Digital Video Steganography: An Overview

Chapter · September 2022

DOI: 10.1007/978-981-19-3015-7_42

2 authors, including:

Rajkumar Soundrapandiyan
VIT University
99 PUBLICATIONS **755** CITATIONS

SEE PROFILE

Digital Video Steganography: An Overview

Suganthi Kumar and Rajkumar Soundrapandiyan

Abstract The recent evolution of digital communication demands securing the integrity of data transfer. Under such necessity, the data hiding practice, steganography allures the attention of security and forensic departments. Steganography is broadly classified into two types depending on the linguistic and technical features. Based on the domain in which the steganography is applied, the technical steganography is categorized into the following types: digital media, network, hardware, circuitry, and genome. Concerning the cover medium, digital media steganography is further classified into four types: image, audio, video, and documents. By widespread usage of video-based applications, video-specific techniques have recently got more emphasis. This rapid growth motivated the authors to provide a comprehensive literature review of this subject. This paper mainly talks about video steganography techniques in the recent decade. In addition, quality metrics used in the performance evaluation process are also discussed. This review is mainly focused on providing an overall guide for new researchers approaching the field of steganography.

Keywords Digital communication · Steganography · Secret communication · Technical steganography · Digital media · Video steganography · Quality metrics

1 Introduction

Communication is an essential part of human life. It was done in different ways at different times based on civilization. However, distance communication had always been challenging in ancient times. But in the present modern age with the advent of communication technologies, remote communication turned out to be much easier.

S. Kumar (✉) · R. Soundrapandiyan
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India
e-mail: k.suganthi@vit.ac.in

R. Soundrapandiyan
e-mail: rajkumarsrajkumar@gmail.com; rajkumars@vit.ac.in

V. K. Asari et al. (eds.), *Computational Methods and Data Engineering*,
Lecture Notes on Data Engineering and Communications Technologies 139,
https://doi.org/10.1007/978-981-19-3015-7_42

Wherein, digital media communication has become inevitable transferring multimedia files and messages between sender and receiver. Howbeit, excessive usage and over-reliance on the same pose several security risks and adversaries such as data intrusion, modification, theft, and impersonation, by unethical third parties, and it leads to having disastrous consequences for the information system. Thus, the process of securing the communication is as important as the communication itself.

There are many security mechanisms available for secure communication. Cryptography is one such approach that converts the message in such a way that it becomes ambiguous to the third party. Yet, it is not sufficient these days as the meaningless content itself draws attention. In such a scenario, steganography, the art and science of secret communication, is the optimal solution. Steganography mechanism establishes secret communication by hiding secret messages into some cover data. Thus, it becomes impossible for the eavesdropper to discern secret communication as steganography conceals its very existence. Nowadays, steganography is attainable for any end users with Internet access. At times, it is preferable to combine cryptography techniques with the steganography system to provide an additional layer of security. But using these techniques separately is not ideal. Watermarking is another data embedding mechanism that is proximate to steganography, which nevertheless has different goals and attributes, i.e., the existence of secret communication is often visible to everyone under certain conditions. The main property of watermarking is to prevent the ownership infringement of digital content. Thus, steganography strives for imperceptible communication to the human visual system (HVS), whereas watermarking puts robustness as a top priority.

The word steganography is the English rendition of the Greek word ‘steganographia’. It means covered (steganos) writing (-graphia). As the name implies, steganography hides the secret messages in some cover media. Thus, it becomes impossible for the eavesdropper to discern secret communication as steganography conceals its very existence. Figure 1 portrays the working mechanism of the steganography. In the practice of steganography, the steganographers such as sender and receiver exchange secret messages using a cover medium through a network. The sender employs some data hiding process to replace the cover data with secret data. At this stage, a ‘stego-key’ can be used in encrypting the secret data before embedding it. Once the encrypted secret data is hidden into the cover medium, it is known as stego-medium, and it is sent to the receiver end via a network. The authorized receiver recovers the secret data from the stego-medium using a data retrieval process. The data retrieval algorithm is often the reversed version of the data hiding process. At times, some third-party steganalyst observes the stego-medium exchange between the steganographers and tries to remove or take out the secret data without the knowledge of steganographers. This action by steganalyst is called steganalysis. Steganalysis is the contrary mechanism to steganography: the art and science of detecting the hidden communication in a cover medium [1]. Steganalysis can be performed in two ways such as active steganalysis and passive steganalysis. The former procedure finds out only the presence (flag-1) or absence (flag-0) of the hidden message. Whereas, the latter tries to extract the entire secret data or certain characteristics of its length. Therefore, the primary motive of the steganography

