ISSN:2231-0711

MRUDULA MEDURI et al | IJCSET(www.ijcset.net) | 2017 | Volume 7 Issue 4, 15-18

Secure End-To-End Video Authentication with Secret Data Sharing

MRUDULA MEDURI,
Assistant Professor, Department of CSE, SRM UNIVERSITY

ABHINAV CHAUDHARY,
Student, Department of CSE, SRM UNIVERSITY

ISHA THAKUR,
Student, Department of CSE, SRM UNIVERSITY

Abstract-- Validation or Authentication has turned into a rising issue for video gushing over lossy networks [4]. In spite of the fact that the propelled video coding gauges, for example, H.264/AVC, effectively lessen the measure of information to be transmitted, the coding reliance gets new difficulties planning proficient stream [4][7] validation plot. We propose a novel joint-outlined layered [5] source– channel versatile plan that incorporates verification [3] into source and channel coding parts to adequately utilize the related data to effectively address the coding reliance with data hiding into the video file using Visual Cryptography, Watermarking and Cryptographic techniques. Specifically, the contending prerequisites of high check likelihood and low confirmation [3] overhead are simultaneously fulfilled by the exquisite plan of layered [5] hash annexing with productive adjustment to the H.264 source coding and channel conditions. An image is then used to hide data into the frames of the video with is then invisible watermarked for extraction of data later.

Keywords—Stream authentication[3], wireless media communication, H.260 video streaming[4][7].

I. INTRODUCTION

Video applications have progressed toward becoming a big bargain nowdays, particularly spilling [4][7] of recordings over the web. A gauge proposes that by the year 2019 more than 80% percent of the web movement will be as video. At present of all web activity a little more than 40% of the downstream [4] movement is video streaming and with the progression of portable innovation and better web structure nowdays laptops and desktops account less rate share of interntet activity than cell phones.

With the ubiquity of the video applications, especially in the remote utilization situations, Security issues emerge. Because of the open-to-air get to mode, helplessness to illicit get to and change of the video information transmitted over remote systems [4] is more. In this paper we concentrate on the issue of validation [3] of video stream [4][7] with the enhancement of data hiding in the video. The expression "confirmation" alludes to a few parts of security, including respectability, source validness [3] and non-renouncement. Where, Integrity remains for the non-malevolent change of information in transmission. Source validness [3] alludes to the media substance is for sure sent by the guaranteed sender. Non-disavowal implies that the sender couldn't prevent the reality from securing sending the media content. On the off chance that the beneficiary can't confirm the got media, it ought not be devoured and accordingly the nature of consumable media is impeded.

The stream [4][7] level plan, content based plans by nature use design acknowledgment like procedures to identify elements and make examination in the validation [3] stage and along these lines definitely experience the ill effects of certain false positive and false negative blunders likelihood.

The wellsprings of the contortion root in every one of the three noteworthy parts: source coding, verification [3] and channel coding. To begin with, channel clamor. In the event that a video cut is lost or impeded amid transmission, it couldn't be appropriately utilized as a part of deciphering. Second, coding reliance. Cut got yet not decodable because of coding reliance. On the off chance that a video cut is effectively gotten yet it is coding reliant on another lost video cut, it couldn't be accurately decoded. Third, unverifiable cut. On the off chance

that cut S is effectively gotten yet all different cuts on which S's hashes are affixed are lost or unverifiable, S couldn't be checked and must be disposed of.

II. RELATED WORK

A. *H.264/AVC Video Coding Standard*

H.264/AVC is the most recent worldwide coding standard by ITU-T Video Coding Expert Group (VCEG) and the ISO/IEC Moving Picture Experts Group (MPEG). It is designed [3] for higher pressure productivity and furthermore network [4] agreeable. It has been generally utilized for different video applications, for example, video broadcasting, video meeting and video streaming [7] and so on.

Other than the higher pressure productivity procedures, H.264/AVC likewise gives an arrangement of elements to upgrade blunder flexibility, which is accomplished by systems, for example, network [4] deliberation layer [5] (NAL), parameter set structure, flexible [5] cut size and flexible [5] macroblock requesting and so on. H.264/AVC has a video coding layer [5] (VCL) that is designed [3] to effectively speak to the video content, and the NAL is utilized to arrange the VCL portrayal of the video such that is advantageous and proficient to be transported by various networks[4].

