Research Inventy: International Journal Of Engineering And Science
Vol.2, Issue 10 (April 2013), Pp 32-39
Issn(e): 2278-4721, Issn(p):2319-6483, Www.Researchinventy.Com

Video Data Hiding Through LSB Substitution Technique

[1]Hemant Gupta, [2]Dr. Setu Chaturvedi
[1,2,]*Technocrats Institute of technology Bhopal*

Abstract: *In this paper propose a video data embedding scheme. It is embedded in AVI (audio video interleave) video. The proposed method for replacing one or two or three LSB of each pixel in video frame. 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 paper calculate peak to signal noise ratio (PSNR) correlation factor analysis and comparison of correlation between original and embedded image for 1bit LSB, 2 bit LSB, 3bit LSB Substitution is given in result section.*

Keywords: *Index terms: LSB, Cryptography.*

I. INTRODUCTION

As the increasing use of digital documents, digital document image processing becomes more and more useful. Data-hiding in document images have received much attention recently. One of the applications of data-hiding in document images is steganography. The purpose of steganography is to communicate information secretly so that others who respect the objects being exchanged cannot notice the existence of extra information hidden in the objects. Steganography comes from the Greek word meaning covered writing. steganography as the hiding of a message within another so that the presence of the hidden message is indiscernible The key concept behind steganography is that the message to be transmitted is not detectable to the casual eye. In fact, people who the are not intended to be the recipients of the message should not even suspect that a hidden message exists [1, 4].

II. 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. These paper were very important to us for studying the basic concept by Saurabh singh ,Gaurav Agarwal"Hiding image to video : A new approach of LSB replacement" [1] in this noval approach of hiding image in video the proposed algorithm is replacing one LSB of each pixel in video frame it becomes very difficult for 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 and we seen that only one LSB substitution are used . The concept of this paper which I used in my work how to used LSB substitution.

Another work on this topic has been presented by Marghny Mohamed,fadwa alafari and Mohamed bamatraf "Data hiding by LSB substitution using genetic optimal key permutation"[2]. In this paper deal three main stenography challenges capacity imperceptibility and security this is achieved hybrid data hiding scheme in corporate LSB technique with a key permutation method. The concept of this paper which I used in my work how to used LSB substitution and how to increase the system performance capacity, security.
Another work on this topic has been presented in the paper by A.K.A frajat, H.A. Jalab, Z.M. Kasirun, "Hiding Data in Video file an overview" [3]. The paper deals steganography using video file as a cover carrier. Video based steganography can be used as one video file separated images in frames or image. Since that the use of the video based steganography can be more eligible than other multimedia files. This paper is mainly concerned with how to cover as video file and how we can make use of the internal structure of the video to hide secure data. The concept of this paper which I used in my research work how to used steganography using video file as a cover carrier.

similar work on this topic has been presented in the paper by Ali K. hmood, B.B zaidan, A.A. zaidan and Hamid A. jalab "An overview on hiding information technique Images " [4]. In this paper shows stenography is the art of communicating a message embedding it into multimedia data it is desired to maximized the amount of hidden information while preserving security against detection by un authorized parties. We seen that hiding secret information in images and LSB in bmp make of for this but approach result in suspicious files that increase the probability of detection. we have also seen that possibility of using the image as a cover carrier for hiding secure data the image based stenography issues has be illustrated .

III. PROBLEM DOMAIN

Now days hacking activities are growing day by day and 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.

The confidential or important information, which sent with normal format, there might, may be a chance of happening misuse cases. These can be avoided by making use of this system. The mechanism, which is used to hide the information in the bmp image files[9,10].

IV. 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[2,3,4].

V. PROPOSED SOLUTION

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 20 equal 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 1 LSB or 2 LSB or 3 LSB substitutions. The last steps make encrypted AVI Video and send by the sender. Receiver end apply decryption is performed.

5.1. Algorithm for the Proposed System

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 other method. This method is probably the easiest way of hiding information in an image and yet it is surprisingly effective [5].

5.1.1 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) [8]. If image size is m_1*n_1 and frame size if m_2*n_2 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

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.

