IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 28-38

Metamorphic Cryptography: A Technique for Providing Security on Video Files

Dhananjay M.Dumbere[1], Nitin J.Janwe[2]
[1]*Department of Computer Science Rajiv Gandhi College of Engineering Chandrapur,India*
[2]Department of Computer Science Rajiv Gandhi College of Engineering
Chandrapur,India

Abstract: *The science of securing a data by encryption is Cryptography whereas the method of hiding secret data inside cover data is Steganography, so that the secret's very existence is concealed. The term Steganography describes the method of hiding cognitive content in another medium to avoid detection by the intruders. This paper introduces an approach wherein cryptography and steganography are combined to encrypt the data as well as to hide the encrypted data in cover medium so the fact that a data being sent is concealed. Combining both cryptography and steganography results to a new technique-Metamorphic Cryptography. The secret video is encrypted using AES algorithm and further encrypted video is embedded with cover video using LSB Algorithm, which results to double layer security to video files being transmitted over the network.*

Keywords: *Cryptography, Steganography, Secret Video, Encrypted Secret Video, Cover Video, Stego-Encrypted Secret Video, Decrypted Secret Video, PSNR, MSE.*

I. Introduction

Cryptography is, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge, the art of encryption. The art of protecting information (plain text) by transforming it (encrypting it) into an unreadable format is called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. Cryptography encrypts the actual message that is being sent. This security mechanism uses mathematical schemes and algorithms to scramble data into unreadable text. It can only be decoded or decrypted by the party that possesses the associated key [1]. The general form of cryptographic technique is shown.

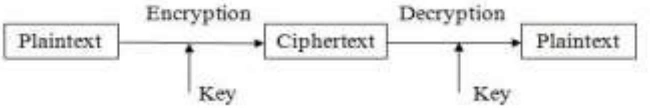


Fig.1. Cryptography Flow

Steganography is the art and science of hiding communication; a steganographic system thus embeds hiddencontent in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography. Essentially,the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity).The embedding process creates a *stego medium* by replacing these redundant bits with data from the hidden message. Modern steganography's goal is to keep its mere presence undetectable, but steganographic systems—because of their invasive nature-leave behind detectable traces in the cover medium. Even if secret content is not revealed, the existence of it is: modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called statistical steganalysis [2].

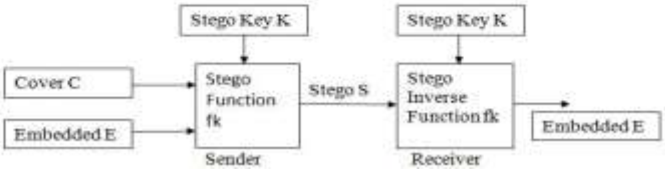


Fig.2. Steganography Flow

II. Proposed Metamorphic Cryptography Approach And Implementation

As per our approach, at source, video is first encrypted using AES algorithm. Further Encrypted Video is encoded with cover video using LSB algorithm. Finally this Stego-Encrypted Video is transmitted over the network to the destination where the receiver decodes the stego-encrypted video which separates encrypted secret video and covers video and later decrypts the encrypted secret video into Secret video. We are implementing proposed metamorphic cryptography [3] approach in Matlab.

