International Journal of Global Engineering (IJGE) E-ISSN: 2456-3099

VOL 2 ISSUE 3 (2018) PAGES 55 - 60

Received: 20/02/2018. Published: 22/03/2018

A 3D Steganalytic Computation and Steganalysis Safe Watermarking

S.Abirami[1], K.Ajantha[2],G.Archana[3],R.Thillaikarasi[4]

Department of Computer Science and Engineering

Students[1,2,3],Assistant professor[4]

Kingston Engineering College,Vellore,TamilNadu,India.

Abstract:

We propose a straightforward yet productive steganalytic calculation for watermarks implanted by two best in class 3D watermarking calculations by Cho et al. The fundamental perception is that while in a spotless model the methods/fluctuations of Cho et al. Standardized histogram canisters are relied upon to take after a Gaussian circulation, in a checked model their appropriation will be bimodal. The proposed calculation assesses the quantity of containers through a comprehensive pursuit and after that the nearness of a watermark is chosen by a carefully fit typicality test or a t-test. We additionally propose an alteration of Cho et al's. Watermarking calculations with the watermark implanted by changing the histogram of the spiral directions of the vertices. Instead of focusing on persistent measurements, for example, the mean or change of the qualities in a canister, the proposed watermarking adjusts a discrete measurement, which here is the stature of the histogram container, to accomplish watermark implanting. Trial comes about show that the adjusted calculation offers not just better resistance against the steganalytic assault we grew, yet additionally an enhanced strength/limit exchange off.

Keywords: Watermarking, High Robust, Sharing multimedia files.

I. INTRODUCTION:

Multimedia files are shared extensively now days on social sharing sites. Sharing takes place between friends and acquaintances on a daily basis. Sharing important files may lead to exposure of personal information and privacy violation, it is a major problem to maintaining privacy when it is shared through social sites. Because of this reason there is need to transfer the multimedia files by embedding or overlapping with any other file. To prevent such kind of activity by a hacker and intruders many security related tools are developed. Already, a method called steganography is used here to provide safer transmission of files through embedding it with image file. By improving that method with watermarking technique we introduced an 3d steganalytic algorithm and digital watermarking. Watermarking is the process of overlapping digital signals (video file) into digital media such as images, audio, video, or files. It provides an secure transmission of multimedia files by using encryption and decryption of the files with the help of symmetry key. This technique used to provide security even though the hacker can hack the message he didn't know the exact message because once the multimedia file is encrypted with video until the decrypted with its key it will be viewed as like an video(overlapped).

II. EXISTING SYSTEM

Digital watermarking is the process of embedding digital signals into digital media such as images, audio, video, or 3D models. In a relationship analogous to that between cryptography and cryptanalysis, as a counterpart to watermarking, steganalysis aims at the detection of watermarks hidden into digital signals. Steganalytic approaches are classified into two categories: specific and universal. The former detects the presence of a message embedded by particular watermarking algorithms, while the latter aims at message detection regardless of the embedding algorithms used.

DISADVANTAGES:

- The causality problem,.
- The main limitation is their weak robustness
- They cannot withstand malicious attacks aimed at destroying the embedded message.

III. LITERATURE SURVEY:

[1]Outsourcing data to cloud servers, while increasing service availability and reducing user's difficulties of managing data. It brings in new concerns such as data privacy, since the server may be honest-but-curious. In this paper, we investigate the searchable encryption problem in the presence of a semi-honest-but-difficult server, which may execute only a fraction of search operations honestly. To fight against this strongest opponent ever, a verifiable SSE (VSSE) scheme is proposed to offer verifiable search ability in additional to the data privacy, both of which are further confirmed by our strict security analysis. Besides, we treat the practicality/efficiency as a central requirement of a searchable encryption scheme.

[2]Prior Searchable Symmetric Encryption (SSE) works focus on single keyword search. Conjunctive Keyword Searches (CKS) schemes improves system usability by retrieving the matching files. Most of existing conjunctive keyword works that use conjunctive keyword searches with fixed position keyword fields. That are not useful for many applications, such as the body of e-mail and unstructured text. In our paper, we propose a new symmetric key encryption scheme which supports a keyword field free method for conjunctive keyword search on encrypted file without needing to specify the positions of the keywords where the keywords can be in any arbitrary order. Furthermore, we introduced an efficient secure index construction based on pseudorandom functions and Bloom filters.We determine how such scheme could be used to guarantee fast, low storage and secure access to the database.

[3]Remote forensics can help investigators perform investigation without need to ship hard drives or travel to a remote location. The increased use of cloud computing technologies, it is becoming more and more difficult to perform post-event forensic investigation. The other server administrator search the relevant information and retrieve the data for the investigators provided a warrant can be provided. Sometimes, the investigators need to keep the investigation subject confidential due to the confidentiality of the crime or the server administrator may be one of the suspects. In this paper, we address how to solve this problem by multiple keyword search over the encrypted data, so that the investigators need to obtain the necessary evidence for keeping the investigation subject confidential.Also the irrelevant data can be protected from exposing to the investigators.