5.1.2 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.

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

LSB is more efficient than MSB, the logic behind using LSB steganolysis 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. Whilst 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[6].

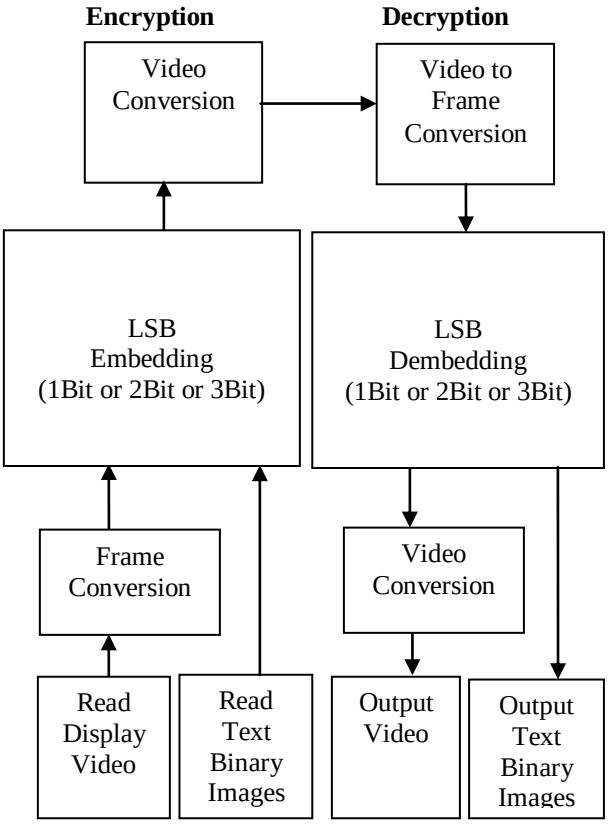

Fig 1: Proposal for data hiding throws LSB Embedding & Dembedding

VI. RESULT

6.1 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 [7].

Pearson's correlation coefficient, r, is widely used in statistical analysis, pattern recognition, and image processing [7]. Applications for the latter include comparing two images for the purposes of image registration, object reorganization, and disparity measurement. For monochrome digital images, the Pearson correlation coefficient is defined as [7]

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

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.

6.1.1 Autocorrelation between Original and Embedded image for 1bit LSB Substitution

It shows relation between original image and embedded image for different frame (Images). When 1 LSB Substitution is applied for each pixel then we find correlation value for each frame approximates 0.9998. We know that 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. It means when 1 LSB applied then data security is increased.

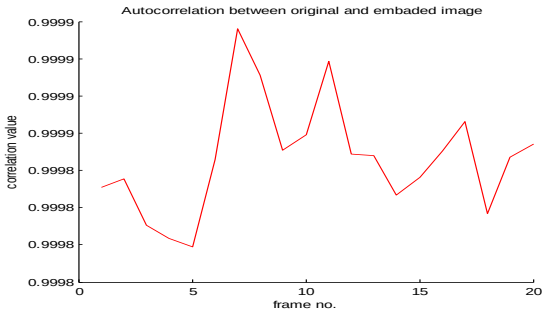

Figure2: Autocorrelation between Original and Embedded image for 1bit LSB Substitution

6.1.2 Autocorrelation between Original and Embedded image for 2bit LSB Substitution

In this Graph show relation between original image and embedded image for different frame (Images). When 2 LSB Substitution is applied for each pixel. Then we find correlation value for each frame approximate 0.9992.We know that 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. It means when 2 LSB applied then data is more secure.

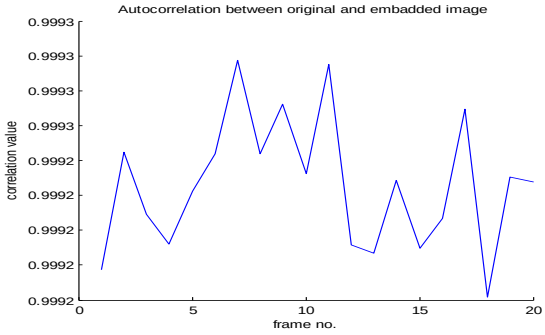

Figure3: Autocorrelation between Original and Embedded image for 2bit LSB Substitution

6.1.3 Autocorrelation between Original and Embedded image for 3bit LSB Substitution

In this Graph show relation between original image and embedded image for different frame (Images). When 3 LSB Substitution is applied for each pixel. Then we find correlation value for each frame approximate 0.9968.

