International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 11 (2015) pp. 27835-27844
© Research India Publications
http://www.ripublication.com

High Payload and Secured Video Steganography Using Compression and AES Crypting System

Mr. T V S Gowtham Prasad
Assistant professor, Dept. of ECE, Sreevidyanikethan Engineering College.
tvsgowtham@gmail.com, phone: 9885760093
Dr. S Varadarajan
Professor, Dept. of ECE, SVU College of Engineering, S V University.
varadasouri@gmail.com, phone: 9949300990.

Abstract

In recent years, extensive efforts have been placed in the field of data hiding due to far reaching utilization of hacking technology by the intruders to steal the valuable information through internet. Many data hiding methods includes cryptography, watermarking and steganography has been proposed. Cryptography and watermarking conceals the secret information insides the host media where as steganography has its significance in the data hiding since it conceals the very existence of secret information inside the host media (text, image, audio and video). In this paper a novel approach of video steganography is proposed that improves the payload capacity without compromising the quality of the Stego file and the security of the hidden information. An uncompressed video sequence is considered as cover data and set of images and text is used as secret information. In the proposed method a lossless compression is used for text and lossy compression is used for image to reduce the data size before crypting the secret data. The cipher text so obtained is embedded into selected frames of the video sequence using optimal LSB polynomial expression. Further, the amount of payload embeds into cover video, Performance of the proposed method and the quality of Stego video is tested using objective quality metrics for image and text data at multiple payload capacities.

Keywords: optimal LSB, Lossy and Lossless compression, AES, Video quality metrics and video steganography.

Introduction

Steganography is an art of embedding secret information inside the host media such as text, image, audio, and video. In front of Steganography algorithms, there are many challenges such as payload capacity, imperceptibility of hidden data, secure data communication and robustness against the attacks by the eavesdroppers [1, 2]. Imperceptibility of hidden data in the cover media and payload capacity are always inversely proportional. As the payload of the secret information increases the quality of the cover media is declined which enhances the probability of recognizing the existence of secret information. Video steganography provides outsized cover media to hide the surreptitious information.

Video steganography can be classified into two categories. One of them hides the secret information into the pixels of the frames of the uncompressed video directly. Another video steganography embeds the message into the motion vectors of the compressed video frames [3]. This paper presents a video steganography algorithm to improve the payload capacity and imperceptibility without compromising the security of the hidden data. Proposed method implements the Compression algorithm that reduces the size of the data to be hidden followed by an Advanced Encryption System (AES). Cipher generated by the AES is then embeds into the preselected frames of the video sequence using polynomial expression based optimal LSB approach.

The rest of paper has been organized as follows. Related research work is discussed in second section. Third section presents the methodology of the proposed system. Section four presents experimental results and discussions. Conclusions are drawn in last section.

Related Work

A 3-3-2 LSB based video steganography scheme in an uncompressed domain is discussed by Kousik et al [5]. Imperceptibility and video quality is the key factor concentrated and worked out using a greedy genetic algorithm. Experimental results are done based on PSNR and image fidelity. But, genetic algorithm is more computationally Complex and also measuring metric are not sufficient to quantify the quality of the video.

Hemant et al proposed a dynamic data protection video steganography based on hybrid and LSB approaches [6]. The proposed method has both AES encryption algorithm and LSB substitution Steganographic methods to increase the security of secret message. Author analyzed the quality of the stego video using single, double and triple LSB substitution approaches and concluded that proposed method provides better stego video when message substitutes in one LSB.

Punita et al proposed an Advanced Encryption Standard system which utilizes symmetric cryptographic schemes [7]. This paper presents fundamental mathematics behind the AES system and the description of cryptographic primitives. Yadav, P. et al proposed video steganography scheme with encryption based on LSB substitution [8]. Encryption of secret data is implemented using XOR with secret key. Author uses stream of video frames as secret data and specific pattern BGRRGBGR is followed to store the secret frames in the cover video.

