSE} = \mathrm{sum}(\mathrm{sum}(\mathrm{squaredErrorImage})) / (\mathrm{rows} * \mathrm{columns}) \quad (1)$$

$$\text{PSNR} = 10 * \log 10(256 \wedge 2 / \text{MSE}) \tag{2}$$

where MAX refers to the maximum amount of bits that can be used to represent a single pixel in an image frame. For illustration, when graphics are rendered using 8 bits, the sum of MAX is 255. The intensity parts of the images are used as the basis for computing the PSNR parameter. However, the safety of the steganography should be evaluated in light of other capabilities of a similar nature. When *T* is increased, there is a corresponding rise in the embedded capacity. The values of *T* for the different datasets are tabulated in Table 3 and Table 4. Consequently, taking into account the accuracy as well as the capability of embedding, our method is able to keep the security under a variety of different thresholds. The algorithm is ineligible for this research since it is founded on the HEVC encoding standard, whereas the other algorithms were created using the AVC encoding standard. This is because different encoding standards have a substantial influence on the final video quality. On the other hand, in Tables 3 and 4, we also present the impact on video quality under various levels.

Table 3 Outcome of security experiments using various thresholds

Threshold	*AR (ploy)*	*AR (linear)*
16	46.52%	59.09%
32	46.52%	59.25%
48	49.96%	68.06%
64	55.03%	80.96%
80	56.05%	83.32%
90	66.18%	85.48%
Threshold	*AR (ploy)*	*AR (linear)*
16	46.52%	59.09%
32	46.52%	59.25%
48	49.96%	68.06%
64	55.03%	80.96%
80	56.05%	83.32%
90	66.18%	85.48%

This is due to the fact that the PSNR result obtained utilising MSU video quality measurement tool is the average PSNR of all video frames, including both P images and I images. On the other hand, information can only be hidden in videos using IPM steganography, and only in I frames.

Table 4 Outcomes of a research on video quality

PSNR IAVC)	*T = 96*	*T = 80*	*T = 64*	*T = 48*	*T = 32*	*T = 16*
Akiyo.yuv	43.72	43.88	43.96	44.12	44. 19	44.21
Bridge-dosc.yuv	33.8	33.76	33.8	33.75	33.87	33.87
Bus.yuv	28.24	28.26	28.29	28.27	28.27	28.30

5 Conclusions

This article examines the numerous challenges and issues that are related to the use of digital video steganography technology for security purposes, as well as the solutions that have been proposed in subsequent works. This method of concealing a specific text file within a video does so in a safe manner, with as little mean square error as possible, and as a result, it yields the highest possible PSNR, or ratio of maximum signals to disturbance. Consequently, embedding data within a video clip facilitates safe data sharing, which prevents the data from being disclosed to an unauthorised receiver and prevents any changes to the secret message. The two individuals can come to an agreement on a different encryption format in order to ensure that no one can access the information that is contained in the video. This can be extended to include the design of a piece of hardware that is capable of making video steganography and is intended for usage by the average customer. Additionally, in comparison to existing approaches, the proposed technique improved security by implementing a data-hiding strategy in the DCT as well as DWT sectors. This made it possible to maintain acceptable video quality even if the technique resulted in hardly perceptible distortion. The next step in this line of research will involve improving the system such that the message may be embedded using a password. Two more different steganographic systems approaches will be deployed on digital images.

References

Ali, A. and Fawzi, A. (2010) 'Modified high capacity image steganography technique based on wavelet transform', *The Int. Arab. J. Inform. Technol*., Vol. 7, No. 4, pp.358–364.

Artz, D. (2001) 'Digital steganography: hiding data within data', *IEEE Internet Computing*, May–June, pp.75–80.

Bhaumik, A.K., Choi, M., Robles, R.J. and Balitanas, M.O. (2009) 'Data hiding in video', in *International Journal of Database Theory and Application*, June, Vol. 2, No. 2, pp.9–16.

Chandramouli, R. and Memon, N. (2001) 'Analysis of LSB based image steganography techniques', *IEEE*, pp.1019–1022.

Hrytskiv, Z., Voloshynovskiy, S. and Rytsar, Y. (1998) 'Cryptography of video information in modem communications', *Electronics and Energetics*, Vol. 11, No. 1, pp.115–125.

Kapotas, S.K. and Skodas, A.N. (2008) 'A new data hiding scheme for scene change detection in H.264 encoded video sequences', in *IEEE International Conference on Multimedia Expo*, pp.277–280.

Kavitha, Kadam, K., Koshti, A. and Dunghav, P. (2012) 'Steganography using least significant bit algorithm', *International Journal of Engineering Research and Applications (IJERA)*, May-June, Vol. 2, No. 3, pp.338–341, ISSN: 2248-9622.

Li, Z., Jiang, J., Xiao, G. and Fang, H. (2006) *An Effective and Fast Scene Change Detection Algorithm for MPEG Compressed Videos*, Springer-Verlag, pp.206–214.

Nie, Q., Xu, B., Feng, B. and Zhang, L.Y. (2018) 'Defining embedding distortion for intra prediction mode-based video steganography', *Comput. Mater. Contin.*, Vol. 55, No. 1, p.59.

Pan, N., Qin, J., Tan, Y., Xiang, X. and Hou, G. (2020) 'A video coverless information hiding algorithm based on semantic segmentation', *EURASIP Journal on Image and Video Processing*, Vol. 2020, No. 1, pp.1–18.

Paulpandi, P. and Meyyappan, T. (2012) 'Hiding messages using motion vector technique in video steganography', *International Journal of Engineering Trends and Technology*, Vol. 3, No. 3, pp.361–365.

Po-Yueh, C. and Hung, L. (2006) 'A DWT based approach for image steganography', *Int. J. Appl. Sci. Eng.*, Vol. 4, No. 3, pp.275–90.

Rabah, K. (2004) 'Steganography the art of hiding', *Information Technology Journal*, Vol. 3, No. 3, pp.245–269.

Shanableh, T. (2012) 'Data hiding in mpeg video files using multivariate regression and flexible macroblock ordering', *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 2, pp.455–464.

Yang, C.H. and Tsai M.H (2010) 'Improving histogram-based reversible data hiding by interleaving predictions', *IET Image Processing*, Vol. 4, No. 4, pp.223–234.