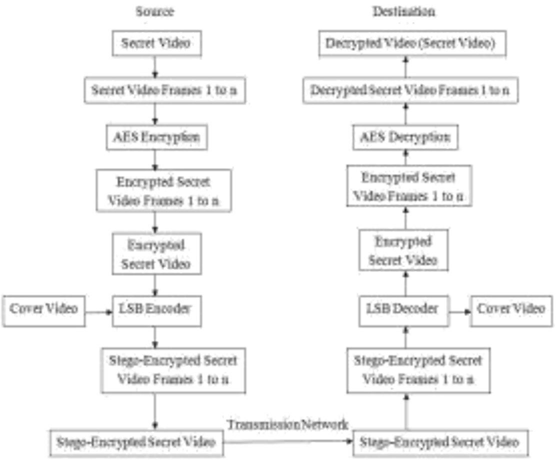

Source
Destination
Secret Video
Secret Video Frames 1 to n
AES Encryption
Encrypted Secret Video Frames 1 to n
Encrypted Secret Video
Cover Video
LSB Encoder
Stego-Encrypted Secret Video Frames 1 to n
Stego-Encrypted Secret Video
Transmission Network
Stego-Encrypted Secret Video
Stego-Encrypted Secret Video Frames 1 to n
LSB Decoder
Cover Video
Encrypted Secret Video
Encrypted Secret Video Frames 1 to n
AES Decryption
Decrypted Secret Video Frames 1 to n
Decrypted Video (Secret Video)

Fig.3. Proposed Metamorphic Cryptography Approach

A. AES Encryption Algorithm

AES is based on the block cipher Rijndael [4, 5, 6] and became the designated successor of the Data Encryption Standard (DES) [7] which has been implemented in a tremendous number of cryptographic modules worldwide since 1977.Matlab [8] is a matrix-oriented programming language, perfectly suited for the matrix-based data structure of AES algorithm which is not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size as shown in Figure-2. It can be implemented on various platforms and carefully tested for many security applications.

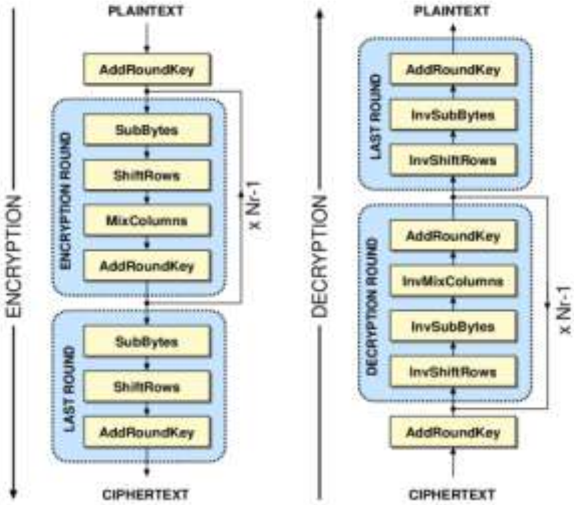
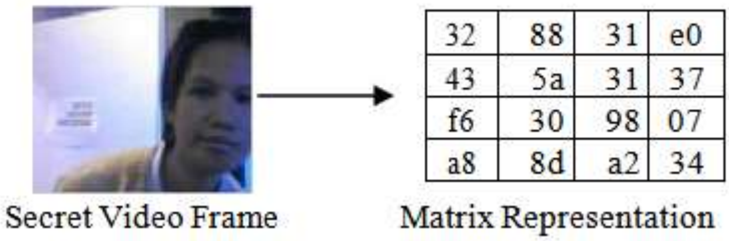


Fig.4. AES Encryption and Decryption

Step1: In Matlab each video frame or image is represented by matrix containing Hexadecimal values. This matrix information (State array) is to encrypted using AES algorithm.For example let the frame is represented by matrix.



32	88	31	e0
43	5a	31	37
f6	30	98	07
a8	8d	a2	34

Secret Video Frame

Matrix Representation

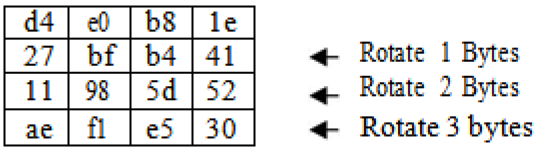
Step2: Let the Cipher Key used in AES algorithm for key Schedule is,

2b	28	ab	09
7e	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

Step3: XOR State Matrix with Key schedule matrix we get,

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

Step4- SubBytes: Replace values of each cell using S-Box Lookup table we get,



d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

Rotate 1 Bytes
Rotate 2 Bytes
Rotate 3 bytes

Step5-ShiftRow: Rotate over 1, 2 and 3 bytes for row R2, R3 and R4 respectively we get,

