National Conference on Recent Advances in Computer Science and IT (NCRACIT)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 1 | ISSN : 2456-3307

A Novel Approach for Video Steganography using LSB Technique

Khalil Ahmad[1], Taseem Nazir[2], Junaid Farooq War[3]

[12]Department of CSE, BGSB University, Rajouri, J&K, India
[3]Department of ECE, BGSB University, Rajouri, J&K, India
khalil447@gmail.com[1],taseem.mufti@gmail.com[2],warjunaid@gmail.com[3]

ABSTRACT

There are many kinds of steganography techniques available among which hiding data in video using logical operation by LSB substitution is a simple method. Here the information will be embedded using the stego key. Here 8 or 16-bit key is used. The input image or text file is encoded with the help of the secret key by performing logical operation using LSB substitution. By using this technique, capacity of embedding bits into the cover image can be increased and possibility of attacks can be decreased.

Keywords: Steganography, LSB, Secret Key, Data hiding

I. INTRODUCTION

Information Hiding techniques have been receiving much attention today. The main motivation for this over encryption and decryption is that here the information is imperceptibly hidden and therefore does not attract attention. This art of hiding information is called Steganography. Steganography or Stego as it is often referred to in the IT community, literally means, "Covered writing" which is derived from the Greek language. Markus Kahn defines Steganography as follows, “Steganography is the art and science of communicating in a way which hides the existence of the communication. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present”. Since redundancy is present in image and audio files they are mostly used for information hiding. Although image and audio files comply with this requirement, research has also uncovered other file formats that can be used for information hiding [1].

II. DOMAIN OF INFORMATION HIDING

The existing schemes of information hiding in images and audio can roughly be classified into the following three categories [6]

- Spatial domain / Time domain
- Transform domain
- Compressed domain

A. Spatial Domain Information Hiding

Data hiding in spatial domain type directly adjust image pixels in the spatial domain for data embedding. This technique is simple to implement, offering a relatively high hiding capacity. The quality of the Stego image can be easily controlled. Therefore, data hiding of this type has become a well-known method for image steganography [10]

B. Least Significant Bit Techniques

The terminology LSB replacement/ LSB matching was discussed by T.Sharp. LSB substitution algorithm is the simplest scheme to hide message in a host image. It replaces the LSB of each pixel with the encrypted message bit stream. Authenticated receivers can extract the message by deciphering the LSB of every pixel of the host image with a pre-shared key. Since only the LSB of pixels is altered, it is visually imperceptible by human eye. The capacity of the algorithm is 1 bit per pixel (bpp). Although this algorithm is visually imperceptible, it can be statistically analyzed by other entity without processing the pre-shared key [8].

III. INCREASING CAPACITY TECHNIQUES

A new and efficient steganography method for embedding secret messages into a gray-valued cover image was proposed by Wu et al. In the process of embedding a secret message, a cover image is partitioned into non-overlapping blocks of two consecutive pixels. A difference value is calculated from the values of the two pixels in each block. All possible difference values are classified into a number of ranges. The selection of the range intervals is based on the characteristics of human vision's sensitivity to gray value variations from smoothness to contrast. The difference value then is replaced by a new value to embed the value of a sub-stream of the secret message. The number of bits, which can be embedded in a pixel pair, is decided by the width of the range that the difference value belongs to. The method is designed in such a way that the modification is never out of the range interval [6]. This method provides an easy way to produce a imperceptible result than those yielded by simple LSB replacement methods. The embedded secret message can be extracted from the resulting steno-image without referencing the original cover image [8].

A. Steganalysis

The art of detecting Steganography is referred to as Steganalysis. Steganalysis is the process of identifying steganography by inspecting various parameter of a stego media[4]. The primary step of this process is to identify a suspected stego media. After that steganalysis process determines whether that media contains hidden message or not and then try to recover the message from it. In cryptanalysis, it is clear that the intercepted message is encrypted and it certainly contains the hidden message because the message is scrambled. But in the case of steganalysis this may not be true. The suspected media may or may not be with hidden message. The steganalysis process starts with set of suspected information streams[9]. Then the set is reduced with the help of advance statistical methods. In the case of Visual detection steganalysis technique, a set of stego images are compared with original cover images and note the visible difference.

IV. VIDEO STEGANOGRAPHY TECHNIQUE

Video Steganography Techniques can be classified into various techniques. One way to categorize video Steganography techniques is on the basis of embedding method i.e. Spatial or Substitution based techniques and transform based techniques. Videos can also be classified on the basis of Compression i.e. Compressed and Uncompressed Video techniques. Another approach to classify video steganography techniques is based on classification i.e. Format based and Video Codec Methods.

A. Least Significant Bit (LSB) Technique

The least significant bit (in bit other words, the 8th) of some or all of the bytes inside an image is changed to a bit of the secret message [12]. Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images, we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image much so the

resultant stego image looks almost same as the cover video. In 8-bit images, one bit of information can be hidden.

