# Gurumukhi Text Hiding using Steganography in Video

Bharti Chandel
Assitant Lecturer
Computer Science and Engineering
Chitkara University
Rajpura, India

Shaily Jain, PhD
Associate Professor
Computer Science and Engineering
Chitkara University
Himachal Pradesh, India

## ABSTRACT

Revolution in telecommunication systems has made the secret information vulnerable to many types of attacks. Steganography provides a method to conceal the very existence of secret message. Due to tremendous growth in technology, secret messages are getting exchanged in many languages other than English through different media like images, videos, and audio and text documents. Video Steganography has become a popular topic due to the significant growth of video data over internet. This paper presents an effective LSB based approach to disguise encrypted Gurumukhi text inside a video. In this paper, besides employing the modified LSB substitution technique at a fundamental stage, advantage of refined OPAP, Canny edge detection and identical match techniques has been taken to improve the results. To provide dual layer of security AES techniques has been used to permute the message before embedding it. Experimental results shows enhancement in security performance, embedding capacity, Bit Error Rate (BER), Peak Signal to Noise Ratio (PSNR), Mean squared error (MSE), Histogram Error values after implementation of this hybrid approach as compared to other video Steganography techniques.

## Keywords

AES, BER, PSNR, Histogram Error, MSE, LSB, OPAP

## 1. INTRODUCTION

Rapid evolution in availability of cheaper and powerful computer facilities and broadband Internet technologies have made possible free streaming of high quality videos on internet and on websites like YouTube, Yahoo videos and Daily motion etc. [1]. The security and privacy of digital media content in applications like pay-per-use TV, video conferencing, medical, industry, to copy right and Intellectual Property Rights (IPR) and in military applications is the main issue of communication network. Videos are most frequently used cover objects for Steganography because of their inimitable rise in communication and high payload, high security against hacking attacks. Steganography using video as a cover object can be achieved mainly through spatial and transform domain [4] techniques. Spatial domain techniques including Least Significant Bit (LSB), Hash LSB (HLSB) and Tri-way Pixel value Differencing (TPVD) has high simplicity and high payload but is highly prone to attacks. Transform domain techniques like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [2] are highly complex but provides high imperceptibility.

Information can be camouflaged in a video frames by extracting frames from videos. Steganography can be mainly achieved in two parts first is embedding information on sender side and second part is extracting that information on receiver side. Video file is considered a mixture of multiple frames or images and audio files in compressed or in uncompressed form. Information can be disguised in frames or in audio part of a video [3]. Least Significant Bit approach is very popular embedding technique as it has low CPU implementation cost and high embedding capacity but causes high distortion which is vulnerable [4] to steaganlysis. To reduce distortion caused by LSB optimal Pixel Adjustment Process (OPAP) can be used which minimizes distortion by adjusting pixel values [5]. To minimize distortions caused by LSB approach secret message bits must be scattered into randomized pixel positions or pixel where brightness level changes sharply i.e. edge pixels [6]. The proposed mechanism has been made efficient by hiding data in 3-bits per pixel in LSBs of each pixel using Identical match at non-edge pixels and OPAP at edge pixels to minimize distortions in cover frame due to change in LSBs of edge pixels. Canny Edge Detection fulfills the optimization and reliability standards of efficient edge detection approach [7]. Advantage and strength of proposed video steganography mechanism in hiding Gurumukhi secret message is improvement in security using AES encryption to provide double layer security against the attack of intruder.

This paper proposes an effective Enhanced LSB approach. The proposed method is developed in MATLAB and is illustrated with AVI (Audio Video Interleave) as a cover object. High Imperceptibility and Security has been achieved through proposed technique. This paper is organized as follows- Section 2 describes Related Work, section 3 describes proposed methodology, section 4 describes the experimental results and section 5 describes the conclusion and future work.

