

A Survey on Video Steganography

Angitha John¹, Anjana Baby²

¹PG Scholar, Department of Computer Science and Engineering, Vimal Jyothi Engineering College Chemperi, Kerala, India- 670632

²Assistant Professor, Department of Computer Science and Engineering, Vimal Jyothi Engineering College Chemperi, Kerala, India- 670632

Abstract: For transmitting the secret data, security issues should be considered because hackers may use frail connection over correspondence system to take data. Steganography helps to send confidential data between two parties. Steganography can be classified as text, image, video and audio steganography. Video steganography is a field of steganography where videos are used to hide information. In a video steganography, we can hide large amount of data because it is the combination of image and sound. Therefore, image and audio steganography techniques can be occupied on the video. In this paper, we present a survey on different video steganography techniques.

Keywords: confidential, histogram, network, secret data, steganography, stego-file, motion vector

1. Introduction

The rise of internet is one of the most important factor of information technology. The digital world is changing at a great speed. New communication technologies come up with new possibilities, by using them you can make yourself, and others, to risks. Many people have trouble assessing these risks especially with regard to the subject of safe digital communication. This is particularly true for people working in an organization as they have to secure their system information. However, also in countries which is considered to be relatively free and uncensored, your data can be used or corrupted by other companies or by other persons. Information security refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction etc.

There are mainly two methods to provide security: cryptography and steganography. Encrypting data helps to en-sure data confidentiality and integrity. Digital signatures are mostly used in cryptography to validate the authenticity of data. Cryptography and steganography have turned out to be progressively vital. Cryptography aims to make the message readable only to the target recipient but not by others through attaining a camouflaged form of message. Steganography is the investigation of inserting and concealing messages in a medium called a cover text with the goal that just the sender and receiver know the presence of message. Earlier days, it was used by the ancient Greeks to hide information about troop movements by tattooing the information on someone's head and then letting the person growing their hair to cover it up. The main goal of both steganography and cryptography is to provide confidentiality and protection of data. The output of steganography is a stego-file which is the combination of input file and secret data. The stego objects will be seen by the Human Visual

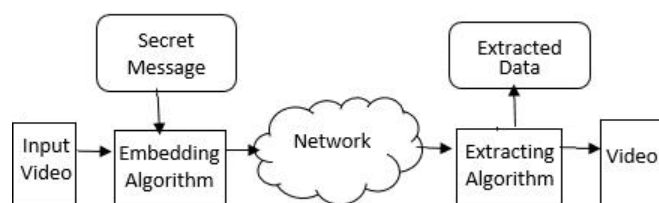


Figure 1: Block diagram of video steganography

System (HVS) as one piece of data because the HVS will not be able to notice the small change that occurs in the cover data [1].

The block diagram of video steganography is shown in the Fig 1. At the sender's side, video is taken as input then it is decomposed into a number of frames. The secret message is embedded into the frames with the help of some embedding algorithms and is send through the network as stego-video. At the receiver's side, the stego-video is processed with some extracting algorithms and the secret data is extracted from the video sequences. The video that is transmitted by the sender to the receiver carries the data, but the presence of the data cannot be detected by an outsider.

Video steganography can be referred to an extension of image steganography. The video stream is a collection of consecutive and equally time-spaced still images accompanied with audio. Image steganographic techniques are also applicable to video steganography. When the hiding capacity increases, a smaller cover file can be used for hiding the secret message. This results a stego-file with a smaller size can be used and that can be easily transmitted over the internet. But increasing the hiding capacity leads to distortions in the stego-file. If an attacker recognizes the distortion, then the presence of the hidden message can be detected. The advantage of using video as a cover medium to store the data is there is large space to store the data. It provides more security against the attacker because the video file is much more complex than image file. Another advantage is that the secret data is not recognized by the human eye as the change of a pixel color is negligible. In video steganography, we can also hide secret data in the audio files as it contains unused bits. When we need to store

more amount of data, video steganography is better method than any other stenographic methods.

