International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

AN OVERVIEW OF HIDING INFORMATION IN H.264/AVC COMPRESSED VIDEO

D. Vetriselvi[1], S. Nandhinee [2], S. Lathika [3]

[1]Assistant Professor, Computer Science Department, JEPPIAAR SRR Engineering College, Tamil Nadu
[2,3]UG Student, Computer Science Department, JEPPIAAR SRR Engineering College, Tamil Nadu

---

Abstract - *Information activity refers to the method of inserting data into a bunch to serve specific purpose(s).In this article, data activity strategies within the H.264/AVC compressed video domain square measure surveyed. First, the final framework of data activity is conceptualized by relating state of AN entity to a that means (i.e., sequences of bits).This concept is illustrated by victimization numerous knowledge illustration schemes like bit plane replacement, unfold spectrum, bar graph manipulation, quality, mapping rules and matrix encryption. Venues at which information hiding takes place are then identified, including prediction process, transformation, quantization and entropy coding .Related data activity strategies at every venue square measure concisely reviewed, along with the presentation of the targeted applications, appropriate diagrams and references .A timeline diagram is built to chronologically summarize the invention of data activity strategies within the compressed still image and video domains since year 1992.Comparison among the thought-about data activity strategies is additionally conducted in terms of venue, payload, bit stream size overhead, video quality, computational complexity and video criteria. Further views and suggestions square measure bestowed to supply an improved understanding on this trend of knowledge activity and to spot new opportunities for information activity in compressed video*

***KeyWords*: *Information hiding, host, H.264/AVC, Compressed video, encoding*.**

1. INTRODUCTION

Data concealment techniques will be accustomed insert a secret message into a compressed video bit stream for copyright protection, access management, content annotation and group action following. Such information concealment techniques may be used for alternative functions. Data concealment techniques to assess the standard of compressed video within the absence of the first reference. The quality is estimated based on computing the degradations of the extracted hidden message. The authors of used data hiding to enable real time scene change detection in compressed video. The information is hidden exploitation the motion compensation block sizes of AN H.264/AVC video .Data concealment is additionally used for error detection and concealment in applications of video transmission. Edge orientation information and variety of bits of a block square measure hidden within the bit stream for that purpose.

The rapid development of multimedia technology and computer networks, digital multimedia data is transferred in public channels. Thus, much attention has been paid to the security of public channel transmission. In the early stages, cryptography is used to protect multimedia data. However, the protection will be disabled after decryption. For this reason, information hiding has been proposed to compliment the drawbacks. Information hiding such as steganography and watermarking is a technique which embeds data into digital media for copyright protection or covert communication. The multimedia data can be imperceptibly transmitted to the recipient compared with cryptography. For spatial domain based method, the secret information is directly embedded into image pixel values. Typical methods include least significant bit (LSB), prediction error, histogram based approaches, modulo operation, quantization based approaches and other methods. Spatial domain based algorithm has little effect on the quality of the cover image, and the embedding capacity is large. However, it usually has poor robustness. In order to improve the robustness, researchers proposed to embed secret information in transform domain. Typical methods include steganography based on discrete cosine transform (DCT), discrete wavelet transform (DWT) and discrete fourier transform (DFT)

Traditional image steganography can guarantee the information security to a certain extent. Nevertheless, the cover image is modified in the steganography process. Hence, most of the traditional steganography algorithms can be detected by the state-of-the-art steganalysis algorithms under a certain payload. With the improvement of the steganalysis algorithms, traditional steganography algorithms have to constantly improve the distortion function to resist detection. From the view of the modification in carriers, the idea of coverless information hiding was proposed. It does not mean that the secret information can be transferred without carrier. Instead, the secret information is hidden by generating carriers or establishing mapping rules between the carriers and it . Typical researches include texture synthesis based schemes and coverless steganography schemes based on mapping rules .For the former, new texture image is synthesized based on the secret information, and the secret information is hidden during image texture synthesis. It resamples the image by an invertible function, but it usually has poor robustness.