## 2. LITERATURE SURVEY

Steganography has been explored very well using different cover objects due to its high demand in hiding information. Video steganography has become a wide area of research as it has high payload capacity and is highly robust against stegnalysis attacks. To implement video steganography mechanism various research papers have been studied papers and some of them have been discussed in brief here in next lines. Authors are very thankful to these authors for providing us information about various embedding techniques in video steganography. G.S Naveen Kumar et.al [2] had merged DWT and LSB to hide a secret video inside a video and achieved good PSNR with minimized distortions .Due to high redundancy in video frames, temporal and spatial features [4] of video streams can be exploited to embed secret information to achieve high payload and high imperceptibility along with constant bit rate.

Hang et.al [5] had proposed a secure data hiding technique in image steganography based on exploiting modification direction and diamond encoding using pixel value differencing to achieve least MSE values. Results have been compared with various methods on the basis of MSE. To achieve low computational complexity and high payload capacity, [7] LSB of edge pixels in image steganography can be used to hide secret information. Chen et.al has done edge detection using hybrid edge detector of fuzzy and canny edge detectors to achieve optimization in edge detection. K. Dasgupta et.al [8] proposed 3-3-2 LSB based mechanism using Genetic algorithm to achieve optimized video steganography with significant improvement in PSNR and cover frame fidelity. In [9] secret bits of information embedded in syndrome-trellis codes (STCs) by exploiting motion vectors in spatial temporal domain to achieve minimum-distortion in video steganography. In [10] Po.Chyi.et al. has investigated High, Medium low embedding video profiles to prove that payload can reach up to 10% of total file size when a good tradeoff is achieved in FLV files. Sheng Du Hu et.al [11] embedded secret video frames with minimum visual distortions in 4 LSB by exploiting non-uniform rectangular partitions in AVI files. In [12] simple LSB technique was used to hide data in video file by hiding message pixel row in first row of cover video file frame. In [13] LSB technique was used along with masking and filtering and transformation technique to embed secret image in cover video file.

## 3. ENCRYPTION TECHNIQUE

AES is cryptography algorithm designed by NIST to replace DES, 3DES in 2001.AES algorithm coverts 128 bit text to cipher text and uses key length of 128,192 and 256 bits keys.

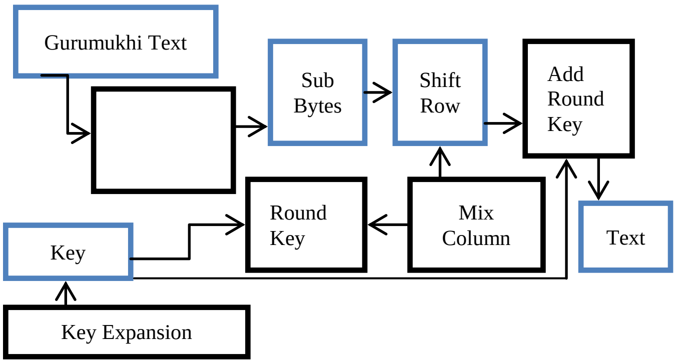

**Fig.1 AES Encryption algorithm encryption procedure**

The AES technique shown in Figure 1, the first phase in encryption procedure is to apply Sub Byte transformation i.e. divide the whole byte into two hexadecimal digits. After division of bytes apply shift rows operation i.e. shift each row in cyclic order using an offset value. In general each nth row apply left circular shift by n-1 bytes. Shift rows operation in this technique completely removes the linear independence of columns. After shifting rows by left circular shifts apply invertible linear transformation on each column i.e. applies Mix Column steps on each column to generate new column. After applying Mix Column step the 128-bit key is converted into sub bytes and added to each round.

In encryption process Gurumukhi Text has been converted to cipher text using AES-128 bit technique which uses 10 rounds, in each round except 10th round secret message goes through four transformations a)Sub-bytes b)Shift-rows c)Mix-columns d)Add round key. 10th round doesn't use Mix column transformation. AddRoundKey is the first phase in both encryption and decryption process of AES-128 bit as shown in Fig.1.

