Volume 1, Issue 4 November 2015 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal

Of

Science, Engineering and Information Technology

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi, Urdu all research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: - Dr. Ashak Hussain Malik House No. 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815,
Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

REVERSIBLE VIDEO DATA HIDING USING HISTOGRAM BASED STATIONARY WAVELET TRANSFORM

RAMANDIP SINGH[1]
CSE, CGC, Jhanjeri Punjab, India

SUKHMEET KAUR[2]
CSE, CGC, Jhanjeri Punjab, India

ABSTRACT

Data hiding is the procedure of furtively implanting data inside an information source without transforming its perceptual quality. Information Hiding is the craftsmanship and art of composing concealed messages in such a route, to the point that nobody separated from the sender and planned beneficiary even acknowledges there is a shrouded message. Generally, in Data Hiding, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. Different great methods are proposed and as of now taken into practice.

Keywords- *Steganography, Cryptography, Least significant bit, Bit error rate, PSNR, MSE*

INTRODUCTION

Computer Technology and the Internet have made a leap forward in the presence of information communication [1]. This has opened an entire better approach for executing steganography to guarantee secure information exchange. Steganography has become an interested field of data hiding techniques. Steganography used in an open-systems environment such as the Internet and Far-fetched applications, privacy protection, authentication, data integrity, intellectual property rights protection [2]. Steganography can also be used misused like other technologies. For instance terrorists may use this technique for their secret secure communication or anti-virus systems can be fooled if viruses are transmitted in this way.

However, it is evident that steganography has numerous useful applications and will remain the point of attraction for researchers [3]. In the past few years, Steganography has become an interested field of data hiding techniques. There are numerous sorts of steganography strategies are accessible among them concealing information in video by LSB substitution is a basic technique [4]. Here the data will be inserted taking into account the stego key. Key is utilized as a part of the type of polynomial mathematical statements with diverse coefficients. By utilizing this, the capacity of inserting bits into the cover picture can be expanded [5].

The crevice between the hypothetical embedding capacity in information concealing and what is achievable by and by can be connected by examination of such issues as fundamental embedding instruments for inserting one bit and modulation/ multiplexing systems for embedding numerous bits. The accompanying issues oblige specific consideration:

- **Distortion:** The distortion presented by watermarking must be indistinctly little for commercial or artistic reasons. However, an adversary meaning to pulverize the watermark

may be willing to endure certain level of visible artefacts. Consequently, the distortions by inserting and by assault are regularly asymmetric, prompting an extensive variety of conceivable watermark-to-c noise ratio.

- **Actual noise conditions:** An embedding framework is generally intended to survive certain noise conditions. The watermarked information may experience a variety of legitimate processing and malevolent assaults, so the actual noise candiffer altogether. Focusing on conservatively at surviving extreme noise would prompt the misuse of actual payload, while targeting aggressively at light commotion could bring about the defilement of inserted bits. In addition, a few bits, for example, the ownership information and control information, are obliged to be more robust.

- **Uneven distribution of embedding capability:** The measures of information that can be embedded frequently differ generally from district to area in picture and video. This uneven embedding capacity causes serious trouble to high-rate embedding.

I. VIDEO DATA HIDING

Recently, information hiding techniques have attracted much research interests from the field of information security [6]. Thus, a data hiding application using steganography. The purpose is to create user friendly steganography application that allows users to hide private data in image/video files. The goal is to make this steganography application less vulnerable to steganalysis [7]. Steganography is a standout amongst the most imperative examination subjects in the field of security communications. The desire to communicate something specific as securely and as safely as could reasonably be expected has been the purpose of exchange since time immemorial. Data is the abundance of any association. This makes security-issues top need to association managing classified information [8].

Whatever is the strategy we decide for the security reason, the blazing concern is the level of security. Information stowing away can be considered as a correspondence issue where the implanted information is the sign to be transmitted. An essential issue is the embedding capacity [9].

II. APPLICATION OF STEGANOGRAPHY

Steganography can be used for wide range of applications such as, in defence organisations for safe circulation of secret data, in military and intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials [10].

In medical imaging, patient's details are embedded within image providing protection of information and reducing transmission time and cost, in online voting system so as to make the online election secure and robust against a variety of fraudulent behaviours, for data hiding in countries where cryptography is prohibited, in improving mobile banking security, in tamper proofing so as to prevent or detect unauthorized modifications and other numerous applications.

