I J C T A, 9(37) 2016, pp. 221-228
© International Science Press

A Substitution Approach to Encrypt Data Obscure in Compressed Video Streams

A.B. Akbar Pasha* **and C. Vimala****

Abstract: Data hiding favored encrypted domain without decryption extract the confidentiality of the content. On supplementary, it is more efficient without decryption followed by data hiding and re-encryption. The approach in which data hiding done directly in the encrypted version of H.264/AVC video stream is progressed, which includes step processes (A)H.264 video encryption,(B)data embedding, and (C)data extraction. Here Chaos crypto system technique is effected to encrypt/decrypt text data before or after data embedding/extraction. Data extraction can be rendered in the encrypted domain or in the decrypted domain to adapt for different application scenarios. Additionally, video file size is closely retained even after encryption and data embedd. Experimental results testifies the feasibility and efficiency of the prospective scheme.

Keywords: H.264 Encrypt Video; Chao's Data Encryption; Bits Substitution in Compressed bit streams; Parameter Analysis.

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 a process defined to keep information in encrypted for secure transmission. This technique enables to store precise information or transmit it across insecure networks, so it is determined to intended recipient only rather by anyone else.

Steganography is a technique to hide information from the observer to establish an invisible communication [8].A steganographic system consists of cover media in which the secret information is embedded. The embedding predicts a stego medium by replacing the information with data from hidden message. To the hidden information, steganography gives a large opportunity to someone unaware of the presence of the hidden message. The priority of steganography is to keep its information undetectable [9]. During transmission the sender must avoid using cover-images which will be easy to predict the presence of secret messages. However auto-generated fractal images results good covers as a result of their complexity and irregularity, they are generated by rigid valid rules that may be easily disrupted by message embedding.

2. METHODOLOGY

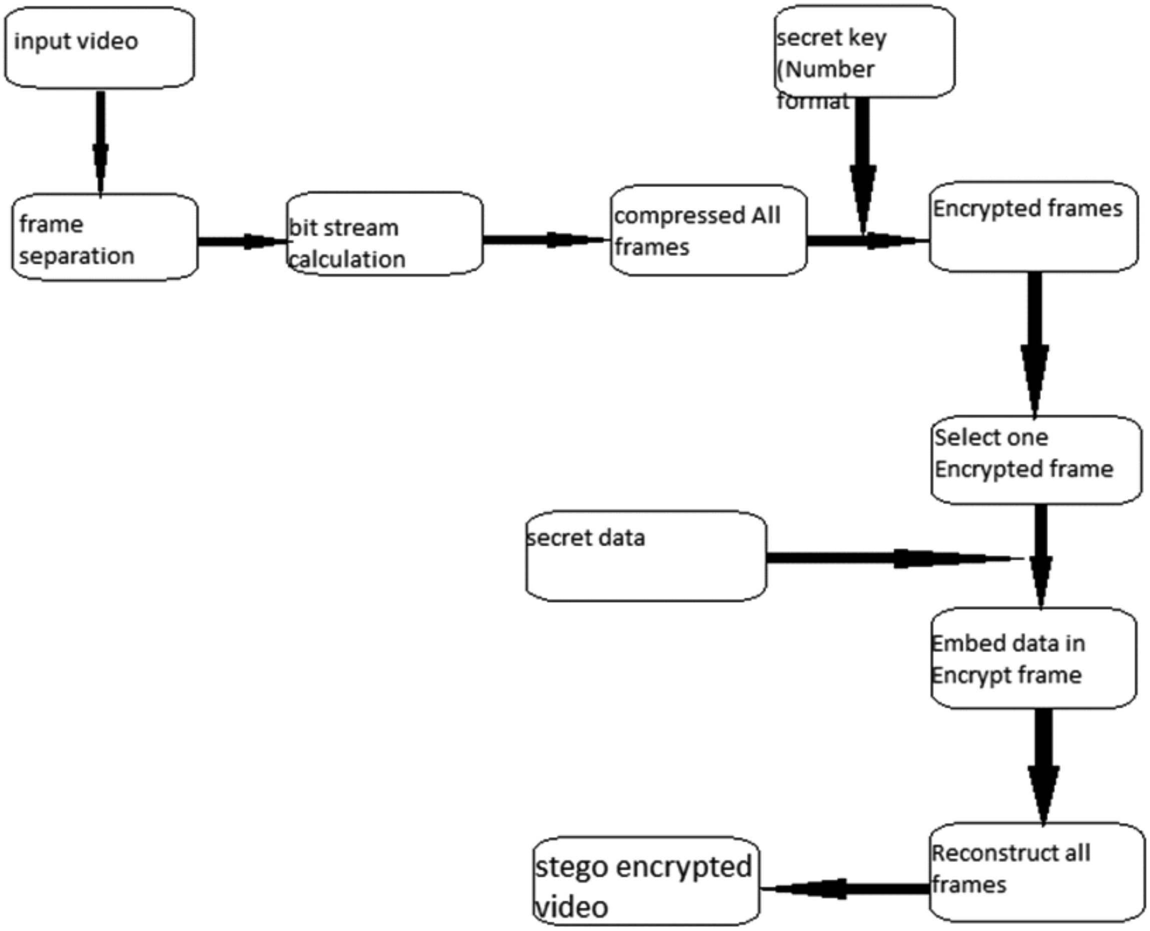
The data hiding is enforced directly in encrypted H.264/AVC video bit stream. It ensure both the format compliance and file size preservation [7]. The proposed scheme can be applied to two different application scenarios by extracting the hidden data from the encrypted video stream or from the decrypted video stream. The process of H.264 encryption and hidden data is proceeded functional as shown in block diagram (1).