IV.PROPOSED SYSTEM :

We propose a specific steganalytic algorithm for determining the presence of a watermark hidden by Cho et al.’s mean and variance based algorithms, which are major 3D watermarking techniques with considerable impact on subsequent research. The proposed algorithm exploits the alteration of the model’s natural statistics caused by Cho et al.’s watermark insertion method. More specifically, watermarking with Cho et al.’s method makes the distribution of the means and variances of the normalized histogram bins bimodal, while it is expected to be Gaussian before watermarking. We also propose a blind 3D watermarking algorithm with improved undetectability and robustness performance over Cho et al.’s. The new algorithm embeds the watermark into the histogram of the radial coordinates of the mesh vertices, as Cho et al.’s does. The main difference is that instead of embedding each watermark bit inside a continuous statistics of the model, e.g., the mean or the variance of a normalized histogram bin, we embed it inside a discrete statistic, that is, the difference in the number of elements of two adjacent bins. Experimental results show that the proposed discrete statistic offers improved performance against both the proposed steganalytic attack and standard watermark removal attacks.

ADVANTAGES:

- A new 3D watermarking algorithm which is more robust than two state-of-the-art techniques in terms of detectability.
- Offers a better distortion/capacity trade-off against standard watermark removal attacks such as smoothing, noise insertion, subdivision and simplification.

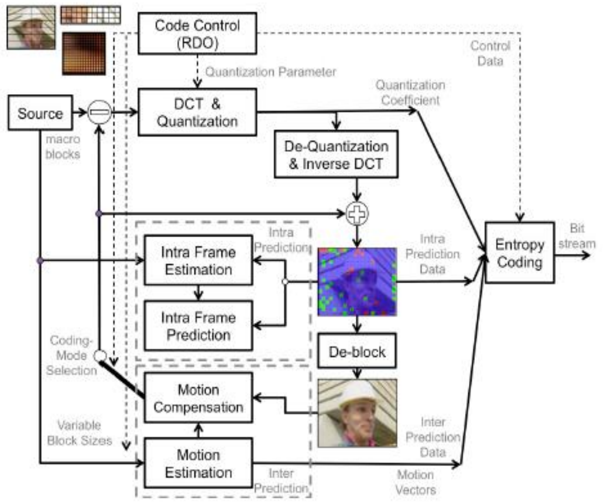

Fig.1. **System Architecture**

V. ARCHITECTURE

In this architecture diagram , the user sends the message where the source message can be of any pdf, document, audio, video etc . Here the code control (RDO) i.e,remote data control that allows to access the windows applications and it acts as an interface between remote data objects .The source message is in blocks that enters to the DCT(Discrete cosine transform) and Quantization trying to encode and decode the source message in an compressible format and reduces the size of the file . The next stage is Intra frame estimation and Intra frame prediction that divides the message into blocks known as macroblocks after that instead of directly encoding the raw pixel values for each block , the encoder will try to find a block similar to the one it is encoding on a previously encoded frame known as reference frame . The other stage is Motion compensation and motion estimation that allows decryption process and grouping the files by adjacently arranging the frames in it , The process of finding a match of pixel block in inter frame coding is called motion estimation. Then these messages is Dequantized and all the stages is combined in entropy coding where the lossless file is retrieved with bit stream .

VI.ALGORITHM:

Step 1: Extract Bit set of Message,

Bit={M0, M1,……, M65535 }

Step 2: The Pixels of cover image, Pixel = {pixel0, pixel,…, pixel65535}

Step 3: Extract LSB-1 set of the cover image, LSB1={A0, A1,…,A65535}.

```
Step 4: Extract LSB-2 set of the cover image, LSB2={B0, B1,…, B65535}.

Step 5: For i=1 to message length does{ If Mi= =Bi Then do nothing Else {

If Mi= =1 and Bi= =0 Then 40

{

Bi=Mi; Ai=0; Pixel (i)-=1 } Else If Mi= =0 and Bi= =1 Then { Bi=Mi; Ai=1; Pixel (i)+=1

 } } }
```

VII .CONCLUSION:

In this work, we surveyed the conventional information hiding methods in the compressed video domain, focusing on the H.264 video compression standard. Commonly considered data representation schemes and the hiding venues were summarized. 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 and the detection process 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. We also aim for exploring new information hiding opportunities in the latest H.265 video compression standard.

VIII. REFERENCES

[1] Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers," in Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012, pp. 917– 922.

[2] S. Hou, T. Uehara, S. Yiu, L. C. Hui, and K. Chow, "Privacy preserving multiple keyword search for confidential investigation of remote forensics," in Multimedia Information Networking and Security (MINES

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[4] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in INFOCOM, 2014 Proceedings IEEE.

[5] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

Received: 20/02/2018. Published: 22/03/2018

[6] X. Yu and Q. Wen, “Design of security solution to mobile cloud storage,” in Knowledge Discovery and Data Mining. Springer, 2012, pp. 255–263.

[7] D. Huang, “Mobile cloud computing,” IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, 2011.

[8] O. Mazhelis, G. Fazekas, and P. Tyrvainen, “Impact of storage acquisition intervals on the cost-efficiency of the private vs. public storage,” in Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012, pp. 646–653.

[9] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, “Virtualized in-cloud security services for mobile devices,” in Proceedings of the First Workshop on Virtualization in Mobile Computing. ACM, 2008, pp. 31–35.

[10] J. Oberheide and F. Jahanian, “When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments,” in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications. ACM, 2010, pp. 43–48.