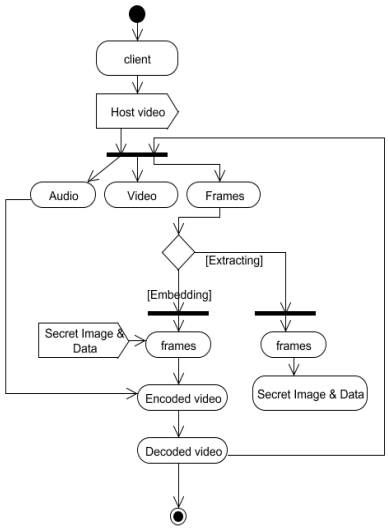
B. *Visual Cryptography*

Visual Cryptography [2] is an extraordinary encryption method to conceal data in pictures such that it can be decoded by the

human vision if the right key picture is utilized. Two straightforward pictures are utilized as a part of Visual Cryptography [2]. Mystery data is contained in one of the pictures and the other picture contains irregular pixel. Just a single of the picture of the two pictures utilized can never be utilized to recover the mystery data. To uncover the mystery data both the layers of the pictures are required. In the event that both the layers of the pictures are imprinted on a straightforward sheet the mystery data is uncovered when these two sheets are covered, this is the most effortless approach to execute the Visual Cryptography [2].

Unbreakable encryption is offered when it is viewed as one-time cushion framework which is accomplished really arbitrary pixels are contained in an irregular picture. To attempt this technique of Visual Cryptography [2] yourself, you can duplicate the case layers [5] which can be gotten effortlessly from the web, and print them onto a straightforward sheet or thin paper and cover them. High contrast pixels ought to be legitimately shown so when printed there ought to be no dispersion or photograph upgrading and so on. You can likewise duplicate and past them on each other in a drawing program like paint and see the outcome quickly, however make a point to choose straightforward drawing and adjust both layers [5] precisely over each other.

III. TECHNICAL WORK



(Fig. 1- Activity Diagram)

A joint source direct versatile plan in the scrambled form of video stream [7] is proposed, which utilizes a solitary code rather than the more traditional strides of source coding took after by channel coding.

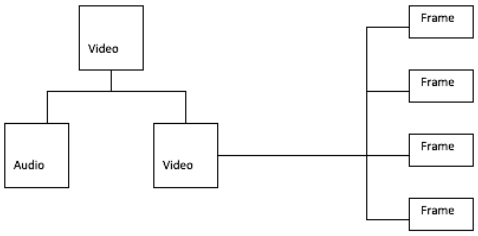
This work incorporates the accompanying three sections, i.e.,

- Video encryption
- Data embedding
- Data extraction.

By investigating the property of video codec an information sender may install extra information in the encoded area by utilizing code word substitution procedure, without knowing the first video content. Keeping in mind the end goal to adjust to various application situations, information extraction should be possible either in the encoded area or in the unscrambled space. Moreover, video record size is entirely saved even after encryption and information implanting.

A. Video Encryption

This incorporates the first module of the work, Frame Selection, where a video document is chosen to conceal the Secret picture and Data. By utilizing the FFMpeg instrument, Video is then part up into three arrangements. To begin with the video will be isolated into sound and video. At that point the video part of this document will be changed over into n number of edges. In future these casings are utilized to conceal the picture and the information.



(Fig. 2 - Level 0 Data Flow)

A1 Frame Selection Command line tool

•ffmpeg is a charge line instrument that proselytes sound or video positions. It can likewise catch and encode progressively from different equipment and programming sources, for example, a TV catch card.

