ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

Data Carrying Methodology with Higher LSB Bit Replacement-A Review

Manisha D. Rakhonde[1], A. A. Chinchamalatpure[2]

PG Student, Department of Computer Science & Engineering, Dr. Sau. K.G.I.E.T., Darapur, Tq-Daryapur, Dist-Amravati, State-Maharashtra, India[1]

Assistant Professor, Department of Computer Science & Engineering, Dr. Sau. K.G.I.E.T., Darapur, Tq-Daryapur, Dist-Amravati, State-Maharashtra, India[2]

ABSTRACT: A new compressed video secure steganography (CVSS) algorithm is proposed. In the algorithm, embedding and detection operations are both executed entirely in the compressed domain, with no need for the ecompression process. The new criteria employing statistical visibility of contiguous frames is used to adjust the embedding strategy and capacity which increases the security of proposed algorithm. Therefore, the collusion resistant properties are obtained. Video steganalysis with closed loop feedback manner is design as a checker to find out obvious bugs. Experimental results showed this scheme can be applied on compressed video steganography with high security properties.

KEYWORDS: Higher LSB, Data Hiding, Extraction, Mean Square Error, PSNR, AVI Video

.

I. INTRODUCTION

Steganography is the transmission of a secret message hidden within an ordinary carrier without revealing its existence. The container (cover file) may be a digital still image, audio file, or video file. Once the secret message has been embedded, it may be transferred across insecure lines or posted in public places. Usually, the data rate of covert data transmission using steganography is low in order to keep the covert data imperceptible within the cover medium. This data rate is somewhat proportional to the volume of the cover medium. For this reason, digital video is a convenient choice for steganography. Nowadays, given the high degree of collaboration and cooperation in modern information systems such as emerging multimedia sensor networks, covert communications becomes a greater threat to forensic analysis than ever. It is imperative to investigate methods to detect and discourage covert communications such as steganography in multimedia networks that acquire highly correlated data.

This work will focus on the particular problem of the compressed video steganography. General speaking, digital video appears in two main distinct encoding formats: the uncompressed and the compressed. The most popular compressed format by far is motion compensated compressed video, specifically the widely accepted standard MPEGx. It achieves compression through the elimination of temporal, spatial and statistical redundancies and with this compression operation. The video bit-stream consists of variable length codes (VLC) that represent various video segments. For video stream usually being offered in compressed form, steganography algorithms that are not applicable in compressed bit-stream would require complete or at least partial decompression [1-4]. This is an unnecessary burden best avoided. If the requirement of strict compressed domain steganography is to be met, the steganography needs to be embedded in the compresseddomainNowadays, there are large amount of video watermarking algorithms been proposed. And some of them are applied for compressed video [5-9]. To be useful, a steganographic technique should not be easily detectable. If the existence of secret message can be detected with a probability higher than random guessing, the corresponding steganographic technique is considered to be invalid. Similar to cryptography steganography may suffer from the attack method (steganalysis). Much of the research work in the field of steganalysis

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

idempotent embedding another major stream is based on the concept of blind steganalysis, which is formed by blind classifiers. The classifier should be trained to learn the differences between cover and stego-image features at first.

II. LITERATURE REVIEW & RELATEDWORK

For studying the concepts of video steganography and watermarking technique we have surveyed many latest papers. Biswajita Datta, Debnath Bhattacharyya, Samir Kumar Bandyopadhay and Kil-hwan Shin, "High Capacity Signature Hiding Technique in Higher Depth of LSB Layer"[21], It gaves basic idea of stegnography. In this papar writers proposed method. They says that ,As target data we consider a very important biometric authentication data – signature. In our proposed technique we consider that the signature image is basically a binary image and we try to hide this binary image within a 24 bit Color image. In our proposed technique we try to adjust the bits of the original string after embedding the data in the 5th LSB layer to reduce difference .Technique for bit adjustment to minimize the change in pixel value due to replacement of 5th LSB layer.