## 4. CANNY EDGE DETECTION

Canny Edge detection was proposed by John F. Canny in 1986 .Canny Edge detection is a highly optimized multi-step technique to select true edges from the cover frame. Canny Edge detection involves processes like Smoothing to remove noise from cover frame, gradient selection to mark edges with larger magnitudes, suppression to mark edges on the basis of local maxima, Compute threshold to find potential edges and last step is hysteresis to remove false edges [12].The canny Edge detection of a Cover Frame is given below

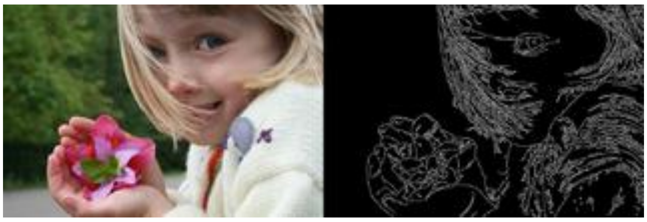

**Fig. 2 Canny Edge Detection of Cover Frame**

## 5. IDENTICAL MATCH AND OPAP

Optimal Pixel Adjustment Process (OPAP) can be used to minimize the distortions caused by embedding secret message bits in pixels of stego frame.

In OPAP technique, if secret message bits are concealed in right most r^th LSBs of an n-bit pixel, then mathematical calculations are applied on n-r^th bits to minimize the distortions by replacing some bits of stego pixel. Suppose a pixel value is p, the value of the right-most r^th LSBs of p is $p^d$ .The p' is the pixel value after embedding m message bits using LSB substitution method and $d_e$ the decimal value of these bits. OPAP technique uses the following mathematical equations to solve distortion problem.

$$\left\{ \begin{array}{lll} p''=p'+2^m & p^d-d_e>2^{m-1} & \text{and } p'+2^m<=255 \\ p'-2^m & p^m-d_e<-2^{m-1} & p'-2^m>=0 \\ p' \text{ otherwise} & & \end{array} \right\}$$

Where p" stands for the final results obtained by OPAP technique. Both pixels of cover frame and stego frame have same number of bits and disguised data can be easily extracted from these right most bits.

Identical match technique embeds information by comparing m bits of secret message with m bits of each n bit pixel. If there is match for m secret message bits in n bit pixel then that index position of that particular pixel will be stored in a matrix for future extraction of message. 2 bit of secret message will be compared with RED part bits, 2 bits with GREEN part bits and 2 bits with BLUE part of each pixel. By summarization it can be said that 6 bits per pixel has been hidden in color frames as each pixel is of 24 bits.

For example consider a RGB pixel value of the cover frame as below:

R: 10001011

G: 10010100

B: 11011101

And a message to be inserted: 1101000

Identical match technique will store index position of similar bits in position matrix. For example first two bits of secret message i.e. "11" are matching with red pixel at position 1 and 2. So position matrix will store those matching bits positions. In the same way next two bits will be compared with Green pixel and next two with Blue. If there is no match found then store those secret message bits in r^th^ and (r-1) ^th^ bits of pixel.

For extraction of secret message bit position matrix is used. Position matrix will determine the location of pixels where secret message bits were embedded. Extraction is the reveres process of embedding of secret message bit.

Through the proposed technique distortions have been minimized which are caused due to replacement of pixels bits with secret information.

# 6. PROPOSED ALGORITHM

In this section, a hybrid video steganography algorithm has been proposed in the spatial domain based on combination of OPAP and Identical Match using Edge Detection technique. The proposed video steganography mechanism is divided into following four phases:

## 6.1 Secret Message Preprocessing Phase

In this Phase, a large size text file with Gurumukhi text message is used as secret message ($S_m$) file and this secret message has been is preprocessed before the embedding phase. Gurumukhi characters don't have ASCII values. Languages, other than English are represented in Unicode format. UNICODE is an international standard to represent that supports major scripts of the World. Many Indic scripts like GURUMUKHI can be easily represented in UNICODE format. For example UNICODE character representation of some character has been given in next paragraph.

