A New Cryptic Steganographic Approach using Video Steganography

Neethu Prabhakaran
PG Scholar
CSE Department
PSNA CET
Dindigul

D.Shanthi
Phd, Professor
CSE Department
PSNA CET
Dindigul

ABSTRACT
Nowadays, Data transmission over internet is not at all secure and they are vulnerable to various attacks. So in order to prevent our valuable information we require special security measures. One of the methods for secure data transmission is cryptography where the information is protected by transforming it into unintelligible format. But we can ensure more security if the existences of the hidden message itself is concealed. Steganography is one such method in which the message may be hidden in image, audio, video, text etc. In this paper a sequential hybrid method to integrate cryptography and steganography in order to provide more than one level security is being proposed. And it is proposed to use video steganography in order to store high capacity data. The secret information is encrypted using the standard encryption algorithm AES. Then the encrypted message is embedded in the motion vector of the compressed video. The motion vector for embedding data is selected based on their associated macro block prediction error. Then the secret message is embedded in both horizontal and vertical component of the motion vector. At the same time in each GOP, the control information for data extraction will be embedded in I frame. At the receiving end the control information in I frame should be extracted first then the encrypted message can be extracted from P and B frames accordingly. The original message is retrieved back by applying decryption algorithm

.General Terms
cryptography, steganography, motion vector, prediction error

1. INTRODUCTION
In the present world of communication, securing the information is one of the necessary requirement. Cryptography and steganography are the popular techniques used for secret communication. Cryptography protects information by encoding it into an unreadable or unintelligible format. The original message or plain text is converted into a coded format called cipher text via an encryption algorithm. Only those who posses secret key can decrypt the cipher text into plain text. Cryptography system can be broadly classified into symmetric and asymmetric key system. Symmetric key system uses the same key for encryption and decryption. Asymmetric key system uses two keys, a public key known to everyone and a private key that only the recipient of message uses. There are many previous works on symmetric and asymmetric algorithms . Although the ultimate goal of cryptography is to hide information from unauthorized individual, most algorithms can be broken and information can be revealed if attacker has enough time, desire and resources. Since in cryptography, the encrypted data package is itself the evidence of the existence of valuable information, cryptography alone is not sufficient to protect data against unauthorized access. So steganography goes a step further and makes the cipher text invisible to unauthorized users thus providing more security. Steganography is the art and science of communication which hides the very existence of the message by embedding it in a carrier file. An eavesdropper can intercept a cryptographic message but he may not even know that a steganographic message exists. Nowadays the problem of unauthorized copying of music file, book, and software is of great concern. To overcome such problem steganography is being used, where some information will be embedded in digital media in such a way that it cannot be easily extracted. There are many type of steganography based on the type of medium which is chosen as the carrier and these include text steganograpy, image steganography, audio steganography, video steganography etc. the remaining part of the paper is organized as follows. Section 2 gives description about related works. The new approach and experimental results are discussed in section 3 and 4. Section 5 is devoted to the conclusion

2. RELATED WORKS
Many security systems are available based on cryptography and steganography. Image steganography is the most common type of steganography. It can be done either in frequency domain or spatial domain**.** Spatial domain techniques embed messages in the intensity of the pixels directly, while for transform domain also known as frequency domain, images are first transformed and then the message is embedded in the image. Morkel et.al in [1] discussed various spatial and frequency domain based on image steganography. Ould et.al in [2] Discussed hiding information within the spatial domain of the gray scale image. Changes made by steganographic method are the key performance metric. The method in [2] gave best values for PSNR measure which means it is robust**.** However image steganography fails if large volume of secret message is to be hidden so in such case video steganography is commonly used. Different video steganographic techniques have been developed based on the position of the video where embedding is done. G. Sahoo et.al, in [3] have proposed a novel methodology for concealing a voluminous data with high levels of security wall by using movie clip as a carrier file. Two embedding techniques have been proposed in their work. One is embedding in the static portion of the frame using a mathematical formula proposed by the authors. The majority of the secret data embedding may be done by the static portion embedding process. If there are still some secret data remains, it can be concealed in the dynamic portion video by using the most useful most be significant bits method. This will create a very minute difference on the interactive and sensitive portion of the frame. A new method for data hiding by H.264 encoder is proposed by Spyridon K et.al.[4]. H.264 encoder uses different block sizes during inter prediction stage. It is a blind data hiding scheme i.e. the message can be

