A Review on Video Steganography Techniques

Kamred Udham Singh

Research Scholar, DST- Centre for Interdisciplinary Mathematical Science, Faculty of Science, Banaras Hindu University, Varanasi.

Dr. Achintya Singhal

Assistant Professor, Department of Computer Science, Faculty of Science, Banaras Hindu University, Varanasi.

Abstract

In the era of information security, Steganography is a most secure method, used for concealing existence of secret data in any digital cover object such as image, audio, video and text files. In the last several decades broad research has been done on image steganography technique due to their easiness of data embedding and data extraction. Hide the existence of the embedded data in any digital object is the main objective of steganography. The main key factors of steganography are Undetectability, robustness and capacity of the concealed data that separate it from related techniques like cryptography and watermarking. Nowadays, video files are much more accepted because of large size and memory requirements. This paper intends to provide a survey on various video steganographic technique and covering its fundamental concepts.

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

Introduction

Today's digital world it is very important for secret communication of any private information in safe and secure manner, it has created new challenge of information security. Here a most important question arise that which method we choose for containing its integrity and degree of security. Severalmethods have been proposed for addressing the issue of information security like cryptography, steganography and watermarking. In Cryptography information encrypted in such form that it becomes meaningless to eavesdroppers using any encryption algorithms such as DES but how strong is the encryption algorithm, it could be broken. Data can be easily replicated and distributed without owner's consent due to lack of security. Watermarking modified the original data by embedding a watermark containing key information such as logo or copyright codes to protect the intellectual properties of digital content.Moreover, in some situation it was necessary todistributionof information without anyone detecting that the communication happened. So steganography comes arise in digital world to handle this case. Steganography technique is the art and science of invisible data communication. The word steganography originated from the Greek language and derived from two Greek words"stegos"which stands for "cover" and "grafia" which stands for "writing" [1].

Steganography developed driven by the necessity to conceal the existence of a secret data communication. Although steganography and cryptography both technique are try to protect data, but neither steganography nor cryptography alone is perfect. Consequently it is better to combine both technique together to increase the degree of security of the system [2]. Though 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 [3].

As video steganography is the focus of this review paper which can be viewed as an extension ofimage steganography. Really, video is a stream of a sequence of successive and equally time-spaced still images. Soseveral image steganographic techniques are relevant to videos as well. Hu et al. [28],], Langelaaret al. [38], Shang [74], and Sherlyetal [76] extended various image data hiding techniques to video.

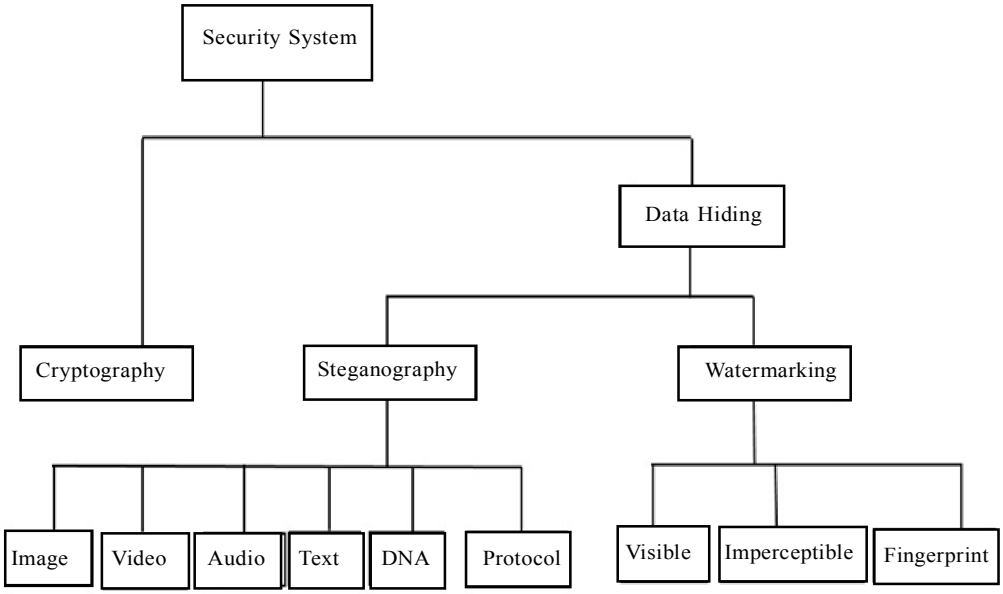

Figure 1: The different disciplines of information hiding [21]

Video Steganographic Techniques

There are various applications such as intelligence agencies and military communications where video steganography can be employed [4]. Lie et al. [5], Yilmaz et al. [6] and Robie et al. [7] proposed another types of applications like video error correction during communication and for transmitting additional information without requiring more band-width [8]. Video steganography was used for hiding data in a video captured by a surveillance system was demonstrated by Zhang et al. [9].

