ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

A Robust System for Video and Data Encryption/Decryption Based On Codeword Encoding/Decoding

Tushar K Shinde, Dr.S.S.Shriramwar, Prof.Vishal Punchbhai

PG Scholar, Department of ETC, PCE Nagpur, Rastrasant Tukdoji Maharaj University Nagpur, Maharashtra, India

Associate Professor, Department of ETC, PCE Nagpur, Rastrasant Tukdoji Maharaj University Nagpur, Maharashtra, India

Assistant Professor, Department of ETC, PCE Nagpur (MH) Rastrasant Tukdoji Maharaj University Nagpur, Maharashtra, India

ABSTRACT: Data hiding in encrypted media is a new topic that has started to draw attention because of the privacy-preserving requirements from cloud data management. In this synopsis, an algorithm to embed additional data in encrypted H.264/AVC bit stream is presented, which consists of video encryption, data embedding and data extraction phases. The algorithm can preserve the bit-rate exactly even after encryption and data embedding, and is simple to implement as it is directly performed in the compressed and encrypted domain, i.e. it does not require decrypting or partial decompression of the video stream thus making it ideal for real-time video applications. The data-hider can embed additional data into the encrypted bit stream using code word substituting, even though he does not know the original video content. Since data hiding is completed entirely in the encrypted domain, this method can preserve the confidentiality of the content completely. Confidentiality is a set of rules that prevents the disclosure of any confidential information to unauthorized individuals or systems. Confidentiality of any information can be achieved by data hiding which is a process to hide data into a cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data.In this synopsis, a novel scheme of data hiding directly in the encrypted version of H.264/AVCvideo stream is proposed, which includes the following three parts, i.e., H.264/AVC video encryption, data embedding, and data extraction. By analyzing the property of H.264/AVC codec,the code words of intra-prediction modes, the code words of motion vector differences, and the code words of residua coefficients are encrypted with stream ciphers. Then a data hider, may embed additional data in the encrypted domain by using code word substitution technique, without knowing the original video content.

KEYWORDS: Data hiding encrypted domain, H.264/AVC, code word substituting, privacy-preserving, decompression, data embedding, data extraction.

I. INTRODUCTION

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files Steganography's ultimate objectives, which are un-detectability, robustness and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. Reversible data hiding in images is a technique that hides data in digital images for secret communication. It is a technique to hide additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message.

Traditionally, data hiding is used for secret communication. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to reveal the presence of the embedment. Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before data hiding is actually performed,such as military images or confidential medical images. In this case, the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image.

Till now, few successful data hiding schemes in the encrypted domain have been reported in the open literature. In a watermarking scheme in the encrypted domain using Paillier cryptosystem is proposed based on the security requirements of buyer-seller watermarking protocols. A Walsh-Hadamard transform based image watermarking algorithm in the encrypted domain using Paillier cryptosystemis presented. However, due to the constraints of the Paillier cryptosystem, the encryption of an original image results in a high overhead in storage and computation. Note that,several investigations on reversible data hiding in encrypted images are reported in literature recently. The encryption is performed by using bit-XOR (exclusive-OR) operation. In these methods, however, the host image is in an uncompressed format.

In another robust watermarking algorithm it is proposed to embed watermark into compressed and encrypted JPEG2000 images.With the increasing demands of providing video data security and privacy protection, data hiding in encrypted H.264/AVC videos will undoubtedly become popular in the near future. Obviously, due to the constraint of the underlying encryption, it is very difficult and sometimes impossible to transplant the existing data hiding algorithms to the encrypted domain. To the best of my knowledge, there has been no report on the implementation of data hiding in encrypted H.264/AVC video streams. Only few joint data-hiding and encryption approaches that focus on video have been proposed.The compression/decompression cycle is time-consuming and hampers real-time implementation. Besides, encryption and watermark embedding would lead to increasing the bit-rate of H.264/AVC bitstream.Therefore, it becomes highly desirable to develop data hiding algorithms that work entirely on encoded bitstream in the encrypted domain However, there are some significant challenges for data hiding directly in compressed and encrypted bitstream.The first challenge is to determine where and how the bitstream can be modified so that the encrypted bitstream with hidden data is still a compliant compressed bitstream. The second challenge is to insure that decrypted videos containing hidden data can still appear to be of high visual fidelity. The third challenge is to maintain the file size after encryption and data hiding, which requires that the impact on compression gain is minimal.

