ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECRET DATA HIDING IN ENCRYPTED COMPRESSED VIDEO BITSTREAMS USING CHAOS CRYPTO SYSTEM

Sonali.A.Chaudhari , Prof. Manoj.D.Bagde
Department of Electronics and Communication
G.H. Raisoni Institute Of Engineering & Management,
Jalgaon, Maharashtra , India

ABSTRACT

Early research works have been done on image. Due to few features of images, such as high correlation among pixels and bulk data capacity , previous encryption algorithms are not suitable. Cloud computing has become an important technology trend, which can provide large-scale storage solution and highly efficient computation for video data. It is desired that the video content is accessible in encrypted form to protect from untrustworthy system administrators. The capability of performing data hiding is done in encrypted H.264/AVC video bitstreams which would avoid the leakage of video information also can help to maintain security and privacy concerns with cloud computing. During H.264/AVC compression, the intra-prediction mode (IPM), motion vector difference (MVD) and DCT coefficients' signs are encrypted. For the purpose of content notation and tampering detection, it is necessary to perform data hiding in these encrypted videos. In system, a novel scheme of data hiding is proposed, which includes three section as follows, i.e., H.264/AVC video encryption, data encryption , and data decryption. Chaos crypto system is used here to encrypt/decrypt secret text data before/after data embedding/extraction. video file size is strictly preserved even after encryption and data embedding .

KEYWORDS: Bits replacement technique, Chaos crypto system, Encrypted bitstreams , H.264/AVC.

INTRODUCTION

With the development of the Internet and multimedia technology, information including video,audio, images, and other multimedia, are being transmitted over the Internet. In recent years, the image encryption technologies based on chaos theory have been developed to overcome the disadvantages present in traditional encryption techniques. Digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy In system, a novel scheme of data hiding directly in the encrypted version of H.264/AVC video stream is introduced, which includes three parts, i.e., H.264/AVC video encryption, data embedding, and data extraction. In H.264/AVC codec code words of residual coefficients are encrypted with stream ciphers. Then, a data hider may embed extra data in the encrypted domain without knowing the original video data.The proposed scheme can achieve excellent performance in the following three different prospects.

- The data hiding is performed directly in encrypted H.264/AVC bitstream.
- The scheme can ensure both the format compliance and the file size preservation.
- The scheme provides better performance in terms of high data security ,computation efficiency, and excellent video quality after decryption

RELATED WORK

In summary, in the existing related technologies [3]–[5], encryption and data embedding are implemented almost simultaneously during H.264/AVC compression process. However, to meet the application requirements, it's necessary to perform data hiding directly in the encrypted domain. In addition, the approaches in [3] and [5] do not operate on the compressed bitstream. That is, encryption and watermark embedding are accomplished in the encoding process, while decryption and watermark detection are completed in the decoding process 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 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.

PROPOSED SYSTEM

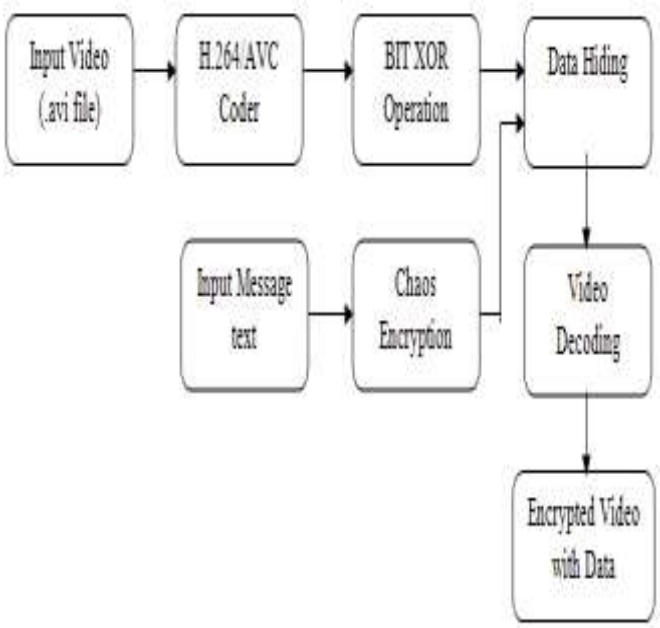

Fig.1 Video Encryption And Data Hiding

In this section, data hiding in the encrypted version of H.264/AVC videos is presented, The processing system involves H.264/AVC Coder, Chaos encryption, and Bits replacement to gives better compression performance and efficient data hiding. The content owner encrypts the original H.264/AVC video bit stream with encryption keys using standard stream ciphers to produce an encrypted video stream. Then, the data-hider can embed the additional data into the encrypted video stream by using Chaos encryption system for text, without knowing the original video content. At the receiver side, the hidden secret data can be extract .

