IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Hiding Data in Video Using Maximum Motion Detection and Intensity Technique

Shaminder Kaur[1*], Paramjeet Singh[2], Shaveta Rani [3]

[1] CSE Department, MRSPTU, Bathinda, India
[2] CSE Department, MRSPTU, Bathinda, India
[3] CSE Department, MRSPTU, Bathinda, India

Available online at: www.ijcseonline.org

Accepted: 16/Jul/2018, Published: 31/July/2018

***Abstract*—** Steganography is a technique used to hide data or identifying information within digital multimedia. Digital steganography is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information. Existing stegography systems for video stegnography used simple techniques to hide the images into videos which can be easily decoded by using some decoding algorithms. Hence a novel video stegnography system must be made that can hide the image in the video in the more secure way so that attacker cannot decode the hidden message from the video. In the proposed work, Least Significant Bit (LSB) will be used to hide the image message into a video. Proposed system hide the image into each of the LSB of each color of each pixel of the input video frame. In the proposed system, from the input video a fame with maximum motion and intensity is extracted which is treated as the target frame for hiding message. In this target frame image will be hide using Least Significant approach. The resultant video becomes the stegno video. Reverse process is performed on the stegno video to extract the image file from that video file. The proposed system is tested on various input videos and various input images are used as message to hide in these videos. It is evaluated that the results of the proposed system are very satisfactory. Performance of the proposed system is also compared with the performance of the existing system and it is evaluated that the proposed system generates the better results in terms of PSNR and MSE than that of existing system.

***Keywords*—** Steganography, LSB, Image Hiding, Message Security, Video Stegnography.

I. INTRODUCTION

Steganography is that the skill and art of composing hid messages such no one, except for the sender and expected beneficiary, associates the presence with the message, a sort of security through indefinite quality. Steganography works by replacement bits of futile or unused data in traditional computer records, (for example, designs, sound, content, HTML, or perhaps floppy circles) with bits of varied, undetectable knowledge. This shrouded knowledge is plain content, figure message, or perhaps footage. In a computer primarily based sound Steganography framework, mystery messages ar put in in processed sound. The mystery message is deep-rooted by marginally modifying the paired grouping of a sound record. Existing sound Steganography programming will install messages in WAV, AU, and even MP3 sound documents. putting in mystery messages in processed sound is usually a a lot of hard method than inserting messages The term Steganography is adjusted from the Greek word steganographia, signifying "secured expressing" and is taken in its advanced frame as which means the stowage away { knowledge|of information} within alternative data.

Elements of a Steganographic Message

Before diving deep into the steganographic procedure, as a matter of initial importance, we've got to understand the various segments of a steganographic message. The beneath list covers all the conceivable components that may be on the market within the steganographic message.

- Secret message
- cover data
- Stego message

The mystery message alludes to the piece of the message that is projected to be coated up. This message can later be disorganized to form it considerably a lot of hard for someone United Nations agency makes an attempt to interrupt the protection to induce hold of the hid information processing message. this is often the essential phase during a steganographic message. Next half is that the cowl data phase. This phase alludes to the compartment during which the mystery message is roofed up. This cowl data phase is

something like processed pictures, advanced recordings, sound documents and content records. The last phase is that the stego message that is as crucial because the mystery message. The stego message phase alludes to the last item.

Video Stegnography

Video steganography, which is the focal point of this survey, can be seen as an augmentation of picture steganography. Truth be told, a video stream comprises of a progression of continuous and similarly time-divided still pictures; once in a while went with sound. Along these lines, numerous picture steganographic strategies are pertinent to recordings too. Hu et al. expanded various picture information concealing calculations to video demonstrating this reality. Video is an extremely encouraging sort of cover-media since it can convey a lot of mystery information.

