ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 5, May 2013

A Data Hiding scheme in motion vector of videos by LSB Substitution

P. Sunitha Kency Paul[1], P.Fasca Gilgy Mary[2], J.Dheeba[3]

***Abstract*—This paper deals with data hiding in the internal dynamics of video. Data hiding is the process of embedding information into host medium. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable in the video. This paper describes how motion vector can be used as a carrier to hide data. The purpose of data hiding is to secretly transmit the secret message. This has overcome the disadvantage of existing hiding data system such as display the fonts differently and easily spotted in text steganography; a proper cover image is needed for image steganography. The advantage of proposed data hiding in video are: user cannot find the original data, it is not easily cracked. it increases the Security and increases the size of stored data. In the proposed method, the secret message bitstream is first encrypted by using RSA algorithm and the encrypted is embedded in the least significant bit by using Least Significant Bit and also use edge detection mechanism for selecting the pixel. The performance is calculated by using Peak to Signal Noise Ratio. The performance analysis shows that the algorithm ensures better security against attackers**

***Index Terms*— Least Significant Bit(LSB), Peak to Signal Noise Ratio(PSNR).**

I. Introduction

In today's world the art of sending & displaying the hidden information especially in public places, has received more challenges. One of the reasons that intruders acquire information from a system is in a form that they can read and comprehend. Intruders may modify it to misrepresent an individual or organization, reveal the information to others, or use it to launch an attack. The solution to above problem is, through the use of steganography. Steganography [2] is a technique of hiding information in cover media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. Steganography become important as more people join the cyberspace revolution.

The word "Steganography" means covered or hidden writing. Its ancient origins are 440 BC. Although the term steganography was only coined at the end of the 15th century. Cryptography became more common in the middle ages and secret writing was employed by the Catholic Church in its various struggles down the ages and by the major governments of the time. Steganography was normally combined with cryptography to further hide secret information. Therefore, different methods have been proposed so far for hiding information in different cover media. It provides secure channels for communicating parties. Information hiding is an emerging research area, [3] which encompasses applications such as copyright protection for digital media, fingerprinting watermarking, and steganography. The main aim of the steganography is to hide secret information within the media, so that its presence in invisible and so there is a reliable communication with the receiver. Eventhough the host data set is corrupted, this steganography makes more difficult for attackers to obtain the secret message from the host data set. Steganography is the art of hiding information the fact is that the communication takes place by hiding the information in other information. The various file formats can be used they are text, image, bitmap picture, audio and video files. The basic structure of Steganography is made up of three components: the carrier, the message and the key. Carrier is also known as cover-object, in which the message is embedded and serves to hide the presence of the message. The carrier can be a painting, a digital image, an mp3. The key is the decode/decipher/displaying the hidden message. The message is the confidential or the authenticated message.

II. RELATED WORK

The majority of today's steganographic systems uses various multimedia objects such as image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication .So, in the modern age so many steganographic techniques have been designed which work with the concerned object. In today's security advancement, a combination of Cryptography and Steganography is used to achieve data privacy over secrecy. Steganography can be applied on digital files (audio/image/video/text, etc.), Steganography can be applied to different types of media .They are:

A. Network Steganography:

All information hiding techniques that may be used to exchange steganograms in telecommunication networks can be classified under the general term of network steganography. The typical steganographic methods which utilize digital media (images, audio and video files) as a cover for hiding the secret message. It also utilizes

Manuscript received April 20, 2013.

***P.Sunitha Kency Paul**, PG Scholar/CSE, Noorul Islam Centre for Higher Education, Thuckalay, TamilNadu, India. (e-mail: sunithakency@gamil.com), Tel: +91 9677718759.*

***P. Fasca Gilgy Mary,** PG Scholar/CSE, Noorul Islam Centre for Higher Education, Thuckalay, TamilNadu, India. (e-mail:fascapragasam@gamil.com), Tel:+919443155933 .*

***J.Dheeba**, Assistant Professor/CSE, Noorul Islam Centre for Higher Education,Thuckalay,TamilNadu,India.(e-mail: dheeba.jacob@gmail.com), Tel: +91 9442009711*

communication protocols control elements and their basic intrinsic functionality. Network steganography covers a various broad spectrum of techniques, which include: Voice-over-IP and WLAN Steganography.

B. Text Steganography:

Text Steganography is considered to be the most difficult kind of steganography due to the lack of redundancy in text as compared to audio or image. It requires less memory and provides for simpler communication. Data Compression is one method that could be used for text steganography. It is used to encode information from one representation to another representation. The obtained new representation of data is smaller in size. One of the schemes to achieve data compression is Huffman coding. Huffman coding assigns smaller length codeword to more frequently occurring source symbols and longer length codeword to less frequently occurring source symbols.

C. Unicode Steganography:

Unicode Steganography look alike characters of the usual ASCII set and really carrying extra bits of information. If, there is no visual difference from ordinary text then the text is displayed correctly. If, there is visual difference from ordinary text then it may display the fonts differently and the extra information is easily spotted.

