

Video Steganography Techniques: A Survey

Kamred Udham Singh

Research Scholar

DST- Centre for Interdisciplinary Mathematical Science,

Institute of Science

Banaras Hindu University, Varanasi

kamredudhamsingh@gmail.com

Dr. Achintya Singhal

Assistant Professor

Department of Computer Science

Institute of Science

Banaras Hindu University, Varanasi

achintya.singhal@gmail.com

Abstract: In digital world, information security is the major issue in digital communication on a network from the third party hackers. Steganography techniques play an important role in information security. These are the secure techniques, used for concealing existence of secret information in any digital cover object *viz.* image, audio, video files. In last several decades, significant researches have been done on video and image steganography techniques because data embedding and data extraction is very simple. However, many researchers also take the audio file as a cover object where robustness and undetectability of information is very difficult task. The main objective of steganography is hiding the existence of the embedded data in any digital cover object. Steganography technique must be robust against the various image-processing attacks. Nowadays, video files are more accepted because of large size and memory requirements. This paper intends to provide a survey on video techniques and provide the fundamental concept of the steganography and their uses.

Keywords: *steganography, data hiding, spatial domain, Transform domain, DWT, DCT.*

1. Introduction

Steganography is the art and science for concealing the information in any digital object *viz.* image, video, and audio whereby only sender and receiver knows the existence of the hidden information [1]. Steganography word is derived from the Greek word *steganos*, it means, "covered or protected", and *graphia* meaning is "writing" which mean "Covered Writing". Last several centuries steganography has been used in different forms. The idea of steganography is thousands of years old. In the 5th century BC Histaiacus shaved a slave's head, tattooed the secret message on his skull when the hair grow again then the tattoo could not be seen and then slave was dispatched with the message [2] [3]. Receiver shaves the skull of slave and gets the message from the tattoo. In present digital scenario, it is very difficult to deliver a private information on a communication network in a safe and secured manner. Therefore, a secret communication is required to protect the information from third party attackers which is the difficult challenge of information security. Here a most important question arise that which method we choose for containing its integrity and degree of security. Several methods have been proposed for addressing the issue of information security like cryptography and steganography. Cryptography encrypt information in such form that it becomes meaningless to eavesdroppers using any encryption algorithms *viz.* RSA, Triple DES, Blowfish, Twofish, and AES but how strong is the encryption algorithm, it could be broken. Data can be easily replicated and distributed over the internet without owner's consent due to lack of security. Watermarking is used to protect the intellectual properties of digital content, in this technique a logo that contain owner information or bit of pattern is inserted in any digital object such as image, audio and video. Some important watermarking application is the protection of intellectual properties of digital content [4] [5] Moreover, in some situation it was necessary to distribution of information without anyone detecting that the communication happened.

Therefore, steganography comes arise in digital world to handle this case. Steganography developed driven by the necessity to conceal the existence of a secret data communication. Although both cryptography and steganography try to protect data, but neither technology alone is perfect but it is better to combine both approaches together to increase the information security. Consequently, it is better to combine both technique together to increase the degree of security of the system [6]. However, steganography is technique for the communication being between two parties. So main concern of steganography is to conceal the existence of the data communication and protecting the hidden data against any, alterations that may happen during communication such as format change or compression but integrity should be maintain. The major difference between Steganography and Cryptography is that the cryptography keeps the contents of information secret while steganography keeps the existence of information secret [7]. Maximum steganography techniques conceal the data inside an image because it is relatively simple to implement in images but nowadays, video files are more accepted because of large size and memory requirements. The figure 1 depicts the various information security disciplines. Applications and the fundamental of information insertion in cover object also depicted.