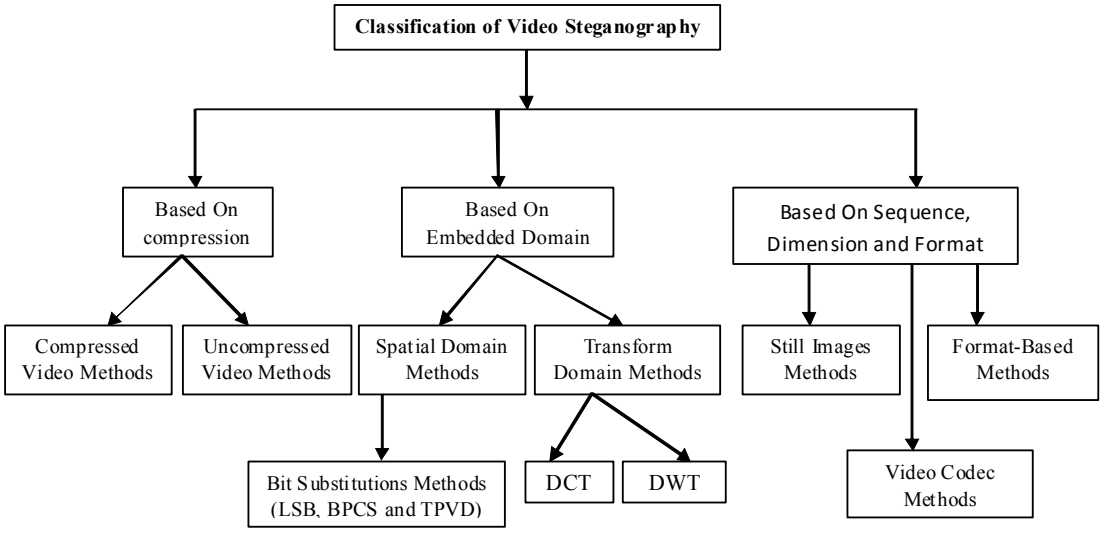

Figure 2: Various Classification of video Steganography

There are various signal processing transform like DWT, FFT and DCT, any one of them can be used as video stenographic 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 [10]. Video steganographic techniques can

classify in a number of ways. Sherly et al. [11] categorize them according to compression, compressed techniques [12, 13] and uncompressed video techniques [15]. Video steganographic techniques can also be classified on the basis of domain of embedding, these are transform domain techniques [14, 16] and spatial domain techniques [17]. Shirali-Shahreza [18] stated that video steganographic techniques can be also categorized on the basis of considering the video as a sequence of still images [17, 19]. Or utilizing the video saving format for data hiding [20]. Or finding new dimensions in the video which helps in the steganographic process [12, 15]. The fallowing figure depicts these possible classifications.

This paper will discuss classification based on embedded domain and cover-up all the literature related to video steganography.

Bit Substitutions Methods

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 carrierfile like video or image and it is capable of embedding huge secret data. Least significant bittechnique operatesby 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 bythe 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 techniquedata will be hidden on the basis of stego key whichis in the form of polynomial equations with different coefficients [22].A. T.Thahab [23] 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 alsofound on the basis of least significant bit algorithm.

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 bitsare 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 [24] and Chang et al. proposed Tri-Way Pixel-ValueDifferencing [25] .BPCS technique can be applied in the both spatial domain and transform domain [26,13]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 which is made up from all the bits of a definite significant location from each binary digit. Regions in the bit planeare categorized into informative and noise-like after that noise-like regions are substituted with the secret information and maintain the perceived quality. Jalab et al. [19] 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 also 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.

Tri-way Pixel-Value Differencing (TPVD)

It is another bit substitution-based method is the Tri-way Pixel-Value Differencing (TPVD) [13] 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 and 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. [11] 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.

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. This data embedding techniques can be easily cracked by an attacker. 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. [27] 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. But, few techniques in steganography used DFT based steganography like McKeon [28] used the 2D DFT for steganography in videos.

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. [29] presented an 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 8x8 ×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. A high bitrate algorithm is proposed by Yang et al. [16] 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 also tamper resistant.

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 which 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 [30] 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. [15] 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.

Adaptive Steganographic Techniques

Adaptive steganography technique is a special case of the two former techniques which is also known as ‘‘Statistics-aware embedding’’ [31], ‘‘Masking’’ [32]. 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 [33]. Sur et al. [34] 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. [12] 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.

Conclusion

This paper presents a short review onvideo steganographic techniques and the key algorithms of video steganography. Steganography, cryptography, and watermarking technique and their differences is also discussed. An overview of steganography is presented and mainlyfocus on video steganography and its applications. Various video steganography techniques and classification of the existing video techniques areexplained 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 good substitute channel for hide data in video files because it have many outstanding features such as large capacity and good imperceptibility.This paper delivers effective review on the design of a video steganographic system.