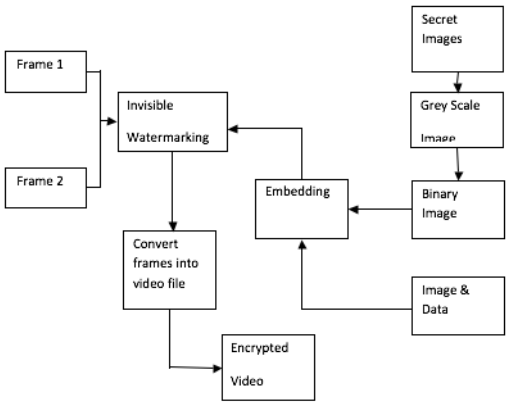
•ffserver is an HTTP and RTSP multimedia [5] streaming [7] server for live and recorded communicates. It can likewise be utilized to time move live communicate

•ffplay is a straightforward media player utilizing SDL and the FFmpeg libraries.

•ffprobe is an order line apparatus to show media data (text, CSV, XML, JSON), see also Mediainfo.

B. Data Embedding

This includes two modules of the work, **Visual Cryptography [2]** and **Data Hiding**.



(Fig. 3 - Level 1 Data Flow)

Visual Cryptography

In this module, any two edges from n number of edges which were gotten before are chosen. At that point a Secret picture is chosen and this picture is then changed over into Gary scale [6] picture and further changed over into Binary picture. At last, the paired picture is part up into two shares. These shares are utilized with the end goal of visual cryptography.

Algorithm Description

The application will take credential to secure as input and will generate secured image as output containing secret data. This image is then feed as input to the visual cryptography algorithm.

Algorithm1: Steganography [2] using genetic algorithm

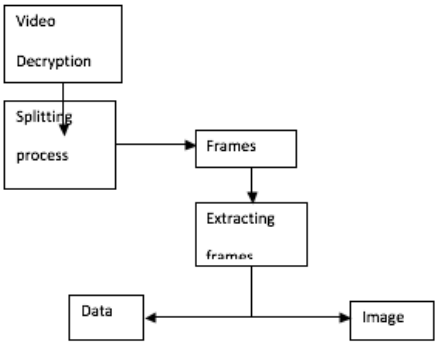
Step 1: Read Encrypted user credentials
Step 2: Read the image for hiding data.
Step 3: Find out the pixel values of that image.
Step 4: Encrypted string is embedded in image using LSB Steganography [2]
Step 5: Modified image pixels are shuffled using genetic algorithm
Step 6: Image is divided into 8*8 blocks.
Step 7: Blocks are repositioned by the needed number of predefined scanning algorithm to shuffle image structure.

Algorithm2: Visual cryptography technique

Step 1: Read the output of Algorithm1 as input.
Step 2: This image file is first converted into a binary image
Step 3: Then each pixel in the secret image is broken into 8 sub pixels, 4 pixels in each share by selecting the random pixel
Step 4: This shares are then transmitted over network [4].

Data Hiding

In this module, the shares which were spitted from the binary picture is utilized to shroud the information to be transmitted. The information is encoded utilizing Paillier calculation or Paillier cryptosystem and by utilizing the Steganography [2] method the figure content is inserted into the two shares. The Invisible Watermarking procedure [3] is utilized to conceal two shares into the chose outlines and after the picture is shrouded, every one of the casings are changed over into video and stir up with sound lastly video is scrambled utilizing the Base 64 Encoder.



(Fig. 4 - Level 2 Data Flow)

Proposed Work

The principle high determination AVI fie is only a grouping of high determination picture called outlines. At first I will jump at the chance to stream [7] the video and gather every one of the casings in bitmap arrange. And furthermore gather the accompanying data:

a. Starting frame: It shows the casing from which the calculation begins message installing.

b. Starting macro block: It demonstrates the large scale obstruct inside the picked outline from which the calculation begins message inserting.

c. Number of macro blocks: It shows what number of large scale obstructs inside an edge will be utilized for information stowing away. These large scale pieces might be successive edge as indicated by a predefined design. Clearly, the more the full scale pieces we utilize, the higher the inserting limit we get. In addition, if the span of the message is settled, this number will be settled, as well. Else it can be powerfully changed.

d. Frame period: It demonstrates the quantity of the bury outlines, which must go, before the calculation rehashes the installing. In any case, if the casing time frame is too little and the calculation rehashes the message all the time, that may have an effect onto the coding effectiveness of the encoder.

