International Journal of Engineering & Technology, 7 (2.24) (2018) 116-120

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Effective Substitution Technique for Data Hiding in Compressed Video Streams

C. Vimala*, P. Aruna Priya

Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Kattakulathur, Kancheepuram, Tamilnadu, India
**Corresponding Author Email: vimalamani09@gmail.com*

Abstract

Data hiding approach is enforced to the encrypted videos for the intent of content notation and tamper detection. Such as, data hiding favored in encrypted domain without decryption extract of the classified content. The substitution techniques is used to data hiding in the compressed video. A video file size is closely maintained even after data encryption and embeds. In this work the data has been restored without any loss with better bit rates, Peak Signal Noise Ratio and testify the feasibility and efficiency of the prospective scheme.

Keywords: *H.264 Encrypt Video, Chao's Data Encryption, Compressed bit streams.*

1. Introduction

In events of storage, the encrypted format of digital video is to be done to maintain during transmission or cloud storage, the most important factor is security of information. Cryptography is defined to keep data or content in encrypted for secure transmission. The approach enables to store precise information or transmit it across unsafe networks, so it is determined to intended recipient only rather by anyone else.Steganography is an approach to hide data from the observer to found an undetectable communication [1]. An stenographic approach covers media in which the top secret information is embedded. The embedding enables a medium by replacing the information with data from hidden message. To the secreted information, this approach gives a more chance to someone unaware of the presence of the hidden message. The scope of steganography is to keep its information undetectable [2]. Usage of cover-images during transmission by sender must be considerably avoided in order to predict the presence of secret messages [3]. As of auto-generated fractal images results good covers as a result of their complexity and irregularity, they are obtained by valid rules that may be easily altered by message embedding[4]. In this paper, remaining section as follow as section 2 two discussed about methodology and section 3 deals with in the prposed system. In section 4 explained result and discussion. Finally the conclusions are discussed in section 5.

2. Methodology

The process of H.264 encryption and hidden data is proceeded functional block diagram as shown in fig 2. Frame processing is the step to prepare the modified video frames by eliminating noise and unwanted object's in the frame in order to escalate the amount of information gained from the frame and sensitivity of the subtraction algorithm[5-6]. Pre-processing is a process of gathering simple image processing tasks that change the input video info in a format. This can be processed by subsequent steps. An Input Video **(.avi file)** shown in fig 2 and fig 3 is taken in account to convert video files into still images for handling it further and to observe the moving objects. By using **aviinfo** command, we can find information for the sequence of images combined from video files and command **frame2im** allow the frames to get converted into images[7]. Establish name to each images and this process will be continued for all the video frames as shown in fig 4 and 5. These frames are labeled as Intra (I), Predicted (P), and Bidirectional (B) frames. At encryption part, each frame is partially branched into uniform size of 16×16 pixels non-overlapping blocks subjectively refered as macro blocks. These macro block each splits into smaller blocks with 4×4 pixels resulting the smallest possible block size[8-9]. These macro blocks are manipulated to Discrete Cosine Transform, entropy coding and quantization. The quantized DCT are further utilized for de-quantization and inverse Discrete Cosine Transform measures for prediction and motion estimation purposes. There are two entropy coding methods are used to encode the quantized transform coefficients.

