Video Steganography through LSB Based Hybrid Approach

Hemant Gupta
Technocrats Institute of technology Bhopal

Setu Chaturvedi
Technocrats Institute of technology Bhopal

Abstract

In this paper, proposed an advance approach for dynamic data protection using LSB and hybrid approach. Steganography is the art of communicating a message by embedding it into multimedia data. The proposed method for replacing one or two or three LSB of each pixel in video frame and apply Advance encryption standard (AES). It becomes very difficult for intruder to guess that an image is hidden in the video as individual frames are very difficult to analyze in a video. In this observation peak to signal noise ratio (PSNR) is grater for 1 bit LSB substation as compared to 3 bit LSB substation so that when number of LSB substation bit increased then security level is also increased and observation correlation coefficient has the value r=1 if the two image are absolutely identical, r=0 if they are completely uncorrelated and r=-1 if they are completely anti correlated for example if one image is the negative of the other.

Index terms:
AES, LSB, Cryptography.

1. Introduction

The steganography word divided into two part first steganos which comes from the Greek mean covered or secret and second graphy mean writing or drawing. The steganography is the technique of hiding information[1,6].

2. Literature Review

For studying the concepts of video steganography, we have surveyed many research papers. In this section we have described the relevant papers of different authors. We thank these authors for providing the knowledge of video steganography.

In [1] Author has proposed a scheme which is very important to us for studying the basic concept of steganography. The author deals which steganography using video file as a cover carrier. Video based steganography can be used as one video file having separate images in frames. Since that the use of the video based steganography can be more eligible than other multimedia files. This author is mainly concerned with how to embed data in a video file in from of bmp images and how we can make use of the internal structure of the video to hide data to be secured. The basic concept of this author which we have used in my research work and the second concept which has been implemented in our research work is how to use steganography using video file as a cover carrier.

[2] Based on similar concept with stenography, is the art of communicating a message embedded it into multimedia data. It is desired to maximize the amount of hidden information while preserving security against detection by unauthorized parties. The image based stenography issues has been illustrated to hide secret information in images and the possibility of using the image as a cover carrier for hiding secure data.

In [3] an image encryption algorithm combining the image encryption based on S-boxes scrambling with error correcting code was developed. The error correcting code could effectively improve the security of image encryption algorithm based on S-boxes scrambling. The basic concept of this author which we have used in my work focuses on maximizing security, capacity factor of data hiding and secures the data through AES.

In [4] author uses an algorithm based on AES expansion in which the encryption process is a bit wise exclusive or operation of a set of image pixels along with the 128 bit key, which changes for every set of pixel. The keys to be used are generated independently at the sender and receiver side based on AES key expansion process. Hence the initial key is shared rather than scaring the whole set of keys. The author gives the information about AES. The AES is provides high encryption quality with minimum memory requirement and computational time.

In [5] the author has proposed an AES technique which presents fundamental mathematics behind the algorithm along with a brief description of some cryptographic primitives that are commonly used in the field of communication security. AES provides better security and has less implementation complexity. It has emerged as one of the strongest and the most efficient algorithm.

In [6] author gave a different concept from above the authors using a new approach of hiding image in video. The algorithm is replaces 1 LSB of each pixel in video frame. It becomes very difficult for a intruder to guess that an image is hidden in the video as individual frame are difficult to analyze in a video running at 30 frame per second. We have seen that the author has used only 1 LSB substitution technique here. This is the basic concept of the author which is implemented in my research work.

In [7] Author has dealt with three main stenography challenges capacity imperceptibility and security. This is achieved by hybrid data hiding scheme in corporate LSB

Manuscript received March 5, 2014
Manuscript revised March 20, 2014

technique with a key permutation method. In my work I have implemented this basic concept of using LSB substitution and the ways to increase the system performance as well as its security.

3. Problem Domain

In the present area the hacking activities are becomes very powerful as compare to the security status. Now hacker can hack the information very smartly because security is not that much appropriate, hacker can easily retrieve data , change data and damage data. Now days Security is not sufficient to stop hacking. Though security status increased at a higher level but the major drawback of new status of security is cost, it became so costly.