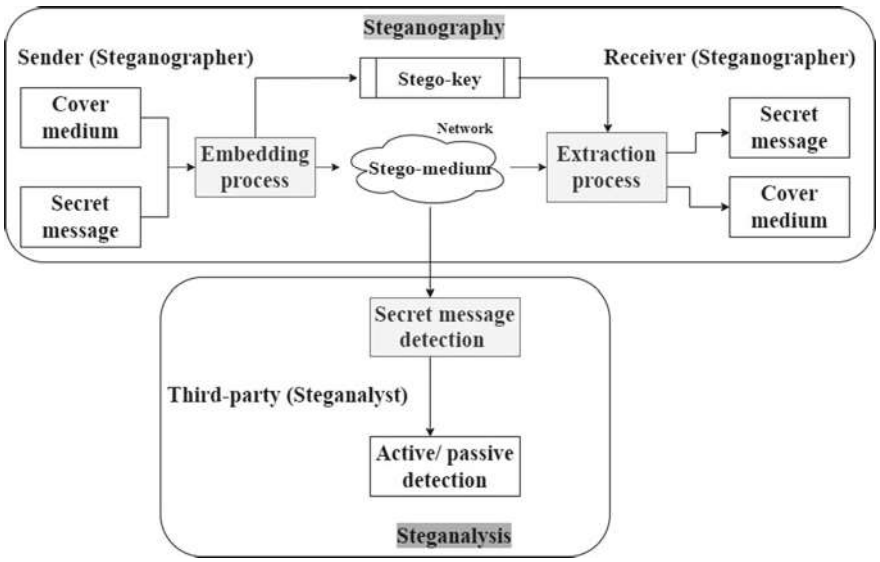

Fig. 1 Representation of steganography and steganalysis mechanisms

algorithm is to devise a secret communication framework that is not detectable by any steganalysis tools. Though the steganography technique conceals the very existence of the secret message from HVS, attacks on them are still possible. Because no matter what the embedding process is, it slightly alters certain properties of the cover medium. This causes quality attenuation in the final stego-medium which may not be noticeable by the HVS but can easily give a clue to some strong steganalysis mechanisms. Hence, the quality of the stego-medium needs to be standardized using computational evaluation metrics. In steganography, the performance or quality is generally measured in terms of three aspects such as imperceptibility, hiding capacity, and robustness.

Imperceptibility: The visual quality of the stego-medium. The cover medium and stego-medium should be identical.

Hiding capacity: The accommodation of secret data in cover medium without visual degradation.

Robustness: The resistance of the secret data inside the cover medium against any kind of attacks. And the secret data should be recovered by the receiver without data attenuation.

However, there are some more prerequisites such as reversibility and computational complexity are also required for better performance. Reversibility is the lossless or absolute retrieval of the secret data at the receiver side. And, computational complexity is the cost of time and space taken for the successful execution of the steganography algorithm which needs to be lesser for better performance. There are many quality metrics and tools available to measure the performance of

steganographic systems. Besides, it is necessary to install well-qualified steganographic systems where the topmost secret communication is indispensable. Medical, military and law enforcement, geographical, entertainment, government, corporate, intelligence agencies, and banking are some of the domains where steganography systems can be applied.

Steganography has become a promising field of research in the latest decade. This rapid growth persuaded the authors to provide a comprehensive review of steganography. This paper mainly presents some recent trends and techniques utilized in the steganography domain. In addition, quality metrics and tools used in the performance evaluation process are also discussed in this paper.

The remaining sections of the paper are as follows: Sect. 2 presents an overview of steganography methods. Section 3 discusses the performance measures, and Sect. 4 concludes the paper.

2 Steganography

The importance of secure communication is raising lately due to data breaches on the Internet and social networks. Steganography is the optimal choice for securing and storing secret information/data. An ideal and perfect steganography system must attain the prerequisites of steganography which include imperceptibility, capacity, and robustness. In addition to these, there are some more requirements such as reversibility and computational complexity for better performance. As mentioned earlier, steganography is the practice of hiding secret data within a cover medium. Based upon the type of cover medium and area in which steganography is deployed, it is broadly categorized into two types as linguistic steganography and technical steganography.

Linguistic steganography is text steganography where written communication language features are utilized to hide secret messages in some non-obvious ways [2]. It is further classified as semantic based and syntax based. The former uses synonymous words or phrases for concealing the secret messages [3, 4]. However, the latter exploits punctuating elements such as full stop (.), comma (,), semicolon (;), and colon (:) for replacing the secret message [5]. Here, the embedding process is performed systematically without affecting the sentence meaning [6].