Balaji, et al proposed Secure data transmission using video Steganography [9]. Author presents video steganography using indexing of secret information into the indexed frames of cover video. A highly secure video steganography using Hamming code is proposed by Mstafa et al [10]. In this paper, hamming code is used to encode the secret message. The resultant is randomized by XOR function and then embeds in to the cover video.

In the research works presented by different authors are mostly concentrating on quality and imperceptibility of data. The performance is quantified using PSNR. In the proposed method along with quality and imperceptibility, payload capacity is also increased using lossy and lossless DCT compression technique. This proposed method is an extension of the dynamic data protection system [7].

Methodology

a). Proposed System**:**

The proposed video steganography system as shown in the fig.1 has two major blocks message Embedding and Extraction blocks. In message embedding block, three stages are involved Data Compression, Encryption and embedding process. Initially, secret message either text data or image is read followed by a DCT compression technique. The Discrete cosine transform converts the data into DCT coefficients and quantized to reduce the inter pixel redundancy. The resultant is further encoded using Huffman coding. Since the Huffman coding provides better entropy and efficiency than other source coding methods. The compressed ad encoded data is in the binary form processed through the symmetric cryptographic scheme called Advanced Encryption standard system.

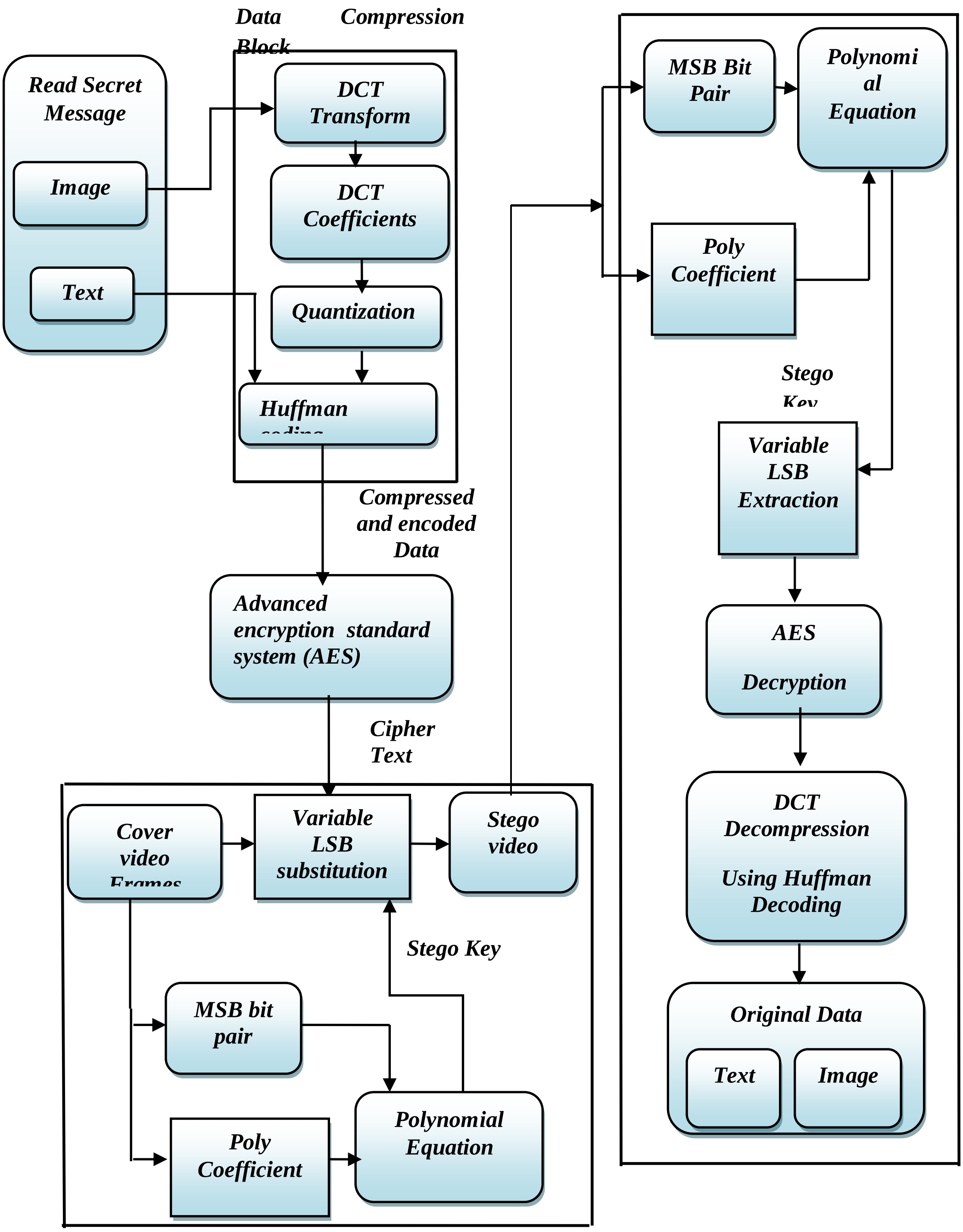


Figure 1: proposed video steganographic system a) message embedding process b) extraction process

Advanced Encryption standard system converts input blocks into states where each state is 4X4 array. These input states are passed through four transforms

