

A Survey on Video Steganography based on Information Concealment using Abstraction and Rework Domain

Vivek Kumar Yadav¹ Sonu Lal²

¹M. Tech. Student ²Assistant Professor

^{1,2}Department of Digital Communication Engineering

^{1,2}IES College of Technology, Bhopal, India

Abstract— Steganography is the art and the science of secret communication, concealing the terribly existence of a communication. Nowadays, cover varieties can take several forms like text documents, audio tracks, digital pictures, and video streams. Since last decade, a wide range of experiments and analysis has been done on image steganography due to their widespread use on internet. At the present time, video files have become most attractive form of communication. These files transmitted very much frequently on social networking websites like Facebook and YouTube leading a need of innovation in video steganography. Data concealment in video includes various kinds of methods, every one among them has their merits and demerits. This work is all about to incorporating the latest developments and trends encyclopedic analysis on miscellaneous video steganographic ways present in the published writings past half decade. Moreover, since safety, security and resilience are vital issues in creating a desired steganographic algorithm, some relevant attacks and steganalysis techniques also are surveyed. The paper concludes with recommendations and smart practices drawn from the reviewed techniques.

Key words: Video Steganography, Information Concealment, Abstraction & Rework Domain, Resilience

I. INTRODUCTION

Cryptography is the initial technology that content owners used to prevent illegitimate data usage. It's the foremost common technique for insulating digital files & definitely one amongst the most effective methods evolved as a branch of science. Prior to transmission, the material is encoded i.e. encryption and the respective decryption key given solely to the persons who have authority to explore the admissible copies of the material. Then after, the encoded material may be circulated there with the help of the web, however would be futile to an attacker who don't have an acceptable key. Once encrypted, the structure of the message is modified. It's futile, meaningless and unintelligible unless it's decrypted [6].

The cryptosystems are classified in two categories: Asymmetric and Symmetric [6]. Same key is used in symmetric, referred as a secret key, used for encryption as well as decryption of message, and in asymmetric cryptosystems, one key is used to encrypt the message i.e. public key and another key used to decrypt the message i.e. private key. Asymmetric cryptosystems are referred to as open or public key cryptosystems too.

Symmetric cryptosystems have a major drawback: "how does one transport the key from the sender to the recipient firmly and in a very tamper proof way?" If someone can transmit the key firmly, in theory, he then would merely use that particular secure channel to transmit his data rather than encoding his data with symmetric

cryptosystems. Generally, certain trustworthy couriers units are provided as a solution to the present drawback.

A. Steganography: An overview

Steganography means that "covered writing". Covering-up the info in ways that stops the detection of hidden messages in the communication is the art it is [1]. At the starting, we are going to pioneer the basic terminologies exploited all through the paper in brief. The terminology "cover object" explains the file used for data concealment. The term "secret message" describes the information which is embedded within the cover object with the help of an embedding module. By combining the cover object and the embedded information, a "stego-object" is generated. For encrypting the secret message before embedding, an encryption key must be used. This secret key is termed as "stego-key". Moreover, the various attacks that attempt to destroy the steganographic algorithm is termed as "steganalysis". Fig. 1 shows a general steganographic model.

The design of an honest steganographic technique faces several challenges. The computational complexity of the algorithm used and whether the used algorithm is blind [2, 3, 4, 5] or non-blind must be considered. Sadly, most of the present algorithms don't discuss their procedure complexities. Mainly, there are four most vital challenges: robustness, tamper resistance, concealment capability and perceptual transparency. All of these characteristics are reciprocal to each other resulting to a dilemma in data hiding. Robustness is defined as the quantity of modification the stego-object can hold before some attacker destroys the hidden data [6]. Whereas, the difficulty for an adversary to alter the hidden message once it's been embedded within the cover object is referred as tamper resistance. On contrary, there is a trade-off between the other two i.e. the concealment capability and perceptual transparency. Once the concealment capability will increase, a smaller cover object might be used for concealment the secret message. This results a stego-object with a smaller size which will be simply transmitted over the web. However, increasing the concealment capability results in distortions within the stego-object. If an adversary acknowledges the distortion, then the presence of the hidden message is detected. And at that instant, steganography has failing because the secret communication was discovered.

