An Efficient Higher LSB Method for Hiding Encrypted Data into Audio and Video Frames of AVI Video Carrier

Ms. Renu R.Dandge **Prof. Dr. V. M. Thakre**

Abstract- **Steganography can be applied in various domains using mobile and embedded devices especially mobile phones. One of the many ways of implementing a secure communication on mobile devices is using a method to hide information. The domain that represents this concept is steganography which focuses on hiding specific messages using specialized techniques in such a way that only the sender and the intended receiver are able to decipher it. This paper focuses on hiding maximum data in carrier video (AVI) with minimum quantization error by applying higher LSB method and increasing the data secrecy level.**

Index Terms— **Higher LSB, Data Hiding, Extraction, Mean Square Error, AVI Video.**

I. INTRODUCTION

Since the dawn of technology, communication has always been in need of novel techniques of data security. The confidentiality, integrity and authenticity of data are of great importance while the communication is done over a network. Due to various aspects and issues in the field of information security, methods like cryptography and steganography have been used. However application of cryptography implies the awareness of a secret cipher, although the cipher may not break but still it may get intercepted and message may also get corrupted, thus making the message useless. Therefore to deal with such security issues one of the solutions is to hide secret information in such a way that users are not aware of its existence, since users do not know about the presence of information and hence secrecy is achieved. This is done through steganography. Steganography suggests hiding any message in unsuspected multimedia data and is used in secret communication between known parties. The security problems of various data communication via Internet can be addressed by Cryptography and Steganography. A novel Video Steganography can hide an uncompressed secret video stream in a host video stream with almost the same size. Steganography involves hiding informations oit appears that no information is hidden atall. The most common use of Steganography is to hide a file inside another file. When information or a file is hidden inside a carrier file, the data is usually encrypted with a password. 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).Steganalysis is an emerging and is rapidly becoming the highlight research in the field of

information security which aims to expose the presence of the hidden data in cover object[6-7].One of the method is based on the concept of blind steganalysis. The classifier should be trained to learn the differences between cover and stego-image feature.

II. LITERATURE SURVEY

Mobility is one of today's working and researching direction and with mobility secure communication also comes into interest. Three types of stegnographic algorithms proposed are: algorithms based on the LSB method, algorithms based on the YUV method and algorithms based on the Karhunen-Loeve Transform(KLT) are proposed. The algorithms based on the LSB method usually operate by hiding the most significant bits of the secret message image pixels within the least significant bits of the carrier image pixels. The YUV method is mainly based on the LSB method. Priorto applying a LSB based algorithm the images are converted from the RGB format to the YUV format. A Karhunen-Loeve Transform (KLT)based algorithm also uses LSB based algorithms. The algorithms based on the LSB method usually operate by hiding the most significant bits of the secret message image pixels within the least significant bits of the carrier image pixels. Tests and comparisons were made using 3 hosts: ARM7basedmicrocontroller, amulti-core architecture digital signal processor and a personal computer LSB method based algorithm on the three platforms mentioned above using different sets of images of different sizes. Thus it concluded that the execution time of a stegnographic algorithm is highly influenced by the size of the carrier image [1]. Medical imaging is an important and vital aid in diagnostic and management decisions. A water marking method is proposed for medical images based on the least significant bits(LSBs).The methodology which involves data insertion and detection is proposed. The techniques used are:-(1)Harris Corner Detector: To detect differences pixels carry the message to be inserted.(2)The Error Correcting Code"Turbocode": To contribute to the data confidentiality, data verification and eventually error correction.(3)Cryptographic Hash Function SHA-1: To generate the hospital center signature and verify the integrity of the received medical image. Thus here the delicate watermarking is inserted whose objectives are to verify the integrity of the medical image and preserve the confidentiality of patient data. [2].The security problems of various data communication via Internet can be addressed by Cryptography and Steganography. The technique proposed is one kind of time-domain method tries to get a larger data-hiding capacity without causing obvious distortion in the host video stream. Therefore a video stream can be embedded into the host video stream after encoding the secret video by applying then on-uniform rectangular partition. Thus here it proposes a novel secure large-capacity uncompressed video steganography algorithm based on that image steganography algorithm. Experimental results show that there is no obvious visual distortion happening in host video stream while the quality of

