ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

ESAVC: An Efficient Scheme for Secure Authentication for Video Compression Coding Using H.264/AVC

Dr.S.Audithan

Principal, P.R.Engineering College, Vallam, Thanjavur, India

Abstract

The main aim of this project is to minimize end-to-end quality degradation incurred by both the wireless channel noise and the authentication failure. In this research work, a novel joint-designed-layered source–channel adaptive scheme has been proposed that integrates authentication into source and channel coding components to sufficiently use the related information to efficiently address the coding dependency and to design the optimal rate allocation scheme for the sake of end-to-end video quality. The proposed algorithm clearly outlines the necessity of this research work.

KEYWORDS: encoding, video, degradation, adaptive scheme, authentication, security

1. INTRODUCTION

Video application has become one of the dominant applications over Internet [1], promoted by the rapid development of the network technologies, media coding standards, and the recent advances of the social media network. Security issues arise with the popularity of the video applications, in particular in the wireless consumption [2]. Although the advanced video coding standards, such as H.264/AVC, efficiently reduce the amount of data to be transmitted, the coding dependency brings new challenges in designing efficient stream authentication scheme [3].

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

Security issues arise with the popularity of the video applications, in particular in the wireless consumption environments [4]. In this research work, the major focus is on the issue of authentication of video stream. The term "authentication" refers to several aspects of security, including integrity, source authenticity and non-repudiation. Integrity refers to that the data is not maliciously changed in transmission. Source authenticity refers to that the media content is indeed sent by the claimed sender. [5] proposed a system in which this study presented the implementation of two fully automatic liver and tumors segmentation techniques and their comparative assessment. The described adaptive initialization method enabled fully automatic liver surface segmentation with both GVF active contour and graph-cut techniques, demonstrating the feasibility of two different approaches. The comparative assessment showed that the graph-cut method provided superior results in terms of accuracy and did not present the described main limitations related to the GVF method. The proposed image processing method will improve computerized CT-based 3-D visualizations enabling noninvasive diagnosis of hepatic tumors. The described imaging approach might be valuable also for monitoring of postoperative outcomes through CT-volumetric assessments. Processing time is an important feature for any computer-aided diagnosis system, especially in the intra-operative phase.

2. LITERATURE SURVEY

This literature survey has several dimensional focus that highlights on Two Pass VBR coding for H.264/AVC, analysis and design of authentication watermarking, efficient authentication and signing of multicast stream over lossy channels and an optimized content aware authentication

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

scheme for streaming JPEG-2000 images over lossy networks. The ideas contributed in the previous papers related to the above said dimensions are discussed below.

2.1 Works on Two Pass VBR Coding For H.264/AVC

Jun Sun et al. proposed a paper and in the first part of this paper, he has derived a source model describing the relationship between the rate, distortion, and quantization steps of the dead-zone plus uniform threshold scalar quantizers with nearly uniform reconstruction quantizers for generalized Gaussian distribution [6]. Extensive experiments demonstrate that the proposed method achieves: 1) average peak signal-to noise ratio variance of only 0.0658 dB, compared to 1.8758 dB of JM 16.0's method, with an average rate control error of 1.95% and 2) significant improvement in smoothing the video quality compared with the latest two-pass rate control method.

2.2 Works on Authentication Watermarking

Chuhong Fei et al. proposed a paper and this paper focuses on the use of nested lattice codes for effective analysis and design of semi-fragile watermarking schemes for content authentication applications [7]. We provide a design framework for digital watermarking which is semi-fragile to any form of acceptable distortions, random or deterministic, such that both objectives of robustness and fragility can be effectively controlled and achieved. Robustness and fragility are characterized as two types of authentication errors.

First, authenticity must be guaranteed even when only the sender of the data is trusted. Second, the scheme needs to scale to potentially millions of receivers [9]. Third, streamed

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

media distribution can have high packet loss. Finally, the system needs to be efficient to support fast packet rates. We propose two efficient schemes, TESLA and EMSS, for secure lossy multicast streams.