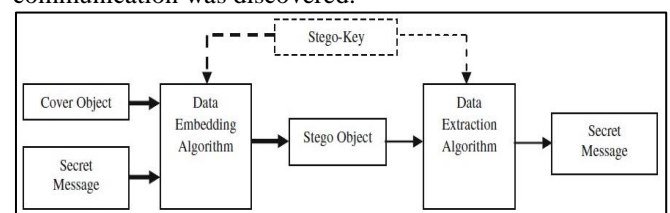


Fig. 1: General Steganographic model. Embedding process is represented with bold arrows, while extraction process is represented with non-bold arrows.

Video Steganography remains an untested field to a great extent. There are only few variety of commercial associations have brought out the necessities for testing steganography algorithms [5]. However, various creative watermarking methods have been presented in previous couple of years and most of them focussed on digital image watermarking, however only a few are wiped out the sphere of Steganography. In recent years, as Steganography techniques become a lot of mature, therefore investigator starts to explore a tougher analysis topic in Steganography. Most of the planned video Steganography schemes are supported by the techniques of image watermarking and directly applied to raw video or compressed video. However, current schemes aren't capable of either adequately protecting hidden information or maintaining the standard quality of the video.

Video Steganography introduces some problems those are not here in image steganography or Image watermarking that could be a similar counterpart to Steganography. Attributable to huge amounts of information and inherent redundancy among frames, video signals are extremely vulnerable to pirate attacks, together with frame averaging, frame dropping, frame interchanging, statistical analysis, etc. A most vital feature of steganography is perceptual transparency. Stego object's noticeable distortions might uncover the hidden communication. Putting a fixed cover image on each frame of the video ends up in issues of maintaining statistical and perceptual invisibleness. Hence, techniques have to be compelled to be developed to monitor a trade-off between them.

II. CLASSIFICATION OF STEGANOGRAPHY

Perceptual transparency is a vital aspect of steganography. Stego-object's distinguishable manipulations might reveal the hidden communication. This leads to certain steganographic techniques which follow a particular model that assists to choose the connotation of each of the pixels and the manipulation limit that the Human ocular system (HOS) cannot distinguish. These models are referred to as ocular masking models. These models utilize the psychological frameworks of the HOS to the application of masking effect. And they perpetually apply Just distinguishable difference (JDD) model. The utmost distortion that the human visual system cannot differentiate is termed as JND model. Wang et al. [26] enforced a visible masking model for pictures and videos that produces a connotation chart of the image/frame in terms of 8x8 pixels element blocks. Their model consists of three main components: Visual Attention Model (VAM), Weighing Model and Just noticeable difference (JND) model.

And Jia et al. [31] bestowed a difference threshold model particularly developed for videos. As for steganography concealment sorts, nearly any digital file set up will be exploited for this motive. However, in fact some set ups are highly desirable than others for this purpose. Knowledge of the fact that the first aim of any steganographic method is to maximise the concealing capability & to reduce the embedding manipulation lead us to utilize file set ups with larger unessential data.

The bits that can be changed without the change being detected easily in the object are called as redundant bits of that object [6]. According to the kind of the cover

objects, steganography can be classified into six main categories as illustrated in Fig. 3.

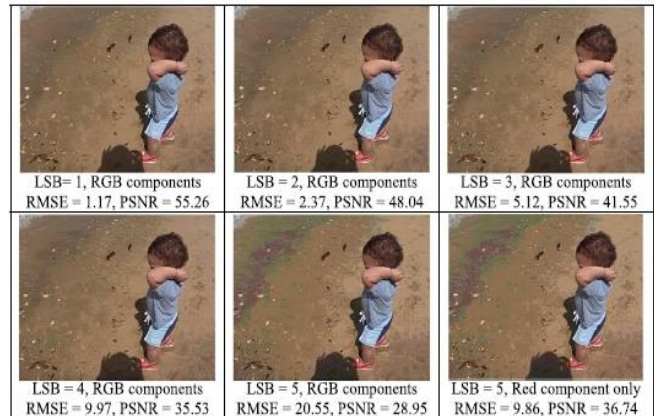


Fig. 2: Illustrates the resulted stego-frames using 1 to 5 least significant bits for hiding