Encryption Algorithm

Input: cover video, secret message, an 8 - bit stego - key.

Output: Stego - Video.

Steps:

1. Choose cover video and secret message.
2. Convert cover video into frames.
3. Enter an 8 - bit stego key.
4. Based on this key we get the frames in which we have to embed the secret message.
5. Get red component of pixel of video frame.
6. The MSB of red component decide whether the secret message is to be hidden in green Component or blue component of the pixel using XOR operation with key. If the value is 0, secret data is hidden in LSB of blue component otherwise secret data is hidden in LSB of green component.
7. Continue from step 6 to step 7 for each frame of cover video until the entire message is hidden.
8. End.

Decryption Algorithm

Input: Stego Video, an 8 - bit Stego - key.

Output: Secret Message.

Steps:

1. Upload the stego video.
2. Convert it into frames.
3. Enter an 8 - bit stego key.
4. Based on the key we get the stego frames in which extraction of secret message is to be performed.
5. The new value from step 4 represents the number of secret message bits to be extracted from the pixel. The MSB bit of red component decides whether the secret message is to be extracted from the green component LSB or from the blue component LSB of the pixel by performing XOR operation between red component and the key.
6. Extract the message from the pixel. Continue step 5 for each frame in stego video until the entire message is extracted.
7. End.