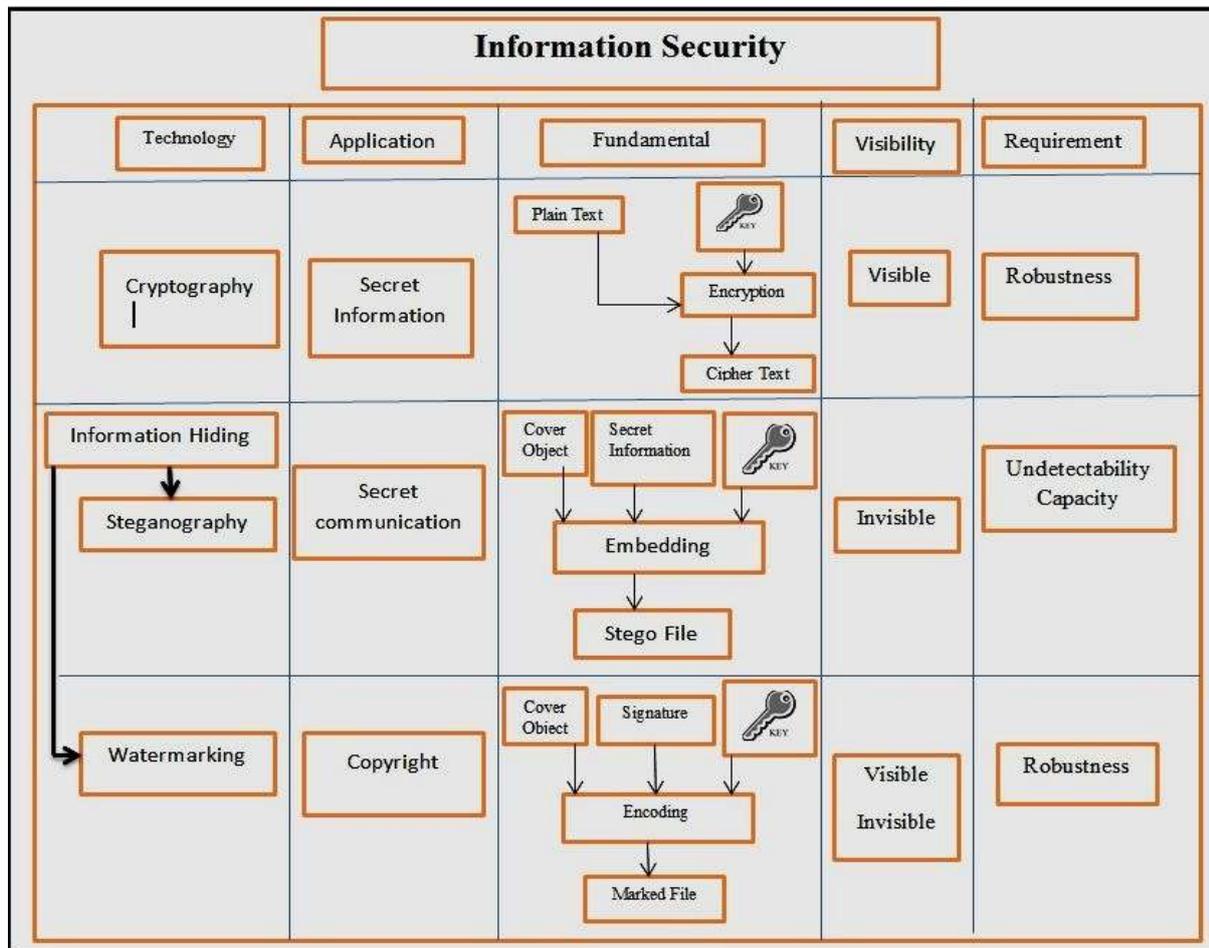


Figure 1. The different disciplines of information Security [8]

Steganography techniques can be classified on the basis of cover medium which is used for data embedding. The figure 2 depict the classification of the steganography. According to J. Fridrich linguistic steganography is a collection of techniques that allows to conceal information within texts based on some linguistic knowledge [9]. Linguistic steganography further categorized into semagrams and open codes. Technical steganography conceal information in digital cover object so it is categorized on the base of digital cover object viz. image, video, audio and text.

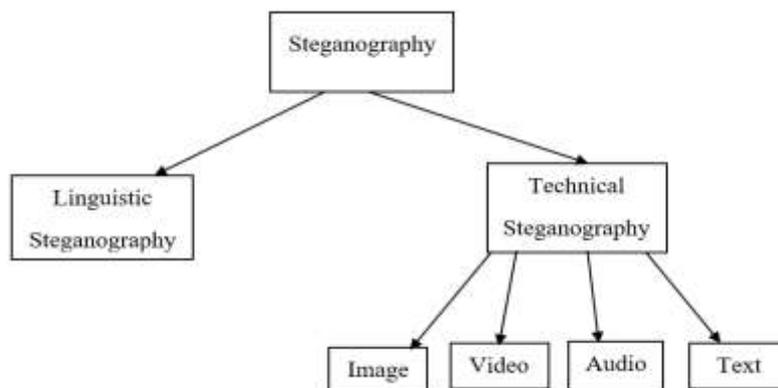


Figure 2. Classification of Steganography

2. Video Steganography Techniques

There are various applications such as intelligence agencies and military communications where video steganography can be employed [10]. Lie et al. [11], Yilmaz et al. [12] and Robie et al. [13] proposed another types of applications like video error

correction during communication and for transmitting additional information without requiring more bandwidth [14]. Video steganography was used for hiding data in a video captured by a surveillance system was demonstrated by Zhang et al. [15].

There are various signal processing transform like DWT, FFT and DCT, any one of them can be used as video steganographic technique to hide data in the frequency domain of the cover object. Secret data can be hide either on per pixel basis or group of pixels called blocks [16]. Video steganographic techniques can classify in a number of ways. Sherly et al. [17] categorize them according to compression, compressed techniques [18, 19] and uncompressed video techniques [21]. Video steganographic techniques can also be classified on the basis of domain of embedding, these are transform domain techniques [20, 22] and spatial domain techniques [23]. Shirali-Shahreza [24] stated that video steganographic techniques can be also categorized on the basis of considering the video as a sequence of still images [23, 25]. Or utilizing the video saving format for data hiding [26]. Or finding new dimensions in the video which helps in the steganographic process [18, 21]. The following figure depicts these possible classifications.