Zhishou Zhang et al. proposed a paper and in this paper, we propose an optimized content-aware authentication scheme for JPEG-2000 streams over lossy networks, where a received packet is consumed only when it is both decodable and authentic [8]. In a JPEG-2000 code stream some packets are more important than others in terms of coding dependency and visual quality. This inspires us to allocate more redundant authentication information for the more important packets to minimize the distortion of the authenticated image at the receiver.

Inspite of all these contributions from literature, there are many breaches that are to be addressed for secure transmission over lossy networks [13-15]. Most of the systems present in literature are expensive in computational manner. So we have proposed a novel layered authentication framework called Joint Media Error and Authenticity Protection (JMEAP) and successfully applied it on JPEG- 2000 images. The layered schemes jointly consider the Authentication and transmission over loss networks [10-12], therefore both high verification probability and low authentication. Joint source channel adaptive scheme in the encrypted version of video stream is proposed, which includes the following three parts, i.e., video Encoding, data hiding, and data extraction. Finally the overheads in the existing System are reduced. The main objective of the proposed work is mentioned below.

(i) To propose an efficient secure data transmission scheme through video using the watermarking technique,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

(ii) To ensure the authentication of sender in video transmissions.

3. ARCHITECTURE OF THE PROPOSED SYSTEM

The architecture of the proposed system consists four major modules such as video upload, video preprocessing, data hiding and data extraction among others.

The invisible watermarking technique is used to select the frames and the frames in which the data is hidden are converted into video. Subsequently, the video is sent to the receiver side. In the receiver side, the video is decrypted and split into component frames and the user extracts the secret image and data by selecting the specific frames which was watermarked. Ultimately, the video is decoded in an attempt to identify the loss of content.

Joint source channel adaptive scheme in the encrypted version of video stream is proposed, which includes the following three parts, i.e., video Encoding, data hiding, and data extraction. The importance of the source coding and channel coding context in the design of optimized end-to-end quality authentication schemes has not been properly recognized until very recently. The Secret image file as well as data will be hidden in the frames of the video and the data will be extracted safely in receiver side. In this system, a user who wants to securely send a secret data to the receiver uploads a video content. Then, the necessary authentication between sender and receiver is done. Followed by that, encoding of video content takes place for efficient encoding. The video is split into multiple frames in order to process it. Now, a particular frame will be selected for storing the secret data inside that particular frame and the frames are encoded using the technique so that it may not be loss or change during the transmission. In the present

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

scenario, the data is encrypted using binary technique. With the help of steganography technique, the cipher text is embedded into frames for secure communication between the sender and the receiver.