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

Step6-Applying MixColumns:Each column of above matrix is multiplied with below fixed matrix. That is,

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}$$

We get,

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

Step7- AddRoundKey: Applying XOR operation with above matrix and Round Key 1. That is,

a0	88	23	2a
fa	54	a3	6c
fe	2c	39	76
17	B1	39	05

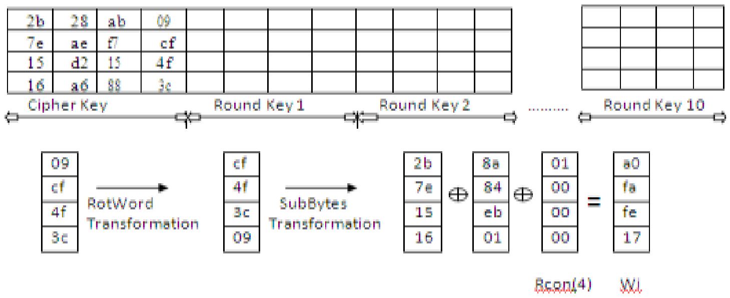
We get,

a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

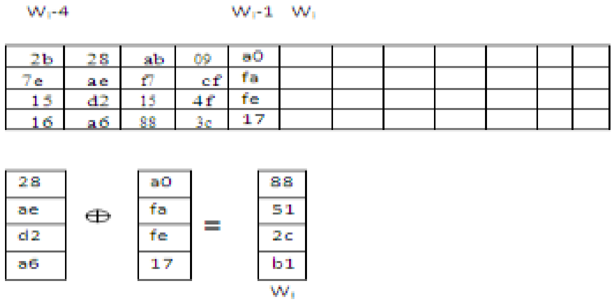
Step8:These all four transformation is performed for 9 rounds.
Final Round (10th) does not include MixColumns transform.

Step9-KeySchedule[9,10]:Words in the position that are a multiple of 4 (w4,w8,…w40) are calculated by applying the RotWord and SubBytes transformation to the previous word Wi-1 of Cipher Key.Futher adding(XOR) this result to the word 4 position earlier Wi-4, plus round constant Rcon .The remaining 32-bit Wi are calculated by adding (XOR) the previous word Wi-1 with the word 4 position earlier Wi-4.

Step9: Operation for Round Key1, used in Step7. Calculating Wi (First Column of Round Key 1),



Step10: Calculating Wi (Second Column of Round Key1)



Step11: Apply step 10 for third and fourth Column of Round Key1.

Step 12: Apply Step 9 and step 10 for Round Key 2 till Round Key 10.

Step 13: After applying all above steps (1 to 12) we finally get Cipher text as,

39	02	dc	19
25	dc	11	6a
84	09	85	0b
1d	fb	97	32

→

Cipher text

This matrix is nothing but encrypted frame of the video. In such a way whole video is encrypted using AES algorithm.

