ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Secret Data Hiding in Encrypted Compressed Video Bitstreams

Sagar Rajkumar Somani[1], P.S.Malge[2]

P.G. Student, Department of Electronics Engineering, Walchand Institute of Technology, Solapur, Maharashtra, India[1]

Associate Professor, Department of Electronics Engineering, Walchand Institute of Technology, Solapur, Maharashtra, India [2]

ABSTRACT: "Advanced Video Coding" standard also known as H.264 and MPEG-4/Part 10 has dominated the video coding standardization community. It is the standard established by International Telecommunication Union (ITU) and International Standard Organization (ISO). Moving Pictures Experts Group (MPEG) is a generic means of compactly representing digital images, video and audio signals. The H.264 is an emerging video coding standard jointly developed by both ISO/IEC and ITU-T. It includes new coding features to give unmatched compression while preserving the quality. H.264 also provides greater network friendliness and higher error robustness making it suitable for use in wide range of applications. The new H.264/AVC standard is designed to provide a technical solution appropriate for a broad range of applications, from streaming internet video to broadcast digital television. It supports a wide range of bit rates and picture sizes. The technical design is highly focused on providing high coding efficiency and robustness to network environments for conventional rectangular-picture camera-view video content. MPEG-2 standard is designed to produce high quality images at higher bit rates with picture sizes exceeding 1600x1200 pixels. MPEG-4 extends this system to provide compression support for TV quality transmission of digital video at picture sizes of up to 1024x768 pixels at 30 frames per second. With the widespread use of technologies like digital television, internet streaming video and DVD video, video compression has become an inevitable component of broadcast and entertainment media. Currently, the video codec that achieves the highest data compression without sacrificing on the picture quality is the MPEG-4 Part 10 Advanced Video Coding, also known as the H.264. This codec has many new features such as Intraframe prediction, 4x4 Integer Transform, Quantization, Context Adaptive Variable Length Coding (CAVLC), etc., which were not available in the earlier standards. The present work has realized some of the above features. The implementation conforms to the baseline, main as well as extended profiles since only Intra (I) frames are used.

KEYWORDS: Encryption, chaos, bit substitution, secret, decryption.

I. INTRODUCTION

Image and Video Compression has been a very active field of research and development for over 20 years and many different systems and algorithms for compression and decompression have been proposed and developed. In order to encourage inter working, competition and increased choice, it has been necessary to define standard methods of compression, encoding and decoding to allow products from different manufacturers to communicate effectively. This has led to the development of a number of key International Standards for image and Video Compression, including the JPEG, MPEG and H.26X series of standards [3-7]. Video compression plays an important role in enabling video processing on multimedia systems. Video compression is essential in order to reduce the storage requirements to manageable levels and to transmit data with the existing channel capacities. The Video Codec that achieves the highest data compression without sacrificing on the picture quality is the MPEG-4 Part 10 Advanced Video Coding, also known as the H.264 [1]. While implementations of the Integer Transform [8, 9] on hardware have been reported, no implementation of Intra Prediction has been found to the best of author's knowledge. Qiang Peng et al. [5] have reported an implementation of the H.264 encoder using a 32-bit RISC CPU on a single chip running on Linux operating

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

system, which can process PAL, SECAM or NTSC video at 80 MHz. An implementation of the Context Adaptive Variable Length Coder, which uses two-stage block pipelining scheme for parallel processing of two 4x4 blocks using cell based design flow has been reported by Tung-Chien Chen et al. [7]. It has been reported as cell based design with 23.6 K logic gates operating at 100 MHz. A "structured truncated Golomb code" for the context based adaptive VLC by Sadaatsu Kato et al. [9] offers similar coding efficiency in comparison with the dedicated unstructured VLC, while reducing the size of memories to store code tables. Ihab Amer et al. [6] have reported VLSI prototype for Context-based adaptive variable length coding for lossless compression. Their architecture for the CAVLC has been realized using VHDL language and simulated using Modelsim. It is synthesized using Synplify Pro 7.1 and the critical path estimated by the Synthesis tool is 31.3 ns. This corresponds to the maximum operating frequency of about 32 MHz. In another paper, a simple and cost effective Video Encoder with memory efficient context adaptive variable length coder is proposed for low cost multimedia applications by Yeong-Kang Lai etal. [8]. It is implemented on a Xilinx FPGA prototyping board. Its maximum operating frequency was reported as 28 MHz.