Addroundkey, subbytes, shiftrows and mixcolumns that perform various operations to compute the cipher text. Except *Addroundkey* remaining operations are invertible [11]. Cipher text so obtained is converted to stream of binary data and given to variable LSB substitution along with frames of the cover video and the stego key. Stego key is obtained by a polynomial expression as a function of MSB pairs of the previous pixel. This stego key selects the random pixel in specified frame to embed the binary data into optimal LSBs. The generated Stego video is further communicated through the internet.

Intended recipient can extract the original secret data by passing the stego video into the inverse process of polynomial based variable LSB substitution method results the cipher text followed by AES decryption system to extract the compressed data. The binary data so obtained is decompressed using inverse DCT and Huffman decoding process. In this embedding process huge amount of secret information is reduced before embedding to minimize the payload and increases the security levels of with hybrid AES crypto and stego process.

b). Embedding and Extraction process:

Embedding process involves three stage DCT compression, generating cipher text using AES system and hiding process polynomial based variable LSB substitution method.

Stage 1: DCT Compression with Huffman Coding

Consider Secret data as an image *f(x, y)* where *x* and *y* represents spatial coordinates and *'f'* represents the gray level intensity at *(x, y)*. Initially image is subdividing into 8X8 matrices and determines the DCT coefficients of each block.

The forward 2D_DCT transformation is given by the following equation:

$$C(u,v) = D(u)D(v)\sum_{\mathrm{x=0}}^{\mathrm{N-1}}\sum_{y=0}^{N-1} f(x,y)\cos\left\{\frac{(2x+1)u\pi}{2N}\right\}\cos\left\{\frac{(2y+1)v\pi}{2N}\right\}$$

$\text{where u, v} = 0,1,2 \ldots\ldots \mathrm{N}-1$

The inverse 2D-DCT transformation is given by the following equation:

$$f(x,y) = D(u)D(v)\sum_{\mathrm{u=0}}^{\mathrm{N-1}}\sum_{v=0}^{N-1} D(u,v)\cos\left\{\frac{(2x+1)u\pi}{2N}\right\}\cos\left\{\frac{(2y+1)v\pi}{2N}\right\}$$

$\text{where x, y} = 0,1,2 \ldots\ldots \mathrm{N}-1$

$$Where\ D(u) = \sqrt{\frac{1}{N}}\ for\ u = 0;\ D(u) = 2\sqrt{1/N}\ for\ u = 1,2 \ldots\ldots N-1.$$

Each block is then compressed through quantization and quantized matrix is then encoded using Huffman coding process.