- Protection of Data Alteration
- Access Control System for Digital Content Distribution
- E-Commerce
- Media
- Database Systems
- Digital Watermarking
- Confidential Communication and Secret Data Storing

III. OBJECTIVES

- To collect low bit-rate videos or general videos
- Analyze the total space in video frames to estimate the applicable points of data hiding
- The search is done using histogram equalization of the video frames and by neglecting the pixels which show high variance
- Embedding the bits of information image in to the image which is decomposed with Stationary wavelet transforms
- Recovering the video data with inverse transform
- Decrypting the video for recovering the hidden message
- Finding the signal to noise ratio for embedding the information
- VIQ video image quality affected by hiding the data
- BER of the extracted message signal to the original
- And correlation of the message bits extracted

IV. PROBLEM FORMULATION

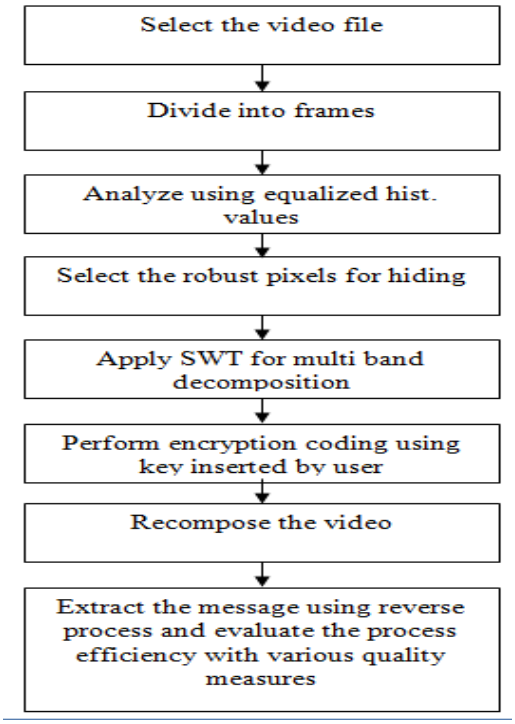
In the current review we have studied the techniques of data hiding for transmission and reception of the secret data without the knowledge of the users, other than the one who knows the hiding of the message is done. The techniques are useful for data encryption and provide the hiding of data with maximum robustness to the visual system, but a main issue is the steadiness of the data under various constrains like space, data length, encryption power which affect the message quality. The following is the new path work of problems to be solved:

- The coding method for hiding the data should be less complex
- The data embedding should incorporate high data density
- The hiding scheme should have high level scrambling efficiency
- The perceptual quality should not be affected

V. PROPOSED METHODOLOGY

- Select the video file to be used
- Divide the video into frames of images with RGB24 data length
- Convert the video frames to 64 bit format
- Using the equalization of histogram values find the suitable pixels for embedding the bits
- Select the secret message text image or code and find the number of bits to encode and encrypt using secret code generated using the user inserted key
- Apply stationary wavelet transform to the video frame and encode the bits of message in wavelet pixels with respect to histogram values
- Apply the reverse transform of the SWT to re-construct the image frame repeat for all the frames in a video
- Then construct the video with the modified frame images
- Calculate the parameters like signal/noise ratio, VIQ, correlation
- Extract the message using secret key and find the correlation of the message bits with that of the original
- Apply the process for various sizes of the message and different video files.

VI. BLOCK DIAGRAM



VII. RESULTS AND DISCUSSIONS

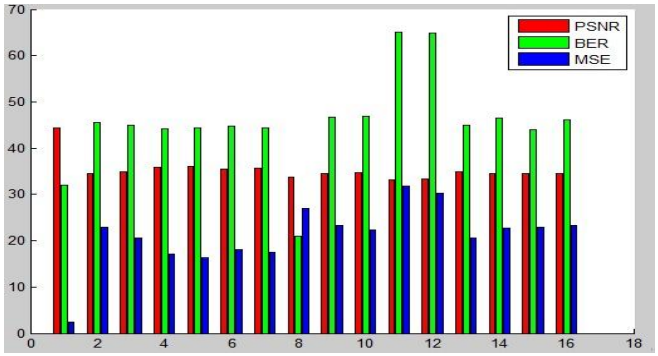


Figure 1 show the graphical results for the proposed system in terms of PSNR, BER and MSE