2. Video Steganography Techniques

Video steganography can be used in different applications such as military, intelligence agencies communications etc. Video steganography techniques can be classified into compressed domain and raw domain.

a) Video steganography techniques in compressed domain

Steganography in compressed domain is an emerging field for secure data transmission. Steganography in videos can be done by utilizing its motion vector components, macro-blocks, intraprediction mode, VLC, quantized coefficients, CAVLC entropy coding etc. H.264 standard has increased the efficiency of video compression when compared with previous standards. [2] Some of the features include flexible macro block ordering, quarter-pixel interpolation, intra prediction in intra frame and multiple frames reference capability etc. There are 3 types of frames: intra (I) frame, predicted (P) frame, and bidirectional (B) frame. During the video compression process, the motion estimation and compensation minimizes the temporal redundancy. The video stream is various related still pictures, a frame can be predicted by using one or more referenced frames based on motion estimation and compensation techniques. Frames can be divided into 16x16 macro blocks (MB) wherein each MB contains blocks that may include the smallest size of 4x4.

1) Intra frame prediction: If a macro block is encoded in intra mode, a prediction block is formed based on previously encoded and reconstructed block. Intra-frame prediction exploits spatial repetition. There is a total of 9 optional prediction modes for each 4x4 luma block; 4 optional modes for a 16x16 luma block; and one mode that is constantly connected to each 4x4 Chroma block. The High Efficiency Video Coding (HEVC) codec can bolster up to 35 intra prediction modes for each block sizes.

2) Inter frame prediction: Inter frame is a frame in video compression which is indicated in terms of one or more frames. Embedding the secret message is done by mapping seven block sizes of H.264 inter frame prediction such as 16x16, 16x8, 8x16, 8x8, 8x4, 4x8 and 4x4 to a number of secret bits. The data hiding of inter frame prediction has limited embedding capacity. Mapping rules of different block sizes can be used to embed the secret data.

3) Motion vectors: In video compression, motion vector is the key element in the motion estimation process. It is used to represent a macro block in a frame based on the position of this macro block in another frame. Motion vector qualities, for example, horizontal and vertical components, amplitude, and phase angles are used in embedding secret information. This method embeds information to pixels of frames in host video which is based on the H.264/AVC Video coding standard. It is designed a motion vector component feature to control embedding, and also to be the secret carrier. The information embedded will not

significantly affect the video sequence's visual invisibility and statistical invisibility.

4) Transform coefficients: Transform domain technique is used to transfer pixels from time domain to frequency domain. [3] Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Integer Wavelet Transform (IWT), Haar Transform, Discrete Curvelet Transform (DCVT) are the transform domain techniques. DCT and DWT are broadly utilized for steganography. In DFT the discrete-time signals are converted into discrete number of frequencies. DCT is similar to DFT which transform the signal or image from spatial domain to the frequency domain. The DCT is used in steganography as the Image is broken into 8x8 pixel blocks and transforms these pixel blocks into 64 DCT. The image can be reconstructed through decompression, by a process known as Inverse discrete cosine transform i.e. IDCT. [4] DWT is the process of transforming the image from a spatial domain to the frequency domain. Wavelets are created by translations and dilations of a mother wavelet. The DWT is the accurate model when compared with DFT and DCT and it is multi resolution description of the image.

5) Entropy coding: Entropy coding is a method of lossless data compression scheme. [5] The entropy coding stage maps symbols representing motion vectors, quantized coefficients, and macro block headers into actual bits. Entropy coding improves the coding effectiveness by assigning fewer number of bits to frequently used symbols and a more noteworthy number of bits to less frequently used symbols. The two types of entropy coding are Context Adaptive Variable Length Coding (CAVLC) and Context Adaptive Binary Arithmetic Coding (CABAC). CAVLC is used to convert residual, zigzag ordered 4x4 blocks of transform coefficients. CABAC exploits symbol correlations by using contexts and also it exploits arithmetic coding which creates non-whole number code words for higher proficiency.

b) Video steganography techniques in raw domain

The input video can be converted into frames as still images, and the data embedding can be taking place on each individual frame. After embedding all the frame scan be combined to form the stego-video. Raw video technique consists of spatial and transform domain techniques. In spatial domain technique the pixel intensities are utilized directly to hide the secret message. Different steganographic techniques on the spatial domain such as LSB substitution, Pixel Value Differencing (PVD), Spread Spectrum, ROI, Histogram Manipulation, Most Significant Bit (MSB), and Quantization Index Modulation (QIM). LSB is the lowest bit in a series of numbers in binary; the LSB is located at the far right of a string. LSB technique is done by replacing some LSBs of pixels from the cover video with the secret message bits so the changes are invisible to the human eyes. [6] PVD uses the difference value between two consecutive pixels in a block to determine how many secret bits should be embedded. MSB is also known as high-order bit is the greatest value in binary number. Here, MSB is used to hide data. [7] The Spread spectrum method spreads the secret

message over the frequency spectrum of sound file which is independent of the actual file.