In our method first we have replaced the 5th bit (from the LSB) of each of the R, G and B component of the cover image with the pixel value of the target image. See the 5 position from LSB ,change that 5th bit if there is 1 than make it 0 and vise versa and reduce difference by flipping i.e. make all previous bit (from LSBside)1 of LSB and vise versa ,So that after hiding data on image not so much changes occurd in it. In below papars videos were used to Hide data.

Arup Kumar Bhaumik, Minkyu Choi, Rosslin J. Robles, and Maricel O. Balitanas [2], the main requirements of any data hiding system are security, capacity and robustness. It is very difficult to archive all these factors together because these are inversely proportional to each other. Authors have focuses on maximizing security and capacity factor of data hiding. The data hiding method uses high resolution digital video as a cover signal. It provides the ability to hide a significant quality of information making it different from typical data hiding mechanisms. They have used the large payloads like video in video and picture in video as a cover image.

Ahmed Ch. Shakir [1], the confidential communications over public networks can be done using digital media like text, images, audio and video on the internet. Simply hiding the contents of a message using cryptography was not adequate. Hiding of message should provide an additional layer of security. To provide the more security the author suggested the new procedures in steganography for hiding ciphered Information inside a digital colour bitmap image. He has used quadratic method depending on the locations concluded by the binary image, beside of public key cryptography. He had concluded that the conjunction between cryptography and steganography produce immune information.

Andreas Westfeld and Gritta Wolf [3], in this work author have described a steganographic system which embeds secret messages into a video stream. Normally the compression methods are used in video conferences for securing acceptable quality. But usually, compression methods are lossy because reconstructed image may not be identical with the original. There are some drawback of compression and data embedding method. Signal noise and irrelevance are common examples of data embedding. But compression methods try to remove signal noise and irrelevance. If signal is compressed more, then there are fewer possibilities of data embedding. The author have solved this problem, they have investigated a typical signal path for data embedding. In this algorithm security is established by indeterminism within the signal path.

Sherly A P and Amritha P P [14], in this paper author have proposed a new compressed video Steganographic scheme. In this scheme the data is hided in compressed domain. The novel embedding technique Triway Pixel Value Differencing (TPVD) is used to increase the capacity of the hidden secret information and for to providing an imperceptible stego-image for human vision. This algorithm can be applied on compressed videos without degradation in visual quality.

Saurabh Singh and Gaurav Agarwal [13] have presented a novel approach of hiding image in a video. In this approach, one LSB of each pixel is replaced by the one bit of secrete message. So it is very difficult to find that image is hidden in the video of 30 frames per second. The analysis is very difficult because each row of image pixels is hidden in multiple frames of the video. The intruder requires full video to unhide image. Authors have described the LSB algorithm in this paper. The proposed algorithm is very useful in sending sensitive information securely.

S.Suma Christal Mary [12] have proposed new Real time Compressed video secure Steganography (CVSS) algorithm using video bit stream. In this, embedding and detection operations are both executed entirely in the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

compressed. The proposed algorithm increases the security because the statistical invisibility of contiguous frames is used to adjust the embedding uncompressed formats may possible as well, so it may support MPEG4 format [15]. Multiple frames embedding are possible. Now we are embedding single frame at a time, but in future multiple frames embedding is also possible.

Yusuf Perwej, Firoj Parwej, Asif Perwej [16] in their work describes An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection. Authors proposing edge detection from Gabor Filter method, using data hiding by the simple LSB substitution method. In the method a set of pixels that constitute a block jointly share the bits from the watermark .The values for the mean square error (MSE) and peak signal to noise ratio (PSNR) are measured. The results indicate the method introduces low noise and hence ensures lesser visible distortions.