Next, the ***technical steganography*** deploys some scientific mechanisms to embed secret messages strategically. This steganography is further categorized into five main types such as network, hardware, circuitry, genome, and digital media.

Network steganography is the latest inclusion of the steganography family. The network steganography is further classified into two types as inter-protocol steganography and intra-protocol steganography [7]. Here, secret data is concealed inside redundant communication mechanisms, and also it creates an embedded communication channel using protocols like UDP, TCP, IP, etc.

A **hardware** type of steganography allows the secret data to be hidden into the space that is unused or holds residual data of a hard disk [8, 9]. Similarly, the software

can also use the steganography approach by hiding secret information inside the code layout. In **circuitry** steganography, the secret data is concealed into an electronic circuit layout [10].

Genome steganography is an emerging technology that embeds the secret data behind the simulated biological structures of deoxyribonucleic acid (DNA). The high randomness in a DNA sequence is used for hiding purposes, where the encrypted secret data is placed as microdots between two primers [11, 12].

The standard and generally used type of steganography is **digital media** steganography. It embeds the secret message within multimedia files like images, video, audio, documents, etc.

Figure 2 exhibits the taxonomy and techniques of steganography. As the realm of steganography is vast as represented in Fig. 2, this paper presents the comprehensive literature only on digital video steganography techniques. Moreover, the recent year has been very progressive for video communication. Wherein, videos gain a wide spectrum of practical significance as they are being shared on social media frequently. There are scores of researches performed on video steganography using a variety of techniques. The following subsection explains video steganography techniques in detail.

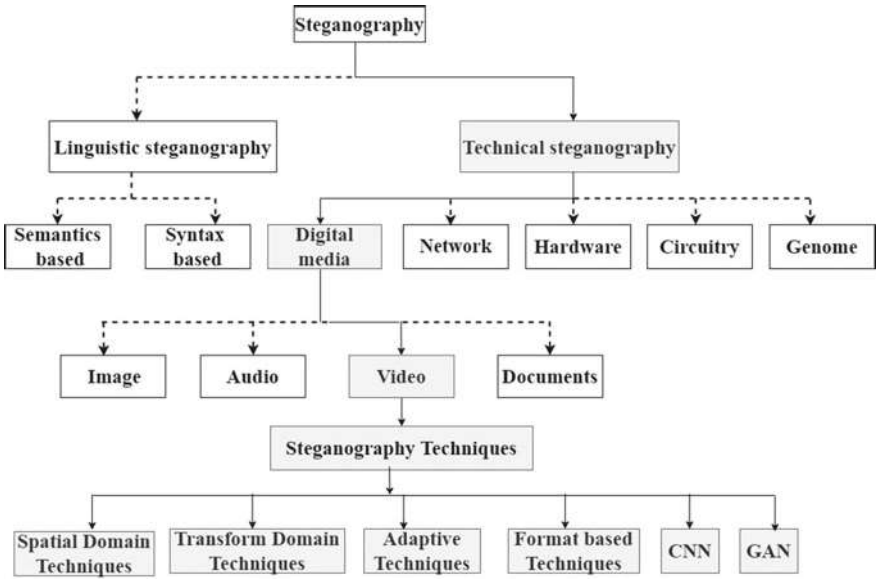

Fig. 2 Taxonomy and techniques of steganography

2.1 Digital Video Steganography

After carefully analyzing all the existing frameworks, the video steganography techniques are primarily classified into seven methods as (1) substitution techniques, (2) transform domain techniques, (3) adaptive techniques, (4) format-based techniques, (5) cover generation, (6) convolutional neural network (CNN), and (7) general adversarial network (GAN)-based methods.

Video steganography techniques. In video steganography, video content is utilized as a cover medium to embed the secret data. Video steganography has recently drawn more attention not only because of the security requirements, but also videos are more favored for the following reasons: (1) The high dimensionality in videos provides large space for data hiding, (2) the shot transitions in videos can be used for embedding purposes as they obscure to the HVS, and (3) the tampers in videos can be managed easily. (4) As videos are the sequence of frames/images, techniques that are feasible for image steganography can also be combined. There has been a lot of research performed on video steganography. The following subsections elaborate on the methods of video steganography and some related existing works of the reviewed techniques.