(A) Video

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 background subtraction algorithm [1][2].

* Department of Telecommunication Engineering, SRM University, Chennai-603203. *Email: akbarpasha90@gmail.com*

** Department of Telecommunication Engineering, SRM University, Chennai-603203. *Email: vimala.c@ktr.srmuniv.ac.in*



Block Diagram 1: Video Encryption and Data Hiding

Pre-processing is a process of gathering simple image processing tasks that change the raw input video info a format. This can be processed by subsequent steps.

Figure 1: Two different Input video files

An Input Video **(.avi file)** shown in Figure (1) 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. Establish name to each images and this process will be continued for all the video frames as shown in Figure (2).

Figure 2: Frame Separations for Input Video

H.264 divides the sequence of frames into several groups of pictures (GOPs). These frames are labeled as Intra (I), Predicted (P), and Bidirectional (B) frames.

At the source part, each frame is divided into uniform size (16×16 pixels) of non-overlapping blocks called macro blocks, and these macro blocks are handled uniquely depending on their types. Each macro block can be further divided into smaller blocks with 4 × 4 being the smallest possible block size [4] [5]. These macro blocks are subjected to Discrete Cosine Transform, quantization, and entropy coding. First, the pixel values in a macro block are used in the DCT and quantization process. The quantized DCT coefficients are further utilized for de-quantization and inverse Discrete Cosine Transform measures for prediction and motion estimation purposes.