B. LSB-Based Embedding and Extraction Algorithm

LSB based technique is most simple and straightforward approach in which message bits are embed in least significant bits of cover image. In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the secret message [11]. LSB Steganography can be classified by two methods LSB replacement and LSB matching. The terminology LSB replacement/ LSB matching was firstly discussed by T. Sharp [12]. First is LSB replacement which is simplest of the LSB steganography techniques. LSB replacement steganography replace the last bits of cover image with each bits of the message that needs to be hidden. Second method is LSB matching [13] in which each pixel of the cover image is taken mainly in a pseudo-random order which is generated by a secret key, if the LSB of the cover pixel matches the bit of secret data no changes are done otherwise, one is added or subtracted from the cover pixel value, at random. If the length of secret message contains fewer bits than the number of pixels in the cover image, changes are spread uniformly throughout the image by pseudo-random permutation. Since there is change of each bits by ± 1, so the degradation of cover image caused by this embedding process would be perceptually transparent. In LSB of 24 bit color image, the least significant bit of each pixel of a specific color channel or all color channels are replaced with a bit from the secret data. For RGB we analysis this LSB replacement technique [11] that replace least two significant bits of each channels Red, Green or Blue with message bits. Altering the LSBs will only cause minor changes in color, and thus is usually not noticeable to the human eye. Algorithm [14] for LSB Based embedding and extracting process is given as-

```
LSB-based Embedding Algorithm Input -: cover C

for i = 1 to Length(c), do
Sj ,⮨ Cj
for i = 1 to Length(m), do
Compute index ji where to store the ith message bit of m Sji ⮨ LSB (Cji) = mi
End for

Output -: Stego Video S
```

```
LSB-based Extracting Algorithm Input -: Secret video S
for i = 1 to Length (m), do
Compute index ji where to store the ith message bit of m Mji ⮨ LSB (Cji)

End for
```

In the extraction process, the embedded Video can be readily extracted without referring to the original cover-Video from the given Stego-Encrypted video S. The set of pixels storing the secret message bits are selected from the Stego-Encrypted Video, using the same sequence as in the embedding process. The n LSBs of the selected pixels are extracted and lined up to reconstruct the secret message bits.

C. Embedding Procedure

In the case of 24 bit color image each pixel is composed of RGB values and each of these colors requires 8-bit for its representation. [R (8 bits), G (8 bits), B (8 bits)].

Encrypted Video Frame

Cover Video Frame

Step1: Take first pixel values of both Encrypted Video Frame

and Cover Video Frame. Let, first pixel value of Secret Video
Frame is-
R- 11001001
G- 10110110

B- 01011100
Let, First pixel value of Cover Video Frame is-
R- 11011100
G- 11000110
B- 10000111

Step 2: Replacing LSB of Cover Video Frame with 1st MSB of first pixel of Encrypted Video Frame. R- 11011101
G- 11000111
B- 10000110
Hence this will be the first Pixel of Embedded Frame

Step3: Let Second Pixel value of Cover Video Frame is-

R- 10110110
G- 10101101
B- 10110100

Step 4: Replacing LSB of Second Pixel of Cover Video Frame with 2nd MSB of first pixel of Encrypted Video Frame.
R- 10110111
G- 10101100
B- 10110101
Hence this will be the Second pixel of Embedded Frame.

Step5: Apply above procedure to embed all Bits of Secret video Frame. Out of 24-bit of Encrypted video frame 3 bit (1bit of R, 1bit of G and 1 bit of B) needs 24 Bit (8-bit of R, 8-bit for G and 8-bit of B) of Cover Video frame for Embedding. Hence to embed all 24-bit of single pixel of Encrypted video frame (8 -bit of R, 8-bit for G and 8-bit of B) 8 pixel values (192 bit) of Cover video frame is required.

Step6: Embedded Frame (Stego-Encrypted Frame) will be,

Stego-Encrypted Frame

D. Extraction Procedure

Step1: Select First pixel of Stego-Encrypted Frame is-

R- 11011101
G- 11000111
B- 10000110

Step2: Remove LSB values of first pixel.

R- 1
G- 1
B- 0
These values are nothing but 1st MSB values of Encrypted Video Frame.

Step3: Select the 2nd pixel of Stego-Encrypted Frame.

R- 10110111	R-1
G- 10101100	G-1
B- 10110101	

Step4: Remove LSB values of second pixel.

R- 1
G- 0
B- 1

Step4: Apply above procedure and collect all 3 bit information B-0

(1bit of R, 1bit of G and 1 bit of B) from Stego- Encrypted Video Frame, which results the separation of Encrypted video Frame and Cover Video Frame.

