International Journal of Engineering Technology and Applied Science

(ISSN: 2395 3853), Vol. 2 Issue 11 November 2016

A Survey on Video Steganography Based on Information Concealment using Spatial and Transform Domain

[1]Pratiksha Singh, [2]Sneha Singh, [3]Sushil Chaturvedi
[1]Mtech-Scholar, [2]Guide & HOD, [3]Co-Guide & Assistant Professor
[123]JNCT, REWA, INDIA

Abstract

Steganography is that the art and science of secret communication, concealing the terribly existence of a communication. Fashionable cowl varieties will take several forms like text documents, audio tracks, digital pictures, and video streams. In depth analysis has been done on image steganography within the previous decade attributable to their quality on the web. Nowadays, video files area unit drawing rather more attention. They're transmitted a lot of and a lot of frequent on web websites like Facebook and YouTube imposing a bigger sensible significance on video steganography. Info concealment in video includes a form of techniques, every of that has its strengths and weaknesses. This paper intends to supply AN up-to-date comprehensive review on the assorted video steganographic ways found within the literature within the last five years. What is more, since security and strength area unit important problems in coming up with an honest steganographic formula, some relevant attacks and steganalysis techniques also are surveyed. The paper concludes with recommendations and smart practices drawn from the reviewed techniques.

Keywords: video Steganography, information concealment, abstraction and rework domain, ability

1. INTRODUCTION

Cryptography is that the initial technology that content house owners would intercommunicate. It's in all probability the foremost common technique of protective digital documents and definitely one amongst the most effective developed as a science. Before delivery, the content is encrypted and also the decipherment secrets provided solely to those that have permission to access the legitimate copies of the content. Then, the encrypted file may be created out there through the web, however would be useless to a pirate while not acceptable key. Once encrypted, the structure of the message is modified. It's nonsensical and unintelligible unless it's decrypted [6].

There are a unit two varieties of cryptosystems: parallel and uneven [6]. Parallel cryptosystems use an equivalent key, referred to as the key, to inscribe and decode a message, and uneven cryptosystems use one key, named as public key, to inscribe a message and a unique key, named as personal key, to decode it. Uneven cryptosystems also are referred to as public key cryptosystems.

Symmetric cryptosystems have a problem: "how does one transport the key from the sender to the recipient firmly and in a very tamper proof fashion?" If you'll send the key firmly, in theory, you then would merely use that secure channel to send your message rather than encrypting your message with parallel cryptosystem. Commonly, trustworthy couriers area unit used as an answer to the present drawback.

1.1 Steganography overview

Steganography means that "covered writing". It's outlined because the art of concealment info in ways in which stop the detection of hidden messages [1]. At the start, we tend to shortly introduce the language used throughout the paper. The term "cover object" describes the file used for concealment info. The "secret message" refers to the info that's embedded within the cowl through an embedding module. A "stego-object" is created combining the duvet object with the embedded information. Just in case of encrypting the key message before embedding, associate secret writing secret's used. This secret's stated as "stego-key". What is more, the term "steganalysis" refers to the various attacks that attempt to break the steganographic formula. Figure 1 shows a general steganographic model.

The design of an honest steganographic technique faces several challenges. The formula's procedure complexness and whether or not the algorithm is blind [2, 3, 4, 5] or non-blind ought to be thought-about. Sadly, most of the present algorithms don't discuss their procedure complexness. Mainly, there are a unit four challenges: strength, tamper resistance, concealment capability and sensory activity transparency. All of those aspects area unit reciprocally proportional to every alternative making the info concealment quandary. Strength is that the quantity of modification the stego-object may face up to before associate mortal destroys the hidden info [6]. Whereas tamper resistance is that the problem for associate wrongdoer to vary the key message once it's been embedded within the cowl object. On the opposite hand, there's a trade-off between the concealment capability and also the sensory activity transparency. Once the concealment capability will increase, a smaller cowl object might be used for concealment the key 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 associate wrongdoer acknowledges the distortion, then the presence of the hidden message is detected. And at that time, steganography has failing because the secret communication was discovered.