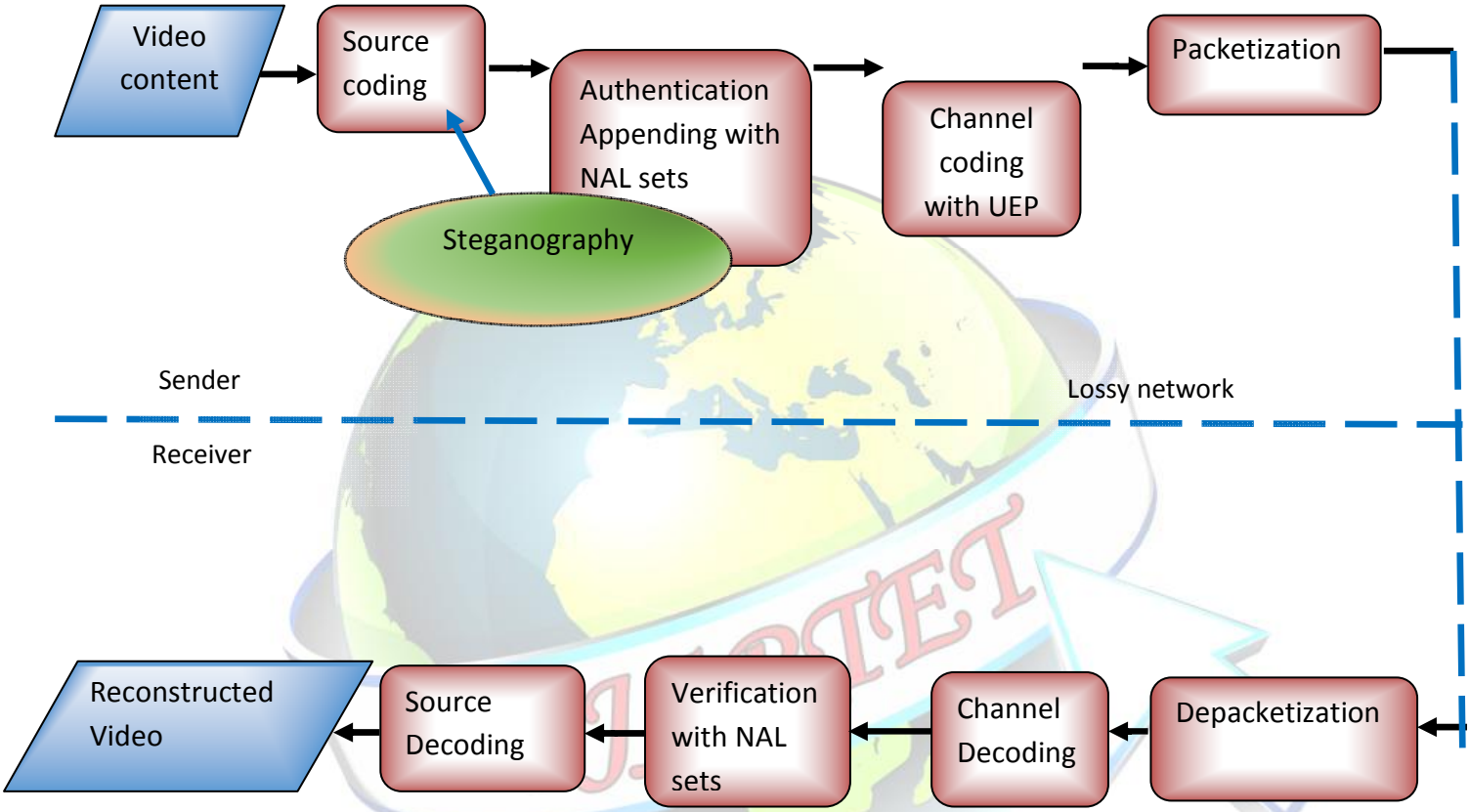

Fig.1 System Architecture

4. EASVE: THE PROPOSED SCHEME FOR EFFICIENT AUTHENTICATION FOR SECURE VIDEO ENCODING

4.1 Video Upload module:

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

In first module, authentication for both sender and receiver will be created in order to provide secure authentication of the sender to the receiver. In this module, initially, the sender will upload the video which is encoded in subsequent steps for further processing as described in the algorithm.

4.2 Video preprocessing:

The output of the video upload module is fed to the input of video preprocessing module. It is the second module, in which the video is split into the constituent frames. A particular frame will be selected for store the secret image as well as data inside it. The frames are encoded using the technique so that it may not result in data losses over the transmission of the video in lossy channels.

4.3 Data Hiding:

In this module, the data is hidden in order to the share it with the receiver. Initially, the data is encrypted using binary technique. Now, by using the Steganography technique, the cipher text is embedded into the frames. The Invisible Watermarking technique is used the selected frames and after the image is hidden over the all frames which are finally part of the video bring transmitted.

4.4 Extracting the Data:

It is the final module in which the video sent by the sender is received by destination. Fig.2 clearly depicts the process of extraction of data and the image from the encoded video. In the receiver system,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

video is decrypted and followed by that, the decrypted video is split into constituent frames. From the constituent frames, both the secret image and the data are extracted by selecting the frames which were watermarked in the sender side. After the successful extraction of the image and the data, the video is decoded to find the loss in the video.