Substitution techniques. It is a spatial domain-based technique. Substitution is deployed in the color components RGB and YUV. Substitution technique includes the following: least significant bit (LSB), bit plane complexity segmentation (BPCS), and tri-way pixel value differencing (TPVD), etc. The LSB technique is one of the widely used substitution methods. This method displaces certain LSBs of the cover data by the bits of secret data. For instance, Chen and Qu [13] developed a video steganography framework embedding the secret bits into the LSBs of pixels from RGB components. Many video steganography-based research works have also employed encryption of secret data before the hiding process [14, 15]. Despite being simple and having a higher payload capacity, LSB method sometimes deteriorates the quality as more significant bits are utilized. This disadvantage was overcome by the evolution methods BPCS and TPVD. BPCS method is benefitted from the fact that the HVS is imperceptible in some color regions. Thus, the BPCS decomposes the frame/image of the video into bit planes. After decomposing, based on the complexity of the regions, the secret data is hidden in minimum perceived quality regions. For example, Kumar et al. [16] developed an LSB substitution-based video steganography framework where the secret data is hidden into the bit plane 4-4-0 LSBs of R-G-B components of the frame. In this method, it is considered that the change in the blue component is more sensitive to HVS. Thus, only red and green components are utilized for embedding. The TPVD is another substitution-based technique. It is the advancement of the pixel value differencing (PVD) method. The PVD first finds the difference between two adjacent pixels and hides the secret data. This method has restricted to ranges; each range has length breadth and height. The TPVD method, in contrast, utilizes all the horizontal, vertical, and diagonal edges for embedding. This improves the capacity.

Transform domain techniques. Generally, transform domain methods are resilient against attacks but computationally intense. Despite its complexity, this method maintains the quality of the stego-medium. In this technique, firstly, each cover frame of the video is converted into its transform domain, then the secret data is concealed into the selected transformed coefficients. Next, the altered transform coefficients are inversed to form the original cover frame format. The transform domain methods include discrete Fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelet transform (DWT). Lately, some transform methods like complex wavelet transform (CWT), integer wavelet transform (IWT), and dual-tree complex wavelet transform are also utilized by the researchers. Here, the DFT method is not so used in steganography as it tends to generate round-off errors [17]. However, the DCT method is very famous in video steganography and widely used in video compression techniques. The main notion of this technique is to hide the secret data behind the compressed domain in a block-wise or frame-wise manner. MPEG-1, MPEG-2, and H.263 are some of the DCT-based compression techniques. Recently, the format H.264/AVC is utilized for the video steganography process. Earlier, Chae et al. [18] presented a data hiding process in MPEG-2 videos. This method initially transforms the secret data and cover content to the DCT domain. Then the quantized coefficients of the secret message are encoded using multidimensional lattice and embedded into the cover DCT coefficients. Similarly, Yang et al. [19] worked on H. 246/AVC compressed videos, where the cover video is converted into a YUV color component. Then the secret data is hidden bit by bit in the DCT domain of the color component. DWT has achieved much attention in the fields of signal processing and video steganography. The decomposed wavelets provide a multi-resolution description and temporal resolution, where frequency and spatial information can be captured. In addition, as DWT does not segment the frame into non-overlapping blocks, it avoids the blocking artifacts. Ramalingam et al. [20] developed a change detection-based video steganography technique. They used DCT coefficients to determine the scene change in the frames and the DWT domain to embed the secret. Hence, this method improves security and minimizes visual degradation.

Adaptive techniques. The adaptive technique targets specific regions or pixels for the embedding process. Combining adaptive methods and spatial and transform domains is an exceptional case [21–25]. Wherein, before the embedding process, the statistical characteristics of cover frames are observed. Based on these observed features, the suitable regions in the cover medium are adopted for the data hiding process. These adopted regions are called the Regions of Interest (ROI). Then, the secret data is hidden within spatial or transform or wavelet domains of the ROI. However, in the case of recognizing the ROI, the video steganography system gets benefitted from the fact that the HVS is deficient in discerning the changes in transient regions [15, 26, 27]. Considering this limitation, many research works have been presented. Hashemzadeh [28] used the motion clue feature points for their video steganography framework wherein the momentum of a particular key point is detected and tracked. And the spatial and temporal behaviors of the key point are observed and used for identifying the appropriate regions to hide the secret data. The secret data is