D. Image Steganography:

The most widely used technique today is hiding of secret messages into a digital image. This technique exploits the weakness of the human visual system (HVS). HVS cannot detect the variation in luminance of color vectors at higher frequency side of the visual spectrum.

E. Audio Steganography:

In audio steganography, secret message is embedded into audio signal which result slight altering in the corresponding audio file. The various methods for audio steganography are: LSB Coding, Spread Spectrum, Phase Coding and Echo Hiding.

F. Bitmap Steganography :

Bitmap type is the simplest type of picture. Structure of these files is that a bitmap image created from pixels that any pixel created from three colors (red, green and blue said RGB) each color of a pixel is one byte information that shows the density of that color. Merging these three color makes color in the pictures. Bitmap Steganography allows for the insertion of binary data into a standard 24-bit uncompressed bitmap image on a bit level such that it is not apparent nor detectable that within the image is another additional information.

III. PROPOSED METHOD

In this paper RSA Algorithm, edge detection schemes and LSB method is used for hiding messages. The video based steganography has been found to overcome capacity problem, because the video consist of number of frames which are placed in sequence one after the others. So that use any frame within the video can be used to hide the secure message with it. The another advantage of this method is that the secret message size can be increase because of many no of frames.

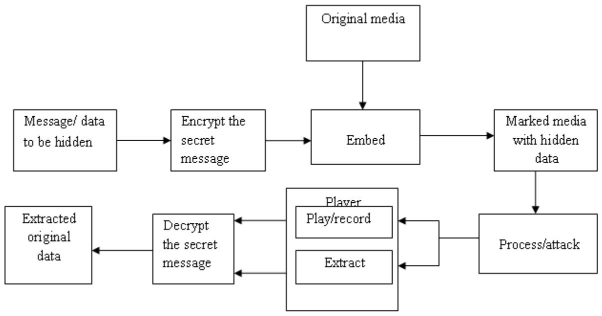

Original media
Message/ data to be hidden
Encrypt the secret message
Embed
Marked media with hidden data
Process/attack
Player
Play/record
Extract
Decrypt the secret message
Extracted original data

Figure 1: Block Diagram for Data Hiding

This proposed method contains following necessary materials and methods for hiding the secret message. They are:

1) Message:

The message is the essential requirement in the proposed system. The message is most important part in the communication while transmitting the secret information over the e-mail or internet communication. But in steganography, it is authenticated or the confidential information which is sends from sender to receiver. This secret message includes text or image.

2) Original Media:

The original media is the media which is used for hiding information. In this original media is a video. After choosing the video, it has to be splitted and choose a frame which will be use as the cover page for embedding the secret information.

3) Encrypted message:

In order to provide more security, the secret data is been encrypted by using RSA algorithm.

4) Embedding:

After choosing the frame and message, the next step is embedding. For the embedding, first edges are identified by using the edge detection mechanism, and by using the LSB method the data are embedded. While embedding the data, edges which are identified by edge detection method is not used for embedding only the remaining pixel are used for embedding the data.

5) Marking the hidden data:

While embedding the data, the hidden data are marked, so that it will be used for the receiver to decode the message. After marking the hidden, it is send to the receiver.

5) Process/Attack:

After the sending the message, either the attacker or authenticated receiver obtains the video.

7) Player:

The receiver after obtaining the video, plays the obtain video to obtain the secret information. The receiver plays the video and decodes the encrypted hidden message.

8) Decrypts the hidden message:

The encrypted message is been decrypted by using the RSA algorithm.

9) Extracted Message:

The message which is obtained after decrypting process is called extracted message.

Initially a video is chosen and divide into frames. For each frame, the parameters may be different for different image content and secret message M. In this steganographic technique RSA, LSB and an edge detection scheme are used for embedding and extracting hidden data in the cover image. In data embedding, first frame is chosen and extracts the edge information from the cover image based on edge detection scheme such as Prewitt and Canny edge detector. The next step is to choose a secret message and encrypting the secret message by using RSA algorithm and then embed the encrypted message bitstream in the cover page. Based on the edge information, it then does some preprocessing and identifies the pixel and hide the data by using "Least Significant Bit Insertion "method. This method modifies the low order bit of each pixel to match the message to hide. Finally, it obtains the stego image for secret message is obtained. Then the performance ratio for Prewitt and Canny edge detection are calculated and compared by using PSNR values.