1 LSB Substitution gives the value for each frame approximate 0.9998 and 2 LSB Substitution gives the value for each frame approximate 0.9992.

We know that 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

It means when 3 LSB applied then data is better secure as compare to 1 LSB Substitution and 2 LSB Substitution.

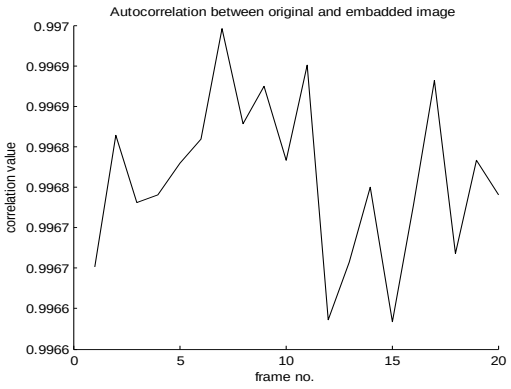

Figure4: Autocorrelation between Original and Embedded image for 3bit LSB Substitution

6.1.4 Comprative Autocorrelation between Original and Embedded image for 1bit LSB and 2bit LSB Substitution

In this Graph show Comparison Autocorrelation between Original and Embedded image for 1bit LSB, 2 bit LSB Substitution. In this graph red line indicate 1 Bit LSB and blue line indicate 2 bit LSB Substitution 2bit LSB Substitution gives the value approximate 0.9992. and 1bitLSB Substitution gives the value approximate 0.9998 and we know that 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 [7]. It gives the 2 bit LSB is more secure as compared to 1 LSB.

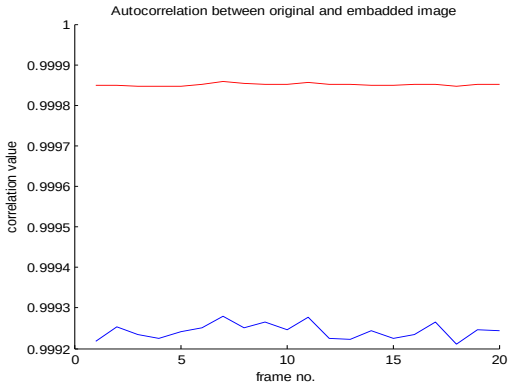

Figure5: Autocorrelation between Original and Embedded image for 1bit LSB & 2 bit LSB Substitution

6.1.5 Autocorrelation between Original and Embedded image for 1bit LSB and 2bit LSB and 3bit LSB Substitution

In this Graph show Comparison Autocorrelation between Original and Embedded image for 1bit LSB, 2 bit LSB,3 LSB Substitution. In this graph red line indicate 1 Bit LSB and blue line indicate 2 bit LSB Substitution and black line indicate 3 bit LSB Substitution It gives the 3 bit LSB substitution is more secure as compared to 2 LSB and 1LSB Substitution. Because 3 bit LSB Substitution gives the value approximate 0.9968 and 2bit LSB Substitution gives the value approximate 0.9992 and 1bitLSB Substitution gives the value approximate 0.9998 so we analyses that 3 LSB substitution gives the minimum value as compare to other like 2 LSB and 1 LSB . we know that 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 . so that 3 bit LSB substitution is more secure as compare to 2 LSB and 1 LSB substitution. [7].