Hence we need better solutions which have good security level with lower cost.

The confidential or important information, which sent with normal format, there might, may be a chance of happening misuse cases [1,2,6].

4. Existing System

Present day transactions are considered to be "un-trusted" in terms of security, i.e. they are relatively easy to be hacked and also we have to consider the transfer of large amount of data through the network will give errors while transferring. Only single level of security is present in the existing systems.

The other problem of existing system is Now days hacking activities are growing day by day & hackers can easily hack important information and security is not sufficient to stop hacking. Though security status increased at a higher level but the major drawback of new status of security is cost, it became so costly. Hence we need better solutions which have good security level with lower cost. [5,6]

5. Proposed Method

As we mentioned in problem domain that the used security techniques is not appropriate to prevent hacking and the new security technique is so costly. Then we need a different technique which is more efficient and provides a better security level. In our research work we are reducing hacking activity done by hacker with hiding the information in images.

We make AVI (audio video interleave) video. The AVI video are large in size but it can be transmitted from source to target over network after processing the source video by using these Data Hiding and Extraction procedure securely and this video are convert into 20equal gray scale images. Grayscale image uses 8 bit for each pixel and able to display 256 different colours or shades of grey. We make text information in set 1, set 2 , set 3 each set contain 20 bmp data images. And apply 1LSB or 2 LSB or 3 LSB substitutions & AES (Advanced Encryption Standard) Algorithm. The last steps make Encrypted AVI Video and send by the sender. Receiver end apply decryption is performed.

6. Methodology

6.1 AES

AES means Advanced Encryption Standard (AES) another method of data protection. AES is publicly accessible and also open cipher approved by the National Security Agency (NSA) for the purpose of top secret information.

AES is a symmetric key encryption technique which will replace the commonly used data encryption standard (DES).It was the result of a worldwide call for submissions of encryption algorithms issued by the US government's national institute of standards and technology (NIST).AES provides strong encryption and has been selected by NIST as a Federal Information Processing Standard in November 2001 (FIPS-197), and in June 2003 the U.S. Government (NSA) announced that AES is secure algorithm and enough to secure classified information up to the top secret level, and this is the highest security level.

The Advanced Encryption Standard algorithm are three cipher key such as 128, 192, or 256-bit encryption key (password).It uses one of three cipher key strengths. Each encryption key size causes the algorithm to behave slightly differently, so the increasing key sizes not only offer a larger number of bits with which you can scramble the data, but also increase the complexity of the cipher algorithm[8].

Features of AES is Key lengths of 128, 192, and 256 bits are supported. Each step in key size requires only two additional rounds.

High-level description of the AES algorithm

Step1: Key Expansion round keys are derived from the cipher key using Rijndael's key schedule

Step2: (Initial Round) Add Round Key using bitwise xor and each byte of the state is combined with the round key.

Step3: (Rounds) according to a lookup table Sub Bytes a non-linear substitution step where each byte is replaced with another

Step4: (Shift Rows) where each row of the state is shifted cyclically a certain number of steps.

Step5: (MixColumns) According to a Mix Columns where mixing operation which operates on the columns of the state in this combining the four bytes in each column.

Step6: AddRoundKey.

Step7: Final Round (no MixColumns).

(a) SubBytes.

(b) ShiftRows.
(c) AddRoundKey.

6.2 LSB Least Significant Bit Hiding (Image Hiding):

Least significant bit (LSB) is the best method for data protection. LSB method is very simple and a commonly used approach for developing Steganography system because the amount of space that an image can provide for hiding data will be more comparing with another other method LSB technique is the easiest way of hiding information in an image and yet it is effective[9,10].