Video encryption often requires that the scheme be time efficient to meet the requirement of real time and format compliance. It is not practical to encrypt the whole compressed video bitstream like the traditional ciphers Alternatively, only a fraction of video data is encrypted to improve the efficiency while still achieving adequate security.

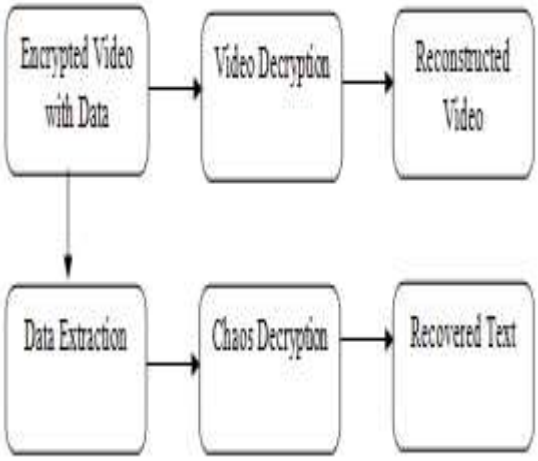

Fig. 2 Data Extraction And Video Decryption

A. H.264/AVC Coder

H.264 is a standard used for video compression, It converts digital video into a format that requires less capacity when it is stored or transmitted. Video compression (or video coding) is an important technology for applications such as Maintaining the Integrity of the Specifications digital television , video conferencing , mobile TV and internet video streaming. In H.264, encoder converts video into a compressed format and a decoder converts compressed video back into an uncompressed format [1].

B. Video Encryption

Test video is segmented into frames .Consider a frame with dimension M×N, M, N represents rows and column. The encoded cover image is encrypted using bitxor technique. The bitxor technique involves generating a random key from the encoded bitstream of the same length as encoded bitstream.

Fig. 3 Original Test Video

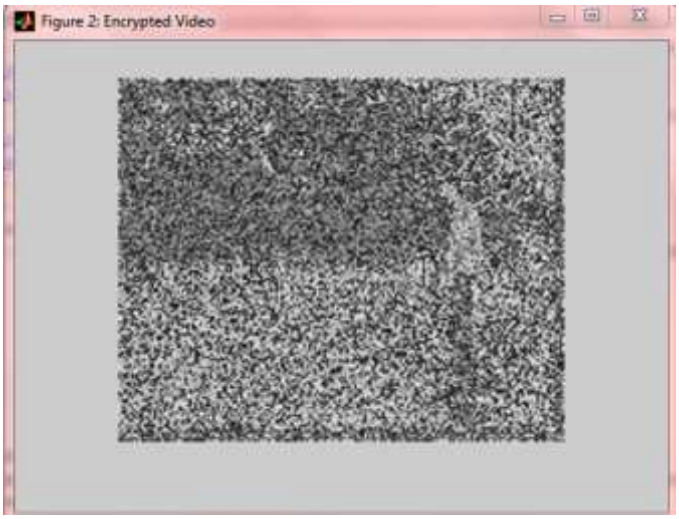

Fig. 4 Encrypted Test Video

C. Chaos Cryptosystem

Chaotic systems are suitable for data message encryption because they have good properties as follows: 1) chaotic motion is neither periodic nor convergent, and the domain is limited. As time goes, the points of the movement trace traverse all over domain. 2) flexing and collapsing are carried continually through the limited domain. Therefore the outputs of chaotic systems are very irregular, similar to the random noise.

The discrete sequences of the chaotic system are given by the following equation .Xn+1 = Tn (xk).

The basic Logistic map is formulated as,

$f(x)=\mu x(1-x)$

Where, x (0, 1). The parameter μ and the initial value x_0 can be adopted as the system key (μ, x_0). The research result shows that the system is in chaos on condition that $3.569 < \mu < 4.0$. Encryption scheme based on Logistic Map the system key or the initial conditions taken are as follows:

$\mu_1 = 3.9$, $x_{01}=0.400005674$ [6].