II. METHODOLOGY

2.1 Video Encryption and Data Hiding:

2.1.1 Input Video:

The encoding process starts with selecting the video for data hiding. Video can be selected from any location of the computer. This video is divided into multiple frames. Each of these frames is an image. The frame is encrypted using any one of the convenient encryption mechanisms.

2.1.2 H.264/AVC coder:

In H.264/AVC coder converts video into a compressed format by setting appropriate macroblock size and quantization respectively.

2.1.3 Video Encryption:

The Advanced Encryption Standard uses XOR on single byte. XOR is used in the key schedule. The last bit of the bitstream is encrypted by applying the bitwise XOR operation with a standard stream cipher.

2.1.4 Input Message:

Input the text data which is to be hided in to an image. The text may be either numerical, alphabets or combination of both. The data which is given as input is converted into its corresponding binary form.

2.1.5 Chaos Encryption

This method is one of the advanced encryption standard to encrypt the secret text data for secure transmission. It encrypts the text data's with encryption key value generated from chaotic sequence with threshold function by bit XOR operation. It is very useful to transmit the secret data through unsecure channel securely which prevents data hacking.

2.1.6 Data hiding

Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. Data Hiding is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message.

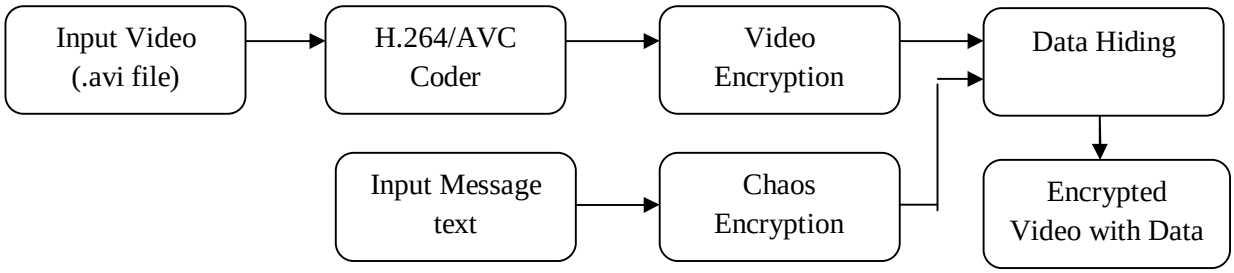
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017



2.1Video Encryption and Data Hiding

2.2 Data Extraction and Video Decryption:

2.2.1 Encrypted Video with Data

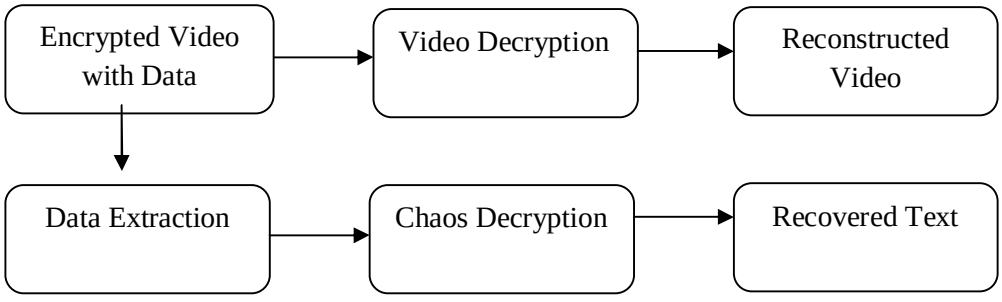
To protect privacy, a data manager may only get access to the data hiding key and have to manipulate data in encrypted video.

2.2.2 Data extraction

In encrypted video guarantees the feasibility in this case. Encrypted video with hidden data is directly sent to the data extraction module.

2.2.3 Video Decryption & Reconstruction

An authorized user, which owned the encryption key, received the encrypted video with hidden data. The received video can be decrypted using the encryption key. Thus the original frames are reconstructed. Therefore, an algorithm is developed to hide the secret data in compressed video bit stream and to achieve better performance in terms of computation efficiency, high data security and video quality after decryption. The parameters such as Mean Square Error, PSNR, Correlation and SSIM will be evaluated to measure its efficiency.