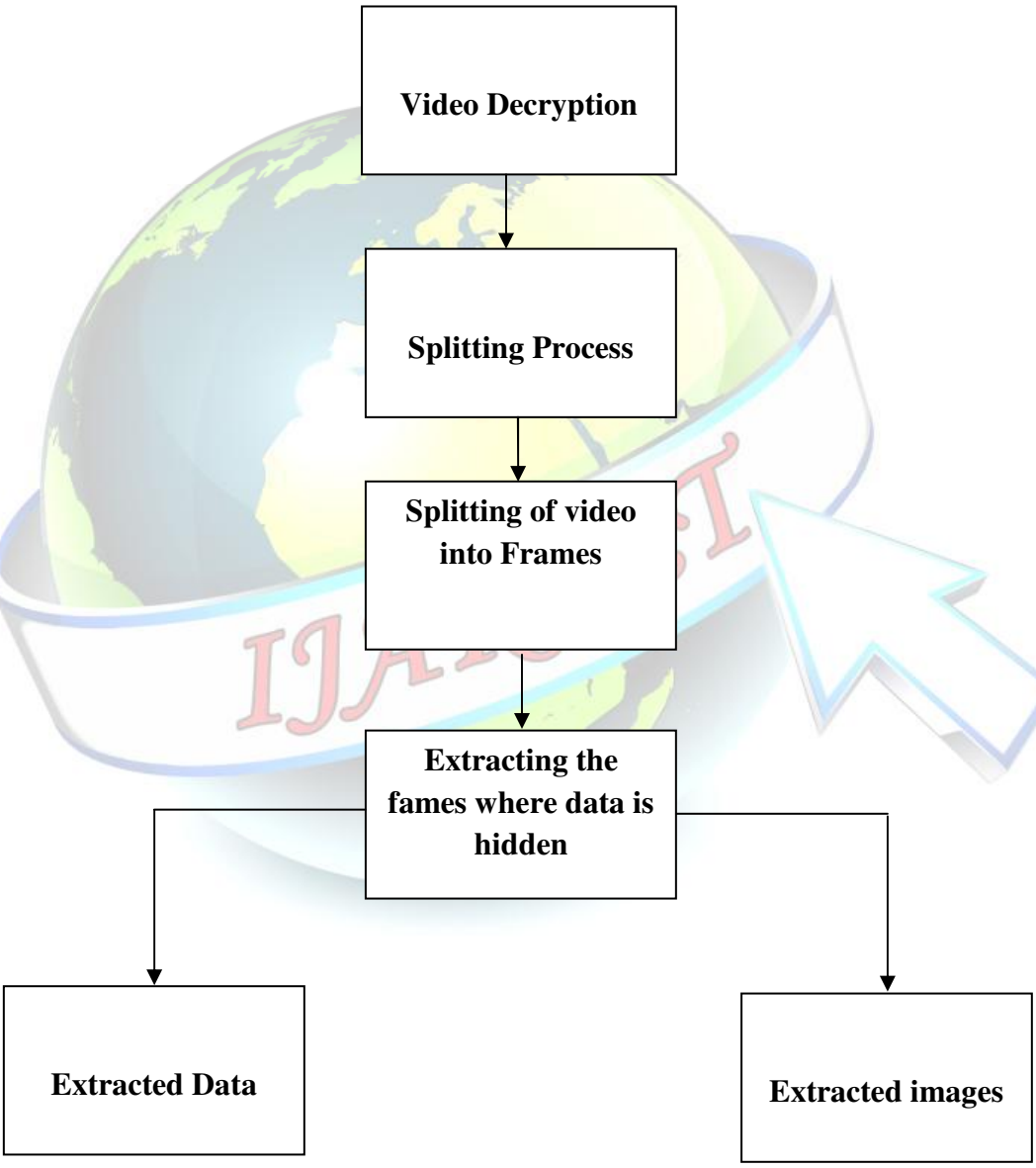

Fig.2 Extraction data and image from the encrypted video

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

5. IMPLEMENTATION OF ESAVC SCHEME

The proposed scheme has been implemented using dot net framework and Microsoft Visual Studio. NET Framework (pronounced dot net) is a software framework developed by Microsoft that runs primarily on Microsoft Windows. It includes a large library and provides language interoperability (each language can use code written in other languages) across several programming languages. Programs written for .NET Framework execute in a software environment known as the Common Language Runtime (CLR), an application virtual machine that provides services such as security, memory management, and exception handling. The class library and the CLR together constitute .NET Framework.

The experimental results are reported based on eight H.264 Video sequences: car phone, Foreman, container, Silent, Mobile, Akiyo, Bridge and Coastguard Sequences. We use IBBPBBP structure in H.264 coding and the number of frames is 17 per GOP. For each GOP, the number of transmission Packets is set to 100.The hash function is SHA-1 with hash size is 160 bits. A signature of length 1024 bits is generated by RSA for each GOP. The detailed analysis of the proposed protocol is mentioned in figure3 and figure 4.