Fig. 1: Input Test video 1

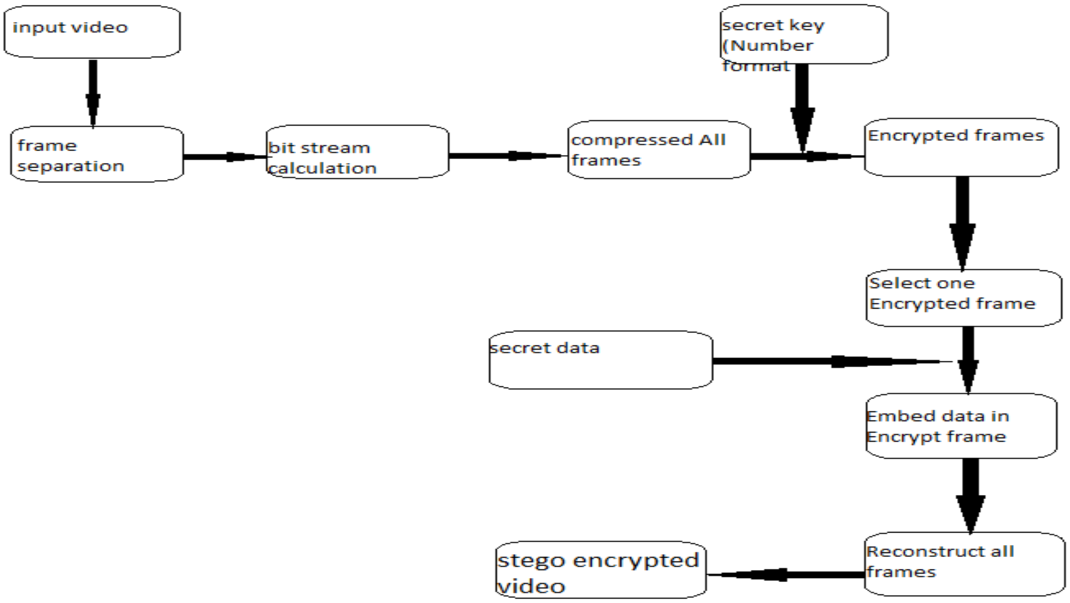

Fig. 2: Block diagram for Video Encryption

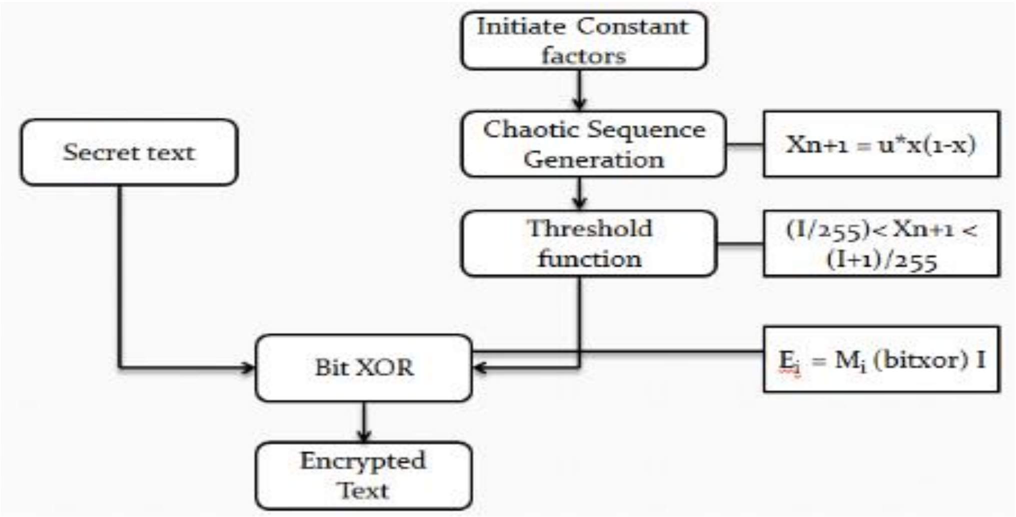

Fig. 3: Chaos encryption flow chart

Fig. 4: Input Test video 2

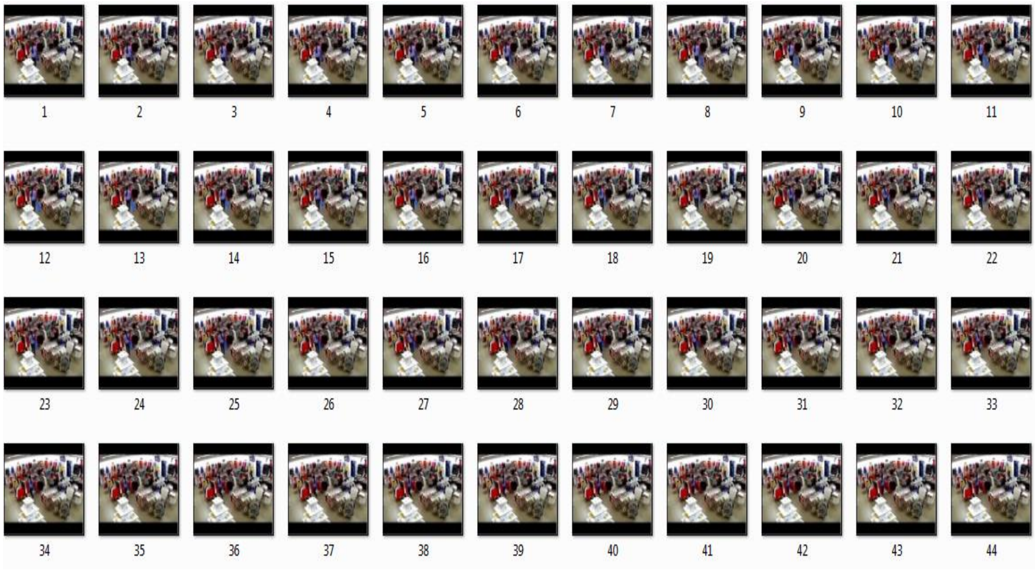

Fig. 5: Frame Separations for Input Video 2

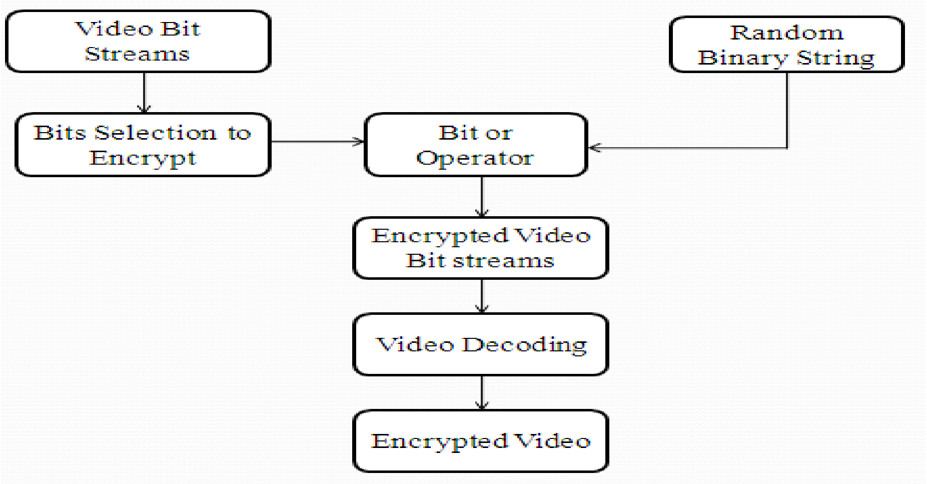

Fig. 6: Video Bits Encryption

3. Proposed Substitution Technique

Data Encryption (Chaos's Encryption) is considering the advanced method of encoding standard to encrypt the confidential text for transmission. The input videos are shown in fig 1 and fig 4. The corresponding video frame separation are shown in fig7 and fig 5. The encryption done by ensuring original text of ASCII