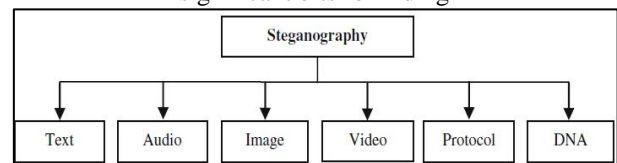


Fig. 3: Types of steganography according to the cover

A. Text Steganography

Text steganography may be a historic technique of steganography. Trendy techniques for text steganography embody line-shift encoding], word-shift secret writing and have specific secret writing. Recently, text steganography isn't used extensively. Text files have terribly restricted quantity of redundant knowledge leading to restricted concealment capability. Additionally, text files might be altered simply resulting in loss of the hidden message.

In metaphysics Technique, to insert data, rather than implicitly abandoning linguistics intact by substituting solely similar words an exact model for the definition is employed to judge consistency between texts. This technique is additionally having constant drawback like NICETEXT that generally it should turn out semantically wrong texts. In Text Steganography by concealment data in Particular Character of the Words method, particular letter from some explicit words are elite to conceal the data. For instance, the initial letter of each different word conceals the key message. Text Steganography with Line shifting method (LSM) is again a helpful method wherever lines are rearranged vertically to certain extent. For instance, lines are rearranged vertically to a certain degree let α or $-\alpha$. For α , the data is one and for $-\alpha$, it is zero. This technique is acceptable for written text. Data is hidden by making Spam Texts in a very hypertext mark-up language file. This approach uses the pliability of hypertext mark-up language concerning case-sensitiveness. By Word Shifting technique, data is hidden within the text by shifting words horizontally and by dynamical the space between the words. Feature cryptography technique alters the structure or aspects of the text to cover knowledge. For instance, stretching or compressing finish portion of certain letters, or by vertical movement of points of letters like 'i', 'j' etc. during this technique an outsized size of information is concealed within the text. By adding Open areas technique, the data is concealed by appending further white areas within the text.

B. Audio Steganography

When secret knowledge is embedded into digital sound, the technique is understood as audio Steganography. This technique embeds the key message in WAV, AU and MP3 sound files [8]. The key message is hid into the audio media by slightly dynamical the binary sequence of the audio file. So as to cover secret data with success, a variety of techniques for inserting data into digital audio are introduced. There are several steganographic techniques for concealment secret knowledge or messages in a very audio in a manner that the modifications created to the audio file are perceptually indiscernible. One amongst the common techniques is LSB cryptography.

Least important bit technique is that the easiest way to insert data in a very digital audio file. By work the smallest amount important little bit of every sampling purpose with a binary message, LSB cryptography permits for an outsized quantity of information to be encoded.

- One LSB: One least important bits of a sample are replaced with one message bits.
- Two LSB: Two least important bits of a sample are replaced with two message bits. This will increase the number of information which will be encoded however conjointly will increase the number of ensuing noise within the audio file yet
- Three LSB: Three least important bits of a sample are replaced with three message bits. This will increase the number of information and noise quite one and two LSB

C. Protocol Steganography

The term protocol Steganography is to embedding data at intervals of network protocols like TCP/IP. We have a tendency to hide data within the header of a TCP/IP packet in some fields which will be either nonobligatory or are never used.

D. Image Steganography

Image is the foremost common cover object used for steganography owing to having a large quantity of unnecessary information. A digital picture may be a cluster of numerals that denotes completely divergent light-weight intensities in varied parts of the picture. A matrix is made out from these numerals and every element on the matrix is named a picture element. There are various digital image file types. The foremost common types are Joint Photographic expert group (JPEG), Graphics Interchange Format (GIF) and Bitmap format (BMP). Completely distinct steganographic methods are there for these file types. For a comprehensive review & study on steganography in pictures, curious spectators may see [6].