2.2 Data Extraction and Video Decryption

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

III. RESULTS

The proposed data hiding scheme has been implemented in H.264/AVC. Before data hiding in encrypted compressed video signal the secret text data was encrypted using chaos crypto system. Then this encrypted secret text data was embed with the encrypted compressed video signal by bits replacement technique. The user has been given choice to choose the number of frames to process for data hiding. Then, in order to adapt different application scenarios, data extraction is done either in encrypted domain or in decrypted domain. So, the proposed data hiding algorithm has been developed which will hide the secret text data in the encrypted compressed video signal, which preserves the confidentiality of the content. The parameters such as mean square error (MSE), peak signal to noise ratio (PSNR), correlation and structural similarity index (SSIM) are evaluated to measure its efficiency.

Fig a. input video

Fig a. shows input video where user can choose .avi files which are to be processed. Fig b. shows frame count and secret data where when user selects .avi files to process, it shows total number of frames it contains and also user can select number of frames to be processed and then it user selects the input secret text data and in this example we are taking input secret data as SagarSomani. Fig c. shows encrypted secret data where the secret data file selected by user is encrypted by using chaos crypto system.

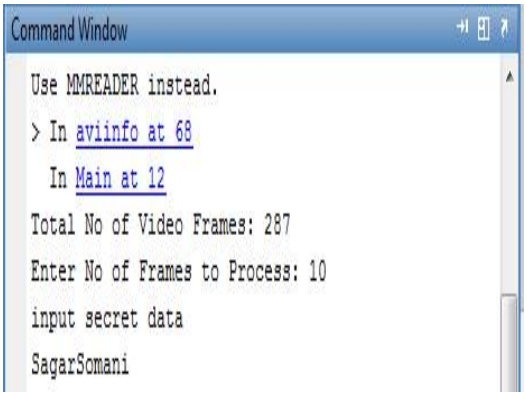


Fig b. Frame count and input secret data

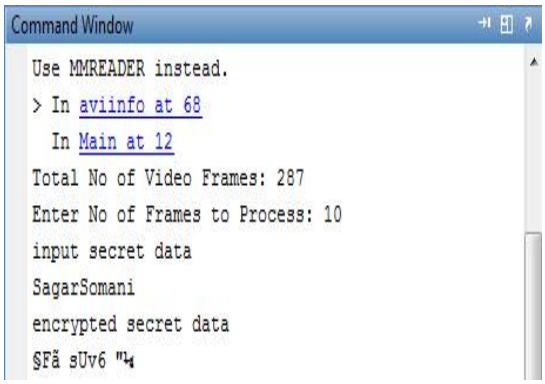


Fig c. Encrypted secret data

Fig d. shows encrypted frames with secret data where the number of frames selected to process by user is embed with the input secret data using bits substitution technique to prevent the confidentiality of the content. Fig e. shows reconstructed frames where the receiver will receive the frames with the secret data and when user decrypts the data by

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

using decryption key, user gets the reconstructed frames back which were chosen to process and also the secret data send by the receiver. Fig f. shows recovered secret data and parameter calculation where secret data send by sender to receiver is received after decryption and the parameters such as mean square error, peak signal to noise ratio , correlation and structural similarity index are evaluated to measure its efficiency.

Fig d. Encrypted frames with secret data

Fig e. Reconstructed frames

```
Command Window
Use MMREADER instead.
> In aviinfo at 68
  In Main at 12
Total No of Video Frames: 287
Enter No of Frames to Process: 10
input secret data
SagarSomani
encrypted secret data
§Fã sUv6 "¼
Secret text was hidden at compressed I frame
Raw Input File Size(in Bytes) :
      253440

Compressed File Size(in Bytes) :
       70928

Compression Ratio :
    3.5732

SagarSomani
Recovered Secret text:
SagarSomani
Mean Square Error :
    0.4236

Peak Signal to Noise Ratio(dB) :
   51.8615

Correlation :
    0.9998
```

Fig f. Recovered secret data and parameter calculation

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

The proposed data hiding scheme has been implemented in H.264/AVC. Before data hiding in encrypted compressed video signal the secret text data was encrypted using chaos crypto system. Then this encrypted secret text data was embed with the encrypted compressed video signal by bits replacement technique. The user has been given choice to choose the number of frames to process for data hiding.