values with secured key generated by using the sequence with logical function given as block diagram as shown in fig 6. It is convenient to transmit the confidential message through unsecured channel by which data hacking prevented. The proposed system implements chaos encryption and processed as in given fig 3. The video encryption flow chart is given in 2 and the video bit encryption given in fig 6. Data hiding is a process to obscure secret message bits into another medium like image, audio or video files. Chaos encryption is used for substitution technique.

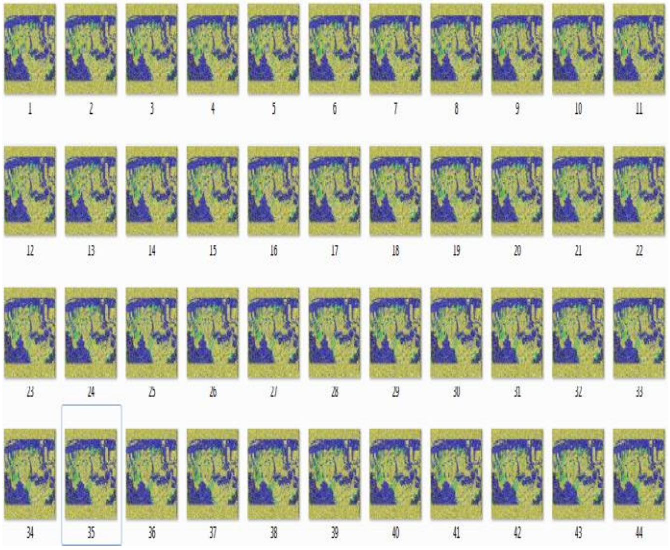

Fig. 7: Frame Separations for Input Video 2

Here, the hiding is performed under compressed bit stream of cover image.