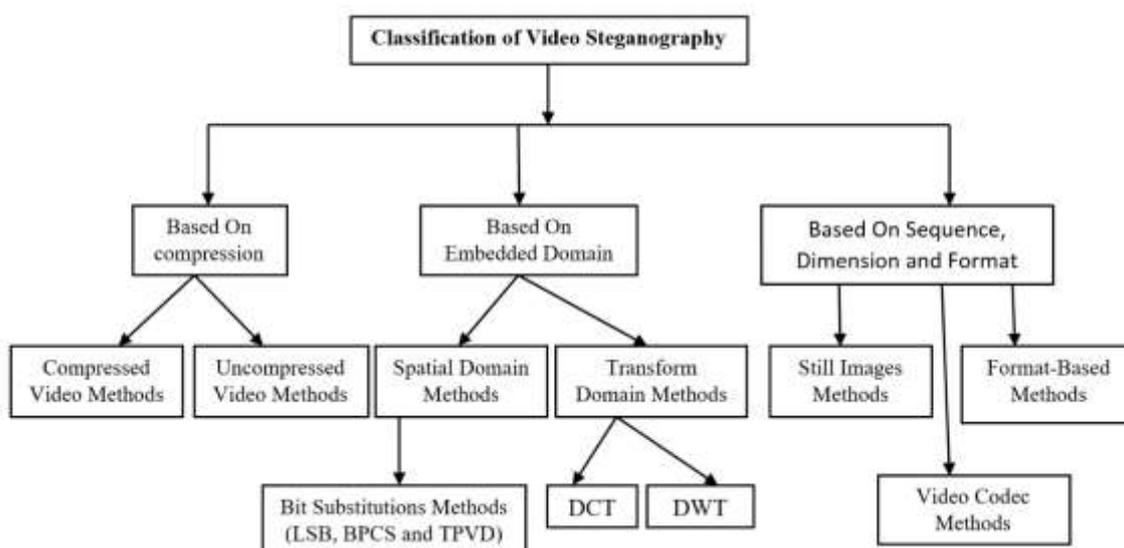


Figure 3: Various Classification of Video Steganography

The subsequent section will discuss classification based on embedded domain and covers most of the literatures in the area.

3. Bit Substitutions Methods

3.1 Least Significant Bit (LSB)

Bit Substitution-based steganography techniques replace the cover bit with the binary equivalent of secret data bit. The main advantages of bit substitution methods are the simple implementation and the high data hiding capacity in comparison to other techniques. Bit Substitution-based technique have many methods such as Least Significant Bit (LSB) method, Bit Plane Complexity Segmentation (BPCS) and Tri-way Pixel Value Differencing (TPVD) etc. Least significant bit (LSB) insertion is an oldest and most famous bit substitution-based approach for embedding data in a carrier file like video or image and it is capable of embedding huge secret data. Least significant bit technique operates by altering LSB bits of the cover file to conceal the secret data bit.

Most of the bit substitution-based methods that exist are really inspired by the LSB technique. Data hiding technique developed to hide the secret data in definite frames of the video file and in definite position of the frame by LSB substitution using different polynomial equation. In this technique data will be hidden on the basis of stego key which is in the form of polynomial equations with different coefficients [27]. A. T. Thahab [28] proposed Digital Color Video Steganography Using YCbCr Color Space and Dynamic Least Significant Bit technique is apply to hide video data file inside the other video cover object .This techniques also found on the basis of least significant bit algorithm.

3.2 Bit Plane Complexity Segmentation (BPCS)

Normally the idea behind the LSB technique is to modify the least significant bits of the pixel with the binary equivalent of secret data. If more significant bits are used to hide the data then it deteriorating the quality of image. Due to this disadvantage of this technique leads to evolution of other technique which trying to overcome this disadvantage. Kawaguchi and Eason

proposed Bit Plane Complexity Segmentation (BPCS) technique [29] and Chang et al. proposed Tri-Way Pixel-Value Differencing [30]. BPCS technique can be applied in the both spatial domain and transform domain [25] to address this problem. The basic idea of BPCS technique is to break down an image/frame into the bit planes and every bit plane treated as a slice of the image that is made up from all the bits of a definite significant location from each binary digit. Regions in the bit plane are categorized into informative and noise-like after those noise-like regions are substituted with the secret information and maintain the perceived quality. Jalab et al. [25] implemented the BPCS technique for hiding data in MPEG video format frames. This technique works in the YCbCr colour space instead of red, green and blue (RGB) components of a pixel for removing the correlation between the RGB and decreasing the distortion produced by data embedding process. It is well known that Human Visual System (HVS) are sensitive modifications in smooth parts than noise-like. Therefore, the BPCS method was applied for computing the complexity of every region in the cover frame. The complexity of every region of the bit plane is computed as the number of on edge transitions from 0 to 1 and 1 to 0, both vertically and horizontally.