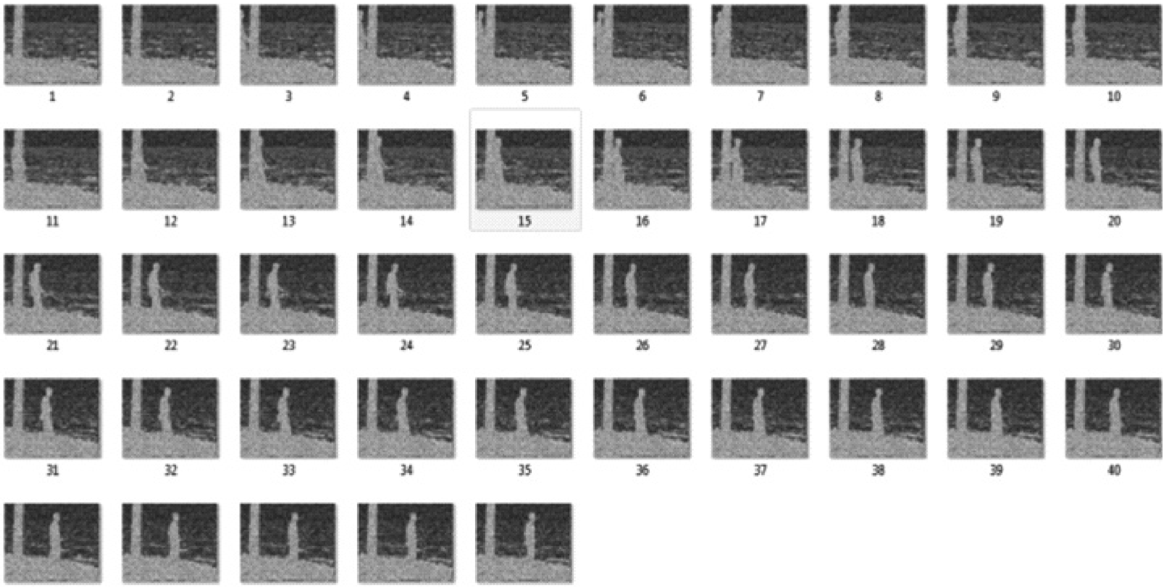
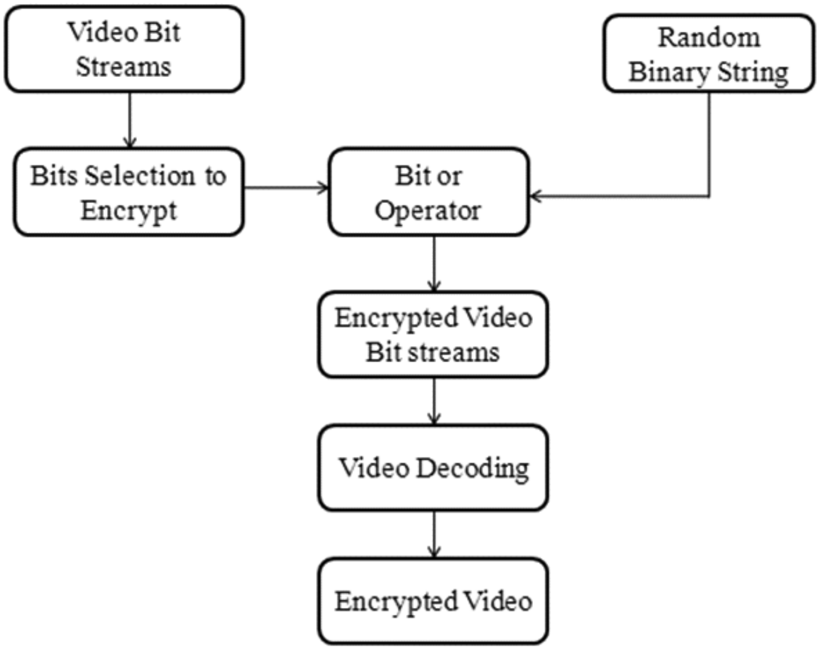


Figure 3: Encrypted Images (Frames)

In I-frame, the pixel values in a block are either coded directly by using coefficients in the transformed domain or predicted (i.e., intra-prediction) using neighboring blocks in the same frame to exploit the spatial redundancies within a frame. In P-frame, motion estimation (i.e., inter-prediction) among two frames can be implemented to take advantage of the temporal redundancies [3]. For that, the previously encoded frame, which itself could be a motion compensated frame, is decoded and its prediction errors, if any, are decoded and added to the decoded frame for motion estimation purposes[13][14]. There are two entropy coding methods are used to encode the quantized transform coefficients are context-adaptive variable length and context-adaptive binary arithmetic coding.