Stage2: Generating Cipher text using AES system.

Compressed and Encoded data is in the form of binary streams. The input and output data for the AES algorithm consist of sequences of 128 bits referred as blocks and the number of bits referred as length. The Cipher Key is a sequence of 128, 192 or 256 bits. Other standards for input, output and Cipher Key lengths are not permitted. Sequence of 8 bits is considered as single entity which is the basic unit in the process of AES algorithm.

AES algorithm performs operations on the two dimensional 4X4 arrays of bytes called state each containing N_b bytes, where N_b is the block length divided by 32. State array is considered as

State[r,c]=initialarray[r+4c] for $0 < r < 4$ and $0 < c < N_b$.

AES algorithm process the state using four transforms *Addroundkey, subbytes, shiftrows, mixcolumns*

SubBytes: This transform is non linear which operates on each bytes of the state using S-box. S-box is invertible constructed by composing two transforms.

1. Take the multiplicative inverse in the finite field GF(28).
2. Apply the following affine transformation (over GF(2)):

$$b_i' = b_i \oplus b_{(i+4)\mathrm{mod}8} \oplus b_{(i+5)\mathrm{mod}8} \oplus b_{(i+6)\mathrm{mod}8} \oplus b_{(i+7)\mathrm{mod}8} \oplus c_i$$

Where ‘i’ represents bit position of the byte in the state array and ‘C’ is the array obtained by multiplicative inverse field.

ShiftRows: This transformation performs cyclic shift in the last three rows of the state. The first is is unchanged, second row is shifted by one byte to the left, third row by two bytes and fourth row by three bytes.

$$\mathrm{shiftstate}_{r,c} = \mathrm{state}_{r,(c+\ \mathrm{shift}\ (r,Nb))\ \mathrm{mod}\ Nb} \text{ for } 0 < r < 4, 0 < c < N_b.$$

Where shift(r, N_b) depends on the row number r.

Mixcolumns: Columns of the shifted state array is considered to be polynomials over GF(2^8) and multiplied modulo x4+1 with a(x) where a(x) = {03}x3 +{01}x2 + {01}x + {02}. Therefore shiftstate(x) = a(x)⊕state(x).

AddRoundKey: The Addroundkey is performed at the starting and the ending of the cipher to provide the randomness to the algorithm.

Shiftstate(r,c)=state(r,c) ⊕w.

Where w is the array of columns of the state array.

Stage 3: hiding process polynomial based variable LSB substitution method

The cipher text so obtained from the AES system is further processed through the variable LSB system to hide in the selected frames of the cover video. The random pixel in the selected frame is determined by defining polynomial equation of second order with poly coefficients {a, b, c}. For example: $P(x) = a\,x^2 + bx + c$.Where ‘x’ is a variable depends on the XORing of MSB bit pair. MSB bit pair contains MSB and its next MSB bits. x =Xoring (7th & 6th bits of pixel).

Poly coefficient *‘a’, ‘b’, ‘c’* are depends on the 5th, 4th & 3rd positions of the pixel. Since the coefficients randomly changes from pixel to pixel, the polynomial equation gives a random positions of the pixel. Once the poly coefficients and variable ‘x’ is substituted, p(x) defines the next random position of the pixel of the selected frame used to hide the cipher bits. Number of LSB use to embed cipher bits is defined by the variable ‘x’. If XORing (7th & 6th bits of pixel) is 0 then 0th bit position i.e., one

LSB is used to hide the data. If XORing (7th & 6th bits of pixel) is 1 then 0th and 1st bit positions i.e., Two-LSB's are used to hide the data.

The extraction of secret message can be done by the reverse process of the embedding process. The cipher text is obtained by processing the frames of the stego video through the variable LSB method. The original is takeout from the cipher from the AES decryption system and decompression process.