3.2 Tri-way Pixel-Value Differencing (TPVD)

It is another bit substitution-based method is the Tri-way Pixel-Value Differencing (TPVD) [19], which is a modified form of the Pixel-Value Differencing method. To maintain the visual quality of cover object it is intuitive to think that data should be concealed in complex parts of the object. It hides the data in the difference of two neighbour pixels value, which are classified into ranges, larger range index shows a sharp area where more secret data can be concealed and smaller range index shows a smooth area where less secret data can be concealed. In the data hiding process first partitioning the cover object image/frame into non-overlapping chunks of two neighbour pixels and its range are determined. After that, number of secret data bits to be concealed is computed based on the range index. Lastly, the essential number of secret data bits is extracted from the secret data, corresponding their decimal value is used to generate a new difference, and the pixel values are adjusted accordingly. This method provides high capacity and imperceptibility for human vision of the concealed secret data. Sherly et al. [17] implemented this technique to hide data in MPEG compressed videos and stated that secret data are hidden in the macro-blocks of the ‘I’ frame with maximum scene modification and in macro-blocks of the P and B frames with maximum magnitude of motion vectors.

4. Transform domain techniques

Although, Bit substitution-based methods are the simplest way for data hiding, but vulnerability is main disadvantage to any cover alteration like compression, format change, etc. An attacker can easily crack this data embedding techniques. Transform domain methods are more complex than Bit substitution-based methods and try to improve the perceptual transparency and the robustness of the generated stego-objects. Any transform-domain technique contains of at least these phases, first transformed the cover object into the frequency domain, in second phase secret data is concealed in some or all of the transformed coefficients. In final phase, modified coefficients are transformed back to the original form of the cover. Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) are types of transform domain. Raja et al. [31] Stated that DFT methods introduce round-off errors, which do not make it ideal for data hiding applications. So due to this reason Discrete Fourier Transform methods are not popular in steganography. However, few techniques in steganography used DFT based steganography like McKeon [32] used the 2D DFT for steganography in videos.

4.1 Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) is a very popular transform and broadly used with image and video compression methods. Chae et al. [33] presented algorithms in this field using texture masking and multidimensional lattice structure and used MPEG-2 compressed videos. Secret data and the cover video frames both are transformed using 8×8 non-overlapping blocks. The secret data coefficients are quantized and then encoded by the multidimensional lattices, after that concealed into the cover frame DCT coefficients. Data hiding is adaptive to the local content of the video frame blocks. Steganographic techniques facing the challenge of improving the data embedding capacity without affecting visual quality. Large quantity of secret data can be embedding in the cover video is main objective of High bitrate techniques. Yang et al. [22] propose a high bitrate algorithm, which works on H.264/AVC Compressed videos. This method first convert the cover video frames to YUV colour space and then 1 data bit is embedded in each 4×4 DCT coefficient block. Strength points of this algorithm are large amount of data embedding capacity, robust to H.264 and MPEG-4 video compression techniques and tamper resistant. Figure 4 exhibits the use of DCT in video steganography techniques.

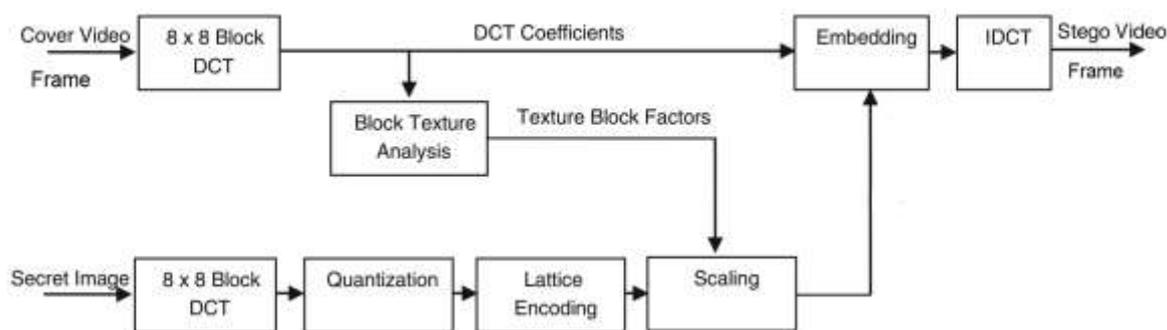


Figure 4: Data hiding process using DCT [7]

4.2 Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform (DWT) is popular in signal processing and video/ image compression. Wavelet transform fragmented a signal into a set of basic functions called wavelets. The DWT has many advantages over DCT like providing a multi-resolution description and permitting for better modelling of Human Visual System (HVS). DWT delivers a multi-resolution analysis that analyzes the signal at diverse frequencies produce different resolutions. Temporal resolution is main advantage of DWT. It captures frequency and frame location information. At each level of transformation, a frame which is transformed with Haar wavelet transform [34] is decomposed into four bands. One of them is approximation band, which represents the input frame after implementing a low pass filter and compressing it to half. Other remaining three bands are high pass filter and called detail band. High-resolution sub-bands permit simple detection of features like edges or textured parts in transform domain. DWT does not need to decompose the input cover object into non-overlapping 2-D blocks, which reduce the blocking artifacts.