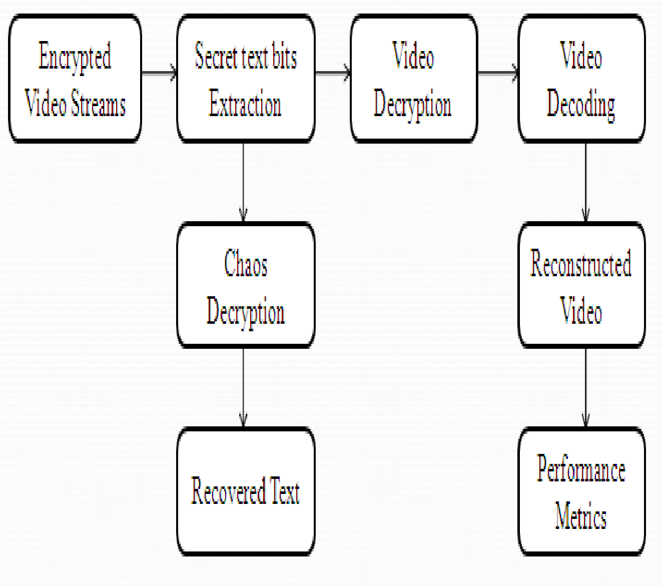

Fig. 8: Data Extraction and Video Decryption

After obtaining of bit streams, it is allowed to encrypt with random binary string using bitxor operation. Before data hiding, the text message will be encrypted using chaos encryption to make second level security during transmission. Bits wrap method is used here to conceal secret text bits under encrypted compressed bit streams.

After hidden the data, image reconstruction and data extraction will be performed to measure the system performance.

At this stage, Secret hidden text messages are extracted from encrypted video streams followed by reconstruction of video frames. Hidden text bits are extracted using bitwise logical operators from the specific bit locations and the extraction of desired number of bits will be accomplished by using logical operators called bitand and bitor. At the end, all message content will be extracted and imposed to chaos decryption module to decrypt the data content with symmetric keys. Then the video bit streams are decoded using h.264 decoder to reconstruct the each encode frame and all the frames concatenated to form recovered original video which shown in block diagram as fig8. Video quality will be measured using some parameters such as PSNR, SSIM, MSE and Correlation .

4. Result and Discussion

The parameter of the Decryption image is systematic measure in terms of MSE and PSNR ratio. The high PSNR value represents the good quality and less PSNR value shows the low quality of the image. The RMSE is inversely proportional to the PSNR values. If PSNR value is high then the RMSE value is low. In table the PSNR value is increased than noisy images which show the image quality is improved. Based on the RMSE value the PSNR values are varied. The PSNR value calculated as follows.

$$\text{PSNR}= 20 \log_{10} \left(\frac{max}{RMSE(x,y)}\right)$$

Where max represents the maximum value of the pixel. For 8bit image 256 is the maximum value of the pixel. The RMSE value calculated as follows

$$\text{RMSE}=\sqrt{\frac{1}{N}\sum_{i=}^{N}(x_i - y_i)}^{2}$$

The index i iterates over all pixels of the images. RMSE value should be less in the denoised images because it is the error value of the reconstructed image. The MSE values are shown in Table 1 for two videos with and without encryption. The PSNR values are shown in Table 2 for two videos with and without encryption. The compression ratios are shown Table 3.

Table 1: MSE Comparison

Video	Mean squared Error	
	Without encrypt data	With encrypt data (CHAOS)
1	22.15	18.5
2	23.18	21.29

In fig 9 shows graphical representation MSE value for with encrypted video and without encrypted video. Similarly the fig 10 shows the PSNR value. From the simulation result the MSE value is low for encrypted videos. The performance measurement of video the PSNR value is high for proposed techniques.tha compressed ratio is shown in fig 11.

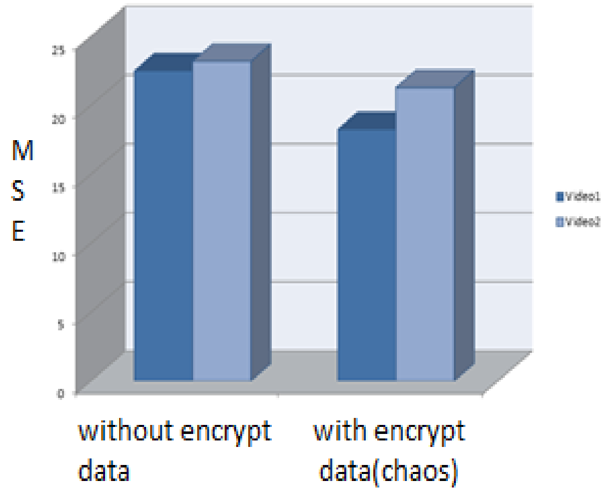

Fig. 9: Graphical representation of Encrypted MSE value

Table 2: PSNR Comparison

Video	Peak signal to noise ratio	
	Without encrypt data	With encrypt data(CHAOS)
1	49.25	50.25
2	48.18	49.29