Experimental Results and Discussions

In the experiment a sample video of 100 frames is considered and the size of the video frame is 720 X1280X3. For convenient just 15 frames has been shown in the figure 2. Figure 3 shows the five secret messages among which two are text data and three are images. Figure 3a and 3b shows image 1 and image 2 which are high and low informative respectively. Figure 3c shows image three which has moderate structure in the pixel distribution. Image 1, image 2 & image 3 are 708KB, 768KB & 768KB of size respectively. Text 1 and Text2 are of different sizes 38KB &17KB respectively.

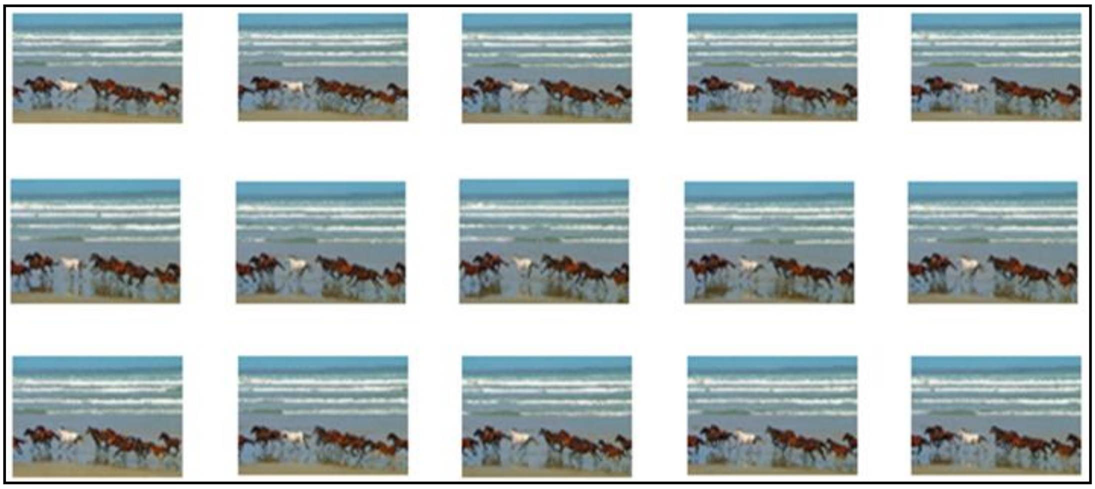
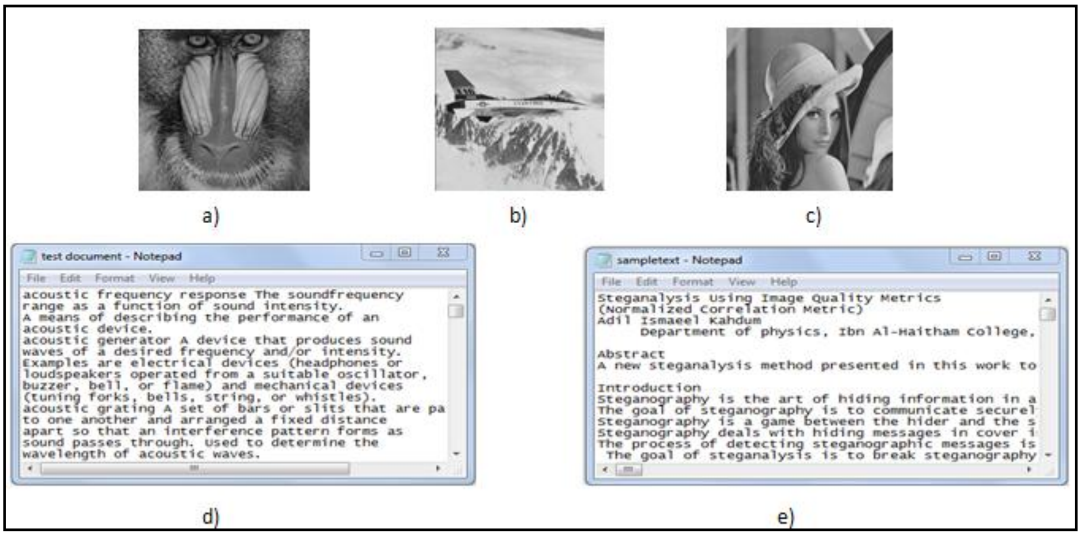