Wavelet transform produces floating-point coefficients, which are used to perfectly rebuild the original signal. Some video steganography techniques trusted on the integer-to-integer wavelet transform. Xu et al. [21] proposed an approach on this technique. In proposed scheme data is embedded in the motion component of video due to these two reasons first is not more affected by compression and second is HVS are not more sensitive to catch the changes in motion areas of video. The methodology of this algorithm is that, in first step motion component of video is computed from frame-by-frame basis, after that computed motion component are decomposed in two-level wavelet decomposition. In last step secret data bit are concealed into low frequency coefficients which are based on the values of coefficients. This technique maintaining the quality of video after the data embedding process. Requires a cover video with large motion component because data hiding capacity is depend on motion component is the disadvantage of this algorithm.

4.3 Adaptive Steganographic Techniques

Adaptive steganography technique is a special case of the two former techniques which is also known as “Statistics-aware embedding” [35], “Masking” [36]. An adaptive technique basically implemented by studying the statistical structures of the cover object before changing with the secret data which helps to identify the best regions to embedded data [37]. Sur et al. [38] proposed an algorithm on temporal redundancy which select macro-blocks with low inter frame velocity and high prediction error as their regions-of-interest (ROI). Furthermore, the number of DCT coefficients used for data hiding is adaptively computed based on the relative stability of the prediction error block. This algorithm offers a very low data hiding capacity.

Mansouri et al. [18] proposed a technique, which combined the features of both spatial and temporal of the video and utilized a spatial key property. The objective of this technique is maximizing both perceptual invisibility and robustness by choosing frame regions, which are perceptually unimportant. High data hiding capacity as it uses both temporal and spatial features of the cover video stream is the main advantage of this algorithm.

5. Format-based techniques

In Format-based steganography techniques, various video formats have been use as cover objects from last decades. These techniques are basically designed for specific video formats viz. .FLV, .AVI, H.264, H.265. H.265/ HEVC (High Efficiency Video Coding) is the latest video compression standards and it is the new successor to Advanced Video Coding (AVC)/H.264, its video compression is better than H.264. H.265 is well adapted for network transmission and provides high compression efficiency [39] [40]. Ke et al. poposed a technique based on Context Adaptive Variable Length Coding (CAVLC) characteristics for H.264/AVC [38] and scheme is depict in figure 4. Priya S. et al. proposed a video steganography scheme for H.264, H.265, and

MJPEG [41]. Various H.264 and H.265 based technique are propose in the literature like Neufeld et al. [43], Liu et al. [44] Fallahpour et al. [45] and K Liao et al. [46]. Mozo et al. [26] proposed a steganography technique for .FLV video formats that is a popular video format on the internet. Author divide the secret message among the video tags of the entire file and adding them after each video tag in such a way that the actual video and audio tags are never modified.

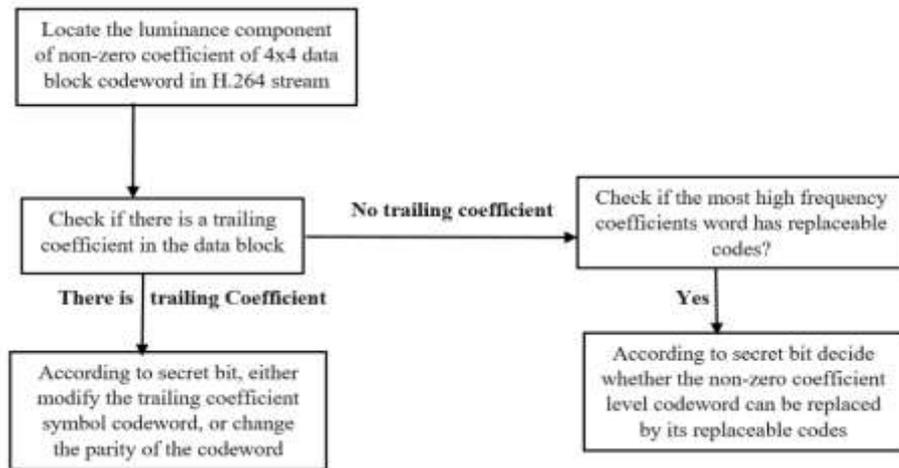


Figure 5: H.264/AVC data hiding algorithm [38]

6. Cover generation techniques

All traditional video steganography techniques, video file is use as a cover object to embedded the information. Sampat et al. [47] present a steganography technique based on video cover generation. Author use the secret key and secret message of own interest to generate the cover video. Video generation process use a function $X(A,D)$ where X is the function to generate the container file using partial message A is the number of samples required to hide the message and D is bits in message to be hidden. This technique requires a database of images for video generation. Advantage of cover generation technique is that sustenance of steganalysis which does not provide the attacker with the original images. Figure 6 depicts the inputs and pre-processing of the technique.