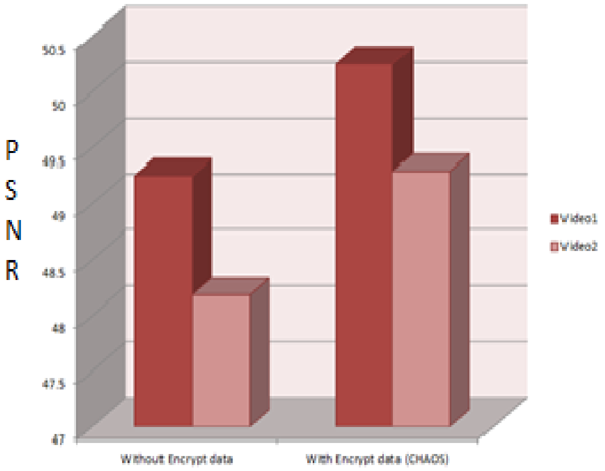

Fig. 10: Graphical representation of Encrypted PSNR value

We also come up with compression parameter using H.264 for the input video files taken here and results are given in table 3.

Table 3: Comparison between Input and output file size on different videos

Video	File size	
	Video 1	Video 2
Input	1039104	1039104
Output	260278	232248
Compression ratio	3.9923	4.4741

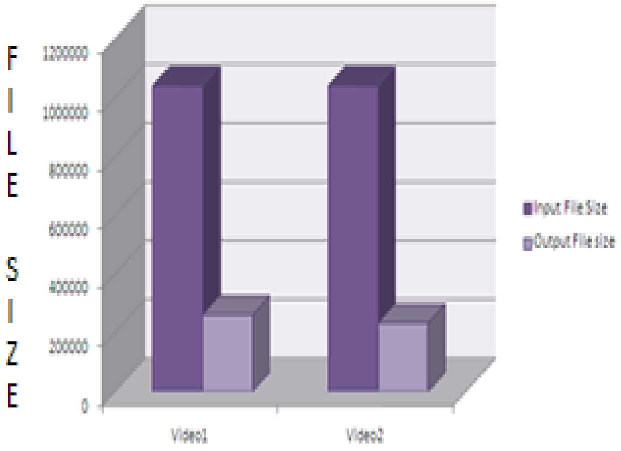

Fig. 11: Graphical representation Compressed video

5. Conclusion

The Experimental results in order to protect videos during transmission. This simulation results protect cloud storage by encryption of compacted video streams. This is also used to hide the information and its provide more security and privacy. The proposed method gives better compression ratio and high Peak Signal Noise Ratio with more compatibility.

References

[1] W. J. Lu, A. Varna, and M. Wu, ‘‘Secure video processing Problems and challenges’’ IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, pp. 5856–5859, May 2011.

[2] W. Hong, T. S. Chen, and H. Y. Wu, ‘‘An improved reversible data hiding in encrypted images using side match’’ IEEE Signal Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.

[3] X. P. Zhang, ‘‘Separable reversible data hiding in encrypted image’’IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012

[4] 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.

[5] Dawn Xu Rang ding Wang and Yun Q. shi Fellow ‘‘data hiding in encryption H.264/AVC video streams by code word substitution’’IEEE Trans.Inf.Forensics security vol 9.no.4 Apr 2014.

[6] Meenakshi R, Kuppusmay K. The use of least significant bit technique at various color spaces for secure steganography with performance evaluation. Int J Adv Res Comput Sci Software Eng;4(6):1047–1051, 2014.

[7] S. Uma Maheswari, D. Jude Hemanth, ‘‘Frequency domain QR code based image steganography using Fresnelet transform’’ International Journal of Electronics and Communications 69 539–544 ,Nov 2015

[8] Xinpeng Zhang‘‘ Reversible Data Hiding With Optimal Value Transfer’’, IEEE transactions on multimedia, vol. 15, no. 2, February 2013.

[9] Weiming Zhang, Biao Chen, and Nenghai Yu ‘‘Improving Various Reversible Data Hiding Schemes Via Optimal Codes for Binary Covers’’ IEEE transactions on image processing, vol. 21, no. 6, June 2012

[10] S.V.Manikanthan and T.Padmapriya “Recent Trends In M2m Communications In 4g Networks And Evolution Towards 5g”, International Journal of Pure and Applied Mathematics, ISSN NO:1314-3395, Vol-115, Issue -8, Sep 2017.

[11] S.V. Manikanthan , T. Padmapriya “An enhanced distributed evolved node-b architecture in 5G tele-communications network” International Journal of Engineering & Technology (UAE), Vol 7 Issues No (2.8) (2018) 248-254.March2018.