1. INTRODUCTION

Data hiding 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 media 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 data hiding 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 media is a convenient choice for data hiding. 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 data hiding in multimedia networks that acquire highly correlated data.

This work will focus on the particular problem of the compressed media data hiding. General speaking, digital media appears in two main distinct encoding formats: the uncompressed and the compressed. The most popular compressed format by far is motion compensated compressed media. It achieves compression through the elimination of temporal, spatial and statistical redundancies and with this compression operation. The media bit-stream consists of variable length codes (VLC) that represent various media segments. For media stream usually being offered in compressed form, data hiding 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 data hiding is to be met, the data hiding needs to be embedded in the compressed domain Now a days, there are large amount of media data hiding algorithms been proposed. And some of them are applied for compressed media [5-9] is useful, a data hiding technique should not be easily detectable. If the existence of secret message can be detected with a probability higher than random guessing, the corresponding data hiding technique is considered to be invalid. Similar to cryptography data hiding may suffer from the attack method. Much of

the research work in the field of analysis has been carried out on images. One approach is based solely on the first order statistics and is applicable only to idempotent embedding another major stream is based on the concept of blind analysis, which is formed by blind classifiers.

There are also two media analyses methods have been proposed by Deepa et al. [17, 18] using collusion principle. And in ref [19] Deepa obtain some new media statistical invisibility properties, which inspired us to design this data hiding. In this work, we propose a secure compressed media data hiding architecture taking account of media [10-13][14-16] statistical invisibility. Also the architecture is with an analysis module, operated in a closed-loop manner to enhance the anti-analysis capability of the stegomedia with data embedded. This paper is organized as follows: Section 2 describes the framework of our secure data hiding system. In Section 3, the embedding mechanism is described in detail. The Section 4 is the perform analysis. We give the experimental results in Section 5. in Section 6, a conclusion is drawn finally.

Objectives:

1. To hide the large amount data behind the carrier.
2. To compare the performance analysis of proposed scheme with existing algorithm like LSB, HLSB, Power spectrum etc.
3. Performance evaluation of proposed algorithm in terms of embeddability criterion, computational cost, computational time, hiding capacity etc.
4. To maintain in dependability between carrier size & secret data.
5. To create unbreakable wall for stegnalyzer while extracting the secret data.
6. To maintain carrier Perceptual quality. It is necessary that to avoid suspicion the embedding should occur without significant degradation or loss of perceptual quality of the cover media.
7. To provide security to hidden message from unauthorized accesses.

2. LITERATURE REVIEW & RELATED WORK

For studying the concepts of media data hiding and data hiding technique we have surveyed many latest papers. 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 media 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 media in media and picture in media 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 media 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 data hiding 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 data hiding produce immune information.

Andreas Westfeld and Gritta Wolf [3], in this work author have described a data hiding system which embeds secret messages into a media stream. Normally the compression methods are used in media 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 media Data hiding 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 medias without degradation in visual quality.

Saurabh Singh and Gaurav Agarwal [13], have presented a novel approach of hiding image in a media. 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 media of 30 frames per second. The analysis is very difficult because each row of image pixels is hidden in multiple frames of the media. The intruder requires full media 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 media secure Data hiding (CVSS) algorithm using media bit stream. In this, embedding and detection operations are both executed entirely in the compressed. The proposed algorithm increases the security because the statistical invisibility of contiguous frames is used to adjust the embedding strategy and capacity. At present we are hiding the data in media format, so in the future implementation of 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 Data hiding 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. Najib Mohd. Salleh[17] in their work authors describes A New Digital Data hiding Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit. Author proposed a new LSB based digital data hiding 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).

3. PROPOSED WORK AND OBJECTIVES

3.1 Algorithm- Sender Side

1. Start
2. Input carrier media.
3. Select secrete data.
4. Convert secrete data to binary format.
5. Select protection region of carrier media.
6. If (Size (Protection Region [PR] < Size (Secrete Binary data) then go to step 7.
7. Embed secrete binary data into PR region of carrier media.

. Stop

3.2 Algorithm- Receiver Side

1. Start
2. Input carrier media
3. Select Protection region from carrier media.
4. Extract Secrete binary data from protection region.
5. Convert secrete binary data to ASCII format.
6. Stop.

Methodology/ Work Plan:

The proposed research work will be carried out in following phases

- **Phase 1: Duration of six month**

  Extensive literature survey and formulating research problem

- Phase 2: Duration of six month

  Analysis of present Data embedding Algorithm and Data extraction techniques.

- **Phase 3: Duration of six month**

  Development and performance evaluation of Novel Data Hiding approach under different carrier size and Key file size.

- **Phase 4: Duration Six month**

  Development and performance evaluation of data hiding algorithm, to improve system performance and reducing the data hiding time.

- **Phase 5: Duration Six month**

  Compare the performance evaluation of our techniques with other techniques.

- **Phase 6: Duration Six month**

  Thesis Writing and Submission

Each phase would be followed by paper presentation/publication in national/International Conference/Journal.

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 Media", International Journal of Database Theory and Application Vol. 2, No. 2, June 2009.

[3]. Andreas Westfeld and Gritta Wolf," Data hiding in a Media 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 Data hiding", i-manager's Journal on Software Engineering, Vol. 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 Data hiding 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: Analysis in Color Images, Binghamton, 2007.

[9]. Neil F. Johnson and Sushil Jajodia,"Exploring Data hiding: Seeing the Unseen", George Mason University.

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

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

[12]. Data hiding on new generation of mobile phones with image and media 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.

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

[14]. D.C. Wu and W.H. Tsai: A data hiding 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 media, 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 Media Data hiding using TPVD", International Journal of Database Management Systems(IJDMS) Vol.2, No.3, August 2010 DOI: 10.5121/ijdms.2010.2307-67.

[17]. 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.

Submitted by: (Ms. Devika Gawande)