extracted directly from the encoded stream without the need of the original host video. First a binary code is assigned to every block types then message is converted to binary and bit and they are separated in pairs. These pairs are mapped into macro block which are then motion compensated. Some of data hiding parameter like Starting frame, Starting macro block, No of macro block, Frame period also have to be considered. The encoder reads these parameters from a file, the same file is read during extraction. When an interframe enters temporal prediction, algorithm decides whether to use for hiding or not according to hiding parameters. If algorithm decides to use the frame it chooses the macro block and performs the motion estimation on them, forces the encoder to choose a specific block type according to message mapping. During extraction , extractor partially decode the bit stream in order to discover the chosen block type of each macro block of each inter frame then it can form the hidden message by knowing the mapping. In order to provide more than one level of security cryptography and steganography needs to be integrated. Dipti kapoor et.al , developed a system integrating cryptography and steganography. AES algorithm is used for encryption and part of the encrypted message is hidden in the DCT of an image and remaining part of the message is used to generate two secret keys for embedding and extraction. Since the number of secret keys is more it makes the system more secure.

Sujay et.al in [2] introduced two methods for combining steganogrpahy and cryptography. One method showed how to secure the image by converting it into cipher text by S-DES algorithm and then hide this text in another image by steganographic method. In the second method image is encrypted directly by S-DES algorithm using a key image and data obtained is hidden in another image. These methods prevents from steganalysis.

While using video as a carrier for steganography the position where video is being hidden is very important. In [7] and [8] the message bits are hidden in some motion vectors whose magnitude is above a threshold value. A single bit was embedded in these motion vectors. Authors in [9] embedded data using phase angle between two consecutive candidate motion vectors. All the above methods focused on attributes of the motion vector like magnitude, phase angle, in this paper a new approach is taken by considering the associated prediction error. So a secure hybrid system of cryptography and steganography is being proposed in this paper.

3. PROPOSED METHOD

A sequential hybrid system, which uses both cryptography and steganography to provide multilevel security, is being proposed. For the encryption part the most secure symmetric algorithm called AES with a key size of 128 is being used. Then the encrypted message is embedded in the stego medium so that one more level of security is ensured. The carrier for steganography can be image, text, audio and video. Image is the most familiar carrier, but the limited size of image will inevitably restrict the capacity of embedding. So transmitting large amount of secret information, steganography in image will not satisfy the demand. Because digital video is composed of series of frames and has greater signal space, steganography in video will provide large embedding capacity. Furthermore, with the development of multimedia and stream media on the Internet, transmitting video on the Internet will not incur suspicion. Besides, the degradation of video quality cannot be observed only by naked eyes, for it may be aroused by video compression of lower quality. For these reasons the secret message is embedded in the video file. Proposed system also targets on the internal dynamics of video compression, specifically the motion estimation stage. This stage is chosen because contents are processed internally during the video encoding/ decoding which makes it hard to be detected. In the proposed system candidate motion vector is selected based on the associated macro block prediction error. The system also focuses in minimizing distortion and time for extraction process since all the control information needed for the extraction is embedded in the intrapredicted frame of the compressed video

3.1Cryptic-Steganography System Design

The proposed cryptic steganographic system is as follows. The secret message is encrypted using most secure encryption algorithm AES and the resulting cipher text is hidden bit by bit in a compressed video stream. The stego embedded video is then transmitted. At the receiving end the embedded cipher text is first extracted from the video then the original message is retrieved back by applying AES decryption. The Fig.1 shows the system design of cryptic-steganography system. The cryptic-stenography system has got four modules. These modules are:

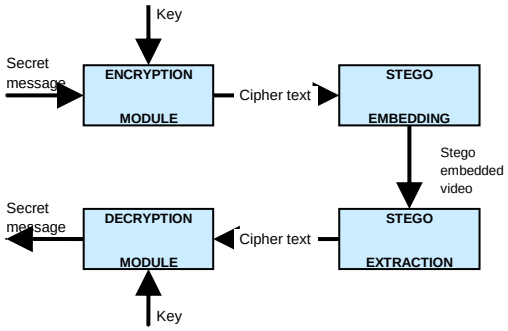

Fig .1 Cryptic Steganography System

3.1.1 Encryption Module

The AES Algorithm is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption and decryption. The data block length is fixed to be 128 bits, while the key length can be 128,192, or 256 bits. In addition, the AES algorithm is an iterative algorithm. Each iteration can be called a round, and the total number of rounds is 10, 12, or 14, when key length is 128,192, or 256, respectively. The 128 bit data block is divided into 16 bytes. These bytes are mapped to a 4x4 array called the state, and all the internal operations of the AES algorithm is performed on the State. For each round 128 bit input data and 128 bit key is required. That is, 4 words of key need in one round. So the input key must be expanded to the required number of words, which depends upon the number of rounds. The output of each round serves as input of next stage. In AES system, same secret key is used for both encryption and decryption. So it provides simplicity in design. In the encryption of the AES algorithm, each round except the final round consists of four transformations:

i) **Sub Bytes:** This function uses an S-box and each byte in the state array is replaced by corresponding byte in the S-box

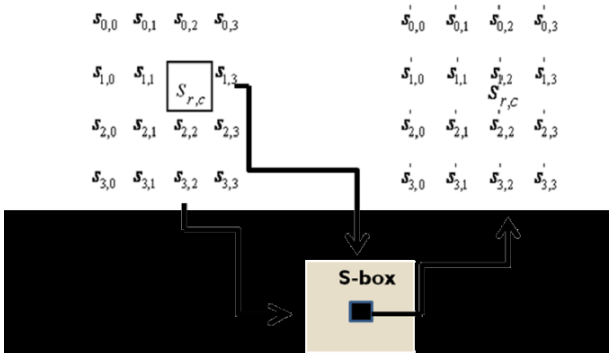

Fig 2 Sub Bytes Operation

ii) Shift Row:

Shift row transformation cyclically shifts the rows of the State over different offsets.

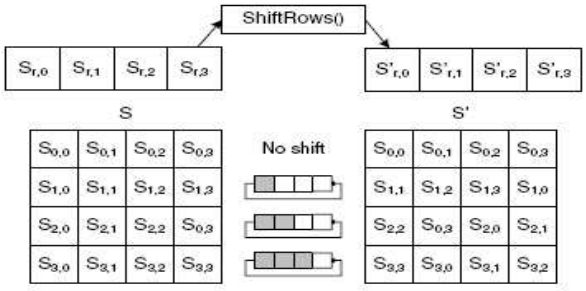

Fig 3 Shift Row Operation

iii) Mix Column

In this operation the column of the State are considered as polynomials over GF (2^8) and each column of the state array is multiplied with a fixed polynomial array. The Mix column component does not operate in the last round of the algorithm.

iv) Add Round Key

A simple bit-wise XOR operation of the current block with a portion of expanded key is done. The operation is viewed as a column wise operation between the 4 bytes of the state array column and one word of the round key