II. RELATED WORK

K.Thangadurai et.al(2014), Steganography alludes to data or a record that has been hidden inside an advanced picture, video or sound document. On the off chance that a man sees the protest in which the data is covered up inside, he or she will have no sign that there is any concealed data. So the individual won't attempt to decode the data. Steganography can be isolated into Text Steganography, Image Steganography, Audio/Video Steganography. Picture Steganography is one of the normal techniques utilized for concealing the data in the cover picture. LSB is exceptionally productive calculation used to implant the data in a cover record. This paper displays the detail information about the LSB based picture steganography and its applications to different record designs. In this paper creators additionally break down the accessible picture based steganography alongside cryptography strategy to accomplish security.

R. Singh et.al(2014), This paper gives a survey of steganography, its different strategies, its points of interest and disservices, applications, it's converging with cryptography systems .Today's the ascent of the web turn into the most imperative factor of data innovation and correspondence however alongside this the danger of data security increments. It's turned out to be critical to offer security to your information with the goal that no unapproved individual can get to it. The steganography is an intense security device with which we can shroud a mystery message inside a protest. The question can be content, picture, sound or video.

S. Sharda et.al (2013), Steganography can be characterized as the investigation of imperceptible correspondence that as a rule manages the methods for concealing the presence of the imparted message. On the off chance that it is accomplished effectively, the message does not pull in consideration from busybodies and assailants. The fundamental destinations of steganography are imperceptibility, strength (protection from different picture preparing strategies and pressure) and limit of the shrouded information. These are the fundamental elements which make it not quite the same as different procedures watermarking and cryptography. This paper incorporates the essential steganography techniques and the fundamental spotlight is on the audit of steganography in advanced pictures.

S. Khosla et.al(2014), The quick advancement of information exchange through web made it simpler to send the information exact and speedier to the goal. Other than this, anybody can change and abuse the profitable data through hacking in the meantime. This paper presents video steganography with computerized watermarking strategies as an effective and powerful apparatus for assurance. This paper is a mix of Steganography and watermarking; which gives a solid spine to its security. Here considers video as set of edges or pictures and any adjustments in the yield picture by shrouded information isn't outwardly unmistakable. This proposed framework not just conceals expansive volume of information inside a video; yet in addition constrains the discernible contortion that may happen while handling it.

Jayaram P.(2011), Today's expansive request of web applications expects information to be transmitted in a safe way. Information transmission in broad daylight correspondence framework isn't secure a direct result of block attempt and uncalled for control by meddler.

III. METHODOLOGY

Proposed system will work on Least Significant Bit (LSB) approach in which image is to be hide in the video file in the frame having maximum motion between the consecutive frames and maximum intensity of pixels is encountered.

Proposed system will work in following steps:
Algorithm to embed the text message into an video
Step 1: Extract the frames from video and Image which is to be hidden.
Step 2: Convert the video frame into jpg equivalent image.
Step 3: Convert the input image to be hidden into its equivalent binary form.
Step 4: Calculate LSB of each color of each pixel of the video frame which has maximum motion in the consecutive frames and maximum intensity of the pixel.
Step 4: Replace LSBs of pixel in video Frame with each bit of secret message one by one.
Step 5: End.

Algorithm to extract the text message from an image
Step 1: Read the stegno video frame i.e. the image in which message is hidden.

Step 2: Calculate LSB of each color of each pixel in video frame based on maximum motion and intensity.
Step 3: Add the LSB of each color of each pixel of the stegno frame in the final message.
Step 4: Convert the extracted binary message into text message.
Step 5: Display the message to the user.
Step 6: End.

IV. RESULTS AND DISCUSSION

The proposed system hides the text data into audio samples using LSB technique. Proposed system is evaluated on the basis of various parameters which are as follows:
The *Mean Square Error (MSE)* : The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE,

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

the
PSNR(Peak Signal to Noise Ratio): is a measure of signal strength relative to background noise. The ratio is usually

$$PSNR = 10 \log_{10}\left(\frac{R^2}{MSE}\right)$$

measured in decibels **SNR.**
The results statistics of the proposed system is shown as below:
Table 1.1 : Result statistics of the proposed system.