3. Literature Review

Yao et al. [8] proposed an effective scheme for reversible data hiding in encrypted H.264/AVC video bit streams. This technique will reduce the inter-frame distortion drift caused by data embedding. In the encryption phase, three types of key coding parameters such as intra prediction modes, motion vector differences and quantized DCT coefficients which are encrypted using stream ciphers without video bit rate increment to obtain the encrypted video. In the data hiding phase, histogram shifting technique in the 4x4 luminance integer DCT block coefficients of P-frame is used so that the data hider can embed data into the encrypted video bit stream without knowing the content of original video. At the receiver end, the embedded data can be extracted either in the encrypted domain or in the decrypted domain.

Ma et al. [9] presented a method based on intra-frame distortion drift, which is introduced after embedding in H.264/AVC videos to reduce the spatial redundancies of video sequences. The data is embedded into the I-frame DCT quantized coefficients of 4x4 luminance blocks, because the human eyes are less sensitive to the brightness. In this technique the intra-frame distortion is not propagated to the neighboring blocks. The encrypted message is embedded into the paired-coefficients based on modulo modulation, in which one is used for embedding the secret data and other one is used to fix the level of distortion.

Ni, Zhicheng et al. [10] the algorithm uses the zero or the minimum point of the histogram and modifies the pixel values to embed the data. From the histogram the zero point and peak points are selected. The gray value of the pixels between these points are increased by 1 i.e., shifting the range of values of the histogram to the right by 1 unit. Pixel at the peak value is added by 1, if the data bit to be embedded is 1, else it is kept intact. In data retrieval, the gray value with maximum point is met, if the value is intact, then 0 is retrieved, otherwise 1 is retrieved. The pixels whose gray value is between the peak point and zero point is met, the gray value of those pixels is subtracted by 1, hence the original image can be recovered. The capacity of the algorithm depends upon the maximum pixels obtained.

Sunil Moon et al. [11] used a steganography technique where it hides image and text inside a video file and uses computer forensics as a tool for authentication so that it increases the data security. Hiding the secret message inside the cover video frames by using 4LSB technique. Computer forensic is used to detect whether the incoming stego-video is original or fake. If the video contains the original data, then it can be decoded by using same secret key which is known to sender and receiver only. 4LSB substitution method is used for embedding large amount of data behind selected frame of video, hence it is very difficult to find in which part of video the data is hidden.

Singh Namrata et al. [12] proposed a video steganography approach where an audio is hidden in the cover video file. The random frames selection is done by using CryptGenRandom. Audio embedding is done in these randomly selected frames. The encrypted secret bits are XORed with the original LSBs of the frames of video. The resultant XORed bits are inculcated at the LSB positions and all the embedded frames are hence regained to image format. While extracting, the random frames are selected and LSBs are extracted and reverse XOR is performed. This leads to the extraction of original LSB bits and encrypted secret message bits.

Rodriguez David et al. [13] an HEVC-compliant method to hide and retrieve information in high-resolution videos by modifying the luminance of certain blocks is proposed. During embedding it will employ 4x4 intra-block per hidden bit. Every block is composed of 16-bits, and every character occupies 8-bits, a total amount of 16x8xL pixels will be modified. Insertion of information is done randomly, the receiver should know the positions to recover the information, both the video and the tuples contained in the NALs are necessary to locate the information. Once the video is decoded, it is possible to access to the proper frame and position to collect the second MSB of the 16 luminance pixels integrating the IB. After computing the mode among these 16 bits, it is possible to interpret the bit that was inserted. To fully identify the ASCII code of the characters inserted, group the 8 recovered bits and choose the one with highest absolute frequency.