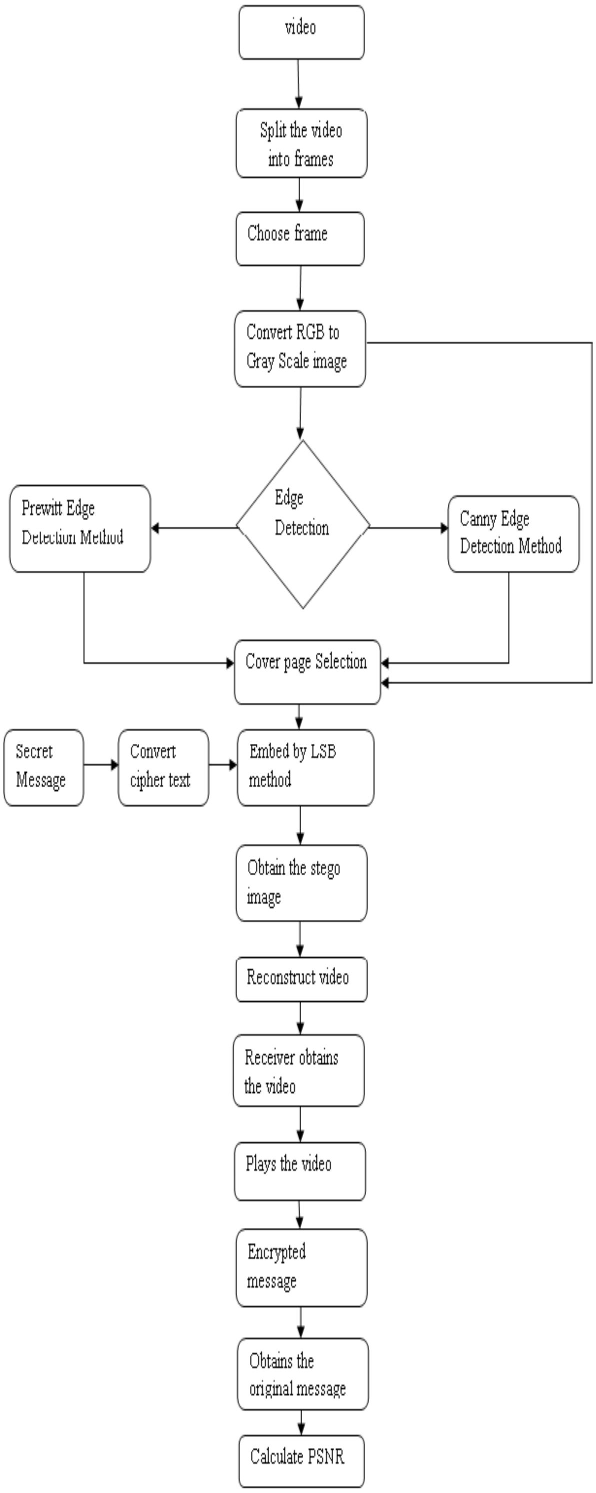


Figure 2: Proposed Data Hiding System

Algorithm:

```
    Input: encrypted message bitstream ,
    Output: Data embedded in the frame
        for each frame do
         initialize ;
        perform edge detection mechanism
        repeat
        set ;
        Obtain the candidate motion vectors:;
        while & do
        replace the least significant bit ;
        end
        end
```

The proposed method includes the following steps. They are:

A. Choose the secret message:

First, a secret message is selected for sending to the receiver. The secret message is the authenticated or the confidential information which is to be send from sender to receiver. Its size may vary depending upon the sender. For example, let the sender choose the secret message as,

Secret message: WE_LOVE_MATH

B. Encrypting the Secret data:

After choosing the secret message, it has to be encrypted for providing more security to the secret message. It is done by using the RSA algorithm.

RSA is an algorithm for public key cryptography. RSA, is known as Ron Rivest, Adi Shamir, and Leonard Adleman. It is a public key algorithm which the one of most popular encryption method because it s a asymmetric algorithms which uses two different key i.e., public key and private key.RSA is a de facto standard and can be used for key exchange and encryption. For encrypting the secret message, first user of RSA creates and publishes the product of two prime number, but the two prime numbers must be kept secret. The public key can be used by anyone to encrypt a message This RSA Algorithm includes three steps. They are: key generation, Encryption and Decryption.

To begin, each letter of the alphabet is associated with a unique number. This will allow to convert secret message into a series of numbers which then perform operations on. The table1 is used for associating each letter with the unique number is given below:

Table I: Each letter with the unique number

Letter	Number	Letter	Number
A	00	N	13
B	01	O	14
C	02	P	15
D	03	Q	16
E	04	R	17
F	05	S	18
G	06	T	19
H	07	U	20
I	08	V	21
J	09	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25
		"__"	26

Instead of letting A=0, it set to 00. This is because once the letter K is reached, it starts using two digits. While mixing of single digits and double digits it would be impossible to convert back to our original message. Also, it is useful to denote spaces in between words with a number.