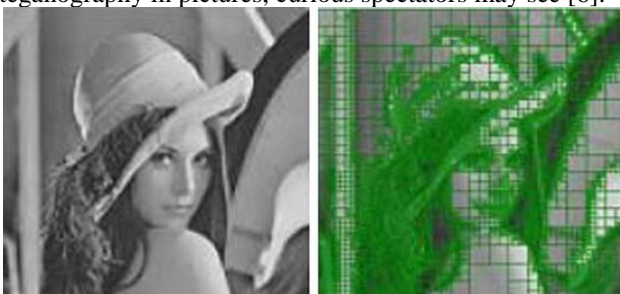


Fig. 4: (a) Original Image (b) resultant grid from partitioning overlaid on the original image

E. Video Steganography

Video steganography, which is the centre of interest of present work, might be seen as an associate degree enhancement of image steganography. Actually, the video stream composed of a sequence of successive and constantly time-spaced immobile pictures; generally along with sound. Therefore, several image steganographic methods are appropriate for videos yet. To verifying this fact Hu et al and Sherly et al [34], extended variety of image info concealment algorithms into video steganography. Video may be a terribly promising form of cover-media since it will carry an outsized quantity of secret knowledge. Additionally, video steganography is changing into important owing to the frequent use and recognition of videos over the web.

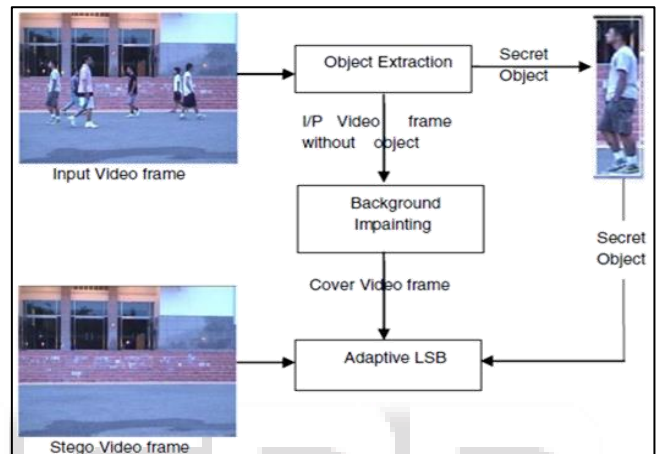


Fig. 5: Adaptive LSB Embedding Process: This figure shows the output stego frame after extracting all the objects in the input frame and embedding them in the background.

F. Networks Protocol steganography

Network Protocol steganography is another form of steganography, which refers to embedding secret info at intervals of network data packets. There are furtive channels within the layers of the OSI model wherever steganography is applied. For instance, Ahsan et al. utilized certain areas of the header of TCP/IP packets for concealment of knowledge. Mazurczyk et al. conferred the concept of retransmission steganography in which a packet received successfully is purposely not acknowledged to implore retransmission. During this case, the re-transmitted packet contains the hidden info rather than the original info.

G. DNA-based Steganography

Most recently, DNA-based steganography techniques truly gained plenty of attention. The high randomness in a very DNA sequence is used expeditiously to cover any message while not being detected. Therefore, DNA is certainly an excellent steganographic media, owing to its tremendous storage capability and also the ability to synthesize DNA sequences in any fascinating length.

III. BACKGROUND

The revolution in digital info has created new challenges for causation a message during a safe and secure approach. No matter technique we elect, the foremost vital problem is its level of safety. Varied methods are flourished for directing the problem of data safety like cryptography and

Steganography. Cryptography gives a noticeable perspective to safeguarding info. It disarranges the key info, in such a way that it converts into nonsense for pirates. However, it is often not continuously sufficient in application because the encoded material itself attracts attention. Regardless however sturdy is that the secret writing algorithmic rule, given enough time and tools, it might be broken. Moreover, some cases need causation info while not anyone pointing out that the communication has happened. In such cases, steganography was the solution.

Steganography is that the technique of hidden communication. The generation of the word steganography originated from the Greek language. It's developed from few Greek words "stegos" which suggests "cover" and "grafia" which suggests "writing" [7]. Steganography developed powered by the requirement to conceal the existence of a secret communication.