Jha Vivek Kumar et al. [14] proposed a new technique of video steganography by implementing pixel randomization, de-randomization and data embedding technique. Prime factorization method is used to scramble pixels of cover video frames. Then the frames of secret video file is inserted into the last 2 bits of the scrambled cover frame of cover video file using spiral LSB technique. The first frame, the index frame which contains the knowledge regarding where the information is stored, in which form, what is file type etc. When the first frame is received properly, and the receiver recognized the information then it is very easy to get hidden information from stego-video file. During extraction process, scrambling the pixels using prime factorization and can extract the data using inverse spiral LSB technique.

Selvigrija P et al. [15] uses dual steganography by combining steganography with cryptography to secure the original videos from unapproved individual. The Linked List method and Feistel Network are used for hiding Information. The secret message is encrypted using Feistel network and then embedded inside the frames of the cover video to obtain Stego frames. The text is embedded inside video frames using Linked List structured message embedding technique, after embedding a byte of information inside one 3*3 pixel, it should also embed the address of the location of next byte of information next to it. The information is extracted from stego frames using Linked List Structured message embedding technique and decrypting the data using Feistel Network to obtain the original message.

Sudeepa K B et al. [16] provides security for information like text/images using video steganography, cryptography, randomization and parallelization. The frames are selected randomly using Feedback Shift Register (FSR) to avoid repetition and the data to be hidden is encrypted using a symmetric key. FSR will generate pseudo random numbers and uses only non-repetitive numbers. The encryption of the data is processed in parallel; hence the embedding is a parallel process. The encrypted data is embedded into the randomly selected frame using LSB method. Inverse technique of embedding is used to extract and decrypt the secret data from the stego-video which is also a parallel process.

Yu Li et al. [17] uses the parity of the coefficients after transformation and quantization of 4x4 luma block to hide the desirable data which is based on H.264 encoded video sequences. The data can be extracted without using the original host video. An appropriate threshold is set based on the size of the message and characteristics of the video sequence. Quantized 4x4 residual blocks are zigzag scanned to find the last nonzero coefficient whose scan location is no less than the threshold can be used to hide the message. This method uses the odd-even difference as the embedding mark. If the embedded bit is 1, the designated point in the video encoding block must be an odd number; if the bit is 0, the designated point must be an even number. This technique can be used for content-based authentication and covert communication.

Himanshu Wadekar et al. [18] proposed steganography using the technique pixel pattern matching and key segmentation. The confidential information is encrypted by using AES algorithm and is divided in the form of Quotient, Divisor and Remainder. A random frame is selected from the input video where the encrypted message is embedded using Pixel Pattern Matching. As the message is embedded, a location key is generated for each pixel. This location key is embedded in different frames in a linked list fashion using LSB technique. When the file is received it is scanned for the location key and the random frame where the data is embedded. The value of data bits is found using the location key. The Encrypted message is computed using the formula $Q \cdot D + R$. Then AES decryption is used to get the original secret message. It is difficult to identify since the location key is divided, encrypted and put away in various video frames alongside this the secret message.

Jie Yang et al. [19] uses a reversible information hiding method, generalized difference spread, which makes use of the information redundancy between adjacent pixel points more than Tian's pixel-to-difference spread method, and generalizes 2-dimensional reversible integer transform to N-dimensional space to obtain more embedding capacity. The motion vectors are used as the carriers. Optimized algorithm can help to embed $2N + 1$ -bit information into N-dimensional motion vector space coding. During extraction, the elements in the vector v may be negative, so the secret bit is the least significant bit of its absolute value. The embedding and extraction algorithm are slightly optimized so that the inverse operation after extracting the secret information can obtain a distortion-free video sequence.

Muhammad Khaerul Anam et al. [20] implemented a random number generator function by developing an application to hide text data in a video file as container. The media file container contained with MP4 format will insert an array text message with a maximum length of 255 characters. In the second stage, the sender enters the secret message key in the form of a number, which is used as a seed value to perform the PRNG function. The application will generate random numbers based on the secret message key with PRNG function and the process is repeated until it produces the sequence of numbers as much as the length of the text message characters. The next stage of the application inserts each character bit of the message into each video pixel bit by using the LSB method. Then the last phase of the app will rearrange it into a whole video called the stego object. Meanwhile, extraction processes are just opposite to embedding.

