AN EFFICIENT TEXT HIDING APPROACH FOR H.264/AVC VIDEO

Harishma S[#1] , T.K.Parani[#2]
[#1]*II Year M.E Student,* [#2]*Assistant Professor*
[#1, #2] *ECE Department, Dhanalakshmi Srinivasan College of Engineering, Coimbatore,tamilnadu, India.*
Anna University

***Abstract*: Nowadays the need for security is becoming more important so that secret messages can be communicated with the authorized person. The secret data is passed through various ways in the form of images and videos for an effective reception. In this paper, a text is encrypted in first method by using chaos encryption and second method by twelve square substitution cipher algorithm. It is hidden inside a compressed video. For the compression of video, H.264/AVC, which is the latest accepted standard, is used. Compression ratio is found out so that the reduction in file size can be determined. The efficiency of the proposed scheme is determined by the values of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and Correlation. Result shows the comparison of both the encryption schemes.**

***Keywords*: Compression ratio, Frames, Least Significant Bit, Mean square error, Twelve square substitution cipher algorithm.**

1. INTRODUCTION

In the new era of the digital world, secured data transmission over the internet have a great role. For the protection of data from the hackers, various cryptographic and steganography methods are preferred. Cryptography method deals with the visible meaningless messages, whereas steganography deals with the invisible messages [1]. Video compression and image compression helps in the fast transmission of the large amount of data. Compression deals with minimizing the size of the file without degrading the quality of the image or video. Videoconferencing has become a daily characteristic of financial businesses. It maintains time, efforts, and travel expenses for big companies, and therefore this communicated video application has to be fully secured against theft, alteration or misuse. Most used compression standards for video are MPEG2/H.262, H.263, and MPEG4 Part 2[3]. H.264/MPEG-4 AVC video compression standard is the truly open industry standard which promises a growth significantly over all earlier video compression standards. Encryption techniques provide the basic technology for constructing secure multimedia system.

In order to provide real time reliable security of digital images and videos, many different encryption algorithms have been put forward to secure networked continuous media When coding efficiency is analyzed, H.264/AVC is having twice as efficient than MPEG-2. It produces higher resolution content at same data rate. ITU-T and ISO/IEC introduced this standard. Full range of video applications is addressed by H.264/AVC standard. Among the multimedia files such as sound and video, the encryption of the video is the difficult task. Video file size is large, when compared to audio files. But these encryption algorithms do not provide multimedia security. Therefore, current research is focused on modifying and optimizing the existing cryptosystems for real time video. The compressed video is encrypted using bit XOR operation and a secret data is hidden in the video using bit replacement method [1], which is again encrypted by *Chaos encryption* and modified using *Twelve Square Substitution cipher algorithm* for providing more security. Hidden data is extracted and the original video is reconstructed in the decryption process. Simulation is done in MATLAB Software. The performance metrics can be calculated in terms of *Compression Ratio* to measure the ability of data compression by comparing the sizes of the image being compressed with the original size .The parameters such as Mean square error (MSE), Peak Signal to Noise Ratio (PSNR), Correlation values are adopted to evaluate the perceptual quality of the video. PSNR value determines the quality of the video. Both the encryption methods are compared. The rest of the paper is described as follows. Existing data hiding algorithms and other encryption methods are presented in Section 2. The proposed encryption method is described in Section 3. Section 4 shows the performance evaluation of the methods. Section 5 represents the experimental results of the system and conclusions are presented in Section 6.

