World Research Journal of Human-Computer Interaction
ISSN: 2278-8476 & E-ISSN: 2278-8484, Volume 1, Issue 1, 2012, pp.-01-03.
Available online at http://www.bioinfo.in/contents.php?id=219

ENCRYPTION AND WATERMARKING USED TO SECURE LIVE VIDEO

YERAWAR A.A.*, VIPLAV KUMAR R. PRASAD, PAWAR V.R., HINGANE A.M.

Department of computer science, J.D.I.E.T. Yavatmal, MS, India.
*Corresponding Author: Email- anushree.yerawar@rediffmail.com

Received: February 28, 2012; Accepted: May 03, 2012

Abstract- Multimedia data are protected by providing the security. Encryption and watermarking is used to secure multimedia data. Encryptions are of various types such as selective encryption, Slice level encryption and full encryption. Slice level encryption is the modern technique used to defend multimedia data. It is beneficial than other encryption systems because it saves much execution time and also reduces the computational work load. In this paper, we provide information of the proposed scheme, discuss the present issues. In this paper, we assume the live video and protect that video by encryption and watermarking.
Keywords- Computational workload, Encryption, Multimedia, Security, Full encryption, Selective encryption, Slice level encryption, Watermarking.

Citation: Yerawar A.A., et al. (2012) Encryption and Watermarking Used to Secure Live Video. World Research Journal of Human-Computer Interaction, ISSN: 2278-8476 & E-ISSN: 2278-8484, Volume 1, Issue 1, pp.-01-03.

Introduction

Multimedia data is the grouping of one of the following medium such as text, motionless images, audio, moving picture, and video. These multimedia contents are protecting by providing the security [9]. By using knowledge of multimedia, the multimedia data can be transfer to/from users having transferable devices such as movable phones. Multimedia data delivery having issues of the objects privileges and the secrecy and therefore defending the multimedia information becomes necessary in multimedia used devices. [2-4], because a big quantity of multimedia information contains enormous sizes, we require a dexterous encryption method for defending the multimedia data at the same time as fulfilling the concurrent necessity [5-8]. In this paper, we proposed the slice level encryption approach for protecting multimedia data. Computational workload essential for this encryption is very less. Encryption basically means to convert the note into code or warped form, so that any anyone who does not have the 'key' to decipher the code cannot analysis it. This is generally completed by using a secret message. A secret message is a form of algorithm used in encryption that uses a certain described technique to mix up the data. The secret message can only be 'deciphered' with a 'key'. A key is the concrete described method' that was used to scramble the data, and therefore the key can also unscramble the data. When the data is unscrambled by the use of a key, that is what is known as 'decryption'. It is the contradictory of encryption and the 'described method' of scrambling is fundamentally applied in reverse, so as to unscramble it. Without encryption and description, there would be no 'security' in the network. Watermarking is also used to secure the data.

Full encryption

In this according to the name whole data is encrypted. So it requires more execution time.

Selective encryption

In this technique whole I-frame is encrypted. It requires the less execution time as compare to full encryption but cannot satisfy actual instance necessity. And it cannot satisfy the actual moment necessity.

Slice level encryption

The MPEG which is the standard of video compression is used to

protect the video.MPEG 2 having the inaccuracy circulation property. Because of this requires less computational workload. The fundamental proposal behind the proposed approach is to reduce the workload of encrypting the I-frames by exploiting the inaccuracy circulation property in MPEG2 standard. The slide contains the micro blocks. Because of inaccuracy circulation Property, if only first micro block is encrypted then the successive micro blocks are encrypted. This technique takes less computational workload and requires less execution time than other approaches. In this, first the live video is captured and then converted it into the number of frames. And after the encryption whole video we are getting as it is. The below figure shows the how much percent of the frames are encrypted. The shaded portion shows the encrypted region. In level 0, there is no encryption takes place. In level 1, only header is encrypted and at level 2, only I block is encrypted. In level 3, I block and I frame is encrypted [1]. SECMPEG is the secure MPEG.

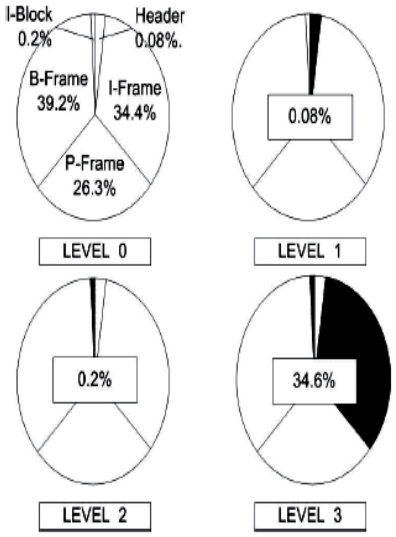

Fig. 1- The size of the data to be encrypted by SECMPEG security level. [1]

Overview of I, B, P-Frames

I-frames are the slightest compressible but don't have need of other video frames to decipher. P-frames can utilize information from preceding frames to decompress and are extra compressible than I-frames. B-frames can utilize equally preceding and frontward frames for information reference to get the maximum quantity of information density. An I-frame is an 'Intra-coded picture', in result a entirely precise image, like a predictable stationary picture file. P-frames and B-frames clutch just fraction of the image information, so they need less space to store than an I-frame, and thus improve video compression rates. A P-frame ('Predicted picture') holds only the changes in the image from the preceding frame. For example, in a scene where a car moves across a stationary background, only the car's movements need to be encoded. The encoder does not need to store the unchanging surroundings pixels in the P-frame, thus saving space. P-frames are also known as delta-frames. A B-frame ('Bi-predictive picture') saves even extra space by using differences between the present frame and both the past and subsequent frames to identify its substances.

Advantages

a. It prevents piracy
b. It takes a smaller amount computational workload
c. It requires less finishing time
d. It works on live video

Experiment Result

In this paper, we are taking a live video. First the live video is captured as shown in fig 2.

Fig. 2- Input

Then the video is converted into frames simultaneously when the video is captured. And stored into a folder. Then we are entered watermark text into first frame and encrypt the frames. Frames rate are depend on us, how much frames are encrypted per second. After that we are getting the following output as shown in fig 3, with watermark text on it.

Fig. 3- Output

Conclusion

In this paper, we proposed slice level encryption approach for protecting video data. This approach reduces the computational workload. It requires less computational workload and also takes less execution time as compares to other approaches. Our experimental result shows the encryption of live video.

References

[1] Seohyun Jeong, Eunji Lee, Sungju Lee, Youngwha Chung Byoungki Min (2011) *Slice level elective encryption for protect-*

ing video data.
[2] Furht B. and Kirovski D. (2005) *Multimedia Security Handbook*, CRC press.
[3] Massoudi A., et al. (2008) *EURASIP J. on Information Securit*.
[4] Liu F. and Koenig H. (2009) *Computer and security,* 29(1), 3-15.
[5] Jakimoski G. and Subbalakshmi K. (2008) *IEEE Tr. Multimedia*, 10(3), 330-338.
[6] Liu X. and Eskicioglu A. (2003) *Proc. of Conf. Communications, Internet, and Information Technology*, 17-19.
[7] Lian S., Kanellopoulos D. and Ruffo G. (2009) *Informatica*, 33, 3-24.
[8] Kulkarni N., Raman B. and Gupta I. (2009) *SCI,* 231, 417-449.
[9] Seidel T., Socek D. and Sramka M. (2003) *Proc. of Central European Conf. on Cryptology*.
[10] *http://www.blurtit.com/q783423.html*.