Title	Value
Videos Tested	10
Images Embedded	10
Accuracy	94%
Proposed Avg. PSNR	53.56
Proposed Avg. MSE	0.53
Proposed avg hiding capacity	21.97%

Table 1.2: Comparison of the proposed system with the existing system on the basis of the PSNR

Cover Video	Frame resolution	PSNR in Existing technique	PSNR in proposed technique	Improvement (%)
Video 1	256*256	46.76	53.25	11.74
Video 2	253*253	46.76	53.30	11.84
Video 3	260*260	46.76	54.12	15.73

The above table represents the comparison of the existing and proposed system on the basis of PSNR parameter. It is shown that the PSNR of the proposed system gives better results than that of the existing system on the same type of the data given.

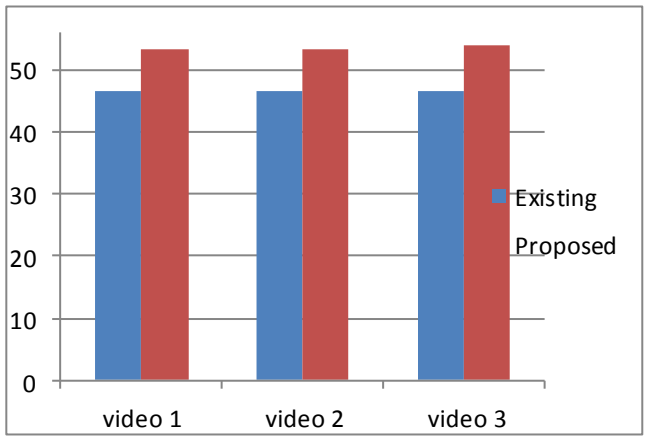

Figure 1.1 Comparison Graph of Existing and proposed system on the basis of PSNR

Table 1.3 : Comparison of the proposed system with the existing system on the basis of the MSE

Cover video	Frame resolution	MSE in Existing technique	MSE in Proposed technique	Improvement (%)
Video 1	256*256	0.61	0.54	11%
Video 2	253*253	0.61	0.51	16.39
Video 3	260*260	0.61	0.50	18.32

The above table represents the comparison of the existing and proposed system on the basis of MSE parameter. It is shown that the MSE of the proposed system is less than that of the existing system on the same type of the data given.

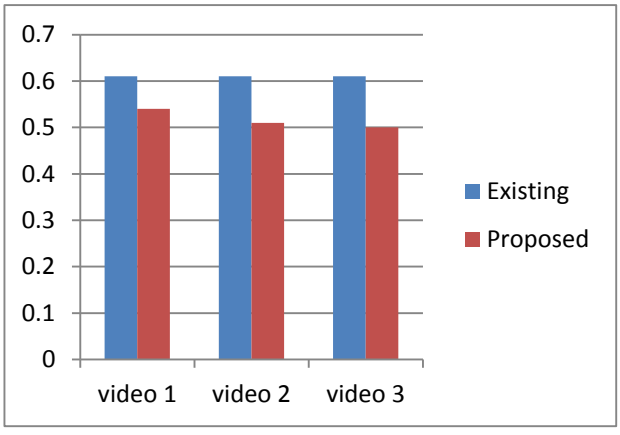

Figure 1.2 : Comparison Graph of Existing and proposed system on the basis of MSE.

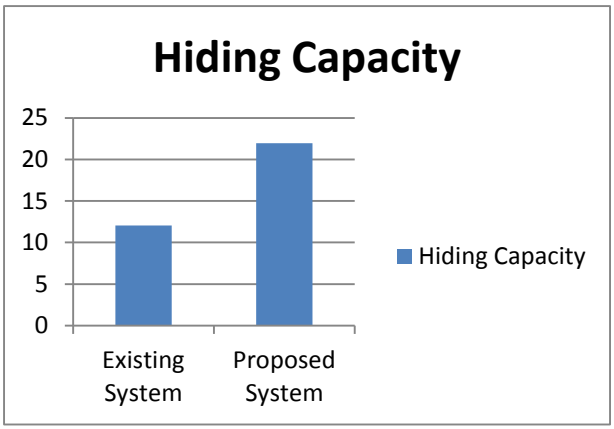

Figure 1.3 : Comparison Graph of Existing and proposed system on the basis of Hiding Capacity