ISSN: 2278 – 7798

2 RELATED WORKS

Data Hiding is the process of secretly adding information inside a data source without modifying its perceptual quality [7]. In data hiding, the actual data is not maintained in its original format and it is changed into other multimedia files like video, image or audio which is secretly hidden inside another object. This information is passed through the network to the recipient. Naïve approach is referred as encrypting the entire video data using standard encryption algorithms [1]. This method can provide substantial high security, but it needs high computational cost. At this time, most of the researches are about selective video data encryption, which can reduce computational cost as it just encrypts only a part of video data. Communication security for streaming audio and video media is harder to accomplish due to variety of constraints. To hide the secret text data, codeword substitution is used in which different codewords of levels are substituted without changing the length of the codewords but the quality of the video is less. With the help of the different values of the index variable, data is embedded either in 6th and 7th or 7th and 8th or 6th and 8th bit locations of the bytes of the image. This method can only be applied to image files. If the receiver knows the data-hiding key, it can find the embedded parameters and easily extracts the bits in an encrypted form. Original data is recovered with the help of data hiding key. Here the accuracy and security is comparatively inefficient [3]. By using Extended Substitution Algorithm, data is encrypted and then the cipher text is placed at two or three LSB positions of the original image. The image parameters like PSNR, Mean, Standard deviation, Entropy does not change when there is an insertion of data at three LSB positions [2].Initially message is encrypted using substitution cipher method, which make the text meaningless and with the help of Discrete cosine transform, the encrypted text is embedded inside a jpeg image. Since the compression of the secret message is not done initially, the security can be less.[4] .By using LSB Matching Revisited algorithm (LSBMR), the secret information can be embedded in the cover frame. By using Lempel Ziv Welch (LZW) compression algorithm, data can be hide in the compressed video format and embed the message using least significant bits(LSB) technique which is an earlier simple approach. It doesn't support MPEG 4 format [5]. H.264/AVC is the latest video compression standard. It builds on the concepts of earlier standards such as MPEG-2 and MPEG-4 Visual and offers the potential for better compression efficiency (i.e. better quality compressed video) and greater flexibility in compressing, transmitting and storing video [6].

3. PROPOSED MODEL

In this paper, an efficient method called *Chaos encryption* and *Twelve Square Substitution Cipher Algorithm* used to encrypt the secret hidden text. Chaos encryption algorithm is used to encrypt/decrypt secret text data before/after data embedding/extraction. Shuffle the positions and changing the grey values of image pixels is combined to confuse the relationship between the cipher-image and the plain-image. The data hiding algorithm will convert the text file characters to pixel values using the chaotic shifter which is generated using a logistic map. Larger key space and key sensitiveness are the main advantages. Chaos decryption algorithm is used to decode or reconstruct the secret text data Logistic map is used for generation of chaotic map sequence [7]. It is useful to transmit the secret image through unsecure channel securely which prevents data hacking. The hidden text is encoded and decoded in I frames. The encrypted and decrypted video is done in P frames. Alphabets, digits and special characters are encrypted in twelve-square cipher algorithm [3]. Six 5 by5 matrices are used and each section is arranged in a square, which is given in table-1. The letters of the alphabet are placed in each of the 5 by 5 matrices and another six 6 by 7 matrices are arranged in squares for digits and special characters, as given in table-2. The special characters and digits are included in the table from the desktop/laptop keyboard.

TABLE 1 PLAIN TEXT AND CIPHER TEXT (ALPHABETS)

SQUARE-1	**SQUARE-2**	**SQUARE-3**
a b c d e	f g h i j	k l m n o
f g h i j	k l m n o	p r s t u
k l m n o	p r s t u	v w x y z
p r s t u	v w x y z	a b c d e
v w x y z	a b c d e	f g h i j
SQUARE-4	**SQUARE-5**	**SQUARE-6**
g m r i t	a b c d e	a b c d e
a b c d e	f h j k l	f h j k l
f h j k l	g m r i t	n o p s u
n o p s u	n o p s u	v w x y z
v w x y z	v w x y z	g m r i t

ISSN: 2278 – 7798

Table 1 is arranged as follows. In Square-1, there are twenty five alphabets excluding the alphabet q, and it is arranged five alphabets in an each row. By taking the first row of square-1 to fifth row place and other rows one position up, square-2 is created from square-1.By taking the first row of square-2 to fifth row place and other rows one position up, square-3 is constructed from square-2 similarly. In square-4, consider a word "gmrit" in the first row which consists of five alphabets and the rest twenty alphabets are arranged in next four rows continuously excluding the alphabets of the word "gmrit". By taking the first row to third row place, square-5 is generated from square-4. Likewise square-6 is made from square-4 by taking the first row to fifth row place. Table 2 is arranged as given. The numerals and special characters from a standard laptop are arranged in six rows and seven columns in square-7. By taking the first row to sixth row place, square-8 is created from square-7.By taking the first row of square-8 to sixth row place, square-9 is created from square-8. By transposing the elements, square-10 is created from square-7.By taking the first row of square-10 to third row place, square-11 is generated from square -10. Square-12 is generated from square-10 by taking the first row into sixth row place, The order of reading plain text is from left to right [4].