Encrypted Video Frame

Cover Video Frame

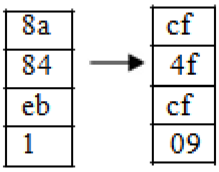
E. AES Decryption Algorithm

The AES decryption basically traverses the encryption algorithm in the opposite direction. Following are the steps involved for AES Decryption.

Step1-KeySchedule: The algorithm for generating the 10 rounds of the round key is as follows,the 4th column of the i-1 key is rotated such that each element is moved up one row.

$$\begin{array}{|c|c|c|c|}\hline 2b & 28 & ab & 09 \\ \hline 7e & ae & f7 & cf \\ \hline 15 & d2 & 15 & 4f \\ \hline 16 & a6 & 88 & 3c \\ \hline \end{array} \rightarrow \begin{array}{|c|}\hline cf \\ \hline 4f \\ \hline cf \\ \hline 09 \\ \hline \end{array}$$

It then puts this result through a forwards Sub Box algorithm which replaces each 8 bits of the matrix with a corresponding 8-bit value from S-Box.



$$\begin{array}{|c|}\hline 8a \\ \hline 84 \\ \hline eb \\ \hline 1 \\ \hline \end{array} \rightarrow \begin{array}{|c|}\hline cf \\ \hline 4f \\ \hline cf \\ \hline 09 \\ \hline \end{array}$$

To generate the first column of the ith key, this result is XOR-ed with the first column of the i-1th key as well as a constant (Row constant or Rcon) which is dependent on i.

$$\begin{array}{|c|}\hline 8a \\ \hline 84 \\ \hline eb \\ \hline 01 \\ \hline \end{array} \oplus \begin{array}{|c|}\hline 2b \\ \hline 7e \\ \hline 15 \\ \hline 16 \\ \hline \end{array} \oplus \begin{array}{|c|}\hline 01 \\ \hline 00 \\ \hline 00 \\ \hline 00 \\ \hline \end{array} = \begin{array}{|c|}\hline a0 \\ \hline fa \\ \hline fe \\ \hline 17 \\ \hline \end{array}$$

The second column is generated by XOR-ing the 1st column of the ith key with the second column of the i-1th key.

$$\begin{array}{|c|}\hline 28 \\ \hline ae \\ \hline d2 \\ \hline a6 \\ \hline \end{array} \oplus \begin{array}{|c|}\hline a0 \\ \hline fa \\ \hline fe \\ \hline 17 \\ \hline \end{array} = \begin{array}{|c|}\hline 88 \\ \hline 54 \\ \hline 2c \\ \hline b1 \\ \hline \end{array}$$

This continues iteratively for the other two columns in order to generate the entire ith key.

2b	28	ab	09
7e	ae	f7	c7
15	d2	15	4f
16	a6	88	3c

→

a0	88	23	2a
fa	54	a3	6c
fe	2c	39	76
17	b1	39	05

Additionally this entire process continues iteratively for generating all 10 keys. As a final note, all of these keys are stored statically once they have been computed initially as the ith key generated is required for the (10-i)th round of decryption.

Step2-Inverse Add Round Key**:**Performs XOR operation between the cipher text and intermediate expanded key corresponding to that particular iteration. E.g., if the diagrams on the left represent the cipher and the key values, the final value after it has generated by this step is shown on the right.

1A	A4	95	3E
A9	B9	4C	3A
13	CD	78	27
86	F1	33	A8

+

D0	C9	95	3E
14	EE	3F	63
F9	25	0C	0C
A8	89	C8	A6

=

CA	6D	74	88
BD	57	73	59
EA	E8	74	2B
2E	78	F8	0E

Step3-Inverse Shift Row – This step rotates each ith row by i elements right wise, as shown below

CA	6D	74	88	
BD	57	73	59	Rotate 1 Bytes
EA	E8	74	2B	Rotate 2 Bytes
2E	78	F8	0E	Rotate 3 bytes

CA	6D	74	88
59	BD	57	73
74	38	EA	E8
78	F8	0E	2E

Step4-Inverse Sub Bytes : This step replaces each entry in the matrix from the corresponding entry in the inverse S-Box as shown in below.