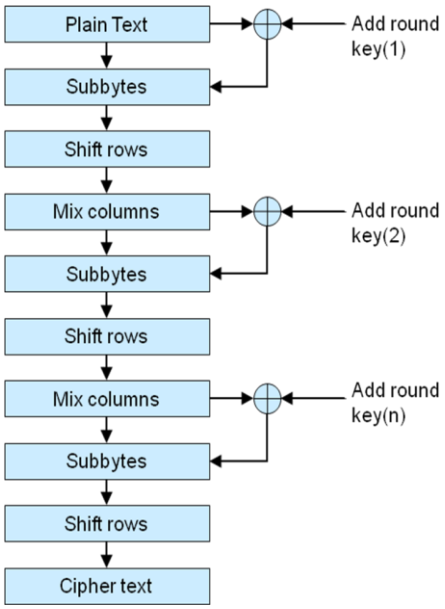

Fig 4 Encryption Module

3.1.2 STEGO EMBEDDING MODULE

After video compression, the host video is organized as GOP which consists of I, P and B frames in a sequence .Embedding is done as GOP by GOP basis. For each GOP, take each P and B frames and simulate the decoder. Select a subset of candidate motion vector from the set of motion vectors according to the criteria that if the associated macro block prediction error is less than the initial threshold value $10\log_{10}(b^2/\sum Bi,j\ E_r(x))< T_{key}$ where b is the size of the macro block, $E_r(x)$ prediction error and T_{key} is the initial threshold value. Now the LSB of both horizontal and vertical component of candidate vector is replaced with 2 bit message at a time. Calculate the associated prediction error $E^h(x)$.Now validate the used value of $T_{key.}$ The used value of T_{key} is validated in order to know the embedded cipher text can be extracted accurately. For this compress E^h using JPEG compression .Then decompress it to produce lossy reconstructed prediction error E_r^h .Now check if this reconstructed prediction error satisfy the above criteria i.e. if it doesn't satisfy means the message cannot be extracted back with this T_{key}. So the T_{key} is decremented until a stopping criteria is met. Once the stopping criteria is met that macro block cannot be embedding and it will be discarded. If the reconstructed prediction error satisfy the criteria then we can ensure cipher text can be extracted accurately and the used value of T_{key} is stored in I frame of the GOP. Now each I frame will have 9 different $T_{key.}$ The above process is repeated for every GOP until the encrypted message is completely embedded. Finally concatenating all these GOP's forms the stego video file. Stego video file thus produced doesn't have much distortion and also doesn't degrade the video quality.

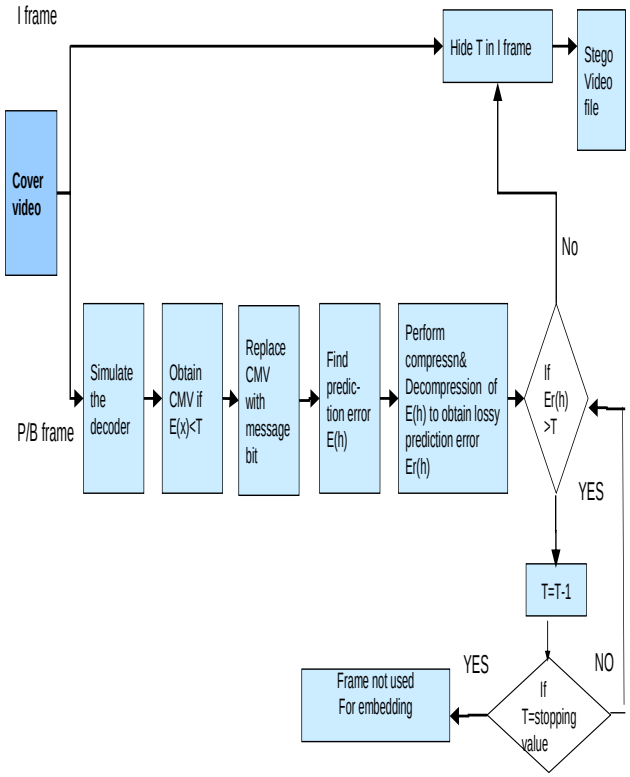

Fig 5 Stego Embedding Module

3.1.3 STEGO EXTRACTION MODULE

The cipher text is embedded in the stego file which can be transmitted in a highly secure manner. Once the file is received by the intended recipient the encrypted text has to be extracted. The extraction process is done as follows, for each GOP extract all the 9 different $T_{key.}$ Values from the I frame. Now decompress each P and B frame to obtain the E_r^h and identify the candidate motion vector by testing this prediction error is less than the corresponding T_{key} value extracted from the I frame. Extract two message bits from the horizontal and vertical component of the motion vector. Concatenating all the extracted bits will constitute the cipher text that is embedded in the host video file.

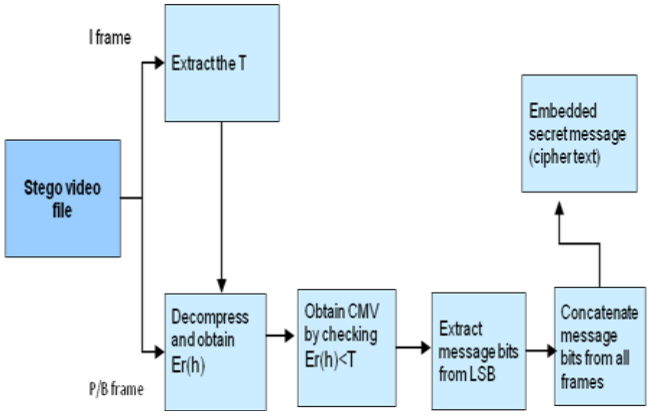

Fig 6 Stego Extraction Module

3.1.4. DECRYPTION MODULE

In the decryption module the inverse operations are performed. Here also 128 bit cipher text block is processed in bytes of array, and the inverse operations are performed in this array. The decryption is also done in an iterative manner where each iteration is called as a round. Same key is using for both encryption and decryption process. These are operations performed in the decryption module:

i) Inverse Sub Bytes

Inverse sub bytes make use of the inverse S-box. Each byte in the state array is replaced by corresponding byte in the inverse S-box.