TABLE 2 PLAIN TEXT AND CIPHER TEXT
(NUMERALS AND SPECIAL CHARACTERS)

.

Table-1 refers when character is an alphabet, otherwise if it is a number or a special character it refers to

SQUARE-7	**SQUARE-8**	**SQUARE-9**
0 1 2 3 4 5 6	7 8 9 ' ~ ! @	# $ % ^ & * (
7 8 9 ' ~ ! @	# $ % ^ & * (	) _ - + = { [
# $ % ^ & * (	) _ - + = { [	}] ; : ' " \
) _ - + = { [	}] ; : ' " \	\ < , > . ? /
}] ; : ' " \	\ < , > . ? /	0 1 2 3 4 5 6
\ < , > . ? /	0 1 2 3 4 5 6	7 8 9 '~ ! @
SQUARE-10	**SQUARE-11**	**SQUARE-12**
0 6 ! & +; <	1 7 @ * = : ,	1 7 @ * = : ,
1 7 @ * = : ,	2 8 # ({ " >	2 8 # ({ " >
2 8 # ({ " >	0 6 ! & +; <	3 9 $) [' .
3 9 $) [' .	3 9 $) [' .	4 ' % _ } \ ?
4 ' % _ } \ ?	4 ' % _ } \ ?	5 ~ ^ -] \ /
5 ~ ^ -] \ /	5 ~ ^ -] \ /	0 6 ! & +; <

table-2

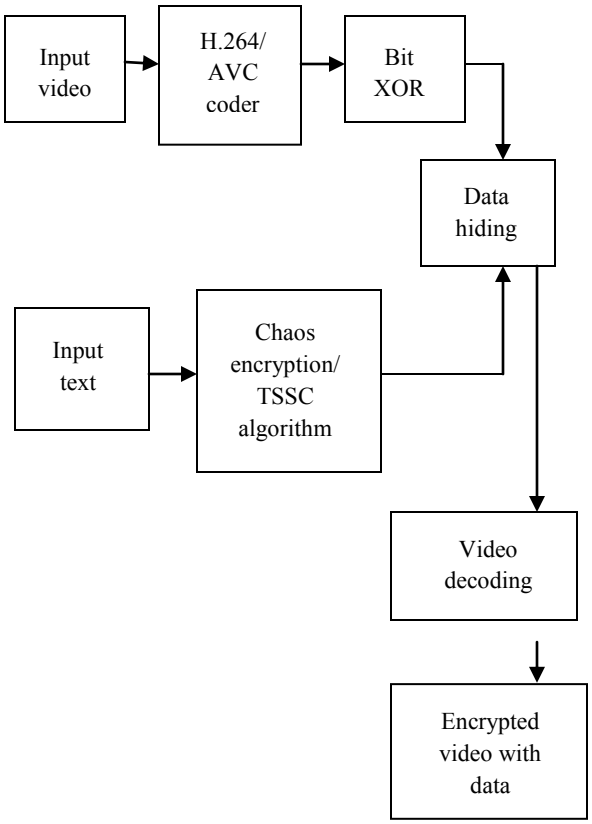

Figure 1: Data hiding using two encryption

The proposed model includes 4 sections

- H.264/AVC Coder
- Stream Ciphers based video encryption
- Chaos encryption and Twelve square substitution cipher algorithm for text
- Bits Replacement based hiding

The uncompressed video is the input which is in .avi format. It is converted into compressed video using H.264/AVC video compression standard. Bit XOR operation is done in the compressed video for stream cipher encryption purpose [1]. A secret text data is hidden using bit replacement method and it is again encrypted using Chaos encryption method and it is compared with twelve square substitution cipher algorithm. Similarly decryption is done to recover the original video and the secret text. The video encryption and data hiding is shown in Figure 1 and thereby original video is reconstructed.