2. RELATED WORK

Xiang Zhang, Fei Peng, and Min Long[1] Provided to boost the lustiness and capability of resisting image steganalysis, a completely unique coverless image steganography formula supported separate cos rework and latent dirichlet

allocation (LDA) topic classification is proposed. First, latent dirichlet allocation topic model is employed for classifying the image info. Second, the pictures happiness to 1 topic area unit selected, and 8 × 8 block discrete cosine transform is performed to these images. Then robust feature sequence is generated through the relation between electrical energy coefficients within the adjacent blocks .Finally, associate degree inverted index that contains the feature sequence, dc, location coordinates, and image path is created. For the aim of achieving image steganography, the secret information is converted into a binary sequence and partitioned into segments, and the image whose feature sequence equals to the secret info segments is chosen because the cowl image in line with the index .After that, all cover images are sent to the receiver. In the whole method, no modification is done to the original images. Experimental results and analysis show that the proposed algorithm can resist the detection of existing steganalys algorithms, and has better robustness against common image processing and better ability to resist compared with the existing coverless image steganography algorithms. Meanwhile, it's immune to geometric attacks to some extent. It has nice potential application in secure communication of huge information setting

Erfani Y, Pichevar R, Rouat J[2] A new audio watermarking technique based on a perceptual kernel representation of audio signals (spikegram). Spikegram is a recent method to represent audio signals. It is combined with a dictionary of gammatones to construct a robust representation of sounds. In ancient part embedding ways, the phase of coefficients of a given signal in a specific domain (such as Fourier domain) is modified. In the encoder of the projected methodology (two-dictionary approach), the signs and the phases of gammatones in the spikegram are chosen adaptively to maximize the strength of the decoder. Moreover, the watermark is embedded only into kernels with high amplitudes, where all masked gammatones have been already removed. The efficiency of the proposed spikegram watermarking is shown via several experimental results. First, robustness of the proposed method is shown against 32 kb/s MP3 with an embedding rate of 56.5 b/second, we tend to showed that the projected methodology is strong against unified speech and audio codec (24-kb/s USAC, linear vatic, and Fourier domain modes) with a mean payload of 5-15 third, it is sturdy against simulated little real area attacks with a payload of roughly 1 b/s. Last, it is shown that the proposed method is robust against a variety of signal processing transforms while preserving quality.

Borges P V K, Mayer J, Izquierdo E[3]. Provided Improves the employment of text color modulation (TCM) as a reliable text document information concealment methodology. Using TCM, the characters in a document have their color components modified (possibly unperceptually) according to a side message to be embedded. This work presents a detection metric associated an analysis deciding the detection error rate in TCM, considering associate assumed print and scan (PS) channel model. In addition, a perceptual impact model is employed to evaluate the perceptual difference between a modified and a non-modified character. Combining this sensory activity model and also the results from the detection error analysis it's potential to work out optimum color modulation values. The planned detection metric conjointly exploits the orientation characteristics of color halftoning to scale the error rate. In explicit, because color halftoning algorithms use different screen orientation angles for each color channel, this is used as an effective feature to detect the embedded message. Experiments illustrate the validity of the analysis and also the pertinence of the strategy

C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. M. Liao [6] A novel image protection theme referred to as "cocktail watermarking" is projected during this paper. We analyze and point out the inadequacy of the modulation techniques commonly used in ordinary spread spectrum watermarking methods and the visual model-based ones. To resolve the inadequacy, two watermarks which play complementary roles are simultaneously embedded into a host image .We also conduct a statistical analysis to derive the lower bound of the worst chance that the higher watermark (out of the two) may be extracted. With this "high" boundary, it's ensured that a "better" extracted watermark is usually obtained. From intensive experiments, results indicate that our cocktail watermarking theme is remarkably effective in resisting varied attacks, as well as combined ones

3. EXISTING SYSTEM

Video burglary is the showing of picking up, imitating and after that offering or appropriating a copyrighted video without the consent of the copyright proprietor. As of now, camcorder burglary is a standout amongst the most huge issues confronting the film business and is the single biggest wellspring of video robbery. Now when this kind of burglary happens, a copy of an video film is gotten from a gigantic screen movie theater using a camcorder and after that scattered general by methods for the Internet with no copyright protection. Client can see the film or else download the motion picture, through this video was pilfered. An unapproved customer may similarly make an illegal copy of a film from a DVD and suitable it through a web server while a privateer may perform unmistakable sorts of deliberate besides, surprising strikes already exchanging a movie to the Web. Video burglary not simply harms the film business by causing hardships of pay however its effect reverberates all through the overall economy and results in mishaps of jobs and associations.