6.2.1 Algorithm for image hiding-

Each pixel (8 Bits) is hided in 8 pixels of video frame (1bit of source image replaces LSB if 1 pixels in target frame). If image size is m1*n1 and frame size if m2*n2 Then number of pixels in one row of 1 frame that can be hided are given by Y=n2/8 pixels, Number of frame that can be hided in a video are given by[6,9,13]

```
Step 1. $X=(n_1/n_2)*8$
Step 2. For i=1 to x        // No of frames.
Step 3. For j=1 to m //No of rows in image.
Step 4. For k=1 to y        //    No of Columns that can be hided in one frame read bits of pixels.
Step 5. Write bits in LSB if frame pixel (8 pixel will be needed).
Step 6.  End for.
Step 7.  End for.
Step 8.  End for.
```

6.2.2 Algorithm for image unhiding-

To unhiding the image, LSB of each pixel in the frame is fetched and a bit stream is constructed to construct the image [6, 9].

```
Step 1. For i=1 to x        // No of frames.
Step 2.For j=1to m1 //No of rows in image.
Step 3. For k=1 to y.
Step 4. Read pixel.
Step 5. Find LSB.
Step 6. End For.
Step 7Construct bit stream to be written in recovered image.
Step 8. End For .
Step 9. End For.
```

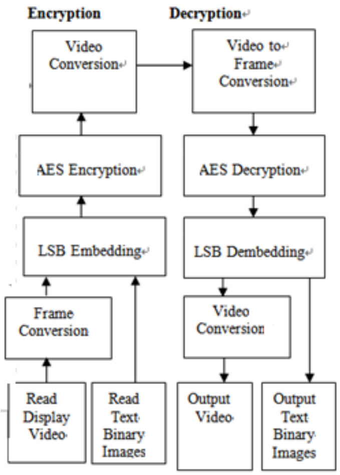


Fig 1: Proposal for data hiding through the LSB & AES

LSB is more efficient than MSB ,The logic behind using LSB steganlysis is that replacing LSB with an encrypted message will not introduce any detectable artifacts. Illustrating the above fact:-

Say the original data is 11101011(235) After the LSB conversion the data will be 11101010 with decimal value 234. While the MSB conversion will result in a value 01101011 having decimal value 117. This clearly goes to elucidate the fact that LSB conversion leads to less artifacts as compared to MSB conversion. Hence arousing less suspicion and serving the desired purpose of transmitting the secret information from one place to another [10].

7. Result Analysis

7.1 Correlation

Digital Image Correlation is a full-field image analysis method, based on grey value digital images that can determine the contour and the displacements of an object under load in three dimensions. The correlation coefficient has the value r=1 if the two image are absolutely identical, r=0 if they are completely uncorrelated and r=-1 if they are completely anti correlated for example if one image is the negative of the other [9].

Pearson's correlation coefficient, r is widely used in statistical analysis, pattern recognition, and image processing [11,12]. Applications for the latter include comparing two images for the purposes of image registration, object recognition, and disparity measurement. For monochrome digital images, the Pearson correlation coefficient is defined as [11].

$$r = \frac{\sum(X_i-X_m)(Y_i-Y_m)}{\sqrt{(X_i-X_m)^2}\sqrt{(Y_i-Y_m)^2}}$$

where x_i is the intensity of the ith pixel in image 1, y_i is the intensity of the ith pixel in image 2, x_m is the mean intensity of image 1 and y_m is the mean intensity of image 2.

7.1.1 Autocorrelation between Original and Encrypted image for 1bit LSB Substitution & AES

It shows relation between original image and encrypted image for different frame (Images). When 1 LSB Substitution is applied for each pixel and AES algorithm then we find no correlation relation.

Because AES algorithm Key lengths of 128, 192, and 256 bits are supported So that hackers cannot easily hack important information and security is sufficient to stop hacking.