REFERENCES

1. Das R, Tuithung T (2012) A novel steganography method for image based on Huffman Encoding. In: 3rd National Conference on Emerging Trends and Applications in Computer Science (NCETACS) 14–18
2. Mercuri RT (2004) The many colors of multimedia security. Commun of the ACM 47(12):25–29
3. Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM, October2004
4. Petitcolas FAP, Anderson RJ, Kuhn MG (1999) Information hiding-a survey. Proc IEEE 87(7):1062–1078
5. Lie W-N, Lin T-I, Lin C-W (2006) Enhancing video error resilience by using data-embedding techniques.IEEE Trans CircSyst Video Technol 16(2):300–308

6. Yilmaz A, Alatan AA (2003) Error concealment of video sequences by data hiding. In: Proc. OfInternational Conference on Image Processing (ICIP) 3:II 679–682
7. Robie DL, Mersereau RM (2002) Video error correction using steganography. EURASIP Adv SignalProcess 2(1900):164–173
8. Stanescu D, Stratulat M, Ciubotaru B, Chiciudean D, Cioarga R, MiceaM (2007) Embedding data in videostream using steganography. In: 4th International Symposium on Applied Computational Intelligence andInformatics (SACI'07) 241–244
9. 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
10. 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.
11. Sherly AP, Amritha PP (2010) A Compressed Video Steganography using TPVD. Int J of Database ManagSyst 2 (3). doi: 5121/ijdms.2010.2307 67
12. Mansouri J, Khademi M (2009) An adaptive scheme for compressed video steganography using temporaland spatial features of the video signal. Int J Imaging SystTechnol 19(4):306–315
13. Noda H, Furuta T, Niimi M, Kawaguchi E (2004) Application of BPCS steganography to waveletcompressed video. In: International Conference on Image Processing (ICIP'04) 2147–2150
14. Shou-Dao W, Chuang-Bai X, Yu L A High Bitrate Information Hiding Algorithm for Video in Video.
15. Xu C, Ping X (2007) A steganographic algorithm in uncompressed video sequence based on differencebetween adjacent frames. In: Fourth International Conference on Image and Graphics (ICIG) 297–30
16. 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
17. 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
18. Shirali-Shahreza M (2006) A new method for real-time steganography. In: 8th International Conference onSignal Processing
19. Jalab H, Zaidan AA, Zaidan BB (2009) Frame selected approach for hiding data within MPEG video usingbit plane complexity segmentation. J Comput 1(1):108–113
20. Mozo AJ, Obien ME, Rigor CJ, Rayel DF, Chua K, Tangonan G (2009) Video steganography using flashvideo (FLV). In: Instrumentation and Measurement Technology Conference (I2MTC'09) 822–827
21. K.U. Singh (2014) A Survey on Image Steganography Techniques. International Journal of Computer Applications (0975 – 8887) p.p.: 10-20
22. A. Swathi,S.A.KJilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations", International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5.
23. A. T.Thahab, "Digital Color Video Steganography Using YCbCrColor Space and Dynamic Least Significant Bit", Journal of Babylon University/Engineering Sciences/ No.(4)/ Vol.(22): 2014
24. 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
25. Chang K-C, Chang C-P, Huang PS, Tu T-M (2008) A novel image steganographic method using tri-waypixel-value differencing. J Multimed 3(2):37–44
26. Jalab H, Zaidan AA, Zaidan BB (2009) Frame selected approach for hiding data within MPEG video usingbit plane complexity segmentation. J Comput 1(1):108–113
27. Raja, K.B., Chowdary, C.R., Venugopal, K.R. &Patnaik, L.M. (2005) A secure image steganography usingLSB, DCT and compression techniques on raw images. In: Proceedings of IEEE 3rd InternationalConference on Intelligent Sensing and Information Processing, 170–176.
28. McKeon RT (2007) Strange Fourier steganography in movies. In: IEEE International Conference onElectro/Information Technology 178–182.

29. Chae JJ, Manjunath BS (1999) Data hiding in video. In: Proceedings of International Conference on ImageProcessing (ICIP 99) 311–315.

30. MulcahyC (1997) Image compression using theHaar wavelet transform. Spelman SciandMath J 1(1):22–31.

31. Provos N, Honeyman P (2003) Hide and seek: an introduction to steganography. Secur&Priv IEEE 1(3):32–44.

32. Johnson NF, Jajodia S (1998) Exploring steganography: seeing the unseen. IEEE Comput 31(2): 26–34.

33. Herrera-Moro DR, Rodríguez-Colín R, Feregrino-Uribe C (2007) Adaptive Steganography based ontextures. In: 17th International Conference on Electronics, Communications and Computers(CONIELECOMP'07) 34–34.

34. Sur A, Mukherjee J (2006) Adaptive data hiding in compressed video domain. In: Computer Vision, Graphics and Image Processing 738–748.