Figure 2: Frames of The Sample Video

Images are compressed using lossy compression implemented by DCT transform followed by Huffman coding. Thresholding has been considered as 100 to quantize the DCT coefficients of the each image. Since secret information is image, message can be conveyed even if there is any loss at the recipient end. But in the text data, loss of information leads to damage of secret information at the recipient end. Hence a loss less compression using Huffman source coding method is chosen for Text1 & 2 secret data. The Compression ratio and compression factors are used to measure the performance of compression method.



```
acoustic frequency response The soundfrequency
range as a function of sound intensity.
A means of describing the performance of an
acoustic device.
acoustic generator A device that produces sound
waves of a desired frequency and/or intensity.
Examples are electrical devices (headphones or
loudspeakers operated from a suitable oscillator,
buzzer, bell, or flame) and mechanical devices
(tuning forks, bells, string, or whistles).
acoustic grating A set of bars or slits that are pa
to one another and arranged a fixed distance
apart so that an interference pattern forms as
sound passes through. Used to determine the
wavelength of acoustic waves.
```

```
Steganalysis Using Image Quality Metrics
(Normalized Correlation Metric)
Adil Ismaeel Kahdum
      Department of physics, Ibn Al-Haitham College,

Abstract
A new steganalysis method presented in this work to

Introduction
Steganography is the art of hiding information in a
The goal of steganography is to communicate securel
Steganography is a game between the hider and the s
Steganography deals with hiding messages in cover i
The process of detecting steganographic messages is
 The goal of steganalysis is to break steganography
```

Figure 3: Secret information a) Image 1 b) Image 2 c) Image 3 d) Text1 e) Text2

The compression ratio is defined as

$$Compression\ ratio = \frac{size\ of\ the\ output\ stream}{size\ of\ the\ input\ stream}$$

The inverse of the compression ratio is called the compression factor :

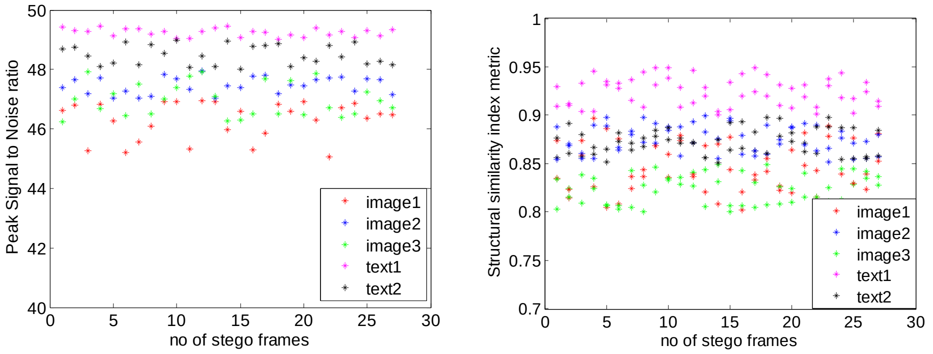
$$Compression\ factor = \frac{size\ of\ the\ input\ stream}{size\ of\ the\ output\ stream}$$

Average length of the code word, compression ratio, compression factor for each secret message is as mentioned in the table 1.