(B) Data Encryption (Chaos's Encryption)

Considering the advanced method of encryption standard to encrypt the secret text for secure transmission. It encrypts the original text ASCII values with encryption key generated from chaotic sequence with threshold function by bitxor operation as given in block diagram (2).Here logistic map is used for generation of chaotic map sequence [2]. It is appropriate to transmit the secret message through unsecured channel by which data hacking prevented. Here we implement chaos encryption in obscuring data using an video file and the encryption flow chart is given in Figure (4).



Block Diagram 2: Video Bits Encryption

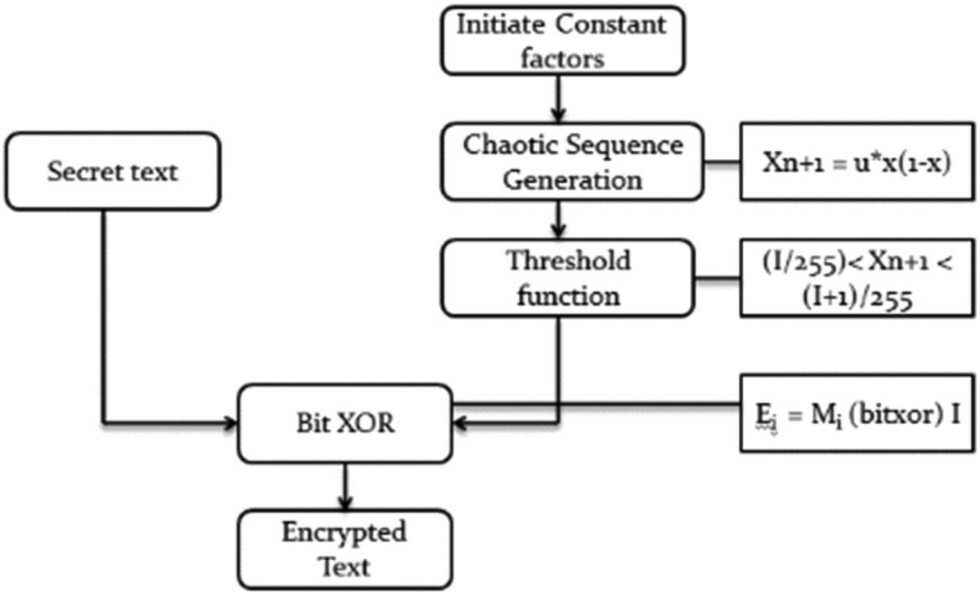


Figure 4: Chaos encryption flow chart

(C) Data Embedding

Data hiding is a process to obscure secret message bits into another medium like image, audio or video files. Here, the hiding is performed under compressed bit stream of cover image. After obtaining of bit streams, it is allowed to encrypt with random binary string using bitxor operation [12]. 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. By performing logical bitwise operations such as 'bitand' and 'bitor' operations [6][16]. After hidden the data, image reconstruction and data extraction will be performed to measure the system performance.