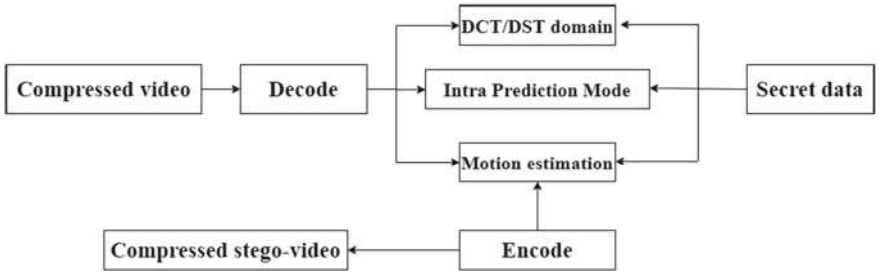

Fig. 3 Format-based steganography

embedded using the LSB substitution method. Similarly, Kumar et al. [29] proposed an optimal video steganography framework. This method determines dynamic key points using motion vectors and dilates them to form dynamic ROI, where the secret data is embedded. Utilizing key points of the frame region for the data hiding process is another fashion of the adaptive technique. Recently, Kumar et al. [16] deployed scale-invariant feature transform (SIFT) and speeded-up robust features (SURF) key points detection algorithms to find the ROI, where the encrypted secret data is embedded. Though this method is highly resilient against attacks, it performs poorly for uncompressed and low visual quality cover videos.

Format-based techniques. This is a video format-specific technique that uses the video coding standards for the data embedment process. Figure 3 is the general representation of the format-based steganography process. In this technique, the video coding processes such as intra-prediction, motion estimation, and DCT/DST coefficients are decoded, and the secret data is embedded in any of these processes. Once the secret data is embedded, it is again encoded to form the compressed version of the stego-video. The recent compression standard H.264/AVC gives a high video compression efficiency. This encoder is the most suited for network communication [30]. Many steganography techniques are designed for this video format. Flash video files (.FLV) are a simple and the most famous compression technique on social networks and have a better compression rate than other techniques. Mozo et al. [31] presented the uncomplicated FLV format-based steganographic system. This method uses the entire video tags of the file to embed the secret data. This addition does not modify the video/audio tags. Hence, the video quality is not affected and also provides huge embedding space. However, the imbalance between the cover and secret data size reduces tamper resistance.

Cover generation. All the above-mentioned steganography techniques use some carrier/cover medium to hide the secret message. However, in the cover generation techniques, the algorithm itself synthesizes a cover medium for communication. Sampat et al. [32] initiated this idea of generating dynamic cover videos. This process generates the cover video using a secret key and secret data itself. This process uses the function F(C, S), where F is the function to develop the cover file and C is the measure of sample required to hide the secret data S. This method acquires an image database to get frames for the cover video generation. However, this method is passive

as the selected frame/image sequence of the cover video is unrelated to each other. This may give a clue to the third party. This may be overcome by having images that are slightly relevant to each other or the slideshow/animation representation of images can be used rather than having an inappropriate video and audio file combination.

Convolutional neural network (CNN). The CNN-based methods have become a trend and are widely used in many video steganographic systems. Because CNN can effectively be applied in various procedures such as image classifications/ recognition, language processing, medical image processing, and recommendation system. This method is completely benefitted from encoder–decoder architecture. Wherein, the secret data and cover video/frames are given as inputs to the encoder to form stego-video. The decoder extracts the embedded secret data. This is the fundamental idea in all the methods. However, the way secret data and cover data are integrated differs from one another. This architectural variation is made in the number of layers used, pooling layer, strides, the convolutional layer, kernel size, activation function utilized, and loss function, etc. The only concern here is the size of secret data, and cover data has to be the same. For example, U-Net architecture-based encoder and decoder model is employed in many works [33–35] for data hiding. The main advantage of U-Net architecture is the improved resolution of the stego-medium as upsampling operators are used. Van et al. [36] suggested a hiding technique using U-Net (H-Net) and a retrieval method using R-Net. Here, rectified linear unit (ReLU) and batch normalization are used. Similarly, Wu et al. [36] proposed a separable convolution with residual block (SCR) for the embedding purpose. This method also uses batch normalization and Exponential Linear Unit (ELU). Generally, in video steganography, 3D convolutional layers are used. Mishra et al. [37] presented VStegNET-based video steganography where the cover video and secret data is given to the autoencoder network to generate stego-video. The reversed network framework is deployed in extracting the secret data.