1. Key Generation:

RSA is a public key cryptography which includes both public key and private key. The public key is used for encrypting message and it will be known to everybody and it can be decrypted by using the private key in a reasonable amount of time. The key generation includes the following steps:

- Choose two distinct prime numbers p and q.
- Compute
  $$n = pq. \qquad (1)$$
- Compute
  $$\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1), \qquad (2)$$
  where φ is Euler's totient function.
- Choose an integer e such that
  $$1 < e < \varphi(n) \text{ and } \gcd(e, \varphi(n)) = 1; \qquad (3)$$
  Where and φ(n) are coprime.
- Determine d as
  $$d^{-1} \equiv e \pmod{\varphi(n)}, \qquad (4)$$
  where d is the multiplicative inverse of e (modulo φ(n)).

Here, it is explained with an example:

Let receiver choose p=31, and q=37 as prime numbers, which gives m=(31)(37)=1147.So that $\phi(n)$=ϕ(1147)=(31−1)(37−1)=1080. Then find an integer e which is relatively prime to 1080. Receiver randomly selects e=17, and (17,1080)=1. So receiver publishes her public key of (17,1147).

If sender wants to send receiver an encrypted message using RSA. Then the sender has to know receiver's public key (17,1147), so sender uses this in the encryption algorithm.

Sender's secret message to states,

WE_LOVE_MATH

After converting to numerical using the table above sender has,

220426111421042612001907

Sender breaks the numerical form of the message into blocks of 3 making sure each block is less than m. The plain text in block are represented as below:

220 426 111 421 042 612 001 907

So,

220=$P1$
426=$P2$
111=$P3$
421=$P4$
042=$P5$
612=$P5$
001=$P7$
907=$P8$

2. Encryption:

Receiver transmits her public key (n, e) to sender and keeps the private key secret. Sender then wishes to send message M to receiver. To encrypt message m with public key (e, n), the following formula is carried out:

$$c = m_i^e \bmod n \qquad (5)$$

Sender then computes for each i from i=1 to i=8, with e=17, and n=1147 taken from Receiver's public key. And the result is the cipher text

$(220)^{17} \bmod 1147 \equiv 611$
$(426)^{17} \bmod 1147 \equiv 1145$
$(111)^{17} \bmod 1147 \equiv 851$
$(421)^{17} \bmod 1147 \equiv 510$
$(042)^{17} \bmod 1147 \equiv 96$
$(612)^{17} \bmod 1147 \equiv 246$
$(001)^{17} \bmod 1147 \equiv 1$
$(907)^{17} \bmod 1147 \equiv 405$

So the sender ciphertext becomes,

611 1145 851 510 96 246 1 405

This cipher text will be convert into binary form and this binary data is used for embedding.

3. **Decryption:**

To decrypt the message with your private key (d), so the following formula is carried out:

$$m = c^d \bmod n \qquad (6)$$

By above method the message is been decrypted. Sender was sending a message to receiver using her public key. Now receiver decrypt a message sent to her, receiver must use her private key.

- Receiver knows m=1147=(31)(37), so ϕ(1147)=1080
- Receiver uses e=17
- The next step is solving d, by multiplicative inverse of e mod 1080

Then receiver wants to solve for d in the linear congruence 17d≡1mod1080. By using the above value, the message will be decrypted.

C. *Choose the video:*

Choose any video and divide the video into frames in order to embed the secret information.

D. *Identifying the edges:*

After dividing the video into frame, a single frame is chosen to identify the edges by using the edge detection mechanism .Before identifying edge, the chosen frame is converted into Gray Scale image. Edge detection [5] - [8] is a very important area in computer vision field. Edges are identified as the boundaries between regions in an image, which are helpful in the segmentation and object recognition. Edge detection aims at identifying points in a digital image at which the image brightness changes sharply. Following edge detectors are handy:

1)Prewitt Edge Detector -3×3 gradient edge detector.

2)Canny Edge Detector – non maximal suppression of local gradient magnitude.

1. Prewitt Edge Detector:

After converting the frame into Gray Scale image, the edges are identified by using the Prewitt Edge detection mechanism.The Prewitt Edge Detector [6] is used in image processing in edge detection algorithm. It is known as the discrete differentiation operator which computes the gradient of the image. It is computed as:

- Consider the arrangement of pixels about the pixel (i, j) as in (7) :

$$\begin{bmatrix} a0 & a1 & a2 \\ a7 & [i,j] & a3 \\ a6 & a5 & a4 \end{bmatrix} \qquad (7)$$

- The partial derivatives can be computed by using (8) and (9):

$$Mx = (a2 + ca3 + a4) - (a0 + ca7 + a6) \qquad (8)$$

$$My = (a6 + ca5 + a4) - (a0 + ca1 + a2) \qquad (9)$$

- The constant *c* implies the pixels value closer to the center of the mask.
- Setting *c* = 1, we get the Prewitt operator as in (10) and (11):

$$Mx = \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix} \qquad (10)$$

$$My = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \qquad (11)$$

Mx and *My* are approximations at (*i*, *j*).

By using the above prewitt edge detection mechanism, the edges are identified from the gray scale image. This edge identified image is used as cover for embedding the secret data.