The fourth challengeis that the hidden data can be extracted either from the encrypted video stream or from the decrypted video stream, which is much more applicable in practical applications.

LITERATURE SURVEY

1) According to D.W.Xu ,R.D.Wang the method of Exp-Golomb code words mapping is gives watermarking in H.264/AVC compressed domain.
2) According to X.P. Zhang the method of A novel reversible data hiding algorithm is gives Reversible Data Hiding
3) According to T. Margaret the method of XOR ciphering technique is give Reversible Data Hiding In Encrypted Imagesby XOR Ciphering Technique

WORKING

ENCODING

1 Run the video files. The video files is simulated using MATALAB simulink
2 The video and audio outputs are available in workspace
3 Read the secret image
4 Convert the image to Grayscale
5 Resize the image as per video frame size
6 Encrypt the secret image
7 Ask user password to select frame (s) from the complete video
8 select two frames for MSB and LSB enconding of the secret image pixel intensity value

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

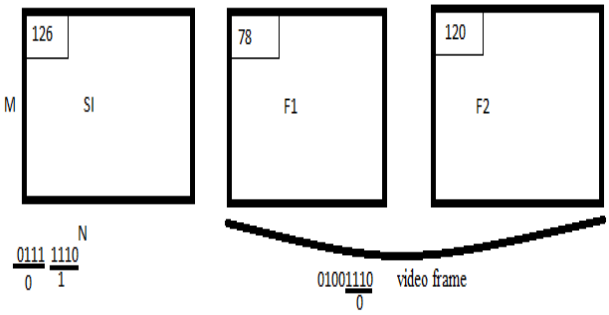


Fig 1: Encoding :- Secret image pixel = 126

9 Loop for frame size (M,N)
10 Convert secret image pixel and frames pixel in binary
Replace frame 1 lower 4 LSB'S by 4 MSB'S of secret image
Replace frame 2 lower 4 LSB'S by 4 LSB'S of secret image
11 Create two new frames that are encoded frames

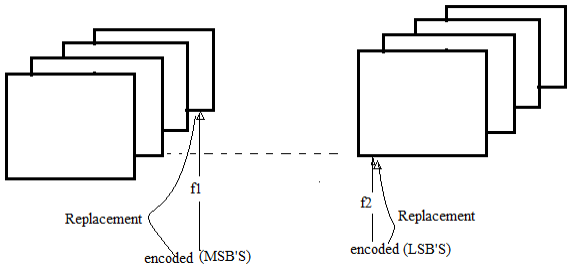
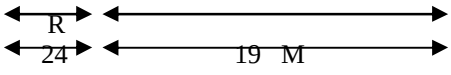


Fig 2 : Replace these two frame that is insert these new two frames in place of old frames in the video

12 Play the video.
13 Ask the user to input text massage
Ex- Tushar Shinde
14 Encrypt the massage using interleving
15 convert the text massage from ASCII to unsigned integer [0,255]
16 Consider any one channel of audio signal
17 find length of text massage – L
18 Divide audio sequence by L and find remainder
19 Subtract the remainder value from audio signal starting from first
Ex : Tushar Shinde
L= 13* 8
= 104
Assume audio length = 2000
Remainder R = 2000/(13*8) = 24



Segment of L

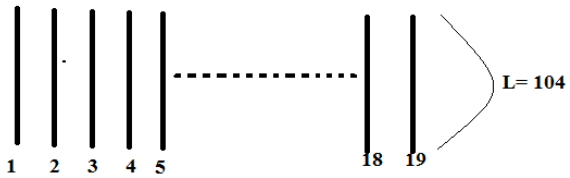
20 Reshape remaining audio into segment of length L as