D. Secret Data Encryption

The secret data to be hidden is encrypted using chaotic mapping. For every individual character from the text to be hidden, the ASCII value of the character and the threshold value from chaotic mapping are taken. A new value is obtained from applying bit xor on these two values. This new value is encrypted data value.

It is process of scrambling original information into unknown form using either symmetric or asymmetric key standard. It is one of the advanced encryption standard called chaos crypto system used. It encrypts the original image pixel values with encryption key value generated from chaotic sequence with threshold function by bit xor operation..

E. Bits Replacement Technique

The encrypted secret data is converted to binary format before being embedded into the encrypted cover image bitstream. Every individual value of the bitstream and the text data are compared for the data embedding process. An empty array is first created which is an index array is created. This index array is created to help us in extraction of the secret data. If the value of the image bitstream and encrypted text are found to be same then in the index array we denote it by “E” and the bit value of the bitstream is unchanged. If the value of the bitstream is 1 and secret text is 0, denote it as “L”and the text is embedded into the bitstream by changing the value of the bitstream to a new value. The new value is obtained by applying bitxand on the corresponding bitstream data and the encrypted text character. Similarly, if the bitstream data is 0 and the encrypted text value is 1 denote it a “H” in the index array; the embedding process is done by changing the value of the image bitstream to a new value, obtained from the bitxor of corresponding bitstream data and the encrypted text character.

F. Data extraction

The data extraction process can be done using the reverse process of the embedding technique, along with the use of the index array.

G. Image Decryption And Decoding

The decryption and the decoding of the bitstream can be achieved by reversing the encryption and encoding processes respectively. The decryption process requires the same key used while encrypting the bitstream . The encrypted bitstream after extraction of the secret data can be perfectly reconstructed to its original video by decrypting the bitstream followed by decoding the bitstream.

ALGORITHM SUMMARY

A. Input

1. Training input .AVI video file.
2. Secret data to be hind .txt file.

B. Processing

1. Read the video (AVI) file consisting of two field Cdata and Color Map.
2. Get video file information.
3. Extract frames from input video.
4. Write an image file into Frames directory.
5. Enter number of frame to process.
6. Initialize parameters for encoding as init_ Frame = 1, end_ Frame = EF, no block _ size = 16, quant = 15, ext = 0.
7. Add '1111' to indicate encoded I frame
8. Apply Chaos encryption for secret data encryption using equation x= u*x*(1-x) and initial condition u=3.99999, x=0.400005674.
9. Generate Chaotic sequence with threshold function formula i= 1:1:255 if (value > (i/255) && value < ((i+1)/255)).
10. Apply Bit Substitution method for hiding data in compressed bitstreams. Created Index array is categorized conditionally into three parts E, H , L for easy secret data extraction.
11. Add '0000' to indicate encoded P frame.
12. Export encoded Video Bitstreams.

C. Output

Extracted secret data and decrypted video is displayed. The entire process of Secret data hiding in encrypted compressed video bitstreams using chaos cryptosystem is summarized in above algorithm.

FLOW CHART

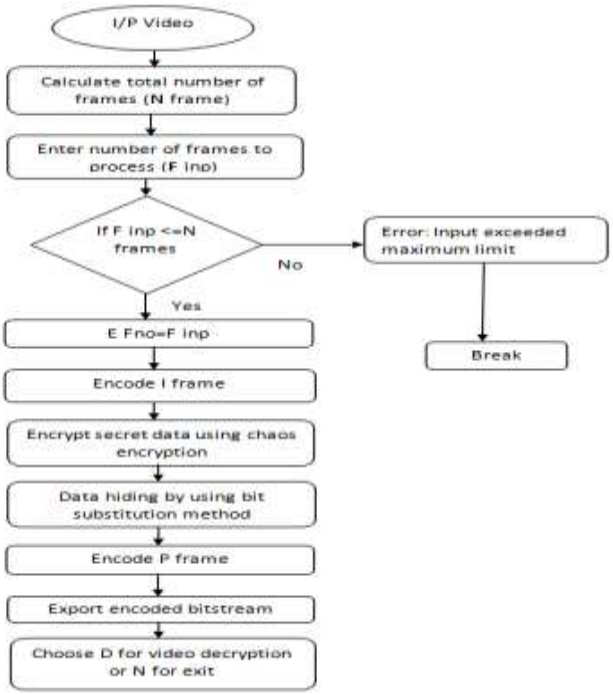

Fig. 5 Flowchart of Implemented Algorithm

EXPERIMENTAL RESULTS

Performance parameters are calculated as Mean square error, Peak Signal To Noise Ratio , Correlation Coeffient , to show the result in graph. This has been implemented using MATLAB 7.10.0 (R2010 a).