General adversarial network (GAN). This is the deep level of CNN [38]. The game theory (GT) is the main component in a GAN architecture for training the generative model utilizing the adversarial processes. In the steganographic process, the GAN architecture contains three models such as generator (G), discriminator (D), and steganalyzer (S). The functionalities of these components include generating stego-medium from the cover frame and secret data, comparing the cover frame and stego-medium, and checking the secret data is robust, respectively. In GAN architecture, the models G, D, and S are considered as players and subjected to compete against each other [29] to produce high-quality stego-medium. Here, player G gets updated from the errors of players D and S. To produce a realistic stego-medium that is closely similar to the cover frame, the error of D and S should be minimized between (0, 1). Volkhonsiy et al. [39] used DCGAN-based steganographic system. It is a simple architecture having three models—G, D, and D. Similar to this, Shi et al. [40] proposed GAN model that has four fractional convolutional layers and one functional layer that uses hyperbolic tangent activation with base (WGAN). In this method, all three players compete against each other until ‘G’ generates high-quality stego-medium, while player ‘D’ recovers the secret data from the stego-medium. However, player ‘S’ steganlyzes on the player ‘G’ to get the probability of hidden

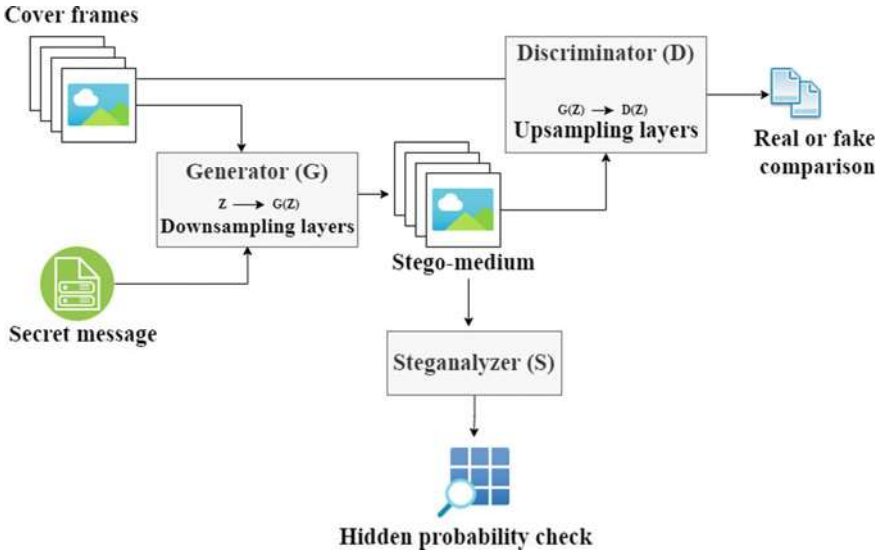

Fig. 4 Working model of GAN

information. Figure 4 is the general working algorithm of GAN as in [41]. Here, the generator fuses the frames of the cover video and secret message to produce stego-medium by downsampling the frames. The discriminator confronts the generator to find out the produced stego-medium is fake or not. The steganalyzer checks for the possibility of hidden information.

3 Quality Evaluation Techniques

In general, the performance of any steganography framework is examined in terms of imperceptibility, hiding capacity, and robustness. As the important requirement of steganography, imperceptibility must be analyzed meticulously. There are various metrics used for the evaluation of visual quality. The visual quality measurements are broadly classified into two types as follows: statistical error-based measurements and structural error-based measurements. The statistical error-based metrics calculate the quality value that differs from its standardized value. The difference between the calculated value and standard value is the error. Here, the error signal and the optical perception are reversely proportional to each other. These metrics use the mean square error to find the quality of the video. Mean square error (MSE), root mean square error, signal-to-noise ratio (SNR), peak signal-to-noise ratio (PSNR), weighted peak signal-to-noise ratio (WPSNR), video quality metric (VQM), normalized absolute error (NAE), normalized least square error (NLSE), and bit error rate (BER) are some of the statistical error-based metrics. Another category is structural

error-based metrics. This method complies with the fact that the HVS can easily draw out structural information than statistical information. Structural similarity index measure (SSIM), structural content (SC), normalized cross-correlation (NCC), and zero normalized cross-correlation (ZNCC) are some of the examples of this kind. All the above-discussed methods find the values for each frame of the video and take the average of it. Moreover, these metrics were designed for images initially. Thus, some video-specific metrics such as video quality measurement (VQM), weighted SSIM ($SSIM^{wt}$), video quality model—general (VQM_g), and moving pictures quality metric (MPQM) are designed to check particularly the video quality.

Robustness is another important requirement in steganographic methods. Wherein, robustness means the ability to recover the secret message at the receiver end without having any data loss despite the attacks in the network. Hence in the robustness analysis process, attacks are imposed on stego-video, and then the secret data is extracted to test its robustness. The metrics employed for imperceptibility analysis can also be used in robustness analysis too. The only difference is the input medium. In imperceptibility analysis, the entire cover medium and stego-medium are given as input data for all the metrics. Herein, robustness analysis, the original secret data, and the extracted secret data are the inputs for the metrics.