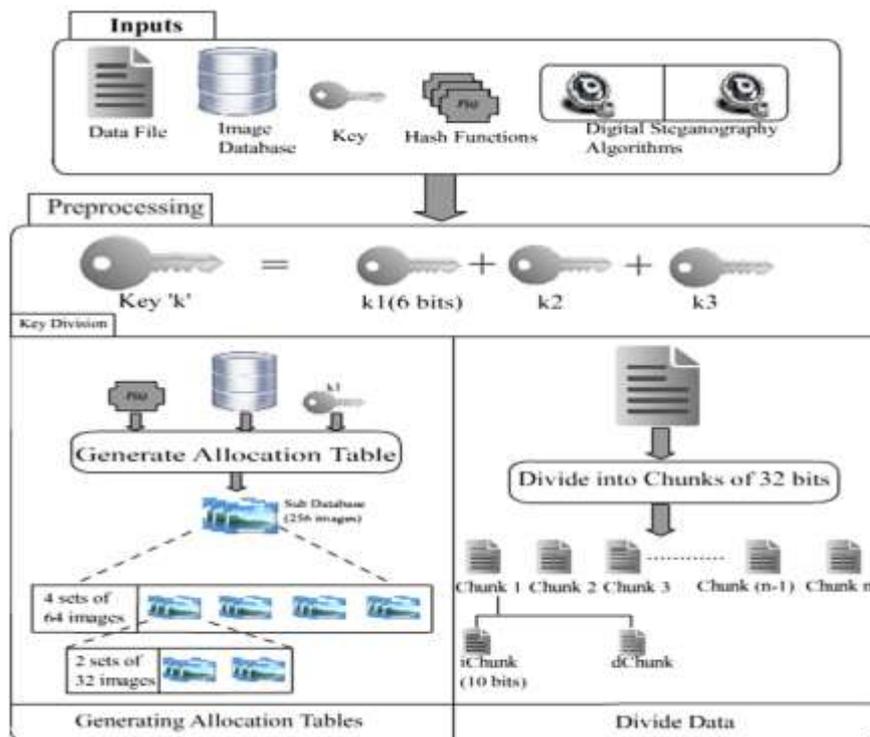


Figure 6: Cover generation technique: inputs and pre-processing [43]

7. Performance Measurement of Steganography Techniques

Performance of any video steganography technique is based on visual quality of the stego–video (cover video + message). Clearly, we can say that the quality of the original of cover video is slight change after secret data embedding in video but the alteration is not noticeable by the human eye. Now how can we decide that the existing steganography technique is perceptually transparent or not. So we calculate the standard metrics that can measure the changes in stego video, these metrics are only approximation to the human perception. HVS (Human Visual System) test is the first measurement of the quality of steganographic objects after embedding the hidden data [48]. These quality metrics are numerically estimate the quality of the video object and these quality metrics can be further divide into two approaches first is error-based approach and second is structural distortion approach. Mean Square Error (MSE) and Signal -to-Noise Ratio (SNR) are widely used as quality metrics due to their low computational complexity and simplicity. Basically, these metrics were initially designed for images so these are not excellent for videos. Two error-based metrics are specially designed for videos, first is Video Quality Metric (VQM) [49] and second is and Moving Pictures Quality Metric (MPQM) [50]. VQM measure that how much video is affected by various types of distortion whereas MPQM takes into consideration two human vision characteristics namely contrast sensitivity and masking [51]. Institute for Telecommunication Science (ITS) develop both VQM and MPQM. Some error-based quality metrics and their formulas are given in the table 1.

Quality Metric	Formula	Parameters
Signal-to-Noise Ratio (SNR)	$SNR = 10 * \log_{10} \frac{\sum_{i=1}^n \sum_{j=1}^m (A_{ij})^2}{\sum_{i=1}^n \sum_{j=1}^m (A_{ij} - B_{ij})^2}$	A _{ij} : one pixel in the cover image B _{ij} : one pixel in the stego-image
Peak Signal-to-Noise Ratio (PSNR)	$PSNR = 10 * \log_{10} \frac{(Max)^2}{\frac{1}{m * n} \sum_{i=0}^m \sum_{j=0}^n (A_{ij} - B_{ij})^2}$ $PSNR = 10 * \log_{10} \frac{(Max)^2}{MSE}$	A _{ij} : one pixel in the cover image B _{ij} : one pixel in the stego-image m*n: represent height and width of the image. Max: represent the maximum value of the colors which is 255
Mean Square Error (MSE)	$MSE = \frac{1}{m * n} \sum_{i=0}^m \sum_{j=0}^n (A_{ij} - B_{ij})^2$	A _{ij} : one pixel in the cover image B _{ij} : one pixel in the stego-image m*n: represent height and width of the image.
Root Mean Square Error (RMSE)	$RMSE = \sqrt{\frac{1}{m * n} \sum_{i=0}^m \sum_{j=0}^n (A_{ij} - B_{ij})^2}$	A _{ij} : one pixel in the stego-image B _{ij} : one pixel in the cover image m*n: represent height and width of the image.