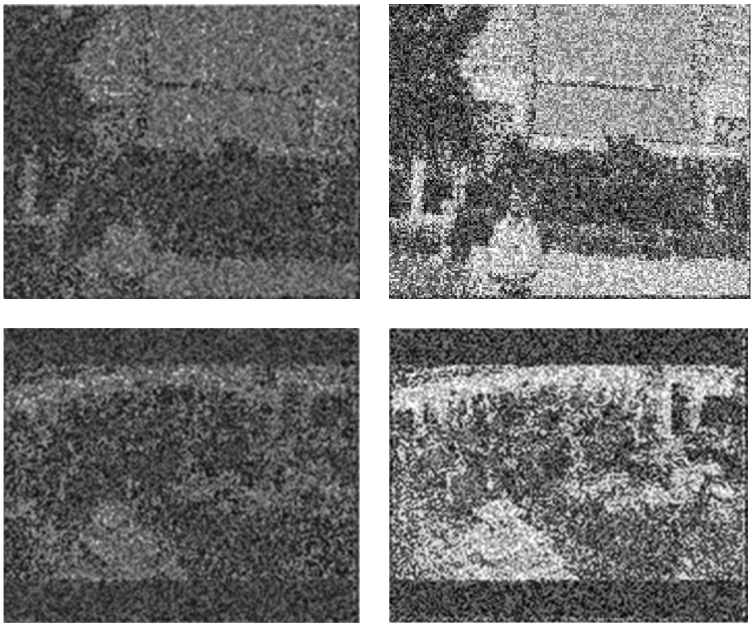
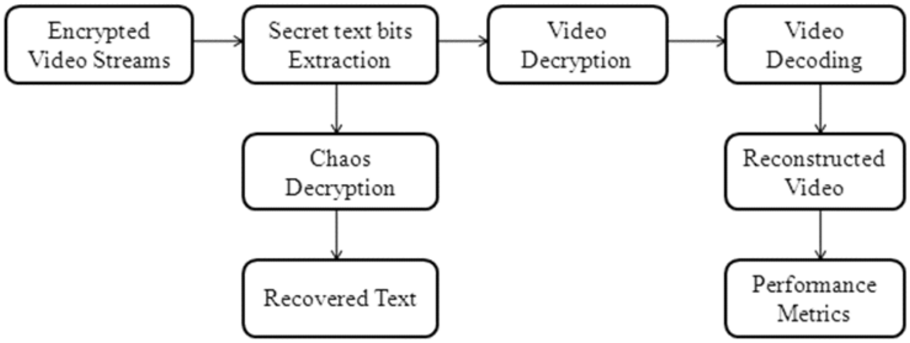


Figure 5: Encrypted video with compression for two different input files

(D) Data Recovery

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 executed by using logical bitwise operators called 'bitand' and 'bitor'. Finally all message characters extracted are enforced to chaos decryption module to decrypt the data with symmetric keys[10][11]. 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 (3). Video quality will be measured using some parameters such as PSNR, SSIM, MSE and Correlation.



Block Diagram 3: Data Extraction and Video Decryption

3. SYSTEM ANALYSIS

The parameter of the reconstructed image is systematic interms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The Mean Square Error is much called as reconstruction error variance σ_q^2. The Mean Square Error over the original image ‘f’ and the reconstructed image ‘g’ at decoder is evaluated as:

$$\mathbf{MSE} = \sigma_q^2 = \frac{1}{N}\sum_{j,k}(f[j,k]-g[j,k])^2$$

Where the sum over j, k represent the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio of signal variance and reconstruction error variance. The Peak Signal Noise Ratio between two images having 8 bits per pixel given in decibels (dBs) is given by:

$$\mathbf{PSNR} = 10\log_{10}\left(\frac{255^2}{\mathbf{MSE}}\right)$$

Commonly when PSNR is 40 dB or greater, then the original images and the reconstructed images are indistinguishable virtually for human eyes.

Table 1
Mean Square Error obtained for two video inputs

	MSE	
	Without Encrypt data	*With Encrypt data (CHAOS)*
Video 1	22.5	18.25
Video 2	23.18	21.29