the reconstructed video stream is also acceptable for the practical use [3].Steganography is the idea of hiding private or sensitive edata or information within something that appears to be nothing out of the ordinary .A proposed system program is able to hide data in digital video files, more specifically in the images or frames extracted from the digital video file (such as AVI files).So it is considered that each video frame that is extracted by the system is an image. The suggested algorithm is based on LSB(Least significant bit insertion)method. B y using the algorithm the result that we obtain on instant images show that it can reach saving up to33.3% of the image for data hiding; which is considered as an enhancement for LSB method(12%oftheimage). Thus with this technique, one can apply hidden information with more space better than other steganography media [4]. The steganalysis is an art of covert signal detection of hidden message, has gained much attention in the field of information security. It is easy to hide message into video and send it the intended recipient by uploading it to social networking and media sharing websites e.g. YouTube. Here An adaptive SS embedding method on 4×4 block is considered .This adaptive SS embedding scheme is robust to H.264compression..Due to the good de correlationability of 3 DDCT, it has widely used for image compression, video compression, video denoising and soon. The proposed scheme uses 3DDC Ttransform to capture traces of message temporal-correlation from the You Tube video [5]. Based on the H.264/AVC Video coding standard, a new video steganography algorithm is proposed and realized. The algorithm designed a motion vector component feature to control embedding and also to be the secret carrier. The proposed methodologies are:- 1) Analysis of Original Steganography Algorithm Based on Motion Vector Components. 2) Improved Steganography Algorithm Basedon Motion Vector Components Differences.
3)Visual Invisibility. The proposed algorithm is tested on a PC(1.8GHzCore26320CPU,1.0GBRAM).Thus a video steganography algorithm used is based on motion vector components differences. This algorithm obtains higher carrier utilization and embedding efficiency, and also has large embedding capacity with good visual invisibility and statistical invisibility [6]. The proposed frame work for CVSS consists of four function parts, the video sequence parser, the scene change detector, the secret message embedded and the video steganalysis. Thus one new secure and file-size preserving compressed domain steganography is proposed [7]. Steganalysis is the art of detecting the presence of the hidden information transmitted through the cover object. The method includes the secret message to be hidden by as light modification of the motion vectors. Subsequently, some improved algorithms about the steganographic scheme in motion vectors were proposed. A feature based algorithmis proposed and the support vector machine (SVM) classifier is utilized to determine the existence of hidden message. The proposed steganalysis scheme analyses the altered statistical characteristics introduced by the embedding process from both the spatial and temporal domain and employing the SVM as a discriminator can detect the presence or absence of the hidden message [8]. Loss les steganography techniques are used in which messages can be sent and received securely. The advantage of using video files in hiding information is the added security again sthacker attacks due to the relative complexity of video compared to image files. Here two steps are followed Embedding Stage and Extraction Stage. Steganography is characterized mainly by two aspects; imperceptibility and capacity. The Proposed algorithm was implemented using MATLAB. The proposed model is more secure again stat tacks because it depends on a list of security parameters. These security parameters are the novel algorithm to extract the message from the video file, the number of the embedded LSB bits, the selected transform domain, and the stegokey data [9].

III. PROPOSED METHODOLOGIES

The proposed methodologies include two main steps: first is to hide information in images and in audio and then on the other side extract the secret data. The algorithms for data hiding and extracting are proposed as follows.

Algorithm (Data Hiding):

- Select AVI Video
- Check AVI header.
- If AVI is uncompressed then go to step 4 else go to step 9.
- Separate Frames and Audio from AVI Video.
- Hide Secret Data using higher LSB bits Algorithm in Frames and Audio.
- Create Video from Stego Frames.
- Insert Sound into Created Video.
- Play stego video.
- Stop

Proposed Algorithm (Data Extraction):

- Select Stego AVI video
- Check it's Header
- If AVI is uncompressed, then go to step 4 else go to step 7
- Separate Frames and audio from AVI video.
- Extract hidden Data from Frames and audio.
- Decrypt data
- Stop.