Table 1: Some error-based quality metrics and their formulas

8. Conclusion

This paper presented a review on video steganographic techniques and the key algorithms of video steganography. Steganography, cryptography, and watermarking techniques and their differences is also discussed. An overview of steganography is presented and with focus on video steganography and its applications. Various video steganography techniques and classification of the existing video techniques are explained which are based on spatial domain, transform domain and other techniques. Advantages and disadvantages of these techniques are focused. Steganography techniques are mainly struggling for achieving a high data-embedding rate. It is a best cover object for information hiding because it have many outstanding features such as large capacity and good imperceptibility. This paper delivers effective review on the video steganography techniques.

References

- [1] R. Chandramouli and N. Memon, "Analysis of LSB Based Image Steganography" IEEE ICIP, pp. 1022-1022, Oct. 2001.
- [2] N.F. Johnson and S. Jajodia, Exploring steganography: Seeing the unseen, IEEE Computer, (1998) 26-34.
- [3] J.C. Judge, Steganography: Past, present, future. SANS Institute publication, http://www.sans.org/reading_room/whitepapers/steganography/552.php, 2001.
- [4] Horng S-J, Rosiyadi D, Fan P, Wang X, Khan MK (2013) An Adaptive Watermarking Scheme for e-government Document Images. Multimed Tools Appl. doi:10.1007/s11042-013-1579-5.
- [5] Horng S-J, Rosiyadi D, Li T, Takao T, Guo M, Khan MK (2013) A blind image copyright protection scheme for e-government. J Vis Commun and Image Represent 24(7):1099–1105.
- [6] Mercuri RT (2004) The many colors of multimedia security. Commun of the ACM 47(12):25–29.
- [7] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, October 2004

- [8] K.U. Singh (2014) A Survey on Audio Steganography Techniques. International Journal of Computer Applications (0975 – 8887) p.p.: 7-14.
- [9] Fridrich J (2004), Information Hiding: 6th International Workshop, IH 2004, Toronto, Canada, May 23-25 2004, Revised Selected Papers, Springer, New York, p 180.
- [10] Petitcolas FAP, Anderson RJ, Kuhn MG (1999) Information hiding-a survey. Proc IEEE 87(7):1062–1078
- [11] Lie W-N, Lin T-I, Lin C-W (2006) Enhancing video error resilience by using data-embedding techniques. IEEE Trans Circ Syst Video Technol 16(2):300–308
- [12] Yilmaz A, Alatan AA (2003) Error concealment of video sequences by data hiding. In: Proc. Of International Conference on Image Processing (ICIP) 3:II 679–682
- [13] Robie DL, Mersereau RM (2002) Video error correction using steganography. EURASIP J Adv Signal Process 2(1900):164–173
- [14] Stanescu D, Stratulat M, Ciubotaru B, Chiciudean D, Cioarga R, Micea M (2007) Embedding data in video stream using steganography. In: 4th International Symposium on Applied Computational Intelligence and Informatics (SACI'07) 241–244
- [15] Zhang W, Cheung SC, Chen M (2005) Hiding privacy information in video surveillance system. In: Proc. of the 12th IEEE International Conference on Image Processing 868–871
- [16] Ankur. M. Mehta, Steven Lanzisera and Kristofer. S. J, December 2008“Steganography 802.15.4 wireless communication “in conference Advanced Networks and Telecommunication Systems,2008. 2nd International Symposium, pp. 1-3.
- [17] Sherly AP, Amritha PP (2010) A Compressed Video Steganography using TPVD. Int J of Database Manag Syst 2 (3). doi:5121/ijdms.2010.2307 67
- [18] 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
- [19] Noda H, Furuta T, Niimi M, Kawaguchi E (2004) Application of BPCS steganography to wavelet compressed video. In: International Conference on Image Processing (ICIP'04) 2147–2150
- [20] Shou-Dao W, Chuang-Bai X, Yu L A High Bitrate Information Hiding Algorithm for Video in Video.
- [21] Xu C, Ping X (2007) A steganographic algorithm in uncompressed video sequence based on difference between adjacent frames. In: Fourth International Conference on Image and Graphics (ICIG) 297–30
- [22] YangM, 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 935–938
- [23] Eltahir ME, Kiah LM, Zaidan BB, Zaidan AA (2009) High rate video streaming steganography. In:International Conference on Future Computer and Communication (ICFCC 2009) 672–675
- [24] Shirali-Shahreza M (2006) A new method for real-time steganography. In: 8th International Conference on Signal Processing
- [25] Jalab H, Zaidan AA, Zaidan BB (2009) Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation. J Comput 1(1):108–113
- [26] Mozo AJ, Obien ME, Rigor CJ, Rayel DF, Chua K, Tangonan G (2009) Video steganography using flash video (FLV). In: Instrumentation and Measurement Technology Conference (I2MTC'09) 822–827
- [27] A. Swathi,S.A.K Jilani, " Video Steganography by LSB Substitution Using Different Polynomial Equations" , International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5.
- [28] A. T. Thahab, “Digital Color Video Steganography Using YCbCr Color Space and Dynamic Least Significant Bit” , Journal of Babylon University/Engineering Sciences/ No.(4)/ Vol.(22): 2014
- [29] Kawaguchi E, Eason RO (1999) Principles and applications of BPCS steganography. In: Photonics East(ISAM, VVDC, IEMB) International Society for Optics and Photonics 464–473
- [30] Chang K-C, Chang C-P, Huang PS, Tu T-M (2008) A novel image steganographic method using tri-way pixel-value differencing. J Multimed 3(2):37–44
- [31] Raja, K.B., Chowdary, C.R., Venugopal, K.R. &Patnaik, L.M. (2005) A secure image steganography using LSB, DCT and compression techniques on raw images. In: Proceedings of IEEE 3rd International Conference on Intelligent Sensing and Information Processing, 170–176.
- [32] McKeon RT (2007) Strange Fourier steganography in movies. In: IEEE International Conference on Electro/Information Technology 178–182.
- [33] Chae JJ, Manjunath BS (1999) Data hiding in video. In: Proceedings of International Conference on Image Processing (ICIP 99) 311–315
- [34] MulcahyC (1997) Image compression using theHaar wavelet transform. Spelman Sci andMath J 1(1):22–31
- [35] Provos N, Honeyman P (2003) Hide and seek: an introduction to steganography. Secur & Priv IEEE 1(3): 32–44
- [36] Johnson NF, Jajodia S (1998) Exploring steganography: seeing the unseen. IEEE Comput 31(2):26–34
- [37] Herrera-Moro DR, Rodríguez-Colín R, Feregrino-Uribe C (2007) Adaptive Steganography based on textures. In: 17th International Conference on Electronics, Communications and Computers (CONIELECOMP'07) 34–34
- [38] Sur A, Mukherjee J (2006) Adaptive data hiding in compressed video domain. In: Computer Vision, Graphics and Image Processing 738–748.
- [39] M. Tikekar, C. T. Huang, C. Juvekar, V. Sze and A. P. Chandrakasan, "A 249-Mpixel/s HEVC Video-Decoder Chip for 4K Ultra-HD Applications," in *IEEE Journal of Solid-State Circuits*, vol. 49, no. 1, pp. 61-72, Jan. 2014.