Next, the hiding capacity is yet another important feature that should be analyzed. Capacity is defined as the rate of secret data that can be embedded within the cover medium. Thus, hiding capacity calculates the secret data distribution rate across the cover pixels. Hence, the unit of hiding rate is bit per pixel (BPP). This calculation can be performed in two ways: overall capacity (HR_{oc}) and algorithm-provided capacity (HR_{ac}). The overall capacity is the hiding ratio of the secret data to the entire cover medium. On the other hand, the algorithm-provided capacity estimates the hiding rate within the Region of Interest (ROI), where the pixels are chosen for the embedding process by the steganography algorithm.

4 Conclusion

This paper presented an overview of steganography and its types and techniques. The paper was introduced with the significance, origin, description, and application of steganography. Then, the broad classifications of steganography based on the cover type were discussed. Various methods of steganography were presented, and technicality-based steganography methods were given special attention. Technical steganography is categorized into five major types: digital media, network, hardware, circuitry, and genome. This paper adopted video-specific digital media steganography techniques for reviewing. After carefully observing all the existing video steganography frameworks, the techniques are majorly grouped into seven types such as (1) substitution techniques, (2) transform domain techniques, (3) adaptive techniques, (4) format-based techniques, (5) cover generation, (6) convolutional neural network (CNN), and (7) general adversarial network (GAN). Each technique was thoroughly scrutinized and precisely presented in the paper. Finally, the

quality evaluation techniques used in analyzing the steganography framework were discussed.

From this survey, we noticed that all the techniques have their pros and cons depending upon the compatibility between the algorithm and the application in which it gets applied. Moreover, none of the reviewed techniques attains all the mentioned prerequisites such as imperceptibility, hiding capacity, and robustness. There is always some sort of imbalance between them. So it is recommended for the new steganography aspirant to focus more on providing a trade-off between these quality requirements while maintaining the algorithm and application agreement.

References

1. Patel A, Shah M, Chandramouli R, Subbalakshmi KP (2007) Covert channel forensics on the internet: issues, approaches, and experiences. Int J Netw Secur 5(1):41–50
2. Hamzah AA, Khattab S, Bayomi H (2019) A linguistic steganography framework using Arabic calligraphy. J King Saud Univ Comput Inf Sci
3. Shirali-Shahreza MH, Shirali-Shahreza M (2008) A new synonym text steganography. In: 2008 International conference on intelligent information hiding and multimedia signal processing. IEEE, pp 1524–1526
4. Wang F, Huang L, Chen Z, Yang W, Miao H (2013) A novel text steganography by context-based equivalent substitution. In: 2013 IEEE international conference on signal processing, communication and computing (ICSPCC 2013). IEEE, pp 1–6
5. Shirali-Shahreza M (2008) Text steganography by changing words spelling. In: 2008 10th international conference on advanced communication technology, vol 3. IEEE, pp 1912–1913
6. Murphy B, Vogel C (2007) The syntax of concealment: reliable methods for plain text information hiding. In: Security, steganography, and watermarking of multimedia contents IX, vol 6505. International Society for Optics and Photonics, p 65050Y
7. Lubacz J, Mazurczyk W, Szczypiorski K (2014) Principles and overview of network steganography. IEEE Commun Mag 52(5):225–229
8. Neuner S, Voyiatzis AG, Schmiedecker M, Brunthaler S, Katzenbeisser S, Weippl ER (2016) Time is on my side: Steganography in filesystem metadata. Digit Investig 18:S76–S86
9. Khan H, Javed M, Khayam SA, Mirza F (2011) Designing a cluster-based covert channel to evade disk investigation and forensics. Comput Secur 30(1):35–49
10. Johnson NF, Duric Z, Jajodia S (2001) Information hiding: steganography and watermarking-attacks and countermeasures: steganography and watermarking: attacks and countermeasures, vol 1. Springer Science & Business Media
11. Wang Z, Zhao X, Wang H, Cui G (2013) Information hiding based on DNA steganography. In: 2013 IEEE 4th international conference on software engineering and service science. IEEE, pp 946–949
12. Risca VI (2001) DNA-based steganography. Cryptologia 25(1):37–49
13. Chen S, Qu Z (2018) Novel quantum video steganography and authentication protocol with large payload. Int J Theor Phys 57(12):3689–3701
14. Sudeepa KB, Raju K, HS RK, Aithal G (2016) A new approach for video steganography based on randomization and parallelization. Procedia Comput Sci 78:483–490
15. Manisha S, Sharmila TS (2019) A two-level secure data hiding algorithm for video steganography. Multidimension Syst Signal Process 30(2):529–542
16. Kumar S, Soundrapandiyan R (2020) Robust approach of video steganography using combined keypoints detection algorithm against geometrical and signal processing attacks. J Electron Imaging 29(4):043007