ii) Inverse Shift Row

Inverse shift row transformation performs the circular shift in the opposite direction for each of the last three rows using different offset.

iii) Inverse Mix Column

In this operation the column of the state are considered as polynomials over GF(2^8) and fixed polynomial is multiplied with each column of state array. The inverse Mix Column component does not operate in the last round of the algorithm.

iv) Inverse Add Round Key

The inverse add round key transformation is identical to add round key transformation because the XOR operation is its own inverse

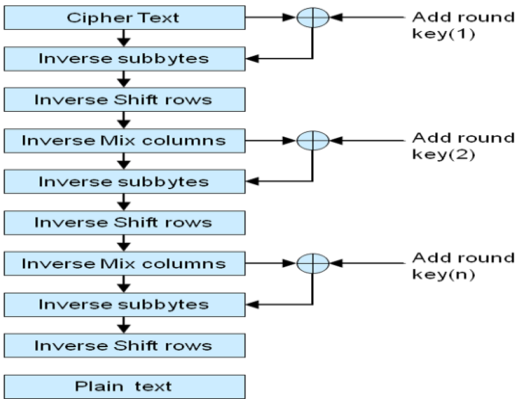

Fig 7 Decryption Module

5. EXPERIMENTAL RESULTS

To demonstrate the accomplished performance of the proposed approach, a number of experiments were conducted using different videos. Here Text data's are the secret information and the secret information is first encrypted using AES algorithm and then encrypted message is embedded in the video file. PSNR value is utilized to evaluate the invisibility of the stego-frames. Figure 3 and 4 shows the P and B frames before and after embedding

Fig 8 B frame before and after embedding

Fig 9 P frame before and after embedding

We observe that there is so significant difference between the two frames. In the table 1 information regarding cover video file has been given PSNR values obtained after embedding shows that quality of video file is preserved.

Table 1 Cover video file information

NAME	FRAME/SEC	NO OF FRAMES
Human.mpg	25	98
Xylophone.mpg	25	230
Football.mpg	25	127
Fish.mpg	25	307

6. CONCLUSION

This paper provides a new hybrid security system which is making use of both cryptography and steganography. Since both information security techniques is being used , it could provide multipe level security. For the purpose of embedding large amount of information .In order to embed large amount of information video steganography is used in this paper. In the proposed system candidate motion vector is selected based on the associated macro block prediction error. The system also focuses in minimizing distortion and time for extraction process since all the control information needed for the extraction is embedded in the intrapredicted frame of the compressed video.

7. REFERENCES

[1] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference(ISSA2005*)*, Sandton, South Africa, June/July 2005 (Published electronically).

[2] M.B. Ould MEDENI, El Mamoun SOUIDI "A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution"

[3]G.Sahoo RajeshKumarTiwari "Hiding Secret Information in Movie Clip: A Steganographic Approach" International Journal of Computing and Applications, Vol. 4, No. 1, June 2009, pp. 87-94.

[4]Spyridon K.Kapotas, Eleni E.Varsaki and Athanassios N. Skodras"Data Hiding in H.264 Encoded Video Sequences" in IEEE 9th Workshop on Multimedia Signal Processing (MMSP07), Oct. 2007, pp. 373–376.

[5]Dipti Kapoor Sarmah, Neha Bajpai "Proposed System for Data Hiding Using Cryptography and Steganography" International Journal of Computer Applications (0975 – 8887) Volume 8– No.9, October 2010.

[6]Sujay Narayana and Gaurav Prasad "Two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions" Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010.

[7]J. Zhang, J. Li, and L. Zhang, "Video watermark technique in motion vector," in Proc. XIV Symp. Computer Graphics and Image Processing, Oct. 2001, pp. 179–182.

[8]C. Xu, X. Ping, and T. Zhang, "Steganography in compressed video stream," in Proc. Int. Conf. Innovative Computing, Information and Control (ICICIC'06*)*, 2006, vol. II, pp. 803–806.

[9]D.-Y. Fang and L.-W. Chang, "Data hiding for digital video with phase of motion vector," in Proc. Int. Symp. Circuits and Systems *(*ISCAS*)*, 2006, pp. 1422–1425.