-
- [40] Y. Tew and K. Wong, "An Overview of Information Hiding in H.264/AVC Compressed Video," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 24, no. 2, pp. 305-319, Feb. 2014.
- [41] Priya S., Amritha P.P. (2016) Information Hiding in H.264, H.265, and MJPEG. In: Suresh L., Panigrahi B. (eds) Proceedings of the International Conference on Soft Computing Systems. Advances in Intelligent Systems and Computing, vol 398. Springer, New Delhi.
- [42] Ke N, Weidong Z (2013) A Video Steganography Scheme Based on H.264 Bitstreams Replaced. In: Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on 447–450
- [43] Neufeld A, Ker AD (2013) A study of embedding operations and locations for steganography in H.264 video. In: Proc. SPIE, Media Watermarking, Security, and Forensics 8665.
- [44] Liu Y, Li Z, Ma X, Liu J (2013) A robust data hiding algorithm for H.264/AVC video streams. *J Syst Softw* 86:2174–2183.
- [45] Fallahpour, M., Shirmohammadi, S., and Ghanbari, M. (2015) A high capacity data hiding algorithm for H.264/AVC video. *Security Comm. Networks*, 8: 2947–2955.
- [46] K Liao, L K and K Liao (2012)"Efficient information hiding in H.264/AVC video coding [J]"*Telecommunication Systems*, vol. 49, no. 2, pp. 261-269.
- [47] 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 of Comput Appl (IJCA)*.
- [48] Hmood AK, Kasirun ZM, Jalab HA, Alam GM, Zaidan AA, Zaidan BB (2010) On the accuracy of hiding information metrics: counterfeit protection for education and important certificates. *Int J Phys Sci* 5(7):1054–1062.
- [49] Pinson MH, Wolf S (2004) A new standardized method for objectively measuring video quality. *IEEE Trans Broadcast* 50(3):312–322
- [50] Van den Branden Lambrecht CJ, Verscheure O, Technology (1996) Perceptual quality measure using a spatiotemporal model of the human visual system. In: *Electronic Imaging: Science & Technology* 450–461.
- [51] Wang Y (2006) Survey of objective video quality measurements. EMC Corp Hopkinton, MA, 1748.