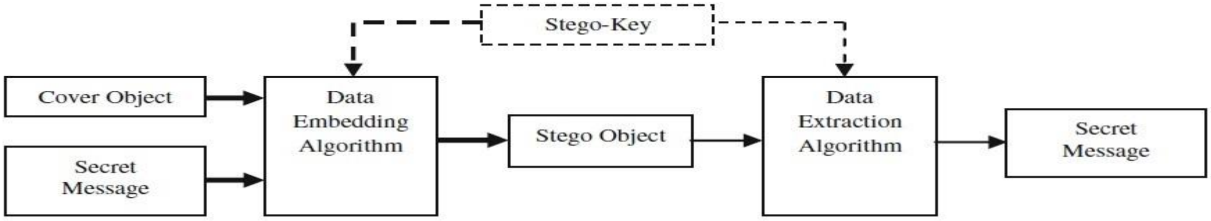

Fig. 1 General steganographic model. Embedding process is represented with bold arrows, while extraction process is represented with non-bold arrows.

Video Steganography remains a for the most part untested field. There’s solely an awfully few variety of commercial associations have printed the necessities for testing steganography algorithms [5]. However, variant various creative watermarking approaches are planned in previous couple of years and most of them focus of 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 area unit supported the techniques of image watermarking and directly applied to raw video or compressed video. However, current schemes aren't capable of either adequately protective hid information or maintain the standard of the Video.

Video Steganography introduces some problems that isn't gift in image steganography or Image watermarking that could be a similar counterpart to Steganography. Attributable to massive amounts of information and inherent redundancy between frames, video signals area unit extremely vulnerable to pirate attacks, together with frame averaging, frame dropping, frame swapping, applied mathematics analysis, etc. sensory activity transparency is an especially vital feature of steganography. Stego object noticeable distortions might uncover the key communication. Applying a set cowl image to every enclose the video ends up in issues of maintaining applied mathematics and sensory activity invisibleness. Thence techniques have to be compelled to be developed to keep up a trade-off between each.

1.2 SORTS OF STEGANOGRAPHY

Perceptual transparency is an especially vital feature of steganography. Stegoobject noticeable distortions might uncover the key communication. As a result some steganographic techniques follow a particular model that helps to choose the connation of every of the pixels and therefore the distortion level that the Human sensory system (HVS) cannot discover. These models area unit referred to as visual masking models. They create use of the physiological &amp; psychological mechanisms of the HVS to try and do the masking impact. And that they perpetually use simply noticeable distinction (JND) model. Difference threshold is outlined as most distortion the human sensory system cannot understand. Wang et al. [18] enforced a visible masking model for pictures and videos that generates a connation map of the image/frame in terms of 8x8 picture element blocks. Their model consists of three main components: difference threshold Model, Visual Attention Model (VAM) and deliberation Model.

While Jia et al. [31] bestowed a difference threshold model specifically designed for videos. As for steganography cowl sorts, nearly any digital file format will be utilized for this purpose. However in fact some formats area unit a lot of applicable than others for this job. Knowing that the first goal of any steganographic technique is to maximise the concealing capability and to reduce the embedding distortion, guide North American country to use file formats with higher redundancy.

The redundant bits of Associate in Nursing object area unit those bits that may be altered while not the alteration being detected simply [6]. Supported the kind of the quilt object, steganography will be divided into six main sorts as illustrated in Figure 2.

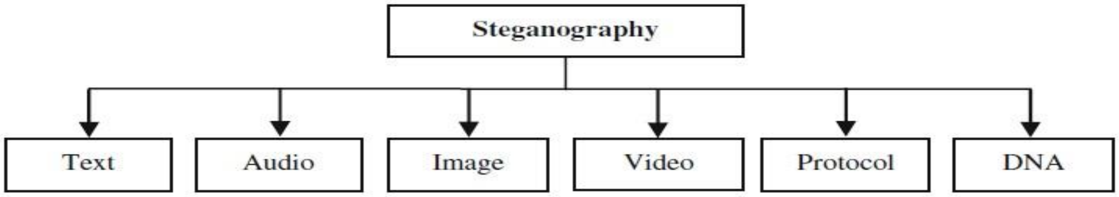

Fig 2 Types of steganography according to the cover

1.2.1 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 effort linguistics intact by substitution solely synonymous words an exact model for which means is employed to judge equivalence between texts. This technique is additionally having constant disadvantage like NICETEXT that generally it should turn out semantically incorrect texts. In Text Steganography by concealment data in Specific Character of Words approach, specific characters from some explicit words are elite to cover the data. For instance, the primary character of each different word hides the key message. Text Steganography by Line Shifting technique (LSM) is another helpful approach wherever lines are shifted vertically to some extent. For instance, lines are shifted vertically to degree say α or – α. For α, the data is one and for – α, the data 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 changes the feature or structure of the text to cover knowledge. For instance, elonging or shortening finish portion of some characters, or by vertical displacement of points of characters like ‘i’, ‘j’ etc. during this technique an outsized volume of information is hidden within the text. By adding Open areas technique, the data is hidden by adding further white areas within the text.