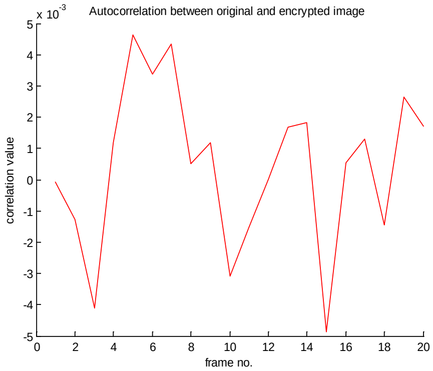


Figure2: Autocorrelation between Original and Encrypted image for 1bit LSB Substitution & AES

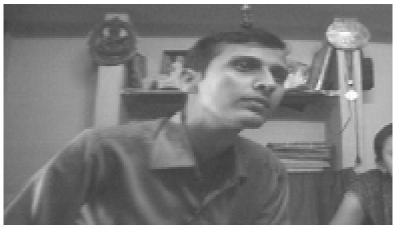


Figure3: Afther apply 1LSB Substitution & AES

7.1.2 Autocorrelation between Original and Encrypted image for 2bit LSB Substitution & AES

It shows relation between original image and encrypted image for different frame (Images). When 2 LSB Substitution is applied for each pixel and AES algorithm then we find no correlation relation.

Because AES algorithm is generated Key lengths of 128, 192, and 256 bits So that hackers cannot easily hack important information and security is sufficient to stop hacking.

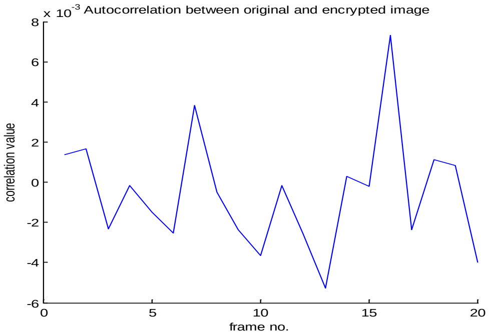


Figure4: Autocorrelation between Original and Encrypted image for 2bit LSB Substitution & AES

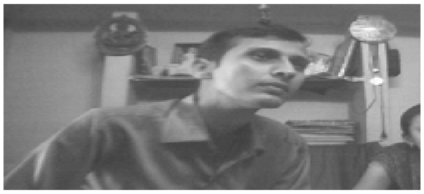


Figure5: Afther apply 2LSB Substitution & AES

7.1.3 Autocorrelation between Original and Encrypted image for 3bit LSB Substitution & AES

It shows relation between original image and encrypted image for different frame (Images). When 3 LSB Substitution is applied for each pixel and AES algorithm then we find no correlation relation.

Because AES algorithm is generated Key lengths of 128, 192, and 256 bits are supported. So that hackers cannot easily hack important information and security is sufficient to stop hacking.

It means when 3 LSB & AES applied then data security is more increased.

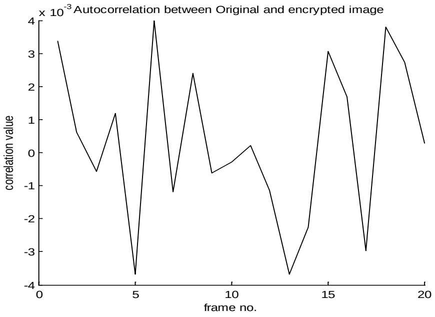


Figure6: Autocorrelation between Original and Encrypted image for 3bit LSB Substitution & AES

Figure7: Afther apply 3LSB Substitution & AES

7.1.4 Autocorrelation between Original and Encrypted image for 1bit,2 bit,3bit LSB Substitution & AES

It shows relation between original image and encrypted image for different frame (Images). When compare 1bit ,2 bit, 3bit LSB Substitution & AES then we find no relation between these. Because AES algorithm is generated Key lengths of 128, 192, and 256 bits are supported. So that hackers cannot easily hack important information and security is sufficient to stop hacking.