2. Canny Edge Detectors:

Here also the frame is converting into Gray Scale image for identifying the edge by using the Canny edge detection mechanism. The Canny edge detector [7] is widely considered to be the standard edge detection algorithm in the industry [10]. The Canny edge detection algorithm is known to many as the optimal edge detector.

The basic steps in the Canny edge detector are as follows:

Step 1:

Based on a Gaussian, image is filtered and the resultant image is a slightly blurred version of the original which is not affected by a single noisy pixel to any significant degree.Here is an example of a 5x5(Gaussian filter), which is used to create the image to the right, with Ơ= 1.4. (The asterisk denotes a convolution operation.)

$$B = \frac{1}{159}\begin{bmatrix} 2 & 4 & 5 & 4 & 2 \\ 4 & 9 & 12 & 9 & 4 \\ 5 & 12 & 15 & 12 & 5 \\ 4 & 9 & 12 & 9 & 4 \\ 2 & 4 & 5 & 4 & 2 \end{bmatrix} \times A \qquad (12)$$

Step 2:

After smoothing and eliminating the noise in the image, the next step is to find the strength of the edge by taking the gradient of the image. It uses a pair of 3x3 convolution masks for estimating the gradient. Among the pair, one estimates the gradient along the x-direction (columns) and the other estimates the gradient the gradient along the y-direction (rows). They are shown below:

-1	0	+1
-2	0	+2
-1	0	+1

Gx

+1	+2	+1
0	0	0
-1	-2	-1

Gy

The magnitude of the gradient and direction are given by using the formula (13) and (14):

$$G = \sqrt{Gx^2 + Gy^2} \qquad (13)$$

$$|G| = |Gx| + |Gy| \qquad (14)$$

Step 3:

Finding the edge direction is trivial once the gradient in the x and y directions are known and generate an error whenever sumX is equal to zero. The formula for finding the edge direction is given as (15):

$$\theta = invtan\left(\frac{Gy}{Gx}\right) \qquad (15)$$

Step 4:

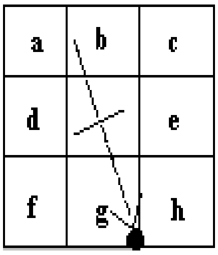
After the edge direction is determined, the next step is to relate the edge direction to a direction that can be traced in an image. If the pixels of a 5x5 image s taken then they are aligned as follows:

x	x	x	x	x
x	x	x	x	x
x	x	a	x	x
x	x	x	x	x
x	x	x	x	x

Then, it can be seen by looking at pixel "a", there are only four possible directions when describing the surrounding pixels.

Step 5:

The magnitude and direction of each and every pixel has to be determined and checked. If the gradient of the particular point is at maximum, then the edges will occur. If the gradient of the point is not at maximum, then it should be suppressed.



From central gradient value interpolate gradient value at ● from gradient values at e, g and h. Repeat in opposite direction. Suppress if non-maximum

Step 6:

Hysteresis is used to track along pixels that have not been suppressed. Hysteresis uses two thresholds and if the magnitude is below the first threshold, it is set to zero (made a non-edge). If the magnitude is above the high threshold, it is made an edge.

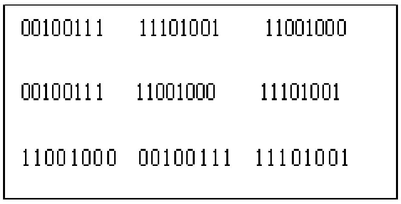
Thus the edges are identified by using the edge detection mechanism. The obtained output is used to perform the next step i.e., data embedding process.

E. Embedding and extracting the secret message:

The secret message is embedded using the LSB method. The concept of LSB Embedding is simple. Based on the edge information, it then does some preprocessing and identifies the pixel and hide the data by using "Least Significant Bit Insertion "method. This method modifies the low order bit of each pixel to match the message to hide. Finally, it obtains the stego image for secret message according to the corresponding extraction algorithm.. The Is (i,j) can be described as follows :

$$\begin{cases} I\ (\mathrm{i,j}) - 1 & \mathrm{LSB}\ (\mathrm{I(i,j)}) = 1 \text{ and } \mathrm{m} = 0 \\ \mathrm{I(i,j)} & \mathrm{LSB}\ (\mathrm{I(i,j)}) = \mathrm{m} \\ \mathrm{I}\ (\mathrm{i,j}) + 1 & \mathrm{LSB}\ (\mathrm{I(i,j)}) \neq 0 \text{ and } \mathrm{m} = 1 \end{cases}$$

For this method, the LSB of each pixel of an image is replaced with the binary version. Then the encrypted message bit stream is embedded in the cover page and it is represented below:

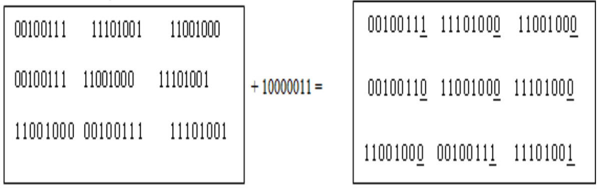


00100111 11101001 11001000

00100111 11001000 11101001

11001000 00100111 11101001

. Basically, the modification only happens in three of the underlined bits out of the eight bytes used. Then the embedding process is represented below:



00100111 11101001 11001000

00100111 11001000 11101001

11001000 00100111 11101001

+ 10000011 =

0010011$\underline{1}$ 1110100$\underline{0}$ 1100100$\underline{0}$

0010011$\underline{0}$ 1100100$\underline{0}$ 1110100$\underline{0}$

1100100$\underline{0}$ 0010011$\underline{1}$ 1110100$\underline{1}$

Extracting is defined as the mapping pixels to image. In the image steganography the extracting process can be done on message which is the stego image. The recipient inputs the stego image, and when applicable, the steganographic key, into an extraction algorithm, which outputs the secret message.

F. *Calculate the PSNR Value:*

The PSNR is used to measure the performance of the reconstructed video. The PSNR is most commonly used as a measure of quality of reconstruction of image [1],[3]. It is an engineering term for the ratio between the maximum possible power of a signal and the power of the corrupted noise that affects the fidelity of its representation . because many signal have a wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale[4]. Given a noise-free m×n monochrome image I and its noisy approximation K, MSE is defined as (16) :

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (16)$$

The PSNR is defined as (17) :

$$PSNR = 10log_{10}\left(\frac{MAX_I^2}{MSE}\right) \qquad (17)$$

Here, MAX_I is the maximum possible pixel value of the image.

Based on the PSNR value the performance is measured for the reconstructed video. The PSNR value is calculated for the embedding the data after identifying the edge by using the Prewitt and Canny Edge Detection Mechanism and data embedding without using the edge detection mechanism. The performance of Canny Edge Detection is high when compared to other methods. So that the edge are maintained without any demage.

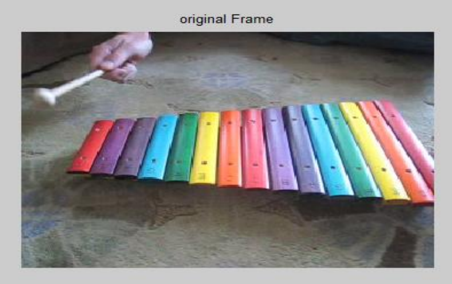
IV. Experimental Results

The edge based steganography is to embed encrypted secret data in the position of pixels, which meets the requirements of both in perception and robustness. The general setting of the chosen video is tabularized in the Table II:

Table II:General and Video Settings

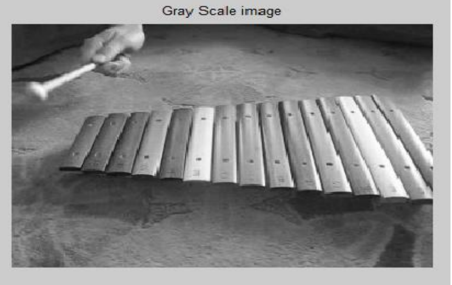
Attribute	Value
Duration	4.7020
Name	xylophone.mpg
Tag	My reader object
Type	Mmreader
UserData	[]
BitsPerPixel	24
Frame Rate	29.9700
Height	240
NumberOfFrames	141
VideoFormat	RGB24
Width	320

The chosen video name is "xylophone.mpg" and there are 141 frames. Since there are 141 frames, more amount of information can be embedded. For a example, a single frame from the video is chosen to performed all the steps that are stated above in the proposed system. After choosing the video, it has to be splitted into frames and has to choose the frame for embedding data. The figure 3 describes about the frame taken out from the video. To find the edges, the frame has to be converted into Gray Scale image as in the figure (4).



original Frame

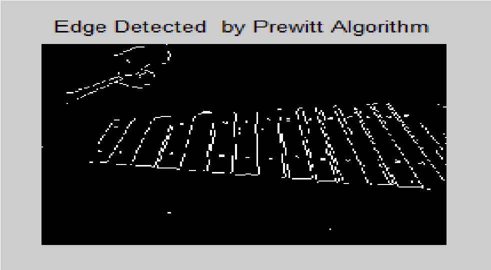
Figure 3: Frame Taken from the Original Video



Gray Scale image

Figure 4: Gray Scale Image of the Original Frame

After converting into Gray scale image, by using Edge Detection Mechanism edges are identified. The figure (5) describes about the edge detected by using Prewitt method and figure (6) describes about the edge detected by using the Canny method.



Edge Detected by Prewitt Algorithm

Figure 5: Edge detected by Prewitt

.