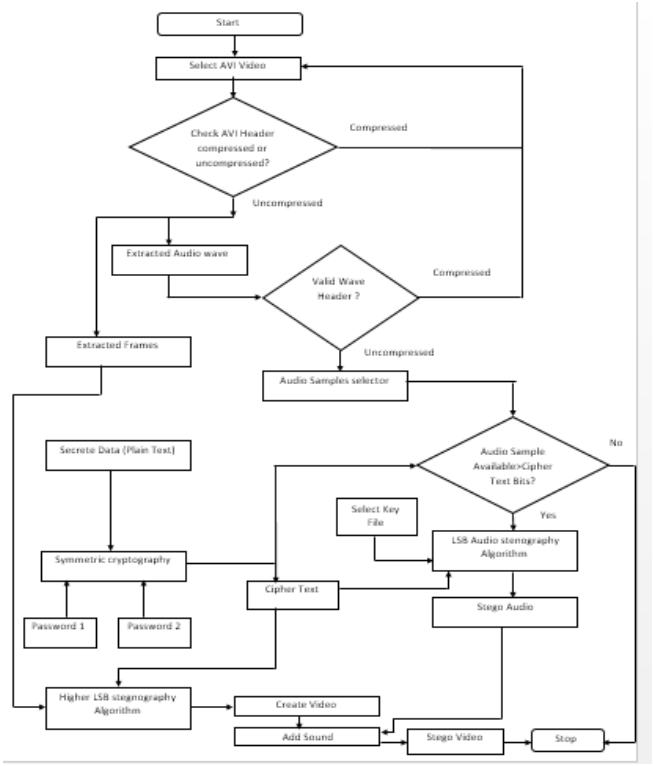

Fig. 1: DFD (for hiding data)

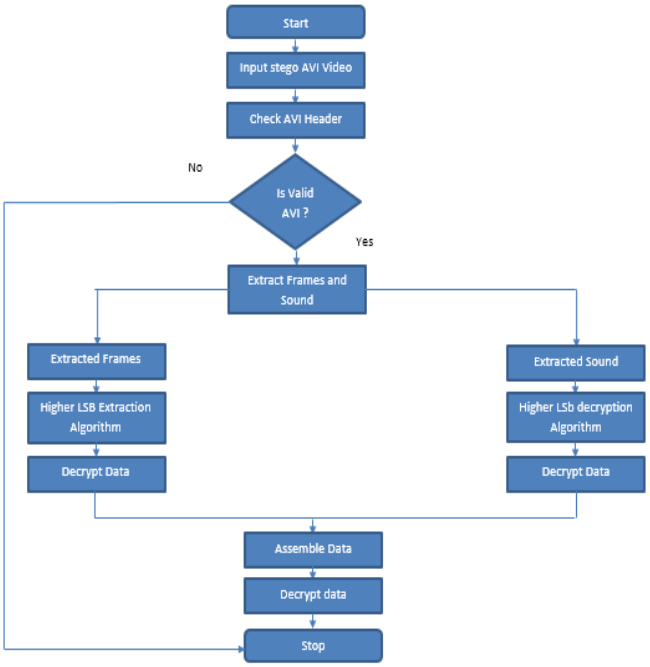

Fig. 2 DFD (for extracting the data)

Higher LSB method for data embedding will be implemented. This new method for data hiding will be proposed that achieves high data hiding capacity along with greater robustness. An individual pixel is represented with 24 Bits in RGB format as shown

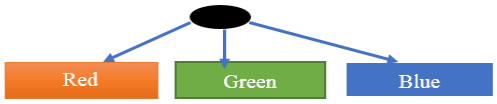

Fig. 3: Individual pixel represented with 24 Bits in RGB format

In above shown diagram, each color componant is represented with 8 bits pixels as

Fig. 4: Color component represented with 8 bits pixels

In proposed methodology, 5 bits from LSB side will be replaced with data bits as shown

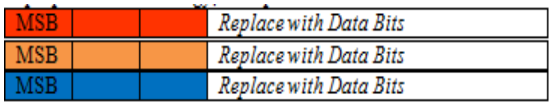

Fig.5 5 bits replaced from LSB side with data

Proposed Higher LSB Algorithm

Step1: Select Pixels.
Step 2: Select R, G, B components.
Step 3: if ((R + 32)>255) ||(R-32) <0), ((G + 32)>255) ||(G-32)<0), ((B + 32)>255) ||(B-32)<0), then discard pixel components else replace its 5 LSB side bits with data bits.
Step 4: Repeat step 2 to 3 until all guard pixel region not scanned.
Step 5: Stop