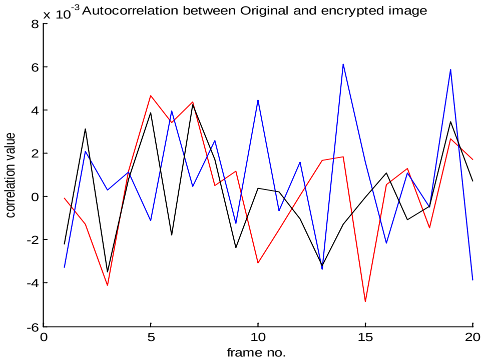


Figure8:Auto correlation between Original and Encrypted image for 1bit ,2bit & 3bit LSB Substitution & AES.

7.1.5 Autocorrelation between embedded and Encrypted image for 1bit LSB Substitution & AES

It shows relation between embedded image and encrypted image for different frame (Images). When 1 LSB Substitution is applied for each pixel and AES algorithm then we find no correlation relation.

Because AES algorithm is generated Key lengths of 128, 192, and 256 bits are supported. So that hackers cannot easily hack important information and security is sufficient to stop hacking.

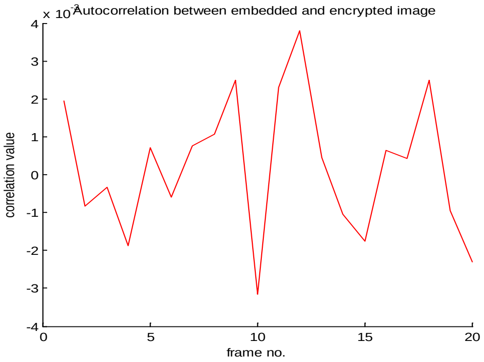


Figure9: Auto correlation between embedded and encrypted image for 1bit LSB Substitution & AES

Figure10: Afther apply 1LSB Substitution & AES

7.1.6 Autocorrelationbetween Embedding and Encrypted image for 2bit LSB Substitution & AES

It shows relation between Embedding image and encrypted image for different frame (Images). When 2 LSB Substitution is applied for each pixel and AES algorithm then we find no correlation relation.

Because AES algorithm is generated Key lengths of 128, 192, and 256 bits are supported.So that hackers cannot easily hack important information and security is sufficient to stop hacking.

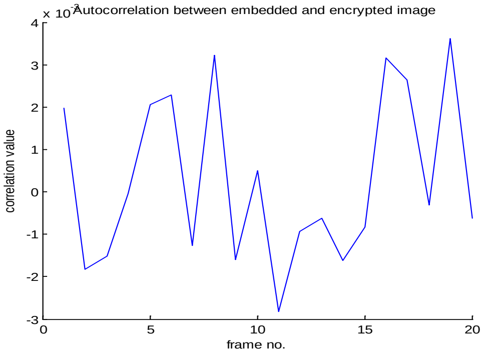


Figure11: Auto correlation between Embedded and Encrypted image for 2bit LSB Substitution & AES

Figure12: Afther apply 1LSB Substitution & AES

7.1.7Autocorrelation between Embedded and Encrypted image for 3bit LSB Substitution & AES

It shows relation between original image and encrypted image for different frame (Images). When 3 LSB Substitution is applied for each pixel and AES algorithm then we find no correlation relation.

Because AES algorithm is generated Key lengths of 128, 192, and 256 bits are supported. So that hackers cannot easily hack important information and security is sufficient to stop hacking.

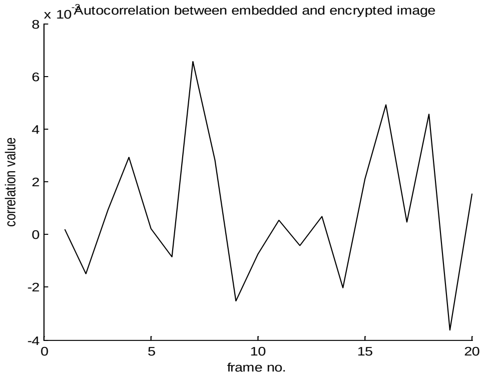


Figure13: Auto correlation between Embedded and Encrypted image for 2bit LSB Substitution & AES