C. Data Extraction

This is the last module of the work, initial an open key is gotten by goal and the Encryption will be done utilizing goal open key. In the wake of encoding the video is transmitted over the system [4]. At the beneficiary end, video is Decrypted and part into casings. At that point the procedure of extraction of picture shares and information occurs by choosing the casings which was watermarked [3]. Subsequent to extricating the Image and the Data, the Data should be Decrypted and the Image got is boisterous, so it is expected to reproduce the picture in order to get the Binary picture.

IV. CONCLUSION

In this paper we presented an efficient stream- level joint source-channel adaptive authentication scheme for wireless H.264/AVC streaming by making full utilization of the H.264 source and channel information and base 64 encryption which authenticates the video on the receiver's end with the enhancement of data hiding within the video using cryptographic technique for encoding the secret data, visual cryptography and invisible watermarking are used for the purpose of hiding the secret data into the image and further into the video for transmission.

REFERENCES

[1] Arup Kumar Bhaumik1 , Minkyu Choi2 , Rosslin J.Robles3 , and Maricel O.Balitanas4 1 Heritage Institute of Technology, Kolkata-700107, India 2, 3,4Hannam University,Daejeon, Korea

[2] Mrs. G. Prema, S. Natarajan, "Steganography [2] using genetic Algorithm along with visual Cryptography for Wireless Network Application", International conference on information communication and embedded systems (ICICES), 2013.

[3] Analysis and Design of Authentication Watermarking Chuhong Fei a, Deepa Kundur b. and Raymond Kwong a aUniversity of Toronto, 10 King's College Road, Toronto, ON Canada M5S 3G4; bTaxas A&M University, 3128 TAMU, College Station, TX USA 77843-3128.

[4] AN OPTIMIZED CONTENT-AWARE AUTHENTICATION SCHEMEFOR STREAMING JPEG-2000 IMAGES OVER LOSSY NETWORKS Zhishou Zhang1,2, Qibin Sun1 , Susie Wee3 and Wai-Choong Wong1,2 1 Institute for Infocomm Research, Singapore 2 Department of ECE, National University of Singapore, Singapore 3 Hewlett-Packard Laboratories, Palo Alto, CA USA.

[5] Flexible Layered Authentication Graph for Multimedia Streaming Xinglei Zhu1 ,Zhishou Zhang1 , Zhi Li 2 and Qibin Sun1 1 Insititute for Infocomm Research, A*STAR, Singapore 2 Department of ECE, National Univerisity of Singapore 1 {xzhu, zszhang, qibin}@i2r.a-star.edu.sg, 2 lizhi@nus.edu.sg.

[6] Rate-Distortion Analysis of Dead-Zone Plus Uniform Threshold Scalar Quantization and Its Application—Part II: Two-Pass VBR Coding for H.264/AVC Jun Sun, Member, IEEE, Yizhou Duan, Jiangtao Li, Jiaying Liu, Member, IEEE, and Zongming Guo, Member, IEEE.

[7] Efficient Authentication and Signing of Multicast Streams over Lossy Channels Adrian Perrigy Ran Canettiz J. D. Tygary Dawn Songy y UCBerkeley,zIBM T.J.Watson fperrig,tygar,dawnsong@cs.berkeley.edu, canetti@watson.ibm.com.

[8] 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.

[9] R. Gennaro and P. Rohatgi, "How to sign digital streams," in *Advances in Cryptology*, pp. 180–197, 1997.

[10] C.-S. Lu and H.-Y. M. Liao, "Structural digital signature for image authentication: An incidental distortion resistant scheme," *IEEE Trans. Multimedia*, vol. 5, no. 2, pp. 161–173, Jun. 2003.

[11] Z. Zhang, Q. Sun, W.-C. Wong, J. Apostolopoulos, and S. Wee, "An optimized content-aware authentication scheme for streaming JPEG-2000 images over lossy networks," *IEEE Trans. Multimedia*, vol. 9, no. 2, pp. 320–331, Feb.2007.

[12] G. Qiu, P. Marziliano, A. T. S. Ho, D. He, and Q. Sun, "A hybrid watermarking scheme for H.264/AVC video," in *Proc. 17th Int. Conf. Pattern Recognit.*, vol. 4. Cambridge, U.K., Aug. 2004, pp. 865–868.