V. CONCLUSION AND FUTURE SCOPE

Steganography is a sort of cryptography in which the mystery message is covered up in an advanced picture. While cryptography is engrossed with the security of the substance of a message or data, Steganography focuses on hiding the specific presence of such messages from recognition. In the proposed system, maximum motion and intensity between every consecutive frames is evaluated. The frame must be found in which maximum motion and intensity is there and this frame is marked as the target frame. This technique provides a large amount of security to the stegno video as it is very difficult for the attacker to guess or find the target frame in which image is hidden. In the proposed work, Least Significant Bit (LSB) will be used to hide the image message into a video. Proposed system hide the image into each of the LSB of each color of each pixel of the input video frame. In the proposed system, from the input video a fame with maximum motion and intensity is extracted which is treated as the target frame for hiding message. In this target frame image will be hide using Least Significant approach. The resultant video becomes the stegno video. Reverse process is performed on the stegno video to extract the image file from that video file. The proposed system is tested on various input videos and various input images are used as message to hide in these videos. It is evaluated that the results of the proposed system are very satisfactory. Performance of the proposed system is also compared with the performance of the existing system and it is evaluated that the proposed system generates the better results in terms of PSNR,MSE and hiding capacity than that of existing system.

FUTURE WORK

In future, system can be extended to hide the image into more than one frames by dividing it into various parts to provide more security. Further, instead of LSB data hiding technique, combination of more than one technique can be used to hide the message.

REFERENCES

[1] K.Thangadurai and G.Sudha Devi, *"An analysis of LSB Based Image Steganography Techniques"*, International Conference on Computer Communication and Informatics, 2014

[2] Rashi Singh,Gaurav Chawl, *"A Review on Image Steganography"*, International Journal of Advanced Research in Computer Science and Software Engineering,Vol. 4, Issue 5, 2014

[3] S. Sharda, S. Budhiraja, *"Performance Analysis of Image Steganography based on DWT and Arnold Transform"*,International Journal of Computer Applications (0975 – 8887) Vol. 69– No.21, 2013

[4] S. Khosla,P. Kaur, *"Secure Data Hiding Technique Using Video Steganography and Watermarking"*, International Journal of Computer Applications (0975 – 8887) Volume 95– No.20, 2014

[5] Jayaram P,Ranganatha H R,Anupama H S, *"Information hiding using audio steganography – a survey"*, The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, 2011

[6] K. Pradhan, C. Bhoi,"Robust Audio Steganography Technique using AES algorithm and MD5 hash",International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 10, 2014.

[7] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn:*"Information Hiding- A Survey"*, Process of IEEE, vol.87,no.7, pp.1062-1078, 1999.

[8] M. Wu, B. Liu. *"Multimedia Data Hiding"*, Springer- Verlag New York, 2003.

[9] N. Taraghi-Delgarm, *"Speech Watermarking"*, M.Sc. Thesis, Comptuer Engineering Department, Sharif University of Technology, Tehran, IRAN, 2006.

[10] M. Pooyan, A. Delforouzi, "*LSB-based Audio Steganography Method Based on Lifting WaveletTransform"*, in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), 2007.

[11] R.A. Santosa and P. Bao, "Audio-to-image wavelet transform based audio steganography," Proc. of 47th Int. Symposium ELMAR, pp. 209- 212, 2005.

[12] X. Huang, R. Kawashima, N. Segawa, Y. Abe. *"The Real-Time Steganography Based on Audio-to-Audio Data Bit Stream"*,Technical report of IEICE, ISEC, vol.106 pp.15-22, 2006.