Vinita V. Korgaonkar et al. [21] proposed a novel approach of hiding secret text in a video by using frequency domain coefficient of frames by combining DCT and DWT technique. DWT and DCT techniques transform a digital image from spatial domain into frequency domain coefficients. DCT is applied for high frequency sub band of DWT. In embedding phase, the cover video is divided into frames and non-key frames are used for embedding purpose. Secret message is divided into sub-blocks and it is embedded into the DWT- DCT coefficient of Y, Cb and Cr of video frame. The reverse of embedding is done in the extraction process.

Sushmitha MC et al. [22] proposed a technique to hide secret video in a cover video using the concepts of steganography and discrete wavelet transform. Perform discrete wavelet transform and obtain LL, LH, HL and HH bands. The secret video is decomposed into frames and the pixel values are stored in the HL, LH and HH bands of the cover video using LSB technique of steganography. Inverse discrete wavelet transform is applied on the LL and modified HL, LH and HH bands. An authorized recipient can reconstruct the secret video. The stego video of size PQ pixels is split into frames and each frame is cropped into PP pixels. Discrete wavelet transforms are applied to the video frames to obtain LL, LH, HL and HH bands. The pixel values of secret video frames are extracted from the coefficients of LH, HL and HH bands and the secret video is generated using the reconstructed secret video frames.

Table 1: Performance Analysis

Paper Title	Parameter
Inter-frame distortion drift analysis for reversible data hiding in encrypted H.264/AVC video bitstreams	PSNR ranges 27.51-37.87dB
A Data Hiding Algorithm for H.264/AVC Video Streams Without Intra-Frame Distortion Drift	PSNR=37.29dB
Reversible Data Hiding	PSNR Is Above 48dB & 5k-60k bits can be embedded

Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security	50% Embedding capacity Compared with other LSB Techniques
Randomized LSB Based Video Steganography for Hiding Acoustic Data Using XOR Technique	PSNR= 22dB
Intra-Steganography: Hiding Data in High-Resolution Videos	PSNR ranges 32-34dB
Video Steganography technique using Factorization and Spiral LSB methods	PSNR=44.481 & 25% Embedding capacity
Dual Steganography for Hiding Text in Video by Linked List Method	quality of Stego video will be equal to the cover video
A New Approach for Video Steganography based on Randomization and Parallelization	Throughput is directly proportional to the number of characters
A New Method of Data Hiding Based on H.264 Encoded Video Sequences	PSNR=36.2
A New Approach to Video Steganography using Pixel Pattern Matching and Key Segmentation	Embedding capacity is high
An Optimized Algorithm Based on Generalized Difference Expansion Method Used for HEVC Reversible Video Information Hiding	PSNR value is greater than 30dB
Random Pixel Embedding for Hiding Secret Text over Video File	SNR=99% & CER= 0.06
A DWT-DCT Combined Approach for Video Steganography	Hiding capacity is High
An Approach Towards Novel Video Steganography for Consumer Electronics	PSNR ranges 68.66 70.80 dB

4. Conclusion

In the period of quick data exchange utilizing internet and World Wide Web, internet is an open correspondence channel because of which it has more noteworthy helplessness to be assaulted by an unapproved party, video steganography has turned into an imperative device for data security. In this paper, we have presented a review and analysis of different video steganography techniques. We have also discussed about the difference between cryptography and steganography. Steganography techniques in compressed domain and raw domain is also discussed.