0A15 ਕ GURMUKHI LETTER KA

0A16 ਖ GURMUKHI LETTER KHA

0A17 ਗ GURMUKHI LETTER GA

0A18 ਘ GURMUKHI LETTER GHA

After converting Gurumukhi font to Unicode format, the Unicode characters will be converted into binary bits. For providing high security, the binary bits are encrypted using AES-128 bit key encryption algorithm. This phase will generate a cipher text to protect the secret Gurumukhi information from intruders.

## 6.2 Edge Detection

Video file is converted into video frames. Each video frame will be processed through canny Edge Detection to divide image into edge and no edge pixel bits. Embedding Gurumukhi text message bits within a Video Cover Frame is a relatively new approach to video steganography. Edge pixels in a video cover frame produce minimum amount of distortion after embedding information bits. Edge pixels are considered as region of interest (ROI) [10] for embedding information bits as there is a sharp change in brightness level in these pixels.

## 6.3 Data Embedding Phase

In data embedding technique 1-1-1 bit approach has been deployed to conceal secret message bits which means (1-bit of RED,1-bits of Green,and 1-bit of Blue) or it can be said that 3-bits per pixel has been hidden as every pixel in a 24-bit cover frame is combination of RED,GREEN and BLUE. After canny edge detection a loop has been used to iterate through all pixels. If the pixel is Edge pixel hide 3 bits of secret Gurumukhi message will be hidden in RED, GREEN and BLUE part of pixel using LSB technique i.e. in right Least significant bit. After embedding secret message bits,pixel values will be optimized using OPAP technique to achieve minimum distortion. If the pixel of current iteratation is non-edge pixel then Gurumukhi secret message will be hidden using Identical match technique i.e. find pixel having value same as that of secret message, then store that position where it will match the secret message bits. After this whole procedure result will be a stego frame with Gurumukhi secret message embedded in it. The same procedure will be repeated for 9 other cover video frames. Fig. 3 illustrates the block diagram of this data concealing phase.

## 6.4 Data Extraction Phase

Data extraction phase is illustrated in Fig.4.The first step in extraction phase is to get the stego video and dividing it into frames through the intended receiver, and extracting whole information about video i.e. frame per second, number of frames, secret key to select random frames from RED component of every pixels of first frame. After detecting random frames, starting from first random frame, apply canny edge detection on each frame and extract the Gurumukhi secret message bits positions using position matrix hidden in each frame. Store the extracted message bits in binary matrix. After extracting all bits, apply AES-128 bit technique to get secret message from the cipher text. The Key for AES -128 is hidden in red pixels of first frame. Apply decryption procedure by getting the AES-128 bit key from the red pixels of the first frame. Apply Unicode character conversion on binary matrix by dividing whole matrix into 8-bit block in order to generate original characters of the original Gurumukhi secret message. Apply whole procedure in reverse on each random frame selected for concealing Gurumukhi secret message. At the end of this phase Gurumukhi language secret message will be received in text file.

# 7. EXPERIMENTAL RESULTS

A dataset of four different videos (AVI Video1, AVI Video2, and AVI Video3, AVI Video4) with the format of Audio Video Interleave (AVI) are used.

The results are obtained using R2010a version of MATLAB software program. All videos contain a MXN pixel resolution at F frames per second, and a data rate of P kbps. Each cover video contains N frames. In all video frames, the secret message appears as a large text file split in bits at random locations of pixels in RGB components of cover frame. Figure 1 is showing the resolution, frame rate and number of frames in all four AVI video files considered for Result analysis.

**Table 1.1 stores the details of video files used in experiment**

| Video Files | Size | Resolution | Fram e Rate | No of Frame |
|---|---|---|---|---|
| AVI_1 | 204 KB | 160X120 | 15 | 120 |
| AVI_2 | 309 MB | 400X292 | 25 | 926 |
| AVI_3 | 13.8 MB | 1280X720 | 29 | 901 |
| AVI_4 | 569 KB | 428X240 | 25 | 350 |