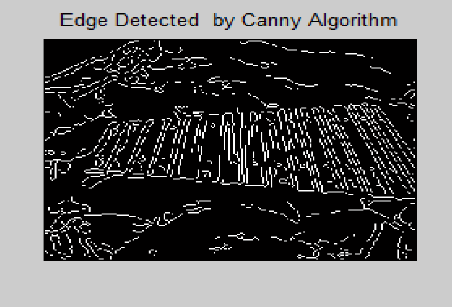


Figure 6: Edge detected by Canny

After identifying the edges in the chosen frame, the next is embedding the secret information, Here three different cover page is used for embedding the secret information. The three different cover pages are figure (4), (5) and (6).

Meanwhile, the secret information has to be selected. Here "WE_LOVE_MATH" secret message is chosen, after that the message has to be encrypted by using the RSA algorithm. Then by using the table I, the corresponding values are substituted. Then the plain text value is converted into cipher text. Then obtained cipher value is converted into binary form and by using the LSB method each bit of information is embedded into the LSB bit of the pixel.

For embedding the secret information, first gray scale image (figure (4)) is used for embed the secret information by using the LSB and the corresponding stego image is obtained as shown in the figure (7).Similarly, by using the figure (5) and (6) as the cover page for embedding the secret binary information, a stego image is obtained for the corresponding figure (5) and (7) as shown in the figure (8) and (9).

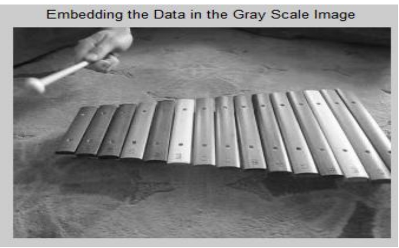


Figure 7: Data embedded in the Gray Scale Image.

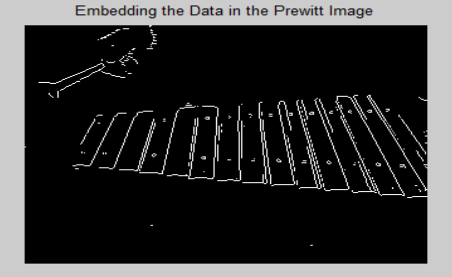


Figure 8: Data embedded in the Prewitt Image.

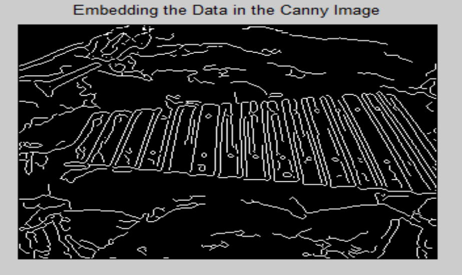


Figure 9: Data embedded in the Canny Image.

The obtained stego information is s gray scale image, but the chosen video is in the RGB color format and when the attacker obtains the video, they could obtain the secret image easily. So in order overcome the above drawback, the obtained stego image is also embedded in the another RGB frame by using the LSB method and it is shown in the figure (10). Now the entire frame is in the RGB format. Then the video is reconstructed and send to the receiver. The receiver obtains the video and the decrypts the encrypted message and obtains the secret message. Suppose, if the attacker obtains video and identify the frame, the attacker could not obtain the secret image because the secret message will in the cipher text and it is difficult decrypt. So the secrecy and privacy is maintained in the proposed method.

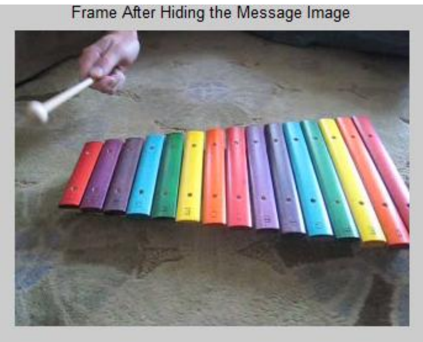


Figure 10: Frame after Hiding the Message Image.

Then the performance is measured for the video is measured by using PSNR method. It is used to measure the video for the embedding the data after identifying edge using the prewitt edge detection mechanism, canny edge detection mechanism and the data embedded without edge detection mechanism and its corresponding values are tabularized in the Table III:

Table III: PSNR

Embedding Technique	PSNR
Embedding after detecting Edges using Prewitt	27.3045db
Embedding after detecting Edges using Canny	22.6238db
Embedding data without edge detection mechanism	18.8486db

This graph describes about the PSNR value of the reconstructed video. The 1 represent the PSNR value of reconstructed video by using Canny Edge Detection Mechanism and its value is 27.3045db whereas 2 represent the PSNR value of the reconstructed video by using prewitt edge detection mechanism whose value is 22.6238db and 3 represent the PSNR value of the reconstruct video without any edge detection mechanism whose value is 18.8486db. From the above figure, we conclude that 1 shows more performance than other two methods.

Table 3 shows the PSNR values by comparing the original image and the embedded image. The comparison is done with prewitt, canny edge detectors and without edge detection mechanism. Video embedding using canny edge detector is found to be the best algorithm to embed. The PSNR for canny is found to be 27.3045db which outperforms the prewitt edge detector. The graphical representation is given figure (11).