The other drawbacks of the existing system are as follows

- Easily removed by an unscrupulous person using simple imager editor.
- It is nearly impossible with a large mark in the middle of the image, the strong disadvantage is that it's harder to see the image itself.

- The criticism of the DCT is the blocking effect.
- DCT images are broken into blocks 8*8 or 16*16 bigger.
- The problems with these blocks is that when the image is reduced to higher compression ratios, these blocks become visible.
- In order to overcome these drawbacks we have proposed the following system with H.264/AVC in compressed video

4. PROPOSED SYSTEM

Information hiding methods designed specifically for compressed video, illustrate possible hiding venues within the H.264 coding structure for information hiding, and review their applications. We considered H.264 (instead of the latest compression standard, i.e., H.265) because of its rich literatures in various applications. Here, we emphasize on the techniques that manipulate the underlying coding structure of H.264 to realize data embedding and how each of the techniques affects the payload bit-stream size overhead, video quality and computational complexity. Nevertheless, at times, information hiding methods designed for image are also reviewed since they can be readily applied to compressed video.

5. SYSTEM ARCHITECTURE

The following diagram shows the overall architecture if the proposed system in details:

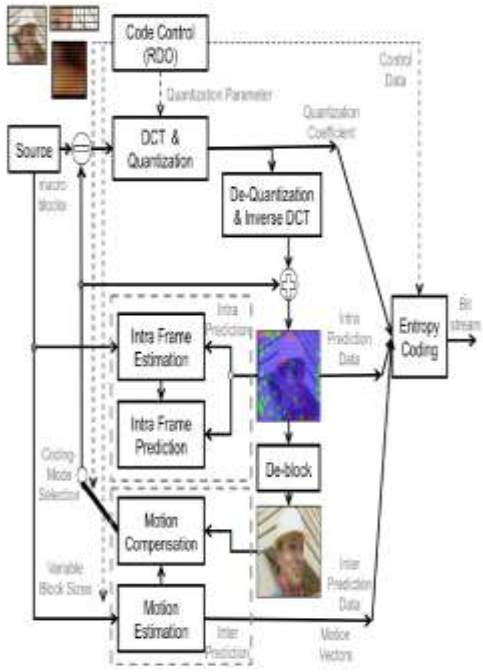

Fig -1: System architecture

The overall system is divided into 4 modules for better and efficient development. We considered H.264 (instead of the latest compression standard, i.e., H.265) because of its rich literatures in various applications. Here, we emphasize on the techniques that manipulate the underlying coding structure of H.264 to realize data embedding and how each of the techniques affects the payload (i.e., the number of bits that can be inserted into the host video), bitstream size overhead, video quality and computational complexity. Nevertheless, at times, information hiding methods designed for image are also reviewed since they can be readily applied to compressed video.

The proposed approach has a number of advantages. It is simple and it is fully compliant with the H.264/AVC syntax using the baseline or the extended profile. Another advantage is that message hiding works for both coded and skipped macro blocks. The proposed solution also works independent of picture type being I (intra), P (predicted) or B (bidirectional predicted).

each of them is shown in table 1.

Number	Intra 4x4 prediction mode
0	Vertical
1	Horizontal
2	DC
3	Diagonal-down-left
4	Diagonal-down-right
5	Vertical-Right
6	Horizontal-down
7	Vertical-left
8	Horizontal-up

Table 1: INTRA 4X4 PREDICTION MODES

The nine intra prediction modes labeled 0, 1, 3, 4, 5, 6, 7

TABLE -1: INTRA 4*4 PREDICATION MODES

6. EXPERIMENTAL RESULT AND ANALYSIS

The system is expected to give accurate result for analysis of the sentiments in the form of pie charts and graphs the system shows the comparision of existing and proposed system. Graph shows the hiding the information using H.264/AVC compressed video