Abdullah Bamatraf, Rosziati Ibrahim and Mohd.NajibMohd. Salleh[17] in their work authors describes A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit. Author proposed a new LSB based digital watermarking scheme with the combination of LSB and inverse bit. The experimental result shows that the proposed algorithm maintains the quality of the watermarked image. When combining different positions of LSB such as the second LSB and the third LSB and fourth LSB and the combination between them. The proposed algorithm is also tested using Peak signal-to noise ratio (PSNR).

III. ANALYSIS OF PROBLEM

The data hiding method uses high resolution digital video as a cover signal. It provides the ability to hide a significant quality of information making it different from typical data hiding mechanisms. They have used the large payloads like video in video and picture in video as a cover image

For data security purpose, there is exchange of bit up to position 5 causes insufficient to hide data so we need further work for data hiding and security of data.

A. Proposed Work and Objectives

a. Algorithm (Data Hiding)

1. Select Video (Compressed / Uncompressed)
2. Extract Frames and sound.
3. Choose Carrier Media (Either Frame or Sound)
4. Convert Carrier Media to binary Format (Sampling of Data)
5. Input Secrete Data
6. Convert Secrete Data to Binary format (Sampling of Data)
7. Replace secrete Data bit with 6th LSB Position bit of carrier media and do flipping or other relevant bits.
8. Recreate carrier media after data hiding.

b. Proposed Algorithm (Data Extraction)

1. Start
2. Input Video (Compressed / Uncompressed)
3. Extract Frames & Sound.
4. Choose Carrier Media (Either Frame or Sound)
5. Extract 6th Position LSB
6. Converts all collected bits into ASCII Format.
7. Stop

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

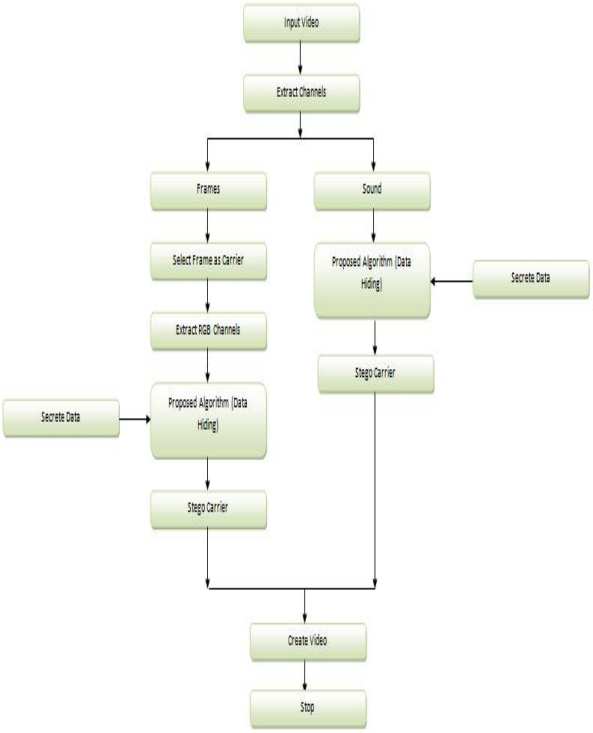

Fig. 1 DFD (Hiding)

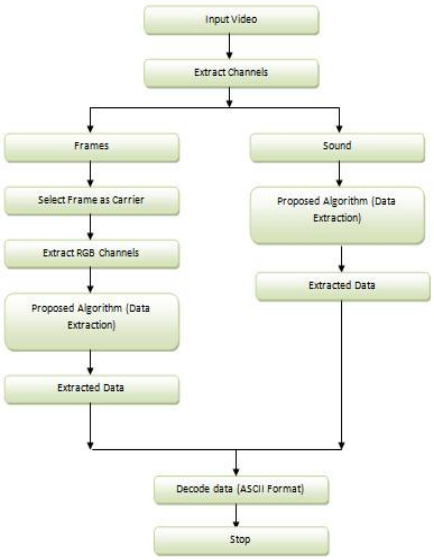

Fig. 2 DFD (Data Extraction)