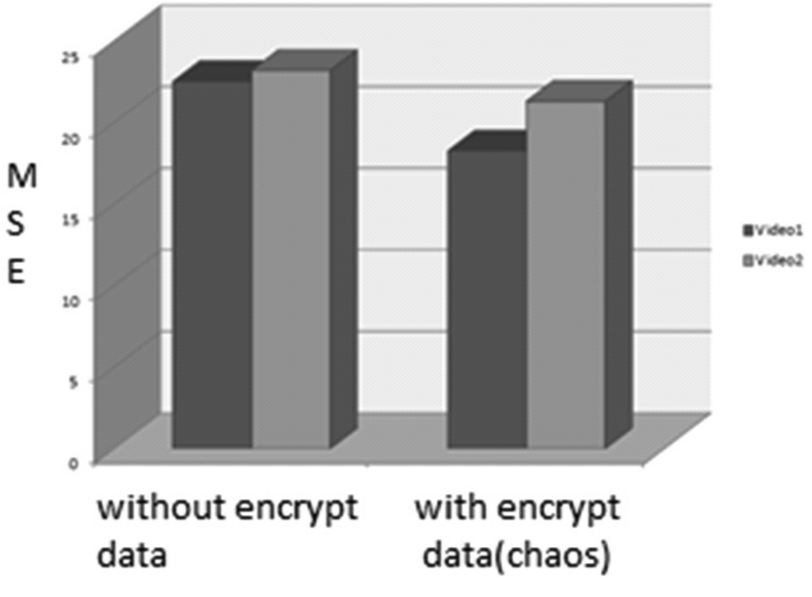


Table 2
Peak Signal Noise Ratio obtained for two video inputs

	PSNR	
	Without Encrypt data	*With Encrypt data (CHAOS)*
Video 1	49.25	50.25
Video 2	48.18	49.29

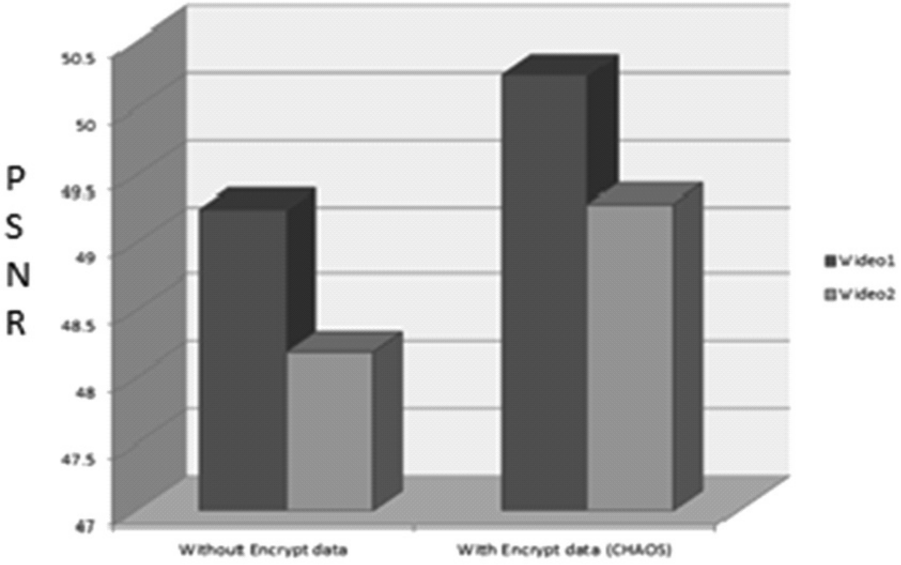
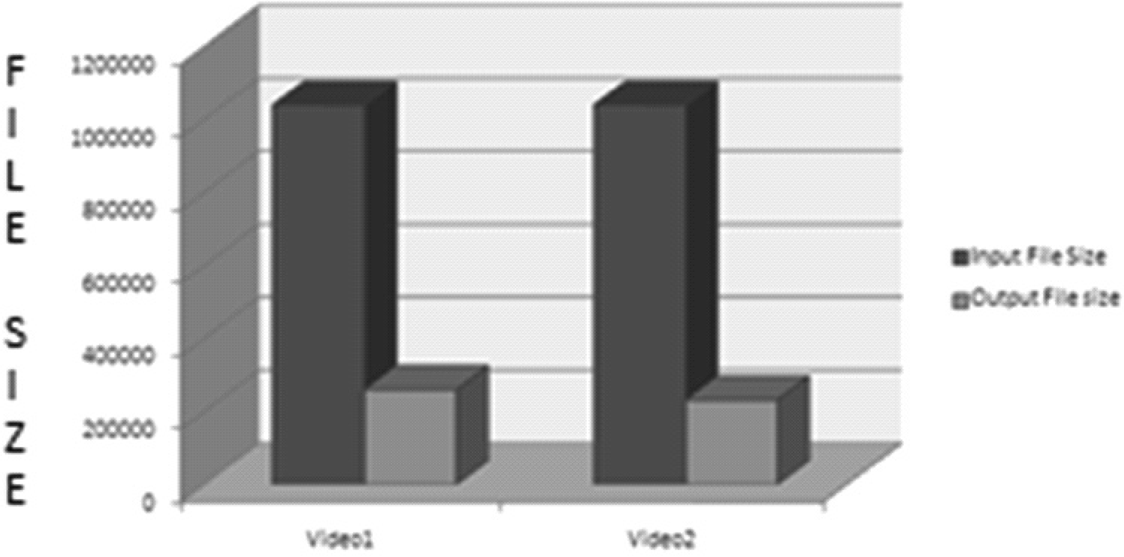