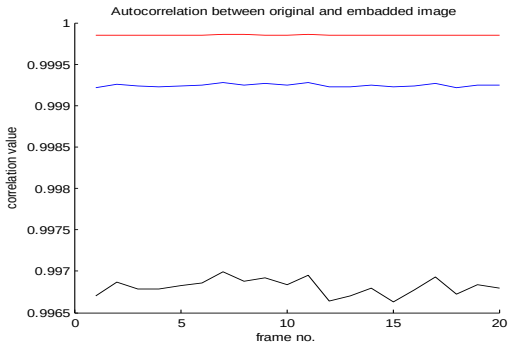

Figure6: Compare Autocorrelation between Original and Embedded image for 1bit LSB ,2 bit LSB,3bit LSB Substitution

Figure7: Original Frame set Image

Figure8: Afther apply 1LSB Frame set Image

Figure9: Apply 2LSB Frame set Image

Figure10: Apply 3LSB Frame set Image

Table 1: Compare Correlation value

Frame No	**Correlation Value**		
(X)	**1 LSB Substit-ute (Y)**	**2 LSB Substitute (Y)**	**3 LSB Substitute (Y)**
1	0.9998	0.9992	0.9967
2	0.9998	0.9993	0.9969
3	0.9998	0.9992	0.9968
4	0.9998	0.9992	0.9968
5	0.9998	0.9992	0.9968
6	0.9999	0.9993	0.9969
7	0.9999	0.9993	0.9970
8	0.9999	0.9993	0.9969
9	0.9999	0.9993	0.9969
10	0.9999	0.9992	0.9968
11	0.9999	0.9993	0.9970
12	0.9999	0.9992	0.9966
13	0.9999	0.9992	0.9967
14	0.9998	0.9992	0.9968
15	0.9998	0.9992	0.9966
16	0.9999	0.9992	0.9968
17	0.9999	0.9993	0.9969
18	0.9998	0.9992	0.9967
19	0.9999	0.9992	0.9968
20	0.9999	0.9992	0.9968

6.2 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[6].

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation..

The PSNR is defined as:

$$PSNR=10.\log_{10}\left(\frac{Max_I^2}{MSE}\right)$$

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

$$PSNR =20.\log_{10}(MAX_I) - 10.\log_{10}(MSE)$$

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

Mean square error (MSE) defined as:

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

6.2.1 PSNR between Original and Encrypted image for 1bit LSB Substitution

In this bar graph shown realtion between original image and encrypted(recived) image . it calculate between numer of each frame and psnr. in this graph show psnr value for each frame is approximate 51.1 db when 1 Lsb subtitution is applied it means 51.1 db correlated the original & encrypted image.

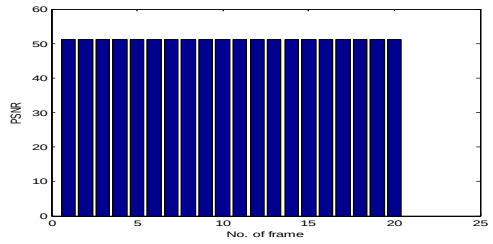

Figure11: PSNR for 1 bit LSB

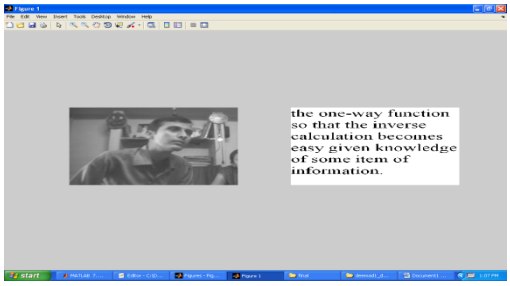

Figure12: Dembedding for 1bit LSB

6.2.2 PSNR between Original and Encrypted image for 2bit LSB Substitution

In this bar graph shown realtion between original image and encrypted(recived) image . it calculate between numer of each frame and psnr. in this graph show psnr value for each frame is approximate 42.7 db when 2 Lsb subtitution is applied .It means 42.7 db correlated the original & encrypted image.