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

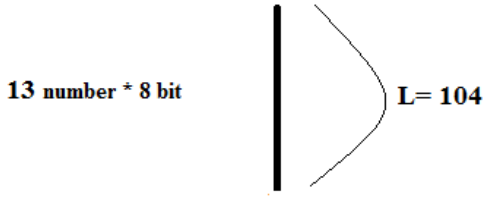
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015



21 Ask user password to select any one segment
password =4



22 for every ASCII value in text massage convert it into binary

1) ASCII value of T= 84 (Say)
01010100 = 84
1 = even parity
0 = odd parity
23 for every number (unsigned integer 8) [0, 255]
Parity
a) if the parity is even and text bit is 1
- Don't change the number
b) if the parity is odd and text bit is 1
- complement's LSB bit of audio
c) if the parity is even and text bit is 0
- complement's LSB bit of audio
d) if the parity is odd and text bit is 0
– don't change the number
24 Replace the encoded audio segment in original signal
25 Play the audio by arranging the audio segment.

DECODING

Just reverse the encoding process

II. CONCLUSION

The synopsis proposes a novel scheme to embed secret data directly in compressed domain first we encrypted the secret image and then we hide the encrypted secret image using MSB and LSB algorithm in H.264/AVC bit stream. And in additional we hide the text message in audio segment insted of video frames, first we encrypt the text meassage by applying interleaving then by using parity encoding we hide the encrypted message in one of the audio channel.In audio we get excelent efficiency,In contrast to the existing technologies discussed above, the proposed scheme can achieve excellent performance in the three different prospects.

III. SIMULATION RESULTS

MSE for 4 MSB encoding in video - 15.5704
MSE for 4 LSB encoding in video - 21.8013
MSE for Audio encoding - 15.5704

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

PSNR for 4 MSB encoding in video - 36.2078
PSNR for 4 LSB encoding in video - 34.746
PSNR for Audio encoding - 91.4273
Your Interleaved hidden text -
'ednihS rahsuT'
Your Original hidden text -
Tushar Shinde