Table 1: Information details of the secret data with compression ratio, factor & average word length

Secret message	Size in Kbytes per frame	Compression ratio	Compression factor	Average length
Image1	708	48.82%	2.0482	5.695
Image2	768	65.74%	1.483	5.290
Image3	768	56.93%	1.7565	5.382
Text1	17	64.60%	1.548	4.519
Text2	38	66.78%	1.497	4.674

The performance of the video steganography has been validated using objective quality metrics peak signal to noise ratio (PSNR) and structural similarity index measure (SSIM)[1]. Typical values of PSNR and SSIM varies from [30 50] & [0 1] respectively. Figure 4a & 4b shows the PSNR and SSIM of the stego frames for each secret data. In the embedding process, same secret image and text is repeatedly hided in each frame select using polynomial based variable LSB method. An interesting information is interpreted from the figure 4 that PSNR values of almost all the stego frames are located in the range 46-47dB.Similarly SSIM of all the stego frames are located in the0.8-0.95. The average PSNR and SSIM of the stego frames are tabulate in table 2.



(a) **(b)**

Figure 4: a) PSNR values of stego frames for various payloads b) SSIM values of stego frames for various payloads

Table 2: Average PSNR and SSIM of the complete Stego video

	Secret message	**PSNR**	**SSIM**
Stego video	Image1	45.7943	0.8396
	Image2	47.2295	0.8283
	Image3	47.5709	0.8797
	Text1	48.5581	0.8767
	Text2	49.3025	0.9212

Conclusions

This paper implements hybrid vide steganography in which information to be hide is compressed then encrypted and embed into the variable LSB's of the selected video frame based on polynomial expression as a function of cover frame. The proposed algorithm is simulated and results have been validated by using PSNR and SSIM. Even the performance of the proposed method can analyzed using video quality metric such as spatio-temporal distortion, video quality metric (VQM) and MOVIE.

References

[1] T.V.S. Gowtham Prasad, Dr. S. Varadarajan, (2013), "Improved Quality of Image Steganography Using POLPA", International Journal of Advanced Research in Electrical, Electronics and Instrumentation, Vol.2.

[2] Ying Wang and Pierre Moulin, “Steganalysis of block-DCT Image Steganography”, University of Illinois at Urbana-Champaign, CCR 00-81268 and CCR 02-08809.

[3] Changyong Xu, Xijian Ping, Tao Zhang, (2006), “Steganography in Compressed Video Stream”, International Conference on Innovative Computing, Information and Control , pg269 – 272, Volume:1, IEEE.

[4] Keren Wang, Hong Zhao, and Hongxia Wang, (2014) “Video steganalysis against motion vector based steganography by adding or subtracting one motion vector value”, IEEE transactions of information forensics and security, vol. 9, pg 741-751,.

[5] Kousik Dasguptaa”, Jyotsna Kumar Mondalb, Paramartha Duttac,(2013) “Optimized Video Steganography using Genetic Algorithm (GA)”, International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA), Elsevier ,131 – 137.

[6] Hemant Gupta , Dr. Setu Chaturvedi, (2013), “Video Steganography through LSB Based Hybrid Approach”, International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, Volume 6, Pg. 32-42.

[7] punita meelu, (2011) “AES Asymmetric key cryptographic system” in international journal of information technology and knowledge management, volume 4, Pg.113-117.

[8] Yadav, P.Mishra, N. ; Sharma, S., (2013), “A secure video steganography with encryption based on LSB technique” IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pg 1 – 5.

[9] Balaji, R. Naveen, G., (2011), “Secure data transmission using video Steganography”, IEEE International Conference on Electro/Information Technology (EIT), Pg 1-5.

[10] Mstafa, R.J. ; Elleithy, K.M., (2014), “A highly secure video steganography using Hamming code” , IEEE international conference on Systems, Applications and Technology, pg 1 – 6.

[11] Kundankumar, Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, (2014) “Text and Image Encryption Decryption Using Advanced Encryption Standard”, International Journal of Emerging Trends & Technology in Computer Science, Volume 3, Issue 3, Pg 118-126.