## 7.1 Quality Analysis

The visual quality of the proposed video steganography is evaluated in terms of Peak Signal to Noise Ration (PSNR), Mean Squared Error (MSE), Bit Error Rate (BER) and Histogram metrics. PSNR computes the distortion produced in cover frame due to embedding of secret message. It is a quality measurement metric which indicates the peak signal-to-noise ratio between cover and stego frame, defined in terms of decibels.

$$MSE = \frac{1}{MXN}\sum_{K=1}^{M}\sum_{l=1}^{N}(I_{Kl} - I'_{kl}))^2 \qquad (1)$$

$$PSNR = 10\log\frac{255}{MSE} \qquad (2)$$

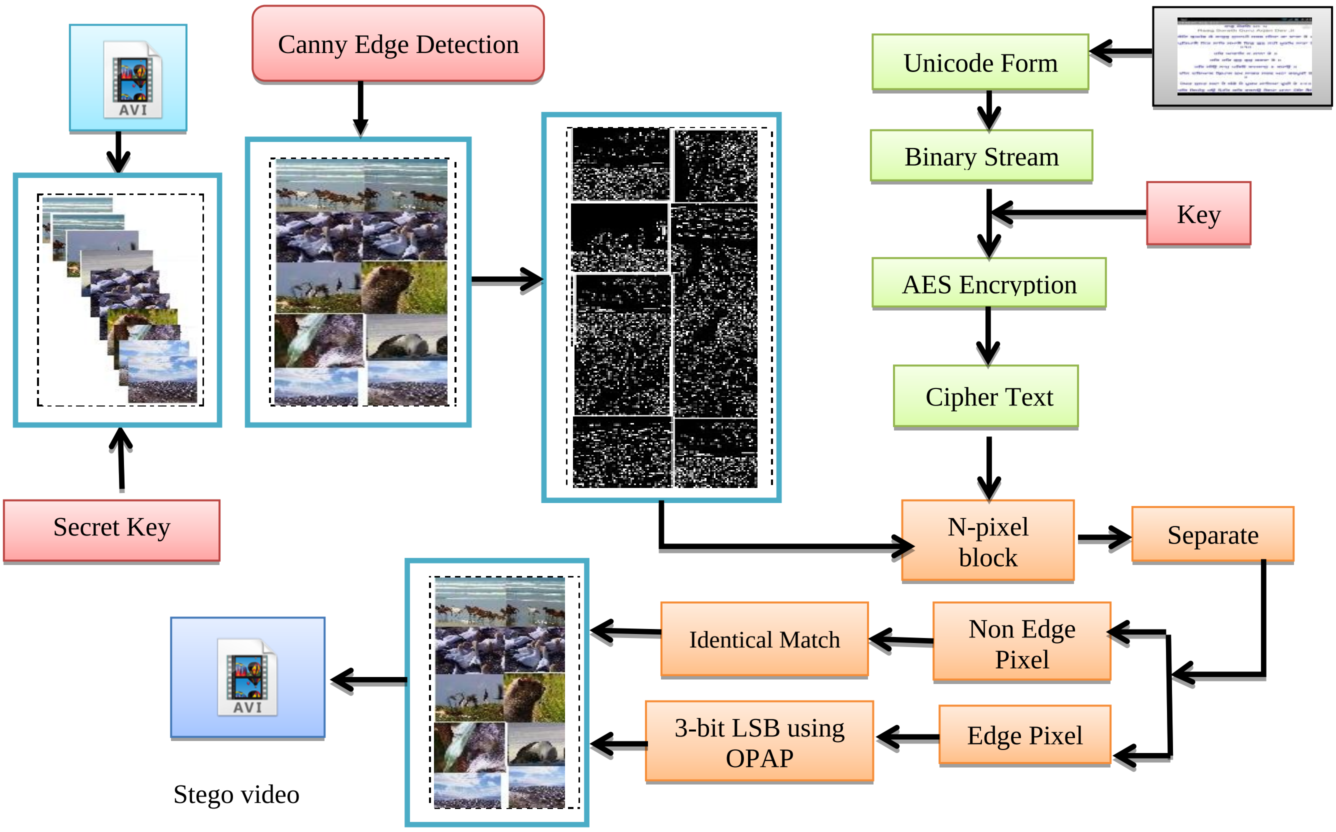

**Fig. 3 Data Embedding Procedure**

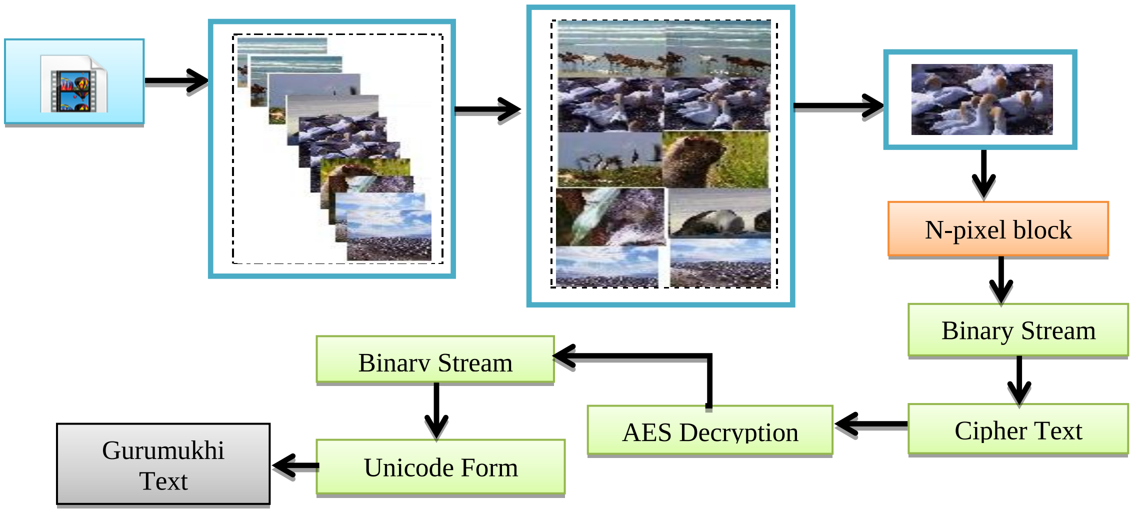

**Fig.4 Data Extraction Procedure**

Where M and N denotes the pixel dimensions of different video cover frames $I_{kl}$ denotes the original cover frame and $I'_{kl}$ denotes the stego frame. In equation (2) 255 indicates the maximum value of a 24 bit colored pixel. PSNR is indirectly proportional to quality distortion. Higher the value of PSNR lesser wills the distortion in cover frame and vice versa. In Figure 1 it is clearly indicated that in selected videos the PSNR value of proposed approach is better than LSB technique. In AVI Video File 1 the PSNR difference of proposed technique and LSB technique is 11.8133dB which is very high.

PSNR results in have shown improvement in LSB technique through proposed technique as shown in graph in Fig.5. MSE (mean squared error) gives the pixel value differences between original and stego cover frame as displayed in Fig. 6.

High mean squared error indicates the high distortions which are visible to human visual system. The embedding capacity was 8172 bytes for a cover frame of MXN size and maximum embedding was 8172X8=65376 bits which indicates very high payload. With tri-layer security, 8172X8 bits can be hidden in cover frame.

Bit error rate (BER) indicates the ratio of error bits per unit time in a given cover frame. Bit error can be defined as the ratio of number of bits with changed values to the total number of bits in a pixel. For example assume a pixel has following value:[0 1 1 0 0 0 1 0 1 1] and the pixel value after embedding secret message bits is [0 0 1 0 1 0 1 0 0 1] .The number of changed bit or errors bits is in this case is 3.So Bit Error rate is 0.3 or 30%. The Bit error rate graph of proposed technique and LSB approach have been shown in the Fig. 7,which represents clearly that the proposed technique has low Bit error rate as compared to least significant approach i.e. the stego frames contains less number of error bits as compared to LSB approach.