CA	6D	74	88
59	BD	57	73
74	38	EA	E8
78	F8	0E	2E

→

10	B3	CA	97
15	CD	DA	8F
CA	0B	BB	C8
C1	63	D7	C3

Step5- Inverse Mix Column: The Inverse MixColumns operation performed by the Rijndael cipher, along with the shift-rows step, is the primary source of all the 10 rounds of diffusion in Rijndael. Each column is treated as a polynomial over Galois Field (28) and is then multiplied modulo x4 + 1 with a fixed inverse polynomial is c−1(x) = 11x3 + 13x2 + 9x + 14. The Multiplication is done as shown below.

$$\begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

The AES decryption initially performs key-expansion on the 128-bit key block. Then the round key signals the start of the actual decryption process once the data process is ready. It starts by executing an inverse add round key between cipher texts with the modified key (generated in the last iteration of the encryption process) from key expansion. After this step, the AES decryption repeats the inverse shift row, inverse sub, inverse add round key, and inverse mix column steps nine times. At the last iteration, it does an inverse shift row, inverse sub bytes and inverse add round key to generate the original data (Cipher Text).

III. PSNR And MSE

Mean Square Error (MSE), MSE is computed by averaging the squared intensity of the original input frame and the resultant output frame pixels as in [15]. Where e(m, n) is the error difference between the original and the distorted images.

$$MSE = \frac{1}{NM} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} e(m,n)^2$$

Peak Signal-to-Noise Ratio (PSNR), Signal–to -noise ratio (SNR) is a mathematical measure of image quality based on the pixel difference between two images [16]. The SNR measure is an estimate of quality of decrypted frame compared with original frame of the video. PSNR is defined as in [17] where s = 255 for an 8-bit image. The PSNR is basically the SNR when all pixel values are equal to the maximum possible value.

$$PSNR = 10log\frac{S^2}{MSE}$$

IV. Outputs And Experimental Result

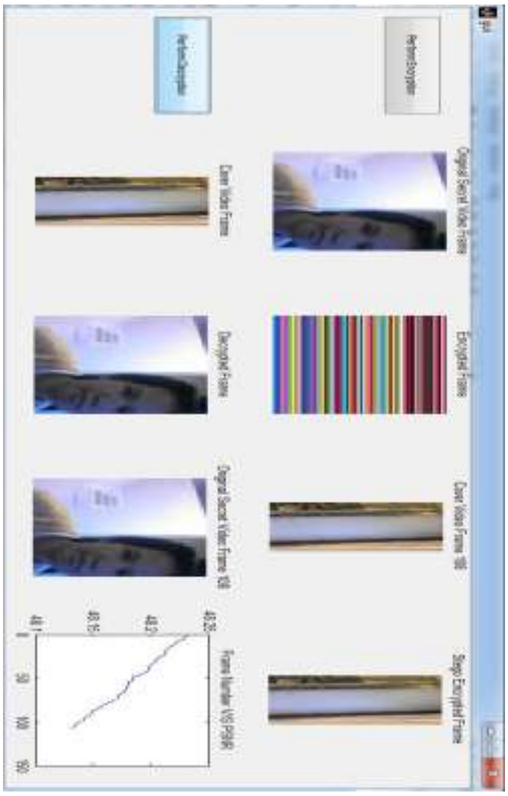


Fig.5. Metamorphic Cryptography Output

We have taken some Videos of length between 18 to 52 sec which flashes near about 25 fps.We applied AES Encryption Algorithm for each frame of Secret video which result to Encrypted Secret Video and later using LSB algorithm we Embed each frame of Encrypted Secret video witheach frame of Cover video resulting Stego -Encrypted Secret Video and finally we decrypt it using AES Decryption Algorithm results to Secret video. Finally we plot the graph between PSNR and Frame Number.