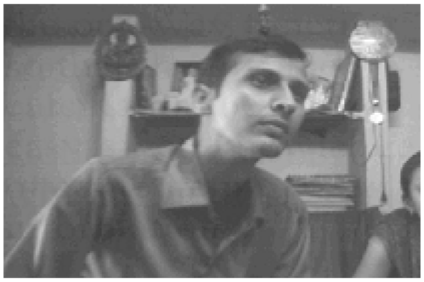


Figure14: Afther apply 3LSB Substitution & AES

7.1.8 Autocorrelation between Embedded and Encrypted image for 1bit,2 bit,3bit LSB Substitution & AES

It shows relation between original image and encrypted image for different frame (Images). When compare 1bit ,2 bit, 3bit LSB Substitution & AES then we find no relation between these. Because AES algorithm is generated Key lengths of 128, 192 and 256 bits are supported. So that hackers cannot easily hack important information and security is sufficient to stop hacking.

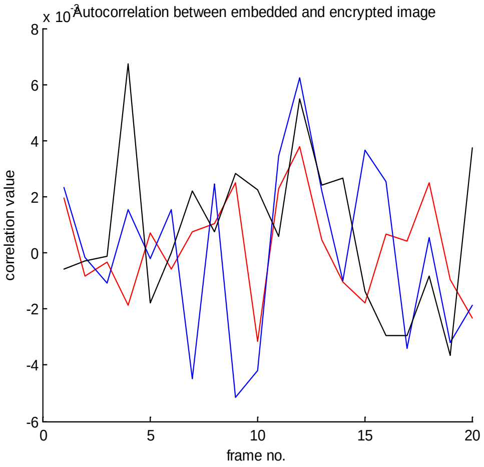


Figure15: Auto correlation between Embedded and Encrypted image for 1bit ,2bit & 3bit LSB Substitution & AES

7.2 PSNR (peak signal-to-noise ratio)

The PSNR stands for peak signal-to-noise ratio. It works between two images. The result is in decibels (dB). PSNR is very popular in image processing. A sample use is in the comparison between an original image and a coded/decoded image[9].

The PSNR is defined as:

$$\mathrm{PSNR}=10.\log_{10}\left(\frac{\mathrm{Max}_I^{\,2}}{\mathrm{MSE}}\right)$$

$$\mathrm{PSNR}=20.\log_{10}\left(\frac{\mathrm{Max}_I}{\sqrt{\mathrm{MSE}}}\right)$$

$$\mathrm{PSNR}=20.\log_{10}(\mathrm{MAX}_I)-10.\log_{10}(\mathrm{MSE})$$

where, MAX_I is the shown maximum possible pixel value of the image.

MSE=_Mean square error

m×n=monochrome image.

$$\mathrm{MSE}=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[\,I(i,j)-K(I,j)\,]^2$$

7.2.1 PSNR for 1bit LSB & AES

In this bar graph shown realtion between original image and encrypted(recived) image for 1 bit LSB subtitution and AES algorithm.

the graph show no realtion between numer of each frame and PSNR. Because Because AES algorithm is generated randomly relation. So that hackers cannot easily hack important information and security is sufficient to stop hacking.

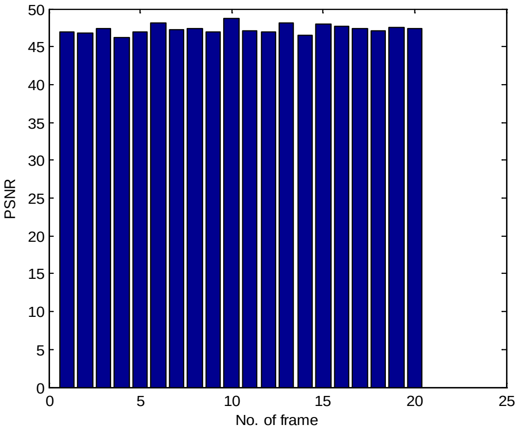
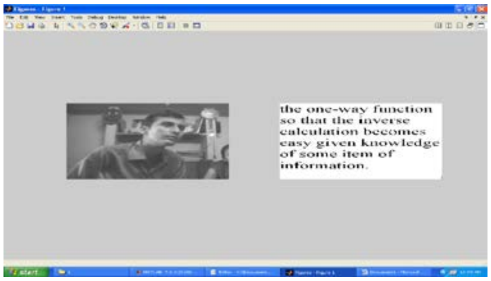


Figure16: PSNR for 1 bit LSB & AES



the one-way function so that the inverse calculation becomes easy given knowledge of some item of information.