ISSN: 2278 – 7798

A. Frame Separation

Video data may be represented as a series of still image frames. The sequence of frames contains spatial and temporal redundancy that video compression algorithms attempt to eliminate or code in a smaller size. Similarities can be encoded by only storing differences between frames or by using perceptual features of human vision. A brief 5 to 10 second video is recorded in .avi format. The application of the temporal resolution requirements have to be considered. It requires a lower resolution and has a significantly higher acquisition rate for the observation of faster events. The size of the video frame is set to 640x480 pixels. The video obtained is read in the computer using MATLAB. The software processes the entire video and converts it into image frames at the rate of 10 frames per second.

The frames can be interlaced based on the accuracy required and computational capability of the system.

The different steps included in frame separation are:

Step 1: An Input Video (.avi files) is converted into still images for processing it and detects the moving objects.

Step 2: Find the information about the sequence of images gathered from video files through 'aviinfo' command.

Step 3: These frames are converted into images with help of the command 'frame2im'.

Step 4: Create the name to each images and this process will be continued for all the video frames.

By using different algorithms, a video frame is compressed and they are called picture types or frame types. I- frames are the least compressible but don't require other video frames to decode. I-frames are coded without reference to any frame except themselves. P-frames can use data from previous frames to decompress and are more compressible than I- frames . H.264 can use multiple earlier decoded pictures as references during decoding and it can also have some arbitrary display-order relationship relative to the picture(s) used for its prediction.

B. FLOWCHART

The flowchart of frame separation is shown in the Figure 2.

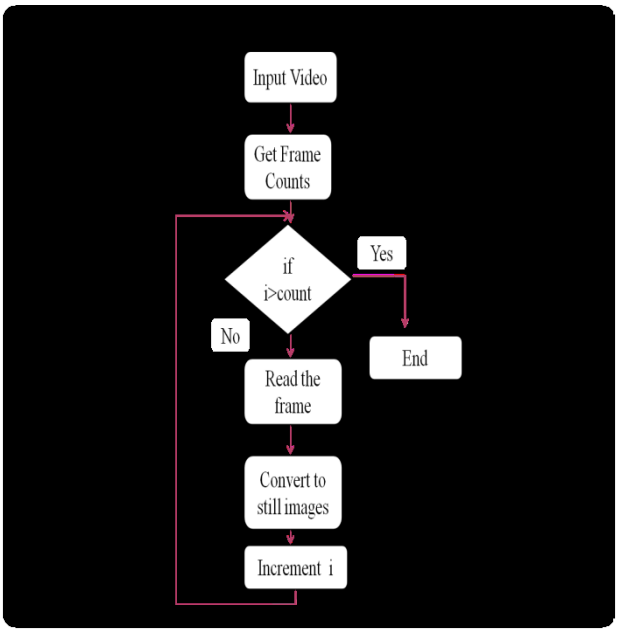

Figure 2: Flowchart of Frame Separation

4. PERFORMANCE EVALUATION

Different performance parameters are used to analyze the reconstructed video and text. By evaluating the parameters, the performance of the encryption method is determined. The following metrics are used to measure the performance and evaluate its practicability:

- *Compression ratio*: As a primary requirement, the compressed file size should be analyzed. The compression ratio is to measure the ability of data compression by comparing the sizes of the image being compressed with the original size. It is used to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form.
- *Mean square error*: The mean squared error (MSE) for our practical purposes allows us to compare the "true" pixel values of our original image to our compressed image. The MSE determines the average of the squares of the "errors" between the actual image and the noisy image. The amount by which the values of the original image differ from the degraded image is considered to be an error [7].
- *Peak Signal to Noise Ratio*: Peak Signal to Noise Ratio (PSNR) is most commonly used to measure the quality of reconstruction of compressed image. The original data is the signal here and the error introduced by compression is the noise. When

ISSN: 2278 – 7798

comparing compression coders-decoders, PSNR is an approximation to human perception of quality of the reconstructed image. Higher PSNR always shows that the good quality of reconstruction. When the PSNR value is higher, the better degraded image has been reconstructed to match the original image and the better the reconstructive algorithm

- *Correlation* : Non-contact, optical technique for obtaining full-field deformation It make use of image processing to go from different images of material, and then analyze the deformation at any point in the field. Finally find the deformation and strain values. Correlation is the optimal technique for detecting a known waveform in random noise

5. EXPERIMENTAL RESULTS

By analyzing the results, the value of the PSNR can be determined. The frame shot separation is shown in the Figure 3.