Even though cryptography and steganography attempt to defend information, however neither technology alone is ideal. Therefore, generally it's higher to mix each approaches along to extend the protection level of the system [8]. During this case, albeit the communication existence was detected and also the steganography was defeated, the offender still has got to break the secret writing to understand the message.

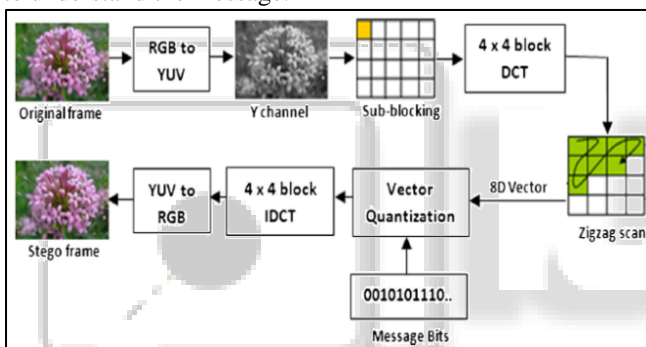


Fig. 6: Details Step of hiding information

PARAMETER	STEGANOGRAPHY	WATERMARKING
Goal	Conceal the existence of the communications	Protect the embedded content against intentional attacks for destruction or removal
Perceptual invisibility	Must Exist	Application dependent
Signature size	Large	Application dependent
Signature structure	May Change	Doesn't Change
Use of key	Optional	Optional
Output	Stego-file	Watermarked file
Goal fails when	Secret message existence is detected	Watermark is changed or removed
Challenges	Perceptual transparency, Hiding capacity and robustness	Robustness

Table 1: Comparison between Steganography and Watermarking

Watermarking is additional method that's subtly associated with steganography. However it is based on completely divergent ideologies and aims. Each methods plant data within the cowl so as to transmit this data unnoticeably. Whereas, in steganography, the communication is administered among 2 divisions. As a result, steganography is principally involved with hiding the presence of the communication and protective the hidden information against any alterations that will happen throughout transmission like format modification or compression. So steganography has restricted lustiness. On the opposite side, watermarking methods are applied once the quilt is accessible to the group who recognize the

existence of the hidden data and should try and destroy it. A very important watermarking application is that the protection of intellectual properties of digital content [9, 10, 11, and 12]. Thence the embedded data ought to be strong against intentional attacks that try and take away or modification the watermark [13]. The literature contains numerous watermarking techniques like [14, 15, 16, 17–19, 20, 21]

The past decade has seen growing interests in steganography, particularly in pictures and video. We have a tendency to found that almost all of the survey papers were dedicated to steganography in pictures and lacking a comprehensive review regarding the steganography in video. Al-Frajat et al. [5] solely presents a summary of the topic. During this Chapter, we have a tendency to gift a comprehensive review of the literature within the last ten years. Additionally some applications of video steganography area unit mentioned. A few pictures of covers area unit accustomed clarify the topic to the reader. Comparisons between the reviewed techniques in terms of benefits and downsides area unit provided. Eventually, we have a tendency to gift recommendations and sensible practices drawn from the reviewed techniques.

Video streams have high degree of spatial and temporal redundancy in illustration and have pervasive applications in lifestyle, so they're thought-about nearly as better option for concealing information.

Video steganography may be utilized in numerous helpful implementation. One usage is to employ video steganography for armed forces and intelligence, investigation agencies communications [23]. Another form of implementation was incontestable by Robie et al. [24], Yilmaz et al. [25] and Lie et al. [33], wherever information concealed in video was utilized for video error correction throughout transmission or for transmission further information (e.g. subtitles) while not requiring larger information measure [27]. A distinct implementation was conferred by Zhang et al. [35], wherever video steganography was utilized for activity information in a very video captured by a closed-circuit television. That is, so as to shield the privacy of licensed folks, their pictures are recovered from the police investigation video and hidden in its background. As a technique of property protection, digital watermarks have recently excited vital interest and become an awfully active space of analysis. Though watermarking may be a recent field of analysis, several techniques have already been projected each within the educational yet as within the trade.