The PSNRs of proposed scheme and extended butterfly scheme (with added error protection) at different packet loss rate (PLR) is depicted in figure 3 and figure 4. The total rate is 96kbps, the frame rate is 20 fps and the packet loss rate is set to 0.01 to 0.1. The proposed scheme outperforms graph based scheme for about 0.4-0.5dB on average. In our experiments, the ratio of authentication rate over the total rate R is in the range of 2.1%-2.4% in the proposed scheme and 13.4%-18.2% in the butterfly scheme. With low authentication rate, more rates could be allocated to source and channel coding, Frames by frame PSNR comparison at 10% PLR .

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

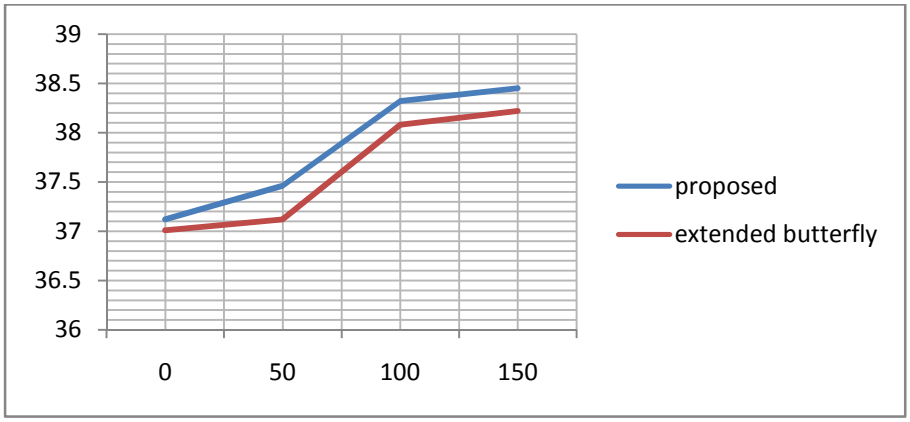

Fig.12 carphone sequence

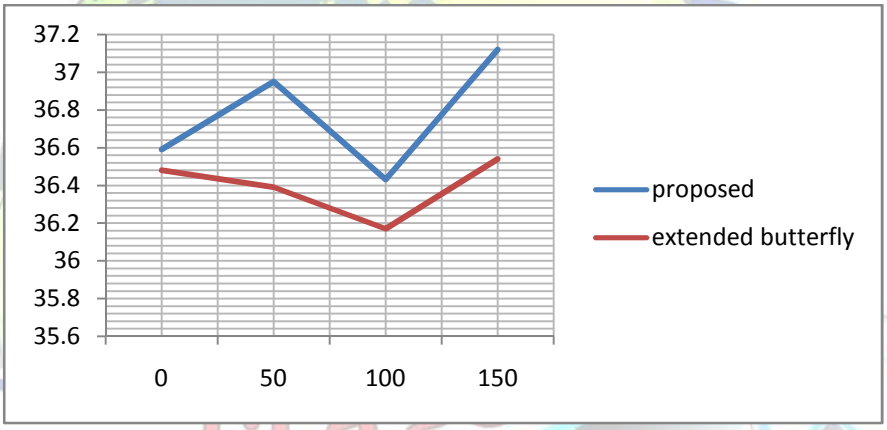

Fig.13 Forman sequence

The proposed protocol is implemented and the results thus obtained are tabulated in Table 1 in which the number of frames is increased from 0 to 10 and finally to 100. The table clearly shows the time taken for processing the number of frames.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

Also, Table 1 and Table 2 show the effectiveness of the proposed scheme in real time scenario. Table 2 shows the results of processing two video sequences. One of the sequence is car phone based and another one is based on foreman video sequence.