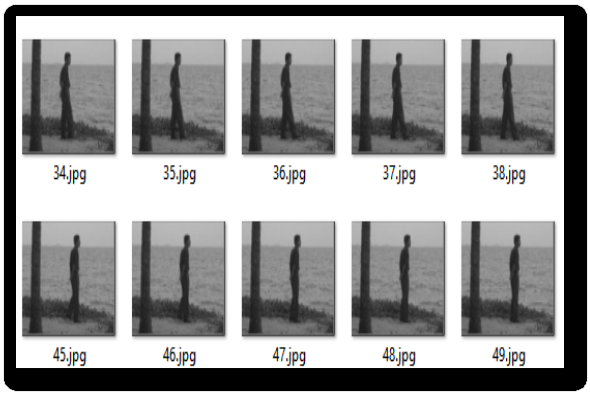

Figure 3: Frame shot separation

The uncompressed input video of 5-10 seconds is shown in the Figure 4.

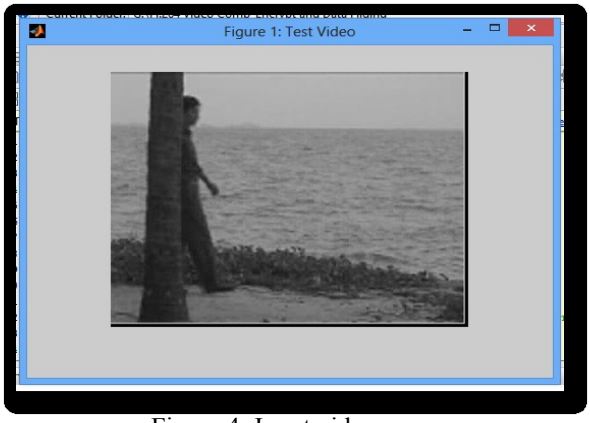

Figure 4: Input video

With inter frame prediction, each frame in a sequence of images is classified as a certain type of frame, such as an I-frame or P-frame. The encoding process is shown in Figure 5.

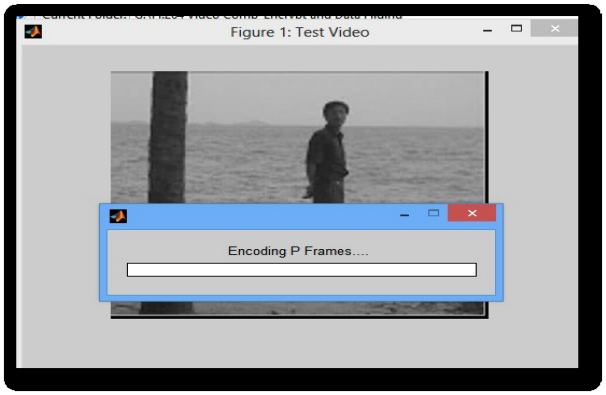

Figure 5: Encoding video

In the encrypted video, there is a secret text data is hidden and the original video is encrypted. The encrypted video is shown in Figure 6.

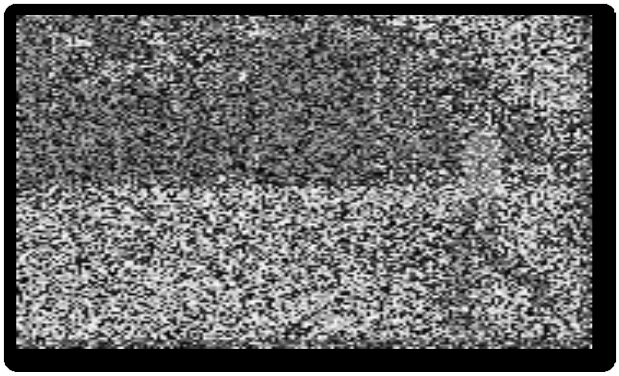

Figure 6: Encrypted Video

The decoding is the inverse process of encoding,. It will decode the videos and secret text data by using chaos decryption method. The decoding section is shown in Figure 7.