V. Conclusion

In this paper we have described the extensive Metamorphic Cryptography approach in order to maintain privacy or security, sensitive data need to be protected before transmission or distribution. The advancements in ubiquitous network environment, and rapid developments in cloud computing have promoted the rapid delivery of digital multimedia data to the users. Multimedia data (images, videos, audios, etc.) are of importance for use more and more widely, in applications such as video-on-demand, video conferencing, broadcasting, etc. Now, it is closely related to many aspects of daily life, including education, commerce, defense, entertainment and politics. Hence Cryptography and Stegnography, these two methods if combined, it would provide double layer protection to the information being transmitted over the network.

References

[1]. William Stallings, “Cryptography and Network Security, Principles and Practice”, Third edition, Pearson Education, Singapore, 2003.

[2]. B. Chen and G.W. Wornell, “Quantization Index Modulation:A Class of Provably Good Methods for Digital Watermarking and Information Embedding”, *IEEE Trans. Information Theory*, vol. 47, no. 4, 2001, pp.1423–1443.

[3]. Thomas Leontin Philjon, Venkateshvara Rao.” Metamorphic Cryptography -A Paradox between Cryptography and Steganography Using Dynamic Encryption”, IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011-978-1-4577-0590-8/11/$26.00 ©2011 IEEE MIT, Anna University, Chennai. June 3-5, 2011

[4]. Eskicioglu, A.M.: “Protecting intellectual property in digital multimedia networks”. IEEE Computer, Special Issue on Piracy and Privacy (2003), 39–45.R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev. in press.

[5]. Meyer, J., Gadegast, F.: “Security mechanisms for multimedia data with the example mpeg-1 video”, Project description of SECMPEG,Technical University of Berlin.

[6]. Spanos, G.A., Maples, T.B.” Performance study of a selective encryption scheme for the security of networked, real-time video”. In: Proceedings of the 4th International Conference on Computer Communications and networks (ICCCN ’95), pp. 2– 10. IEEE Press, Las Vegas 20–23 September 1995.

[7]. Yi, X., Tan, C.H., Siew, C.K., Syed, M.R.: “Fast encryption for multimedia”,IEEE Trans. Consumer Eletronics **47**(1), 101–107 (2001).

[8]. J¨org J. Buchholz,” Matlab Implementation of the Advanced Encryption Standard”.

[9]. Jialin Huang, Xuejia Lai,” Transposition of AES Key Schedule”, Department of Computer Science and Engineering Shanghai Jiaotong University, China.

[10]. Abd-ElGhafar,A. Rohiem,A. Diaa, F. Mohammed,” Generation of AES Key Dependent S-Boxes using RC4 Algorithm ”, 13th International Conference on Aerospace Sciences & Aviation Technology, ASAT- 13, May 26 – 28, 2009.

[11]. Chan, C.K., Cheng, L.M., 2004. “Hiding data in images by simple LSB substitution”. Pattern Recognition 37 (March), 469–474.

[12]. T. Sharp, “An implementation of key-based digital signal steganography,” in Proc. Information Hiding Workshop, vol. 2137, Springer LNCS, 2001, pp. 13–26.

[13]. R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE 2001.

[14]. Neil F. Johnson,S. Katzenbeisser,”A survey of steganography technique”.

[15]. C. A. B. R. H. S. P. E. S. Z. Wang,"Image quality assessment: from error visibility to structural similarity," IEEE Trans. Image Processing, vol. 13, no. 4, pp. 600-612, 2004.

[16]. L. M. Jean-Bernard Martens, "Image dissimilarity," Signal Processing, vol. 70, no. 3, pp. 155-176, 1998.

[17]. I.A., B.S., K. S.Ismail Avcibas, "Statistical Evaluation of Quality Measures in Image Quality Compression," Journal of Electronic Imaging.