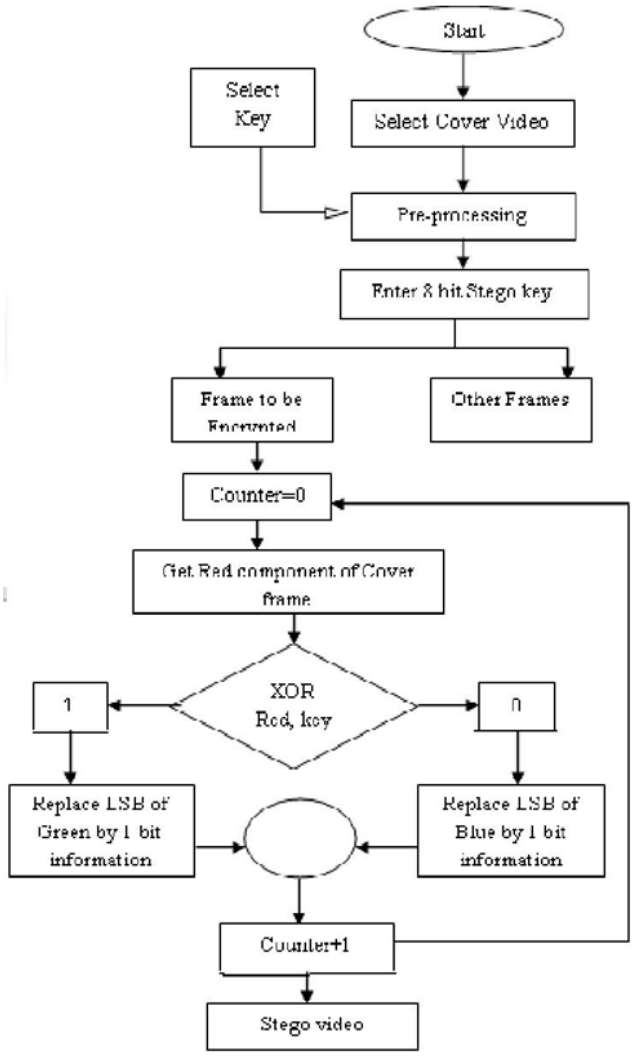

Figure 1. Flowchart for Encryption

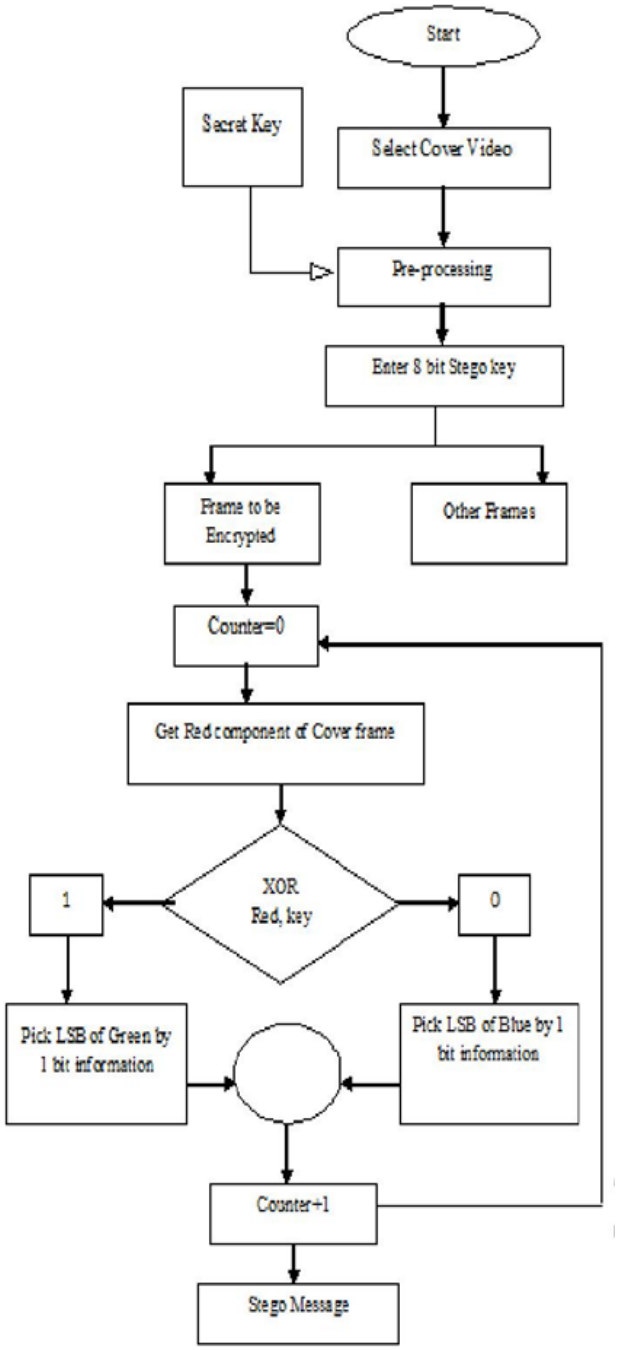

Figure 2. Flowchart for Decryption

IV. RESULTS

Secret Message/Capacity	PSNR	BER
Manual text	103.404	0.571
Color Image	62.6534	0.571
Grayscale	62.1088	0.571
Binary Image	71.6393	0.571
Text File	87.0048	0.571

V. CONCLUSION

In this paper, the algorithm to embed the information in video is implemented using stego key method. Here 8 or 16 bit key is used. The input image or text file is encoded with the help of the secret key by performing logical operation using LSB substitution. By using this technique capacity of embedding bits into the cover image can be increased and possibility of attacks can be decreased. Experimental results reveal that the proposed method achieves a minimum PSNR of 62.1088 for Grey Scale frames with a maximum BER of 0.571.

VI.REFERENCES

[1] H. Qi, W. Snyder and W. Sander, "Blind Consistency Based Steganography for Information Hiding In DigitalIEEE International Conference on Multimedia and Expo, 2002. ICME'02. Proceedings 2002, Volume: 1 , pp: 585 – 588, August. 2002.

[2] A Survey on various types of Steganography and Analysis of Hiding Techniques Navneet Kaur, Sunny Behal. "International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014"

[3] G. Elmasry and Y. Shi, "2- D Interleaving for Enhancing the Robustness of Watermark Signals Embedded in Still Imag International Conference on Multimedia and Expo (II) pp. 731 – 734, 2000.

[4] Information hiding using audio steganography – a surveyThe. "International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011 "

[5] Hiding the Text Information using Steganography. "M.GraceVennice, Prof. T.V.Rao, M. Swapna, Prof. J.Sasikiran/ International Journal of Engineering Research and Applications (IJERA) "

[6] Data Hiding Using Video Steganography - A Survey. "Swetha V et al | IJCSET(www.ijcset.net) | June 2015 | Vol 5, Issue 6,206 - 213 "

[7] D. Kundur, D. Hatzinakos, "Digital Watermarking using Multi - resolution Wavelet Decomposition, "In IEEE ICASSP'98, volume 5, pages 2659 – 26 62, Seattle, May 1998.

[8] H. Liu, J. Liu, J. Huang, D. Huang and Y. Shi, "A robust DWT - based blind data hiding algorithm,"

IEEE International Symposium on Circuits and Systems, ISCAS 2002, Volume: 2, pp. II - 672 - II - 675, May 2002.

[9] C.C. Chang, T.C. Lu, "A difference expand oriented data hiding scheme for restoring the original host images", J. Systftw... 79 so (12) (2006) 1754 – 1766.

[10] H. B. Kekre, Archana A. Athawale, Pallavi N. Halarnkar, "Increased Capacity of In Hiding in s LSB method for text and Image, International Journal of Electrical, Computer and Systems Engineering , volume 2, No. 4 http://www.waset.org/ijecse/v2/ v2 - 4 - 34.pdf (Europe) .

[11] S.D. Lin and C.F. Chen, A Robust DCT - based Watermarking for Copyright Protection, IEEE Transactions on Consumer Electron, vol. 46, no. 3, pp. 415 - 421, 2000.

[12] Navneet Kaur, Sunny Behal "A Survey on various types of Steganography and Analysis of Hiding Techniques",International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 20 14.