Generally speaking, video steganography is that the extension of image steganography. A video file will merely be viewed as a sequence of pictures, yielding video information activity like image information activity. Although, there are several features that distinguish video steganography and image steganography. Because the video data is moving, less probabilities of perception of the concealed information in contrast with pictures. Additionally to the picture abuse that may be implemented on the isolated frames of video; there are rather more abuses for videos like lossy compression, modification of frame speed, formats swapping, addition or deletion of frames throughout video process. Administering a video stream as multiple two-dimensional pictures, doesn't take into account

the dependencies that exist among pixels in their three dimensions [29]. The activity capability is way higher within the case of video. Videos give new dimensions for information activity like activity messages in motion elements. The audio elements of the video file also can be utilized for information activity.

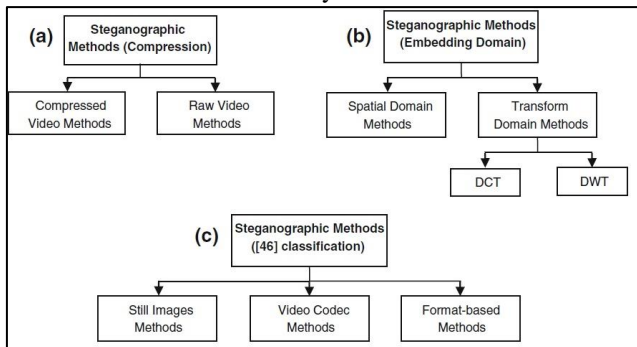


Fig. 6: Various classifications of Steganographic methods

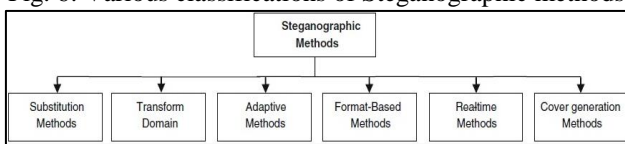


Fig. 7: Adopted classification for Steganographic methods

But as a result of the variety of the published methods, this analysis embraced a close categorization galvanized with the prevailing ones. Though, in some cases a definite categorization might not be attainable. Fig. 7 illustrates the selected categorization. Every subdivision can in short describe the final methodology and a few connected literature techniques.

IV. CONCLUSION

This paper proposed an all-inclusive review of video steganographic methods. Distinction among steganography cryptography and watermarking has been mentioned. An outline of steganography victimization completely divergent cowl varieties was conferred & remarkable recognition has been given to video steganography and its implementations. Varied categorizations of the prevailing methods were narrated. We have a tendency to adopt a categorization in line with the domain of embedding, during which strategies are classified into three classes: spatial domain methods, remodel domain methods, and alternative methods. Methods pertaining to every domain have been mentioned and contrast among those methods was also described with their virtues and drawbacks. Moreover, well-liked image and video quality metrics out there within the published documents were mentioned.

REFERENCES

[1] (2008) Objective Perceptual Multimedia Video Quality Measurement in the Presence of a Full-Reference, ITU-T Rec. J. 247
 [2] Abbass AS, Soleit EA, Ghoniemy SA (2007) Blind video data hiding using integer wavelet transforms. Ubiquit Comput Commun J 2(1)
 [3] Ahsan K, Kundur D (2002) Practical data hiding in TCP/IP. In: Proc. Of Workshop on Multimedia Security at ACM Multimedia