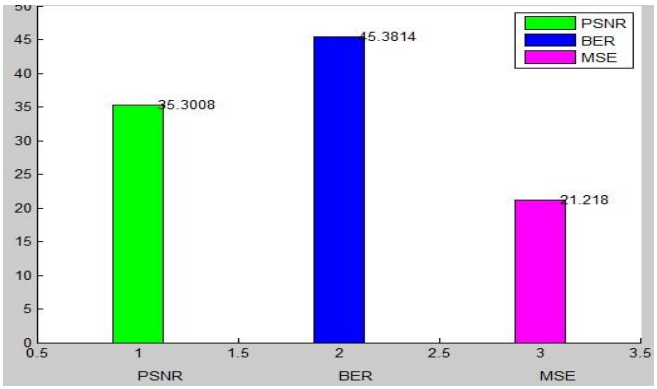


Figure 2 show the cumulative graphical results for the proposed system in terms of PSNR, BER and MSE

Table 1 shows the results for the proposed system under CORR, PSNR, BER and MSE

Frame No.	1	2	3	4	5	6
CORR	0.767	0.773	0.75	0.745	0.74	0.695
PSNR	44.42	34.54	34.99	35.79	35.98	35.54
BER	31.91	45.54	44.89	44.14	44.41	44.72
MSE	2.349	22.85	20.62	17.15	16.4	18.17

Table 2 shows the results for the base system under CORR, PSNR, BER and MSE

Frame No.	1	2	3	4	5	6
CORR	NaN	NaN	0.606	NaN	0.603	0.6
PSNR	28.95	28.81	28.8	28.77	28.75	28.79
BER	38.75	39.85	39.78	39.92	39.82	39.59
MSE	82.78	85.59	85.79	86.4	86.66	85.86

VIII. CONCLUSION

In this research work we reviewed many papers on steganography techniques. These papers are good enough and have wide future scope. Steganography has its own place in the field of security. Steganography used in an open-systems environment such as the Internet and Far-fetched applications, privacy protection, authentication, data integrity, intellectual property rights protection. Steganography can also be used misused like other technologies. For instance terrorists may use this technique for their secret secure communication or anti-virus systems can be fooled if viruses are transmitted in this way. However, it is evident that steganography has numerous useful applications and will remain the point of attraction for researchers.

IX. REFERENCES

[1] Saurabh Singh, "Hiding Image to Video" in International Journal of engineering science & technology Vol. 2(12), 6999-7003, 2010.

[2] Marghny Mohamed,"Data hiding by LSB substitution using genetic optimal key permutation" in International arab journal of e-technology, vol.2, no 1 January 2011.

[3] A.K. Al Frajat "Hiding data in video file An overview" Journal of applied sciences 10(15):1644-1649, 2010.

[4] Tao Zhang, Wenxiang Li, Yan Zhang, Xijian Ping" Detection of LSB Matching Steganography Based on Distribution of Pixel Differences in Natural Images" , Publication Year: April-2010, Page(s): 548 – 552

[5] Ross J. Anderson and Fabien A.P. Petitcolas, "On the limits of steganography," IEEE Journal on Selected Areas in Communications (JSAC), Special Issue on Copyright & Privacy Protection, Vol. 16 no. 4, pp 474-481, May 1998.

[6] T Mrkel, JHP Eloff and MS Olivier ."An Overview of Image Steganography,"in proceedings of the fifth annual Information Security South Africa Conference, 2005.

[7] J. Siegfried, C. Siedsma, B.J. Countryman, C.D. Hosmer, "Examining the Encryption Threat," International Journal of Digital Evidence, Vol. 6, pp. 23-30, December 2004.

[8] "Stretching the Limits of Steganography", RJ Anderson, in Information Hiding, Springer Lecture Notes in Computer Science v 1174 (1996) pp 39-48

[9] Scott Craver, "On Public-key Steganography in the Presence of an Active Warden," in Proceedings of 2nd International Workshop on Information Hiding, April 1998, Portland, Oregon, USA. pp. 355 - 368.

[10] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt, " Digital image steganography: Survey and analysis of current methods ", Journal of Signal Processing, Elsevier, Volume 90, Issue 3, March 2010, pp. 727-752.

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- Dr. Ashak Hussain Malik House No-221, Gangoo Pulwama - 192301 Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com