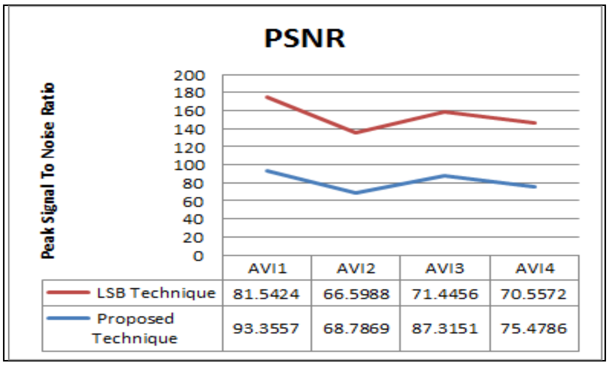

**Fig.5 Peak Signal to Noise Ratio Comparison of video files**

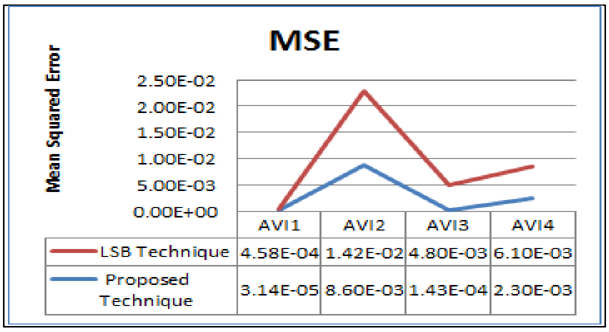

**Fig.6 Mean Squared Error Comparison of video files**

## 7.2 Embedding Payload

The proposed video steganography algorithm has a high embedding capacity according to the reference [12]. Experimental results have been done using 10000 bytes i.e. 80000 bits. Proposed technique has very high capacity as MSE value for proposed technique is 0.00032 which is very low as compared to [5].The average value of MSE and PSNR values Fig. 8 shows Histogram representation of original and stegoframe. Histogram Error shows the distribution of intensities in a colored image i.e. 24 bit pixels image. Using Histogram Error various graphs can be plotted by making a histogram plot that represents the number of pixels with different ranges as shown in Figure. Histogram error shows the similarity or level of distortion in cover frame and stego frame. More is the similarity between plots lesser will be the error. Fig. 8, Fig. 9 Fig. 10 shows the histogram plots of one frame from AVI video file 1, 2, 3. It is clear from the graphical representation that the proposed technique has made less distortion in cover frame which are almost negligible. Proposed technique has provided enhanced results in terms of MSE i.e. least distortion in stego frame. The averagehas also been compared with [12] which clearly indicates better results as compared to Adaptive random and OPAP approach in terms of MSE and PSNR values as compared to DWT Domain technique [13], [10], [11], [9] with improved PSNR (more than 70dB) and BER (0.0012 to 0.0042).