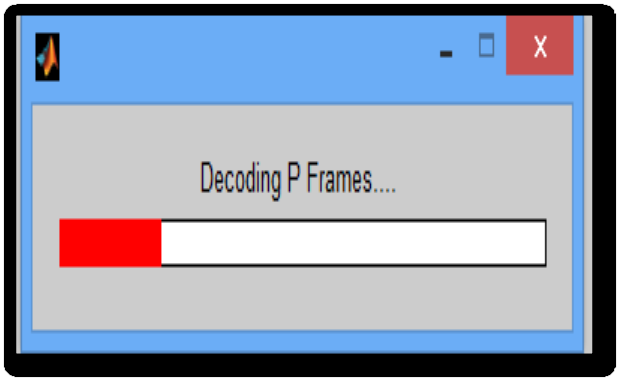

Figure 7: Decoding Process

ISSN: 2278 – 7798

The original video and secret text data is reconstructed and analyzed the compression ratio. The reconstructed video is shown in the Figure 8.

Figure 8: Reconstructed video

The comparison graph is plotted in the MATLAB using plot function. Blue line represents Twelve square substitution cipher algorithm and Green line represents the Chaos encryption method is shown in Figure 9.

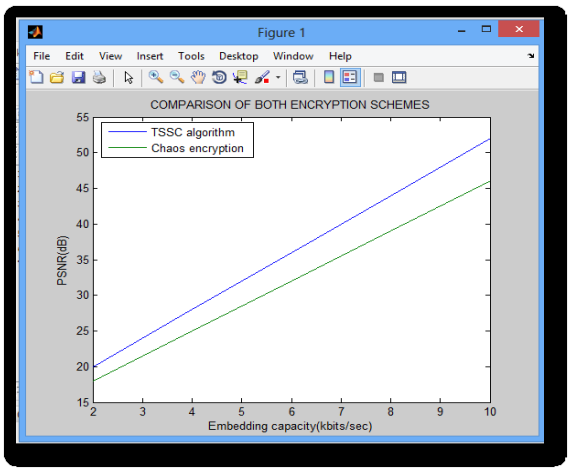

Figure 10: Comparison graph

The value of the PSNR for both schemes is shown in the given table 1

Table 1: Encryption Schemes comparisons

ENCRYPTION SCHEMES	**PSNR (dB)**
Chaos encryption	46
TSSC algorithm	52

5. CONCLUSION

Till now, text hiding in H.264/AVC compressed video is not popular. In this paper, a text is hidden in the encrypted H.264/AVC using chaos encryption method and it is compared with the other encryption method called twelve square substitution cipher algorithm. Double layered security is one of the important factors. It reduces the time consumption because chaos encryption deals with shuffling of grey values. Multiple substitutions are one of advantage of the twelve square substitution cipher algorithm. Identification of video tampering is the main purpose. Performance of the system can be analyzed through Peak Signal to Noise Ratio values. The main applications are in the field of medical and surveillance systems. In the future, text hiding can be applied in same video with different frames.

REFERENCES

[1] Dawen Xu, Rangding Wang, and Yun Q. Shi, Fellow, "Data hiding in encrypted H.264/AVC video streams by codeword substitution", IEEE transactions on information forensics and security, Vol. 9, No. 4, pp. 596-606, 2014.

[2] Gutte R. S, Chincholkar Y. Dand Lahane P. U "Steganography For Two And Three Lsbs Using Extended Substitution Algorithm" ICTACT Journal On Communication Technology, Vol. 04, Issue: 01, pp.685-690, 2013

[3] Mrunalinee Patole, Sheela A Bankar **"**Security of Information Using Cryptography and Image Processing" International Journal of Science and Research, pp. 449-455, 2012.

[4] Shamim Ahmed Laskar and Kattamanchi Hemachandran "Secure Data Transmission Using Steganography and Encryption Technique" International Journal on Cryptography and Information Security, Vol.2, No.3, 2012.

[5] Shanthakumari R and Malliga. S "Video Steganography Using LSB Matching Revisited Algorithm", IOSR Journal of Computer Engineering, Vol.16, Issue 6, pp.01-06, 2014.

[6] Wiegand T, Sullivan G. J, Bjontegaard G, and Luthra A, "Overview of the H.264/AVC video coding standard," IEEE Transaction Circuits System Video Technology, Vol. 13, No. 7, pp. 560–576, 2003.

[7] www.wikipedia.com

ISSN: 2278 – 7798