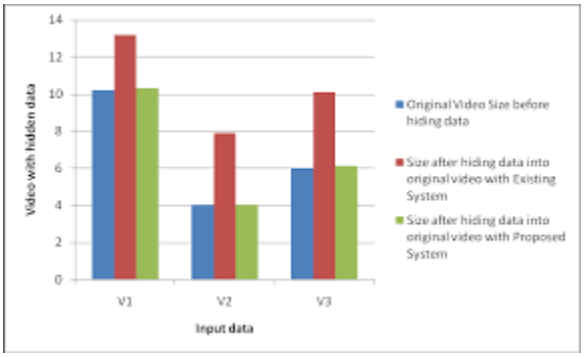

Fig -2: Comparision of existing system and proposed system

The result of work is the comparison between the existing system and proposed system. In that first we take the

original video, here preserved the size means that original video size and after embedding the data into video size remains same. In the existing system once activity knowledge into video contains the additional size than the first video size and also the planned system once embedding knowledge into video contains the same size compare to the original video size.

Fig 2 Comparison of existing system and proposed system.

PSNR (Peak Signal to noise ratio), is widely used video quality metrics. PSNR are used to measure the perceptual quality of video, which illustrate the video quality between the original video and video after extraction and encryption process. Therefore, the visual quality of the decrypted video containing hidden data is expected to be equivalent or very close to that of the original video that is comparison of PSNR. By modifying the compressed bit stream to embed additional data, the most important challenge is to maintain perceptual transparency, which refers to the modification of bit stream should not degrade the perceived content quality. .

7. SCOPE OF THE SYSTEM

Data concealment techniques may be wont to introduce a secret message into a compressed video bit stream for copyright protection, access management, content annotation and dealing chase. Such knowledge concealment techniques also can be used for alternative functions. Data concealment techniques to assess the standard of compressed video within the absence of the first reference. The quality is estimated based on computing the degradations of the extracted hidden message. The authors of used data hiding to enable real time scene change detection in compressed video. The information is hidden victimization the motion compensation block sizes of Associate in Nursing H.264/AVC video. Data concealment is additionally used for error detection and concealment in applications of video transmission. Edge orientation data and range of bits of a block square measure hidden within the bit stream for that purpose

8. FUTURE WORK

If a technique or set of techniques could be devised to detect steganography.It would be interesting to conduct a survey of images available on the internet to determine if steganography is used, by whom and for what purpose. Steganographic applications are available on the Internet, but it is not know if they are being used.

9. CONCLUSION

In this paper we surveyed the conventional info concealing ways within the compressed video domain, that specialize in the H.264 video compression customary. Commonly thought-about information illustration schemes and also the concealing venues were summarized. The general trend of information hiding in the compressed video domain was presented. Then, we categorized the existing information hiding methods based on the venues at which they operate and highlighted their strengths and weaknesses. Video criteria such as motion alleviation, GOP size and bitrate were recommended as guidelines to select appropriate technique for information hiding, and future research directions were suggested. This survey is limited to the techniques that manipulate the underlying coding structure of H.264 to realize data embedding. The decoding process (e.g., in multi-bit watermark application) and the detection process (e.g., in zero bit watermark application) as well as the security issues involved will be investigated as our future work. In addition, we aim at proposing new information hiding methods or consolidating the existing ones for actual application purposes such as video compression, motion tracking, etc..

REFERENCES

[1] Xiang Zhang ; Fei Peng ; Min Long" Robust Coverless Image Steganography Based on DCT and LDA Topic Classification"IEEE Transactions on multimedia,vol.20,no.12,Dec 2018.

[2] Erfani Y, Pichevar R, Rouat J. "Audio Watermarking Using Spikegram and a Two-Dictionary Approach," IEEE Trans. Inf. Forensics and Security, vol. 12, no. 4, pp. 840-852, Apr. 2017.

[3] Borges P V K, Mayer J, Izquierdo E. "Robust and transparent color modulation for text data hiding," IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1479-1489, Oct. 2008.

[4] A. Piva, F. Bartolini, and M. Barni, "Managing copyright in open networks," IEEE Internet Computing, vol. 6, no. 3, pp. 18–26, May 2002.

[5] C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.

[6] C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. M. Liao, "Cocktail watermarking for digital image protection," IEEE Transactions on Multimedia, vol. 2, no. 4, pp. 209–224, Dec. 2000.