Table 1 PROPOSED

Total no of frames	Proposed Scheme
0	38.48
10	37.46
100	37.32
150	38.45

TABLE 2 PSNR (dB): PROPOSED SCHEME

(QCIF SEQUENCE, 150 FRAMES, RATE 96K BPS, FRAME RATE 20 FPS)

	PLR=0.01	PLR=0.05	PLR=0.1
Carphone	38.48/38.02	38.41/37.94	38.26/37.82
Foreman	36.91/36.48	36.75/36.39	36.43/36.17

6. CONCLUSION

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

The proposed Scheme is able to achieve 100% effective verification probability while maintaining low authentication overhead, i.e., all media slices recovered from the lossy channel can be decoded and authenticated and show that the authentication overhead is low. The eminent future works of this research work relies on the successful transmission of secure data based on BASE 64 coding technique.

Forming the entire system to be a high performance capability and low error transmission can be useful research in this direction. Its applications include the reduction of of transmission and error rate for video streams.

REFERENCES

[1] Ross J. Anderson, Francesco Bergadano, Bruno Crispo, Jong-Hyeon Lee, Charalampos Manifavas, and Roger M. Needham. A new family of authentication protocols. Operating Systems Review, 32(4):9– 20, October 1998.

[2] M. Bellare, J. Kilian, and P. Rogaway. The security of cipher block chaining. In Yvo Desmedt, editor, Advances in Cryptology - Crypto '94, pages 341–358 Berlin, 1994, Springer-Verlag. Lecture Notes in Computer Science Volume 839.

[3] Xinglei Zhu, Chang Wen Chen, "A Joint Source-Channel Adaptive Scheme for Wireless H.264/AVC Video Authentication", IEEE Transactions on Information Forensics And Security, VOL. 11, NO. 1, pp. 141-153, JANUARY 2016.

[4] Xinglei Zhu, Chang Wen Chen, "A Joint Source-Channel Adaptive Scheme for Wireless H.264/AVC Video Authentication", IEEE Transactions on Information Forensics And Security, VOL. 11, NO. 1, pp. 141-153, JANUARY 2016.

[5] Christo Ananth, Karthika.S, Shivangi Singh, Jennifer Christa.J, Gracelyn Ida.I, "Graph Cutting Tumor Images", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 4, Issue 3, March 2014,pp 309-314

[6] Z. Li, Q. Sun, Y. Lian, and C. W. Chen, "Joint source-channel authentication resource allocation and unequal authenticity protection for multimedia over wireless networks," IEEE Trans. Multimedia, vol. 9, no. 4, pp. 837–850, Jun 2007.

[7] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of secure watermark-based authentication systems," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 43–55, 2006.

[8] Z. Zhang, Q. Sun, J. Apostolopoulos, and W.-C. Wong, "Rate-distortionauthentication optimized streaming with generalized butterfly graph authentication," in Proc. IEEE Int. Conf. Image Process. (ICIP), Oct. 2008, pp. 3096–3099.

[9] X. Zhu and C. W. Chen, "A joint source-channel adaptive scheme for wireless H.264 video authentication," in Proc. IEEE Int. Conf. Multimedia Expo (ICME), pp. 13–18, Jul. 2010.

[10] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," in Proc. IEEE Int. Conf. Image Processing (ICIP), Lausanne, Switzerland, Sep. 1996, pp. 243–246.

[11] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," Signal Process., vol. 66, no. 3, pp. 283–301, 1998.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 2, February 2017

[12] G. C. Langelaar, R. L. Lagendijk, and J. Biemond, "Real-time labeling methods for MPEG compressed video," in Proc. 18th Symp. Inf. Theory Benelux, Veldhoven, The Netherlands, May 1997.

[13] T.-Y. Chen, V. Istanda, T.-H. Chen, D.-J. Wang, and Y.-L. Lin, "H.264 video authentication based on semi-fragile watermarking," International Journal ofInnov. Comput., Inf. Control, Vol. 6, no. 3, pp. 1411–1420, 2010.

[14] B. G. Mobasseri and Y. N. Raikar, "Authentication of H.264 streams by direct watermarking of CAVLC blocks," Proc. SPIE, Security, Steganography, Watermarking Multimedia Contents IX, Vol. 6505, no. 1W, pp. 1–5, Feb. 2007.

[15] X. Gong and H.-M. Lu, "Towards fast and robust watermarking scheme for H.264 video," in Proc. IEEE Int. Symp. Multimedia, pp. 649–653, 2008.