References

- [1] Mstafa, Ramadhan J and Elleithy, Khaled M and Abdelfattah, Eman, Video steganography techniques: taxonomy, challenges, and future directions, Systems, Applications and Technology Conference (LISAT), 2017 IEEE Long Island, pp. 1–6.
- [2] Mstafa, Ramadhan J and Elleithy, Khaled M, Compressed and raw video steganography techniques: a comprehensive survey and analysis, Multimedia tools and applications, vol. 76, (2017) pp. 21749–21786.
- [3] Divya.A, S.Thenmozhi, Steganography: Various Techniques In Spatial and Transform Domain International Journal of Advanced Scientific Re-search and Management, vol. 1 Issue 3, (2016).
- [4] Sadek, Mennatallah M and Khalifa, Amal S and Mostafa, Mostafa GM, Video steganography: a comprehensive review, Multimedia tools and applications, vol. 74, (2015) pp. 7063–7094.
- [5] <http://web.cs.ucla.edu/classes/fall03/cs218/paper/>.
- [6] Kaur, Harpreet and Rani, Jyoti, A Survey on different techniques of steganography, MATEC Web of Conferences, vol. 57, EDP Sciences, (2016), pp. 02003.
- [7] Souma and , Pal and , Prof and Kumar, Samir and Bandyopadhyay, Samir, various methods of video steganography, International Journal of Information Research and Review, vol. 3, (2018), pp. 2569–2573.
- [8] Yao, Yuanzhi and Zhang, Weiming and Yu, Nenghai, Inter-frame distortion drift analysis for reversible data hiding in encrypted H. 264/AVC video bitstreams, Signal Processing, vol. 128, (2016), pp. 531–545.
- [9] Ma, Xiaojing and Li, Zhitang and Tu, Hao and Zhang, Bochao, A data hiding algorithm for H. 264/AVC video streams without intra-frame distortion drift, IEEE transactions on circuits and systems for video technology, vol. 20, (2010), pp. 1320–1330.
- [10] Ni, Zhicheng and Shi, Yun-Qing and Ansari, Nirwan and Su, Wei, Reversible data hiding, Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS'03, vol. 2, (2003), pp. II–II.
- [11] Sunil K. Moon, Rajeshree. D. Raut, Analysis of secured Video Steganography using Computer Forensics Technique for Enhance Data Security, IEEE International Conference on Image Information Processing (ICIIP), (2013), pp. 660–665.
- [12] Singh, Namrata and Bhardwaj, Jayati, Randomized LSB Based Video Steganography for Hiding Acoustic Data Using XOR Technique, 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE), (2017), pp. 1–7.
- [13] Rodríguez, David and Del Barrio, Alberto A and Botella, Guillermo and Cuesta, David, Intra-Steganography: Hiding Data in High-Resolution videos, 2018 IEEE/ACM 22nd International Symposium on Distributed Simulation and Real Time Applications (DS-RT), (2018), pp. 1–8.
- [14] Jha, Vivek Kumar and Mukherjee, Srilekha and Roy, Subhajit and Sanyal, Goutam, Video steganography technique using factorization and spiral LSB methods, 2017 International Conference on Computer, Communications and Electronics (Comptelix), (2017), pp. 315–320.
- [15] Selvigrija, P and Ramya, E, Dual steganography for hiding text in video by linked list method, 2015 IEEE International Conference on Engineering and Technology (ICETECH), (2015), pp. 1–5.
- [16] Sudeepa, KB and Raju, K and HS, Ranjan Kumar and Aithal, Ganesh, A new approach for video steganography based on randomization and parallelization, Procedia Computer Science, vol. 78, (2016), pp. 483–490.
- [17] Li, Yu and Chen, He-xin and Zhao, Yan, A new method of data hiding based on H. 264 encoded video sequences, IEEE 10th international conference on signal processing proceedings, (2010), pp. 1833–1836.

- [18] Wadekar, Himanshu and Babu, Aishwarya and Bharvadia, Vaishali and Tatwadarshi, PN, A new approach to video steganography using pixel pattern matching and key segmentation, 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), (2017), pp. 1–5.
- [19] Peng, Bo and Yang, Jie, An optimized algorithm based on generalized difference expansion method used for HEVC reversible video information hiding, 2017 IEEE 17th International Conference on Communication Technology (ICCT), (2017), pp. 1668–1672.
- [20] Anam, Muhammad Khaerul and Sarwoko, Eko Adi and Suharto, Edy and Khasburrahman, Kharis, Random pixel embedding for hiding secret text over video file, 2017 1st International Conference on Informatics and Computational Sciences (ICICoS), (2017), pp. 41–46.
- [21] Korgaonkar, Vinita V and Gaonkar, Manisha Naik, A DWT-DCT com-bined approach for video steganography, 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), (2017), pp. 421–424.
- [22] Sushmitha, MC and Suresh, HN and Manikandan, J, An approach towards novel video steganography for consumer electronics, 2017 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), (2017), pp. 72–76.