[4] Alattar AM, Alattar OM (2004) Watermarking electronic text documents containing justified paragraphs and irregular line spacing. In: Proc. of SPIE 685–695
 [5] Al-Frajat AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB (2010) Hiding data in video file: an overview. J of Appl Sci (Faisalabad) 10(15):1644–1649
 [6] Anderson RJ, Petitcolas FAP (1998) on the limits of steganography. IEEE J Sel Areas Commun 16(4): 474–481
 [7] Bailey K, Curran K (2006) an evaluation of image based steganography methods. Multimed Tools Appl 30(1):55–88
 [8] Balaji R, Naveen G (2011) secure data transmission using video Steganography. In: IEEE International Conference on Electro/Information Technology (EIT) 1–5
 [9] Calderbank AR, Daubechies I, Sweldens W, Yeo B-L (1997) Lossless image compression using integer to integer wavelet transforms. In: Proceedings of International Conference on Image Processing 596–599
 [10] Carli M, Campisi P, Neri (2006) A Data hiding driven by perceptual features for secure communications. In: International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICN/ICONS/MCL) 85–85
 [11] Chae JJ, Manjunath BS (1999) Data hiding in video. In: Proceedings of International Conference on Image Processing (ICIP 99) 311–315
 [12] Chandramouli R, Memon ND (2003) Steganography capacity: A steganalysis perspective. In: Proceedings of SPIE 173–177
 [13] 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
 [14] Chang F-C, Hang H-M, Huang H-C (2007) Layered access control schemes on watermarked scalable media. J VLSI Signal Process Syst Signal Image Video Technol 49(3):443–455
 [15] Channalli S, Jadhav A (2009) Steganography an Art of hiding data. Int J Comput Sci Eng (IJCSE) 1(3): 137–141
 [16] Cheddad A, Condell J, Curran K, Mc Kevitt P (2009) A skin tone detection algorithm for an adaptive approach to steganography. Signal Process 89(12):2465–2478
 [17] Cheddad A, Condell J, Curran K, Mc Kevitt P (2010) Digital image steganography: survey and analysis of current methods. Signal Process 90(3):727–752
 [18] 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
 [19] 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
 [20] Fridrich J, GoljanM, Du R (2001) Detecting LSB steganography in color, and gray-scale images. Multimed IEEE 8(4):22–28

- [21] Hamid N, Yahya A, Ahmad RB, Al-Qershi OM (2012) Image steganography techniques: an overview. *Int J Comput Sci Secur (IJCSS)* 6(3):p168–p187
- [22] Hanafy AA, Salama GI, Mohasseb YZ (2008) a secure covert communication model based on video steganography. In: *Military Communications Conference (MILCOM 2008)* 1–6
- [23] Handel TG, Sandford Li MT (1996) Hiding data in the OSI network model. In: *Proceedings of the First International Workshop on Information Hiding* 23–38
- [24] Robie DL, Mersereau RM (2002) Video error correction using steganography, *J Adv Signal Process* 2(1900): 164-173
- [25] Yilmaz A, Alatan AA (2003) Error concealment of video sequence by data hiding. In: *Proc. Of International Conference on Image Processing (ICIP)* 3:II 679-682
- [26] 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
- [27] 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
- [28] Hu S, KinTak U (2011) a Novel Video Steganography Based on Non-uniform Rectangular Partition. In: *IEEE 14th International Conference on Computational Science and Engineering (CSE)* 57–61
- [29] Huang H-C, Chu S-C, Pan J-S, Huang C-Y, Liao B-Y (2011) Tabu search based multi-watermarks embedding algorithm with multiple description coding. *Inf Sci* 181(16):3379–3396
- [30] 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
- [31] Jia Y, Lin W, Kassim AA (2006) Estimating just-noticeable distortion for video. *IEEE Trans Circ Syst Video Technol* 16(7):820–829
- [32] Johnson NF, Jajodia S (1998) Exploring steganography: seeing the unseen. *IEEE Comput* 31(2):26–34
- [33] 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
- [34] Sherly AP, Amritha PP (2012) A Compressed Video Steganography using TPVD. *Int J of Database Manag Syst* 2(3). Doi:5121/ijdms.2010.2307 67
- [35] 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* 868-871S
- [36] Mazurczyk W, MI S, Szczypiorski K (2011) Retransmission steganography and its detection. *Soft Comput J* 15(3): 505-515
- [37] Kim Y-W, Moon K-A, Oh I-S (2003) A text watermarking algorithm based on word classification and inter word Space statistics. In: *Proc. of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03)* 775–779
- [38] Langelaar GC, Lagendijk RL (2001) Optimal differential energy watermarking of DCT encoded images and video. *IEEE Trans Image Process* 10(1):148–158
- [39] Latif A (2013) an adaptive digital image watermarking scheme using fuzzy logic and tabu search. *J Inform Hiding and Multimed Signal Process* 4(4):250–271