17. Raja KB, Chowdary CR, Venugopal KR, Patnaik LM (2005) A secure image steganography using LSB, DCT and compression techniques on raw images. In: 2005 3rd international conference on intelligent sensing and information processing. IEEE, pp 170–176
18. Chae JJ, Manjunath BS (1999) Data hiding in video. In: Proceedings 1999 international conference on image processing (Cat. 99CH36348), vol 1. IEEE, pp 311–315
19. Yang M, Bourbakis N (2005) A high bitrate information hiding algorithm for digital video content under H. 264/AVC compression. In: 48th Midwest symposium on circuits and systems. IEEE, pp 935–938
20. Ramalingam M, Isa NAM (2016) A data-hiding technique using scene-change detection for video steganography. Comput Electr Eng 54:423–434
21. Mstafa RJ, Elleithy KM, Abdelfattah E (2017) A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC. IEEE access 5:5354–5365
22. Singh D, Singh B (2015) Data hiding in videos using background subtraction. In: 2015 2nd International conference on recent advances in engineering & computational sciences (RAECS). IEEE, pp 1–5
23. Chung KL, Chiu CY, Yu TY, Huang PL (2017) Temporal and spatial correlation-based reversible data hiding for RGB CFA videos. Inf Sci 420:386–402
24. Mstafa RJ, Elleithy KM (2016) A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes. Multimedia Tools Appl 75(17):10311–10333
25. Mansouri J, Khademi M (2009) An adaptive scheme for compressed video steganography using temporal and spatial features of the video signal. Int J Imaging Syst Technol 19(4):306–315
26. Fernando WAC (2006) Sudden scene change detection in compressed video using interpolated macroblocks in B-frames. Multimedia Tools Appl 28(3):301–320
27. Rajalakshmi K, Mahesh K (2018) Robust secure video steganography using reversible patch-wise code-based embedding. Multimedia Tools Appl 77(20):27427–27445
28. Hashemzadeh M (2018) Hiding information in videos using motion clues of feature points. Comput Electr Eng 68:14–25
29. Kumar S, Soundrapandiyan R (2021) A multi-image hiding technique in dilated video regions based on cooperative game-theoretic approach. J King Saud Univ Comput Inf Sci
30. Juurlink B, Alvarez-Mesa M, Chi CC, Azevedo A, Meenderinck C, Ramirez A (2012) Understanding the application: an overview of the h. 264 standard. In: Scalable parallel programming applied to H. 264/AVC decoding, pp 5–15
31. Mozo AJ, Obien ME, Rigor CJ, Rayel DF, Chua K, Tangonan G (2009) Video steganography using flash video (FLV). In: 2009 IEEE instrumentation and measurement technology conference. IEEE, pp 822–827
32. Sampat V, Dave K, Madia J, Toprani P (2012) A novel video steganography technique using dynamic cover generation. In: National conference on advancement of technologies–information systems & computer networks (ISCON–2012), Proceedings published in Int J Comput Appl (IJCA)
33. Wu P, Yang Y, Li X (2018) Image-into-image steganography using deep convolutional network. In: Pacific rim conference on multimedia. Springer, Cham, pp 792–802
34. Wu P, Yang Y, Li X (2018) Stegnet: mega image steganography capacity with deep convolutional network. Future Internet 10(6):54
35. Duan X, Jia K, Li B, Guo D, Zhang E, Qin C (2019) Reversible image steganography scheme based on a U-Net structure. IEEE Access 7:9314–9323
36. Van TP, Dinh TH, Thanh TM (2019) Simultaneous convolutional neural network for highly efficient image steganography. In: 2019 19th International symposium on communications and information technologies (ISCIT). IEEE, pp 410–415
37. Mishra A, Kumar S, Nigam A, Islam S (2019) VStegNET: video steganography network using spatio-temporal features and micro-bottleneck. In: BMVC, p 274
38. Pinson MH, Wolf S (2004) A new standardized method for objectively measuring video quality. IEEE Trans Broadcast 50(3):312–322

39. Volkhonskiy D, Borisenko B, Burnaev E (2016) Generative adversarial networks for image steganography
40. Shi H, Dong J, Wang W, Qian Y, Zhang X (2017) SSGAN: secure steganography based on generative adversarial networks. In: Pacific rim conference on multimedia. Springer, Cham, pp 534–544
41. Hayes J, Danezis G (2017) Generating steganographic images via adversarial training. arXiv preprint arXiv:1703.00371