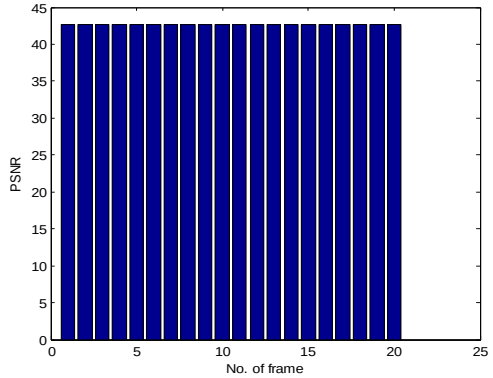

Figure13: PSNR for 2 bit LSB

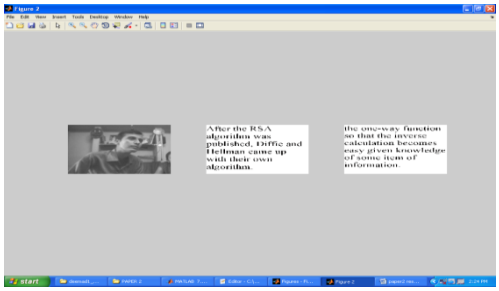

Figure14: Dembeding for 2bit LSB

6.2.3 PSNR between Original and Encrypted image for 3bit LSB Substitution

In this bar graph shown realtion between original image and encrypted(recived) image . it calculate between numer of each frame and psnr. in this graph show psnr value for each frame is approximate 35.7db when 3 Lsb subtitution is applied .It means 35.7db correlated the original & encrypted image.

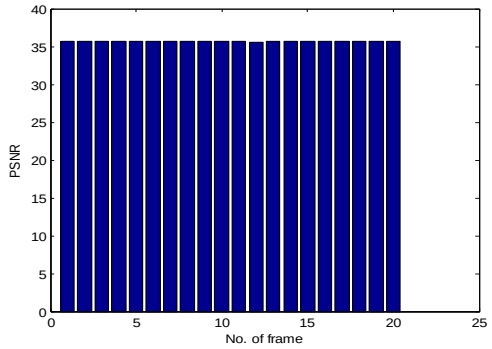

Figure15: PSNR for 3 bit LSB

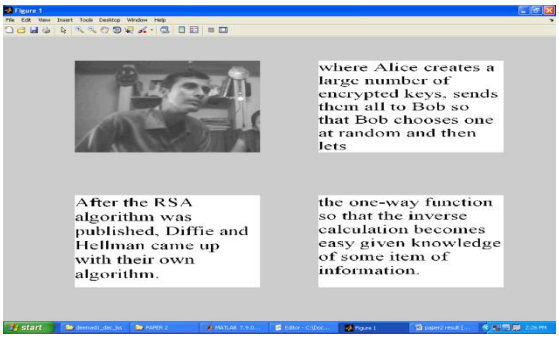

Figure16: Dembedding for 3bit LSB

VII. CONCLUSION:

In this paper, an advanced data hiding method by using different bit using LSB substitution is proposed and also analyzed Correlation between Original and embedded image for 1bit LSB & 2 bit LSB & 3 bit LSB Substitution. 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 also calculated PSNR (peak signal-to-noise ratio) between original image and encrypted(recived) image. PSNR value for each frame is approximate 35.7db when 3 Lsb subtitution is applied. PSNR value for each frame is approximate 42.7db when 2 Lsb subtitution is applied. PSNR value for each frame is approximate 51.1db when 1 Lsb subtitution is applied.so result is show that number of LSB Substitute is increase then PSNR is decreased and data security is simultaneous increased.

REFERENCES:

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

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

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

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

[5] Mohammed A.F. Al husainy”Image Steganography by mapping pixel to letters” in Journal of computer science 5(1),33-38, 2009

[6] M. Abomhara , ”International journal of computer theory and engineering” ,volume 2 ,1793-8201,2010

[7] Liu bin “an Image method based on correlation analysis and image fusion” in IEEE applied International conference on parallel and distributed computing, application and technology0-7695-2405-2/05, 2005

[8] P. Mohan Kumar” A new approach for hiding data in image using image domain methods” in International journal of computer and internet security volume 2, 69-80, 2011.

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

[10] P. Mohan Kumar” A new approach for hiding data in image using image domain methods” in International journal of computer and internet security volume 2, 69-80, 2011.