IV. SIMULATION RESULTS

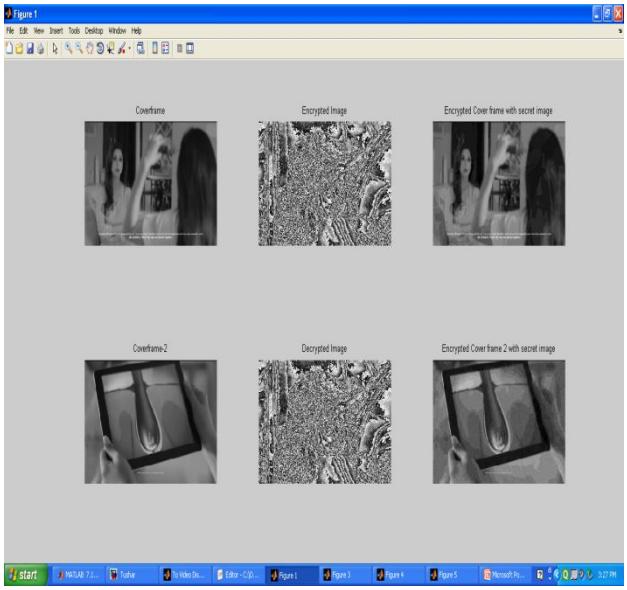


Fig 3 coverframe with encrypted secret image

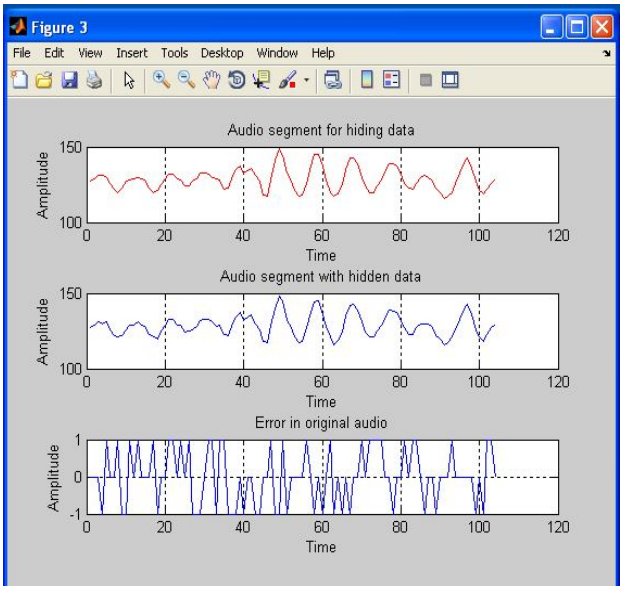


Fig 4 Audio segment for hiding data

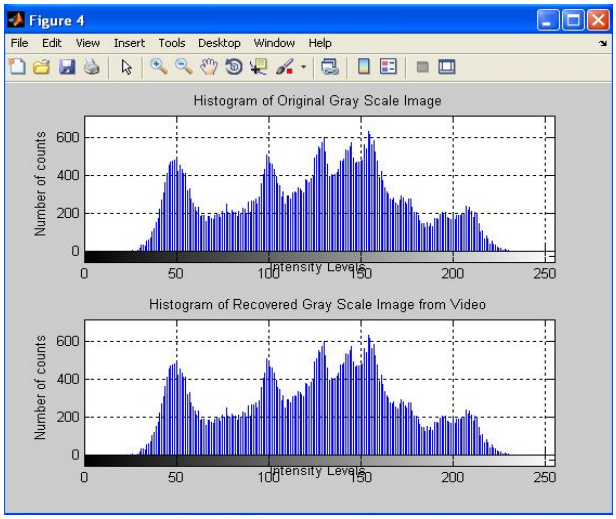


Fig 5 Histogram of original and gray scale image

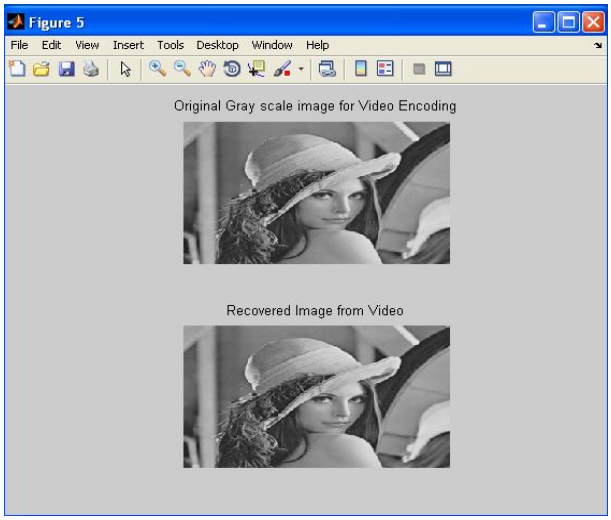


Fig 6 original gray scale for video encoding and Recovered image from video

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

REFERENCES

1 X. P. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2,pp. 826–832, Apr. 2012.
2 W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process.Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.
3 D. W. Xu, R. D. Wang, and J. C. Wang, "Prediction mode modulated data-hiding algorithm for H.264/AVC," J. Real-Time Image Process.,vol. 7, no. 4, pp. 205–214, 2012.
4 X. P. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
5 D. W. Xu and R. D. Wang, "Watermarking in H.264/AVC compresseddomain using Exp-Golomb code words mapping," Opt. Eng.,vol.50, no.9, p. 097402, 2011.
6J. G. Jiang, Y. Liu, Z. P. Su, G. Zhang, and S. Xing,"An improved selective encryption for H.264 video based on intra prediction mode scrambling,"J. Multimedia, vol. 5, no. 5, pp. 464–472, 2010.

BIOGRAPHY

Tushar K Shinde is a Student of M-Tech (2nd year pursuing) in the Electronic and Communication Depatment,Priyadarshini college of Engineering,Nagpur (RTMNU). His research interests are Computer Networks (wireless Networks),Image processing etc.