Table 1.Performance Results

Test videos	Mean Square Error	Peak Signal to Noise Ratio (dB)	Correlation Coefficient
Input Video 1	0.4744	51.369	0.998
Input Video 2	0.3847	52.280	0.999
Input Video 3	0.3969	52.143	0.998
Input Video 4	0.4422	51.674	0.998
Input Video 5	0.4147	51.953	0.999
Input Video 6	0.3330	52.906	1.000
Input Video 7	0.4208	51.889	0.999

Fig. 6 Shows the graphical representation of results for every Input video.

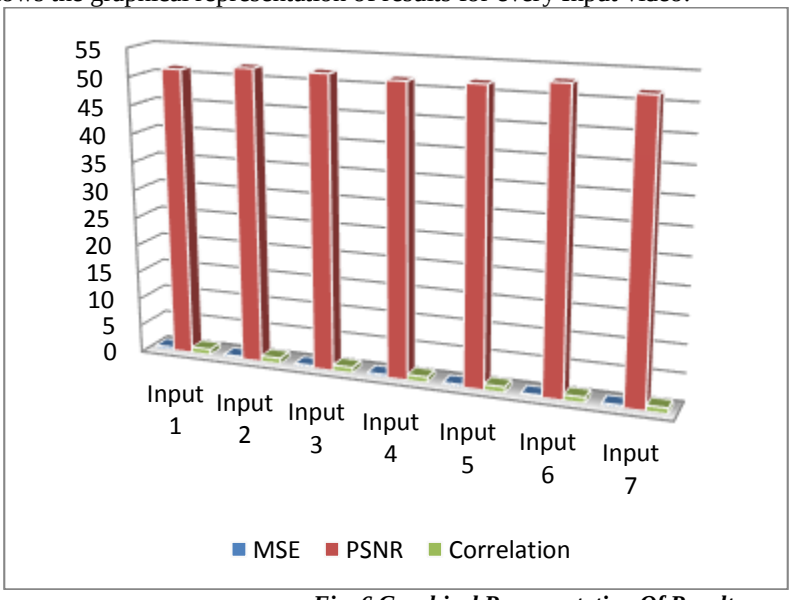

Fig. 6 Graphical Representation Of Results

Proposed method gives excellent results in according to following Advantages

1. It avoids the leaks of video content in storage of clouds.
2. Reduced time consumption process.
3. It is useful to perceive video tampering.

CONCLUSION

System gives excellent output results as data hiding is done by chaos encryption and bit replacement method. The results shows Correlations tends to 1 and PSNR having maximum value 52.906 dB. This system was generated the video with less error under maximum data hiding capacity. The proposed system gives better compatible approach and flexibility with better efficiency rather than prior methods. It preserve the confidentiality of the content completely.

ACKNOWLEDGEMENTS

Authors would like to express sincere thanks and deep gratitude to Prof. H. K. Bhangale, Head of E&C Department who extended wholehearted co-operation to complete this work successfully.
Authors are also express deep and sincere gratitude to the principal, G.H. Raisoni institute of engineering & management, Jalgaon for being a constant source of inspiration

REFERENCES

1. Dawen Xu, Rangding Wang, and Yun Q. Shi, Fellow, IEEE "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution",Vol. 9, No. 4, April 2014.
2. 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.
3. 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.
4. P. J. Zheng and J. W. Huang, "Walsh-Hadamard Transform In The Homomorphic Encrypted Domain And Its Application In Image Watermarking," in Proc. 14th Inf. Hiding Conf., Berkeley, CA, USA, 2012, pp. 1–15.
5. A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, "Robust Watermarking Of Compressed And Encrypted JPEG2000 Images, " IEEE Trans. Multimedia, vol. 14, no. 3, pp. 703–716, Jun. 2012.
6. Sangeeta Mishra Sanjeev Ghosh Payel Saha ,"Chaos Based Encryption Technique for Digital Images" Kandivali (E), Mumbai-400101.
7. Po-Yueh Chen and Hung-Ju Lin "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 2006. 4, 3: 275-290