1.2.2 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.

a) One LSB: One least important bits of a sample are replaced with one message bits.

b) 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

c) 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

1.2.3 Protocol Steganography

The term protocol Steganography is to embedding data at intervals 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.

1.2.4 Image Steganography

Images are the foremost common cowl objects used for steganography owing to having a large quantity of redundant knowledge. A digital image may be a cluster of numbers that represent completely different light-weight intensities in varied areas of the image. A grid is made out from these numbers and every purpose on the grid is named a picture element. There are varied digital image file formats. The foremost common are Joint Photographic specialists cluster (JPEG), electronic image format (BMP) and Graphics Interchange Format (GIF). Completely different steganographic techniques exist for these file formats. For a close survey on steganography in pictures, interested readers will talk to [6].

1.2.5 Video steganography

Video steganography, which is that the focus of this work, is viewed as associate degree extension of image steganography. In fact, a video stream consists of a series of consecutive and equally time-spaced still images; generally accompanied with audio. Therefore, several image steganographic techniques are applicable to videos yet. Hu et al and Sherly et al. [34], extended variety of image knowledge concealment algorithms to video Steganography proving this truth. 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.

1.2.6 Protocol steganography

Protocol steganography is another form of steganography, which refers to embedding secret knowledge at intervals network packets. There are covert channels within the layers of the OSI network model wherever steganography is used. For instance, Ahsan et al. used some fields from the header of TCP/IP packet for concealment knowledge. Mazurczyk et al. conferred the concept of retransmission steganography wherever a with success received packet is purposely not acknowledged to invoke retransmission. During this case, the re-transmitted packet carries the key knowledge rather than the first knowledge.

1.2.7 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 may be a excellent steganographic media, owing to its tremendous storage capability and also the ability to synthesize DNA sequences in any fascinating length.

1.3 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 question is its degree of security. Varied approaches are developed for addressing the problem of data security like cryptography and Steganography. Cryptography provides a noticeable approach to securing info. It scrambles the key message, such it becomes nonsense to eavesdroppers. However, this is often not continuously adequate in apply because the encrypted content 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 noticing that the communication happened. In such cases, steganography was the solution.

Steganography is that the art and science of invisible communication. The origin of the word steganography comes from the Greek language. It’s derived from two Greek words “stegos” which suggests “cover” and “grafia” which suggests “writing” [7]. Steganography evolved driven by the requirement to activity the existence of a secret communication.

Although cryptography and steganography try and 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 communications existence was detected and also the steganography was defeated, the offender still has got to break the secret writing to understand the message.

Table 1 Comparison between Steganography and Watermarking

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

Watermarking is another technology that's closely associated with steganography. However it lies on completely different philosophies and goals. Each technologies plant data within the cowl so as to send this data unnoticeably. However, in steganography, the communication is administered between 2 parties. As a result, steganography is principally involved with concealing the existence of the communication and protective the embedded information against any modifications that will happen throughout transmission like format modification or compression. So steganography has restricted lustiness. On the opposite hand, watermarking techniques area unit used once the quilt is accessible to parties World Health Organization 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. [22] 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 good candidates for activity information.

Video steganography may be then utilized in numerous helpful applications. One application is to use video steganography for military and intelligence agencies communications [23]. Another form of application was incontestable by Robie et al. [24], Yilmaz et al. [25] and Lie et al. [26], wherever information activity in video was used for video error correction throughout transmission or for transmission further information (e.g. subtitles) while not requiring larger information measure [27]. A distinct application was conferred by Zhang et al. [28], wherever video steganography was used 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 area unit extracted from the police investigation video and embedded 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. However, there are a unit several aspects that differentiate between video steganography and image steganography. Because the video content is dynamic, lower probabilities of detection of the hidden information compared with pictures. Additionally to the image attacks that may be applied on the separate frames of video; there are a unit rather more attacks for videos like lossy compression, modification of frame rate, formats interchanging, addition or deletion of frames throughout video process. Handling 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.