B. Data Hiding in Frame & Audio Wave file

We developed a novel method that is able to shift the limit for transparent data hiding in audio from the fourth LSB layer to the sixth LSB layer, using a two-step approach. In the first step, a watermark bit is embedded into the 6th LSB layer of the host audio using a novel LSB coding method. In the second step, the impulse noise caused by watermark embedding is shaped in order to change its white noise properties. The standard LSB coding method simply replaces the original host audio bit in the 6th layer (i = 1..... 8) with the bit from the watermark bit stream. In the case when the original and watermark bit are different and 6th LSB layer is used for embedding the error caused by watermarking is 2^5 quantization steps (QS) (amplitude range is [-32768 to 32767]). The embedding error is positive if the original bit was 0 and watermark bit is 1 and vice versa. The key idea of the proposed LSB algorithm is watermark bit embedding that causes minimal embedding distortion of the host carrier. It is clear that, if only one of 8 bits in a sample is fixed and equal to the watermark bit, the other bits can be flipped in order to minimize the embedding error. For example, if the original sample value was 0...010002=810, and the watermark bit is zero is to be embedded into 6th LSB layer, instead of value 0...000002=010, that would the standard algorithm produce, the proposed algorithm produces sample that has value 0...001112=710, which is far more closer to the original one. However, the extraction algorithm remains the same; it simply retrieves the watermark bit by reading the bit value from the predefined LSB layer in the watermarked audio sample. In the embedding algorithm, the (i+1)th LSB layer (bit ai) is first modified by insertion of the present message bit. Then, the algorithm given below is run. In case that the bit ai need not be modified at all due to being already at a correct value, no action is taken with that signal sample. Underlined bits (ai) represent bits of watermarked audio.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

```
if host sample a>0
        if bit 0 is to be embedded
        if a_{i-1} =0 then a_{i-1} a_{i-2} .... a_0 = 11...1
        if a_{i-1} =1 then a_{i-1} a_{i-2} .... a_0 = 00...0 and
            if a_{i+1}=0 then a_{i+1} = 1
              else if a_{i+2}=0 then a_{i+2}=1
              .....
              else if a_15 =0 then a_15 = 1
        else if bit 1 is to be embedded

          if a_{i-1} =1 then a_{i-1} a_{i-2} .... a_0 = 00...0
          if a_{i-1} =0 then a_{i-1} a_{i-2} .... a_0 = 11...1 and
              if a_{i+1}=1 then a_{i+1} = 0
                else if a_{i+2}=1 then a_{i+2}=0
                .....
                else if a_15 =1 then a_15 = 0
          else if bit 1 is to be embedded

if host sample a<0
        if bit 0 is to be embedded
        if a_{i-1} =0 then  a_{i-1} a_{i-2} .... a_0 = 11...1
        if a_{i-1} =1 then  a_{i-1} a_{i-2} .... a_0 = 00...0 and
            if a_{i+1}=0 then a_{i+1} = 1
              else if a_{i+2}=0 then a_{i+2}=1
              .....
              else if a_15 =0 then a_15 = 1


            else if bit 1 is to be embedded
        if a_{i-1} =1 then a_{i-1} a_{i-2} .... a_0 = 00...0
        if a_{i-1} =0 then a_{i-1} a_{i-2} .... a_0 = 11...1 and
            if a_{i+1}=1 then a_{i+1} = 0
              else if a_{i+2}=1 then a_{i+2}=0
              .....
              else if a_15 =1 then a_15 = 0
        else if bit 1 is to be embedded
```

Fig. 3 Sixth bit LSB replacement algorithm

IV. CONCLUSION

Data security is a complex and mutable subject. In addition to algorithms, there are more things to think about. The study of data security reveals many conclusions, issues and thoughts. This project aims to explain and sort them; hopefully to be useful is future research.

REFERENCES

[1]. Ahmed Ch. Shakir," Steno Encrypted Message in Any Language for Network Communication Using Quadratic Method", Journal of Computer Science 6 (3): 320-322, 2010 ISSN 1549-3636 © 2010 Science Publications.