Then, in order to adapt different application scenarios, data extraction is done either in encrypted domain or in decrypted domain. So, the proposed data hiding algorithm has been developed which will hide the secret text data in the encrypted compressed video signal, which preserves the confidentiality of the content.

The parameters such as mean square error (MSE), peak signal to noise ratio (PSNR), correlation and structural similarity index (SSIM) are evaluated to measure its efficiency.

Below table shows result of parameters calculated for secret data hiding in different videos for different quantization parameter(QP) values. Six different videos are used with different frame size and same text data was embed into the videos and parameters named mean squared error (MSE), peak signal to noise ratio (PSNR), correlation, structural similarity index (SSIM) are calculated by setting different values of quantization parameter(QP).It has been observed that when quantization parameter(QP) is set to 15, better results are obtained.

Setting quantization parameter value (QP) to a high value means that more coefficient are set to zeros, resulting in high compression at the expense of poor decoded image quality. Setting quantization parameter (QP) to a low value means that more non-zero coefficients remain after quantization, resulting in better decoded image quality but lower compression.

Video	QP	MSE	PSNR	Correlation	SSIM
Ball Video (50)	15	0.2943	53.4559	0.9995	0.9932
	24	1.2224	47.2692	0.9993	0.9775
	28	1.9969	45.1350	0.9993	0.9699
	32	3.4976	42.6971	0.9991	0.9607
Inp(2) (127)	15	0.2132	54.9211	0.9994	0.9967
	24	1.2756	47.1807	0.9990	0.9814
	28	2.4429	44.4432	0.9985	0.9685
	32	4.7701	41.6955	0.9975	0.9524
Inp (30)	15	0.5104	51.0547	0.9993	0.9964
	24	3.1283	43.1789	0.9983	0.9820
	28	6.7720	39.8240	0.9972	0.9650
	32	14.8095	36.4269	0.9942	0.9323
Inp2(3) (287)	15	0.5039	51.1090	0.9992	0.9940
	24	2.7700	43.7077	0.9985	0.9736
	28	5.5127	40.7195	0.9975	0.9570
	32	10.8521	37.7783	0.9955	0.9344
Inp2 (60)	15	0.4565	51.5399	0.9993	0.9922
	24	2.3251	44.4709	0.9988	0.9668
	28	4.4832	41.6204	0.9977	0.9419
	32	8.7039	38.7414	0.9970	0.9035
Video2 (73)	15	0.4923	51.2129	0.9991	0.9923
	24	2.3831	44.3605	0.9978	0.9661
	28	4.3884	41.7091	0.9963	0.9415
	32	8.7162	38.7307	0.9935	0.8973

Table3.1 Result analysis for different Quantization Parameter (QP) values.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

IV. CONCLUSION

An algorithm to embed additional data in encrypted H.264/AVC bit stream is presented, that consists of video encryption, data embedding and data extraction phases. Since data hiding is executed entirely in the encrypted domain, a unique method is developed that preserves the confidentiality of the content completely. With an encrypted video containing hidden data, data extraction can be carried out either in encrypted or decrypted domain, which provides two different practical applications. The proposed scheme, viz. encryption and data embedding preserves file-size, whereas the degradation in video quality caused by data hiding is quite small.

REFERENCES

[1] W. J. Lu, A. Varna, and M. Wu, "Secure video processing: Problems and challenges," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.
[2] B. Zhao, W. D. Kou, and H. Li, "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol," Inf. Sci., vol. 180, no. 23, pp. 4672–4684, 2010.
[3] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," Proc. SPIE, vol. 6819, pp. 68191E-1–68191E-9, Jan. 2008
[5] X. P. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
[4] 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.
[5] X. P. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012
[6] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.
[7] X. P. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[8] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.
[9] Dawen Xu, Rangding Wang, and Yun Q. Shi,"Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution," IEEE Transaction on information forensics and security, vol. 9, no. 4, April 2014.