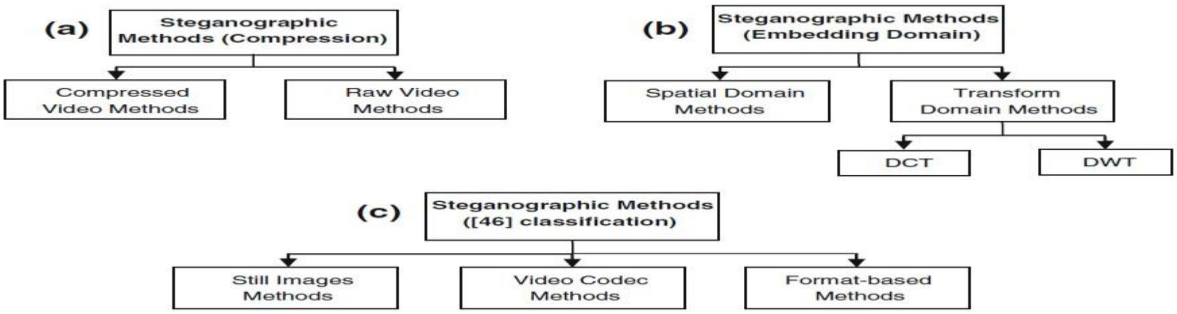

Fig. 3. **Various classifications of Steganographic methods**

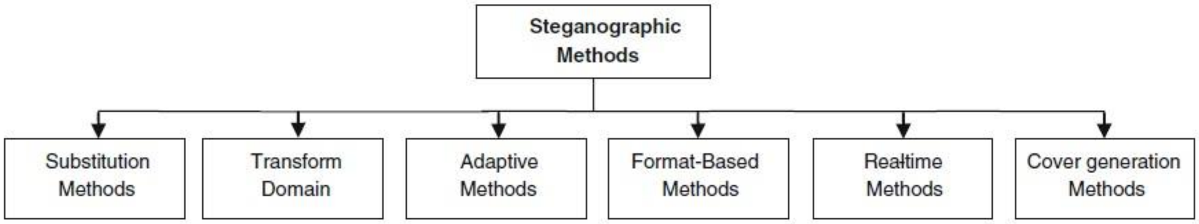

Fig. 4 Adopted classification for Steganographic methods

But as a result of the variety of the literature techniques, this survey adopted a close classification galvanized from the prevailing ones. Though in some cases a definite classification might not be attainable. Figure four illustrates the chosen classification. The remainder of this section is organized as follows: the reviewed techniques are mentioned in six subsections. Every subdivision can in short describe the final methodology and a few connected literature techniques.

1.4 CONCLUSION

This paper presents a comprehensive review of video steganographic techniques. Distinction between steganography, cryptography, and watermarking were mentioned. An outline of steganography victimization completely different cowl varieties was conferred and special attention was paid to video steganography and its applications. Varied categorizations of the prevailing techniques were illustrated. We have a tendency to adopt a categorization in line with the domain of embedding, during which strategies area unit classified into three categories: spatial domain techniques, remodel domain techniques, and alternative techniques. Techniques happiness to every domain were mentioned and comparisons between those techniques were conferred lightness their blessings and disadvantages. Moreover, well-liked image and video quality metrics out there within the literature were mentioned. Finally, steganalysis was surveyed from the purpose of read that improves the look of fine steganographic systems.

1.5 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. UbiquitComputCommun J 2(1)
3. Ahsan K, Kundur D (2002) Practical data hiding in TCP/IP. In: Proc. OfWorkshop 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 ApplSci (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 ComputSciEng (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 ComputSciSecur (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 Ii MT (1996) Hiding data in the OSI network model. In: Proceedings of the First International Workshop on Information Hiding 23–38

24. 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

25. 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

26. Horng S-J, Rosiyadi D, Fan P, Wang X, Khan MK (2013) An Adaptive Watermarking Scheme for egovernment
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. InfSci 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 CircSyst Video Technol 16(7):820–829

32. Johnson NF, Jajodia S (1998) Exploring steganography: seeing the unseen. IEEE Comput 31(2):26–34
33. Johnson NF, Jajodia S (1998) Steganalysis: The investigation of hidden information. In: Information Technology Conference 113–116
34. Katzenbeisser S and Petitcolas F (2000) Information Techniques for Steganography and Digital Watermarking. Artec House
35. 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
36. 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
37. Kim Y-W,Moon K-A, Oh I-S (2003) A text watermarking algorithm based on word classification and interword
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