Table 3
Comparison between Input and Output file size on different videos

	Video 1	*Video 2*
Input File Size	1039104	1039104
Output File Size	260278	232248
Compression Ratio	3.9923	4.4741



4. CONCLUSION

The Experimental results present encryption of compressed video streams and hiding information privacy to protect videos during transmission or cloud storage. Here, H.264 video coding standard was used for compress monochrome video effectively with better reduced bit rates. Chaos encryption was used here to encrypt/decrypt secret text data before/after data embedding/extraction. Bits replacement method was used to embed secret message bits with compressed bit streams to prevent the video from tampering. We recover original data without any loss. These methodologies given the better bitrates, high Peak Signal Noise Ratio and high structure similarity index values with more compatibility.

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

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. 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.

8. T. Morkel, J.H.P. Eloff, M.S. Olivier, "*Anoverview/imagesteganography*", http://mo.co.za/openistegoverview.pdf.

9. Sellars, Duncan, "*Introduction to Steganography*", http://www.cs.uct.ac.za/courses/CS400WINIS/papers99/dsellars/stego.html.

10. Reversible Watermarking Algorithm, Using Sorting and Prediction Vasiliy Sachnev, Hyoung Joong Kim, Member, IEEE, Jeho Nam Senior Member, IEEE, Sundaram Suresh, and Yun Qing Shi, Fellow, IEEE transactions on circuits and systems for video technology, Vol. 19, No. 7, July 2009 .

11. Reversible Data Hiding Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei su IEEE transactions on circuits and systems for video technology, Vol. 16, No. 3, March 2006.

12. Expansion Embedding Techniques for Reversible Watermarking Diljith M. Thodi and Jeffrey J. Rodríguez, Senior Member, IEEE transactions on image processing, Vol. 16, No. 3, March 2007 .

13. Reversible Image Watermarking Using Interpolation Technique Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, and Zhang xiong IEEE transactions on information forensics and security, Vol. 5, No. 1, march 2010 .

14. Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection Xiaolong Li, Bin Yang, and Tieyong Zeng IEEE transactions on image processing, Vol. 20, No. 12, December 2011 .

15. Reversible Data Hiding With Optimal Value Transfer, Xinpeng Zhang, Member, IEEE transactions on multimedia, Vol. 15, No. 2, February 2013.

16. Improving Various Reversible Data Hiding Schemes Via Optimal Codes for Binary Covers Weiming Zhang, Biao Chen, and Nenghai Yu IEEE transactions on image processing, Vol. 21, No. 6, June 2012 .