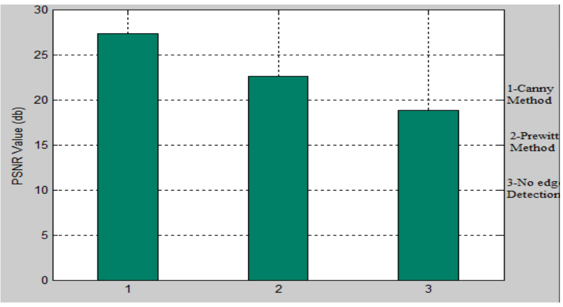


Figure 11: PSNR value for reconstructed video

V CONCLUSION

In this paper video steganography is performed by using RSA algorithm, edge detection algorithm and LSB algorithm. Edge detection is the initial step in object recognition. This edge detection technique is used to identify the edge in the cover image by using prewitt and canny edge detection techniques. Then the secret message is been encrypted by using RSA algorithm and embedded the secret message using the LSB algorithm and then performance is calculated by using PSNR. However RSA algorithm is the best encrypted mechanism because if the attacker obtains the video and decodes the video, the attacker can only obtain the cipher text not the original secret message. So the RSA algorithm provides more secrecy and privacy. The PSNR value used to represent reconstruct video performance ratio for prewitt and canny edge detection method. The canny edge detection algorithm performs better than prewitt edge detection algorithm and without edge detection mechanism. Because, Canny algorithm is adaptable to various environments. Its parameters allow it to be tailored to recognition of edges of differing characteristics depending on the particular requirements of a given implementation.

V. REFERENCES

[1] Hussein A. Aly, Member, IEEE," Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error", *IEEE Transactions On Information Forensics And Security*, Vol. 6, No. 1, March 2011.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

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

[4] S. K. Kapotas, E. E. Varsaki, and A. N. Skodras, "Data hiding in H.264 encoded video sequences," in *IEEE 9th Workshop on Multimedia Signal Processing (MMSP07)*, Oct. 2007, pp. 373–376.

[5] N. Senthilkumaran, R. Rajesh, "Edge Detection Techniques for Image Segmentation – A Survey of Soft Computing Approaches" International Journal of Recent Trends in Engineering, , No. 2, May 2009 Pg 250 to 254.

[6] Tanvir Ahmed Abbasi, Mohammad Usaid Abbasi "A Novel Architecture for Prewitt Edge Detector" 2009 Old City Publishing, Inc. Pages 203 to 211.

[7] Mohamed Roushdy. "Comparative Study of Edge Detection Algorithms Applying on the Grayscale Noisy Image Using Morphological Filter" *GVIP Journal*, Volume 6.December, 2006 Pages 17 to 23

[8]Jae-Gil Yu1, Eun-Joon Yoon2, Sang-Ho Shin1 and Kee-Young Yoo, Dept. of Computer Engineering, Kyungpook National University Daegu, Korea," A New Image Steganography Based on 2k Correction and Edge-Detection", Fifth International Conference on Information Technology: New Generations 978-0-7695-3099-4/08 © April 2008 IEEE.

[9] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography incolor, and gray-scale images," *IEEE Multimedia*, vol. 8, no. 4, pp.22–28, Oct. 2001.

[10]Ehsan Nadernejad," Edge Detection Techniques: Evaluations and Comparisons", *Applied Mathematical Sciences*, Vol. 2, 2008, no. 31, 1507 - 1520.

AUTHOR BIOGRAPHY

P.SUNITHA KENCY PAUL was born on 11th February 1990 is a native of Kumaracoil, Thuckalay, Kanyakumari District. She graduated in B.Tech Information Technology from Jayamatha Engineering College, Aralvoimozhi under Anna University in 2011. Currently she is pursuing M.E Computer Science and Engineering in Noorul Islam Centre of Higher Education, Thuckalay. Her research interests include Wireless Communication, Data mining, Image processing, Steganography.

P.FASCA GILGY MARY was born on 13th February 1987 is a native of Nagercoil, Kanyakumari District. She graduated in B.E Computer Science and engineering from Jayaraj Annapackiam CSI College of Engineering, Nazareth under Anna University in 2008. Currently she is pursuing M.E Computer Science and Engineering in Noorul Islam Centre of Higher Education, Thuckalay. Her research interests include Wireless Communication, Data mining, Image processing.

J.DHEEBA, received the B.E degree in Computer Science and Engineering from Anna University, Chennai in the year 2005 and M.E degree in Computer Science and Engineering from Anna University, Chennai in the year 2007. She is now an Assistant Professor at Noorul Islam University, India and currently working towards the Ph.D degree as a part time scholar in the department of Information and Communication Engineering, Anna University, India. Her research interest includes Medical Image Processing, Soft Computing and Artificial Intelligence.