[2]. Arup Kumar Bhaumik, Minkyu Choi, Rosslin J. Robles, and Maricel O. Balitanas," Data Hiding in Video", International Journal of Database Theory and Application Vol. 2, No. 2, June 2009.

[3]. Andreas Westfeld and Gritta Wolf," Steganography in a Video Conferencing System", Information Hiding 1998, LNCS 1525, pp. 32-47, 1998. Springer-Verlag Berlin Heidelberg 1998.

[4]. Cheng Cheok Yan, "Introduction on Text Compression Using Lempel, Zip, Welch (LZW) method".

[5]. D. P. Gaikwad and Dr. S.J. Wagh, "Color Image Restoration for Effective Steganography", i-manager's Journal on Software Engineering, Vol.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

4 l No. 3 l January - March 2010 65, pp.65-71.

[6]. D.P. Gaikwad and Dr. S.J. Wagh, "Image Restoration Based LSB Steganography for Color Image", AISA- PACIFIC Regional Conference in ICTM-2010 on Innovations and Technology Management at Mumbai.

[7]. Richard E. Woods & Rafael C. Gonzalez "Digital Image Processing" Book.

[8]. F5 algorithm implementation: 2009, Fridrich, J.R.Du, M. Long: Steganalysis in Color Images, Binghamton, 2007. [9]. Neil F. Johnson and SushilJajodia, "Exploring Steganography: Seeing the Unseen", George Mason University. [10]. Steganography on new generation of mobile phones with image and video processing abilities, as appeared

Computational Cybernetics and Technical Informatics (ICCCCONTI), 2010 International Joint Conference on 27-29 May 2010 in Timisoara, Romania ISBN: 978-1-4244- 7432-5.

[11]. Saurabh Singh and Gaurav Agarwal, "Hiding image to video: A new approach of LSB replacement", International Journal of Engineering Science and Technology Vol. 2(12), 2010, 6999-7003.

[12]. S. Suma Christal Mary, "Improved Protection In Video Steganopgraphy Used Compressed Video Bitstream ," International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766, ISSN: 0975-3397.

[13]. Y. J. Dai., L. H. Zhang and Y. X. Yang.: A New Method of MPEG Video Steganographying Technology .International Conference on Communication Technology Proceedings (ICCT), 2003.

[14]. D.C. Wu and W.H. Tsai: A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, Vol. 24, pp. 1613–1626, 2003.

[15]. F Hartung., B. Girod.: Steganoing of uncompressed and compressed video, Signal Processing, Special Issue on Copyright Protection and Access Control for Multimedia Services, 1998, 66 (3): 283-301.

[16]. Sherly A P and Amritha P P,"A Compressed Video Steganography using TPVD", International Journal of Database Management Systems(IJDMS) Vol.2, No.3, August 2010 DOI: 10.5121/ijdms.2010.2307-67.

[17]. Abdullah Bamatraf, Rosziati Ibrahim and Mohd. NajibMohd. Salleh in their work authors describes A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit.

[18]. G. Paul, I. Davidson, I. Mukherjee and S. S. Ravi, Keyless Steganography in Spatial Domain using Energetic Pixels, In Proceedings of the 8th International Conference on Information Systems Security (ICISS), vol.7671, LNCS, Springer (2012), 134 - 148.

[19]. Deepa put paper A steganalysis module, operated in a closed-loop manner to enhance the anti-steganalysis capability of the stegovideo with data embedded.

[20]. Yusuf Perwej, Firoj Parwej, Asif Perwej in their work describes An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection.

[21]. Biswajita Datta, Debnath Bhattacharyya, Samir Kumar Bandyopadhay and Kil-hwan Shin, "High Capacity Signature Hiding Technique in Higher Depth of LSB Layer", Contemporary Engineering Sciences, Vol.7, 2014, no. 15, 731 – 736.