Data Hiding in Audio Wave file

A new method can be proposed that is able to hide data in audio using the fourth LSB layer, which uses a two-step approach. In the first step, a data bit is embedded into the i^{th} LSB layer of the host audio using a novel LSB coding method. In the second step, the impulse noise caused by data 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 i^{th} layer (i=1... 16) with the bit from the data bit stream.

```
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_{j+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_{j+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_{j+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_{j+2}=0
              .....
              else if a_15 =1 then a_15 = 0
        else if bit 1 is to be embedded
```

Fig. 6: 4th bit LSB replacement algorithm

IV. CONCLUSION

After implementing the proposed method the aim which is to increase the data hiding capacity without affecting the quality of image will be achieved. The resultant stego image in which the secret data is embedded will be obtained. This resultant image will appear to be same as input image. Through proposed method, quantization error of 32 bit occurs which may affect image intensity but preserves it's quality. Also the 4th LSB method implemented in audio will increase the depth of data embedding without affecting the transparency of audio signal. The steganalysis of the proposed algorithm will be challenging since bits flipping will take place and hence any intruder will not be able to identify the hidden data.

V. FUTURE WORK

To improve the data hiding capacity even more, the future work includes modifying and implementing 6th LSB method. Thus ultimately increasing the depth of hiding the secret data in required video and send it securely to intended party.

REFERENCES

[1]. Daniela Stanescu,ValentinStangaciu, MirceaStratulat "Steganography on new generation of mobile phones with image and video processing abilities"(ICCC-CONTI 2010) Timisora, Romania.IEEEInternational Joint Conferences on Computational Cybernetics and Technical Informatics,978-1-4244-7433-2/10, May 27-29, 2010

[2]. MohamedAliHAJJAJI ,AbdellatifMTIBAA , El-beyBOURENNANE "A Watermarking of MedicalImage: Method Based "LSB" JournalofEmergingTrendsinComputingandInformationSciences", ©2009-2011CISJournal, VOL.2,NO.12, PP 714-721,December2011

[3]. ShengDunHu,KinTakU," ANovel Video Steganography based on Non-uniformRectangularPartition" The 14th IEEE International Conference on Computational Science and Engineering, 978-0-7695-4477-9/11, PP: - 57 – 61, 2011

[4]. MohamedElsadigEltahir,MissLaihaMatKiah , BilalBahaaZaidan ,AosAlaaZaidan," HighRateVideoStreamingSteganography" IEEE, International Conference on Future Computer and Communication, 978-0-7695-3591-3/09, PP: - 672-674, 2009

[5]. HongZhaoHongxiaWang, HafizMalik," Steganalysis Of Youtube Compressed Video Using High-Order Statistics In 3d DctDomain",EighthInternationalConferenceon IntelligentInformationHiding and MultimediaSignalProcessing, 978-0-7695-4712-1/12, PP:- 192-194, 2012

[6]. WANGJue, ZHANGMin,SUNJuan-li," Video Steganography Using MotionVector Components"2011 IEEE, 978-1-61284-486-2/11, 2011

[7]. BinLiu,FenlinLiu,ChunfangYangandYifengSunZhengzhou," Secure Steganography in Compressed Video Bitstreams",The Third International Conference on Availability, Reliability and Security, 0-7695-3102-4/08, PP: - 1382-1389, 2008

[8]. ChengqianZhang,YutingSu,ChuntianZhang,"A New Video Steganalysis Algorithm against Motion Vector Steganography",NationalHighTechnologyResearchandDevelopmentProgramofChina(NO. 2006AA01Z407), 978-1-4244-2108-4/08 2008 IEEE, PP 1-5, 2008

[9]. AmrA. Hanafy,Gouda I. Salamaand YahyaZ. Mohasseb,"ASecureCovertCommunication Model Based On Video Steganography" ,2008IEEE,978-1-4244-2677-5/08, PP:- 1-6, 2008

[10]. VivekSampat, KapilDav, JigarMadia," A Novel Video Steganography Technique using Dynamic Cover Generation" National Conference on Advancement of technologies-Information System & Computer Networks, PP 26-29, 2012

[11]. PadmashreeG,Venugopal P S,"Audio Steganography and cryptography: using LSB algorithm at 4th and 5th LSB layers" ,International journal of Engineering and Innovative Technology(IJEIT),VOL.2, Issue 4 , PP 177-181,October 2012

[12]. 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.