Figure17: Dembeding for 1bit LSB & AES

7.2.2 PSNR for 2bit LSB & AES

In this bar graph shown realtion between original image and encrypted(recived) image for 2 bit LSB subtitution and AES algorithm. the graph show no realtion between numer of each frame and psnr. Because Because AES algorithm is generated randomly relation. So that hackers cannot easily hack important information and security is sufficient to stop hacking. In this observation peak to signal noise ratio (PSNR) is decreased when number of LSB substation bit increased then security is also increased.

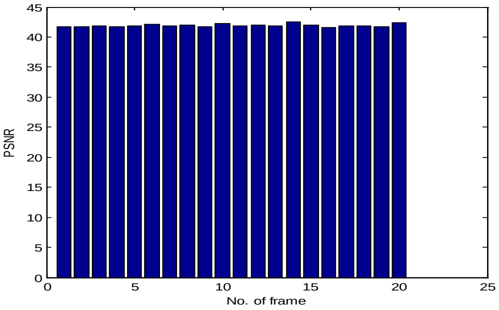
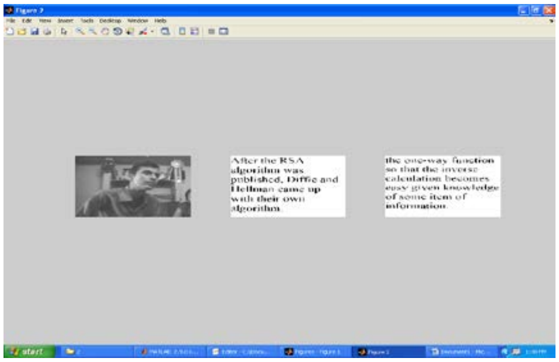


Figure18: PSNR for 2 bit LSB &AES



After the RSA algorithm was published, Diffie and Hellman came up with their own algorithm.

the one-way function so that the inverse calculation becomes easy given knowledge of some item of information.

Figure19: Dembeding for 2bit LSB & AES

7.2.3 PSNR for 3bit LSB & AES

In this bar graph shown realtion between original image and encrypted(recived) image for 3 bit LSB subtitution and AES algorithm. the graph show no realtion between numer of each frame and psnr. Because Because AES algorithm is generated randomly relation. So that hackers cannot easily hack important information and security is sufficient to stop hacking. In this observation peak to signal noise ratio (PSNR) is decreased when number of LSB substation bit increased then security is also increased.

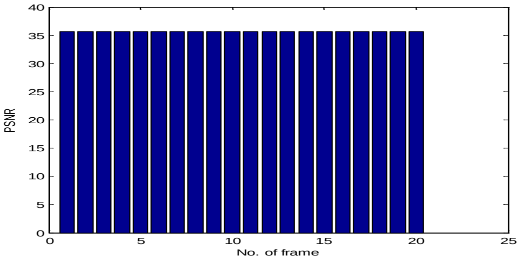
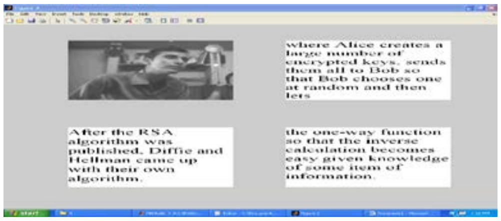


Figure20: PSNR for 3 bit LSB & AES



where Alice creates a large number of encrypted keys, sends them all to Bob so that Bob chooses one at random and then lets

After the RSA algorithm was published, Diffie and Hellman came up with their own algorithm.

the one-way function so that the inverse calculation becomes easy given knowledge of some item of information.

Figure21: Dembeding for 3bit LSB & AES

7.2.4 Encrypted image for 3bit LSB &AES

In this figure show encrypted image both image and information are mixed. So that hackers cannot easily hack important information and security is sufficient to stop hacking.

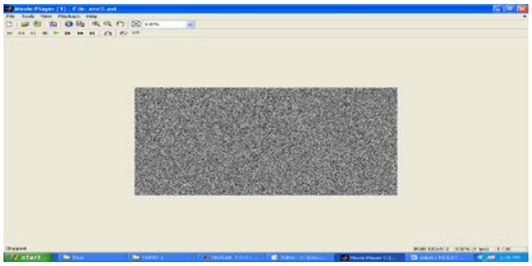


Figure22: Encrypted image for 3bit LSB &AES

8. Conclusion

In this paper, a data hiding method by using Single bit, two bit, three bit LSB substitution and Advanced Encryption Standard. Algorithm is performed. We are calculating PSNR and correlation factor.

We calculate correlation between Original and embedded image for 1bit LSB & 2 bit LSB & 3 bit LSB Substitution and AES method. In this paper observation PSNR is decreased when number of LSB substation bit increased simultaneous security is also increased.

We are also calculating correlation between Original and embedded image for 1bit LSB & 2 bit LSB & 3 bit LSB Substitution & AES method. In this observation PSNR is decreased when number of LSB substation bit increased. So that hackers cannot easily hack important information and security is sufficient to stop hacking.

Result analyze the correlation coefficient has the value r=1 if there is not difference in the original image. The number of LSB Substitute is increase then correlation factor is decreased.

In this paper observation Autocorrelation between original image and encrypted image for different frame (Images). we find no relation between these. Because AES algorithm is generated Key lengths of 128, 192, and 256 bits are supported. So that hackers cannot easily hack important information and security is sufficient to stop hacking.

References:

[1] A.K. Al Frajat ”Hiding data in video file An overview” Journal of applied sciences 10(15):1644-1649, 2010.

[2] Ali K Hmood ”An overview on hiding information technique in images” Journal of applied sciences 10(18)2094-2100, 2010.

[3] Niu Jiping ”Image encryption algorithm based on rijndael S-boxes” in IEEE applied International conference on computational intelligence and security 978-0-7695-3508-1\08, 2008.

[4] B. Subramanan “Image encryption based on aes key expansion” in IEEE applied second international conference on emerging application of information technology, 978-0-7695-4329-1/11, 2011.

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

[6] Saurabh singh “Hiding Image to Video” International Journal of engineering science & technology Vol. 2(12), 6999-7003 ,2010.

[7] Marghny Mohamed”Data hiding by LSB substitution using genetic optimal key permutation ” in International arab journal of e-technology ,vol.2,no 1,11-17, January 2011.

[8]]P.Karthigaikumar “Simulation of image encryption using AES algorithm”IJCA special issue on computer science New dimensions &perspectives, 166-172, 2011.

[9] M.Wu, Hiding in image and video Part I fundamental issues and solutions ,IEEE Trans Image processing,12(6):685-686, 2005.

[10] M.Wu ,E. Tang and B.Liu,”Data hiding in digital binary image ,”in IEEE ICME New York City, NY,USA ,July 2000.

[11] J.L. Rodgers, J. L. and W.A. Nicewander, “Thirteen Ways to Look at the Correlation Coefficient”, American Statistician 42, 59-66 ,1995.

[12] Liu bin, Li zhitang, Li Yao an Image method based on correlation analysis and image fusion”International conference on parallel and distributed computing, Application and technology 0-7695-2405-2/05 ,2005.

[13] P.Mohan Kumar and K.L.Shunmuganathan “A New approach for hiding data in images using image domain method” in International Journal of computer and internet security ISSN 0974-2247 volume 3 ,number PP 69-80, 2011