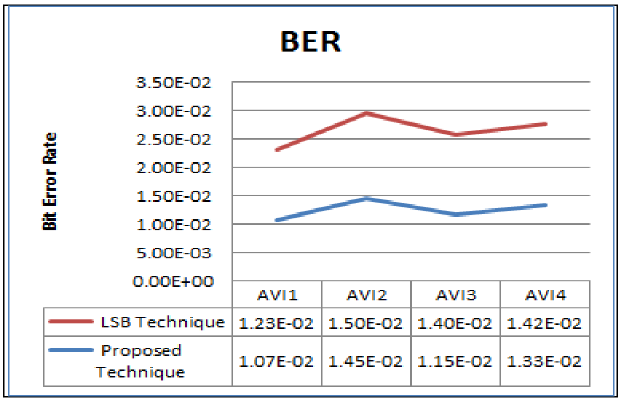

**Fig.7 Bit Error Rate Comparison of Video Files**

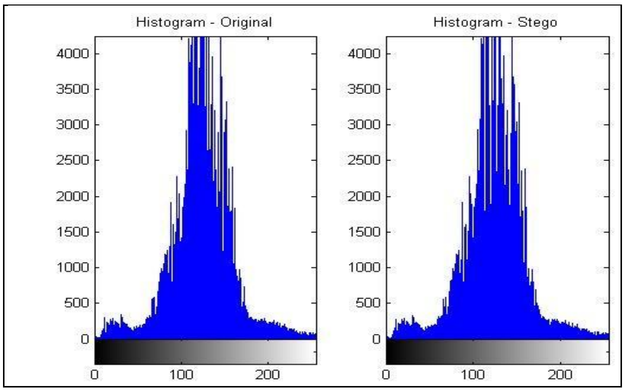

**Fig.8 Histogram plot of one frame of AVI Video File 1**

Security has also been enhanced as compared to [7] techniques. Maximum payload in proposed technique can be 1280X720X3 =30412800 bits which is very high value.

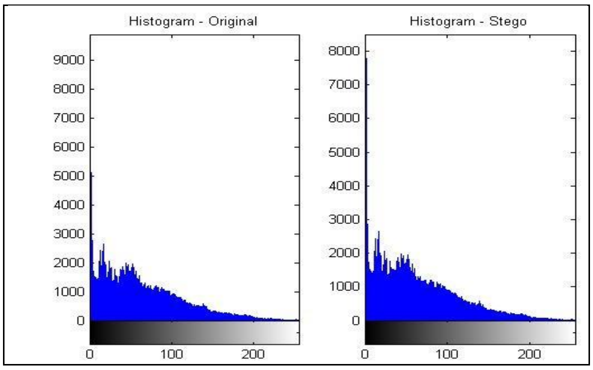

**Fig.9 Histogram plot of one frame of AVI Video file 2**

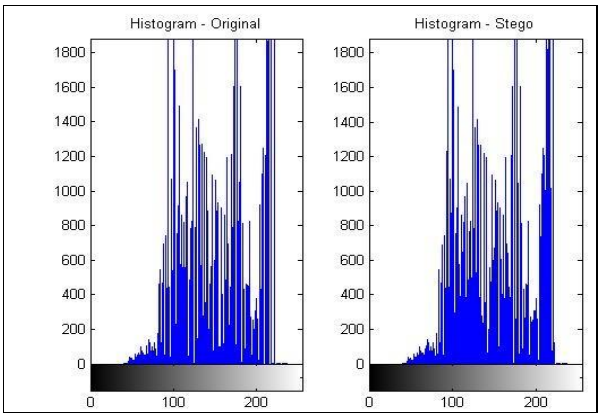

**Fig.10 Histogram plot of one frame of AVI video file 3**

## 8. CONCLUSION

In this paper, an enhanced steganography algorithm has been proposed by exploiting spatial temporal domain to hide Gurumukhi secret message inside a cover AVI Video file using modified LSB approach. The Proposed technique has different phases. First phase is the convert Gurumukhi text message to UNICODE form and then conversion of UNICODE to Cipher text using AES 128 bit encryption algorithm. In second phase canny edge detection has been applied on 10 random frames selected using a secret key to differentiate between edge and non-edge pixels. Random frame selection using secret key has provided tri layer security layer to this steganography approach. The third phase was to embed secret information to hide data on edge pixels using OPAP and at non edge pixels using Identical match approach. Identical match and OPAP techniques provides least distortion in cover frames which are leading to high quality cover frame with high PSNR values and least mean squared error and least bit error rate. Due to combination of LSB approach, OPAP and Identical match the payload capacity is very high in proposed technique. The secret message bits are embedded in RED, GREEN and BLUE pixels of random frames. Distortion in these colors is not visible to Human Visual System (HVS) as clearly indicated in Histogram plots of frames. The performance of the proposed video steganography algorithm is verified through a series of experiments using four AVI VIDEO files. Experimental results have proved that the proposed approach has a high payload and with high imperceptibility, high security and least distortions in terms of MSE and BER. Our future work will verify the robustness of our proposed algorithm against various attacks such as video processing using steganalysis.

## 9. REFERENCES

[1] Sadek, M. M. Khalifa, S. Amal, G. M. Mostafa, “Video Steganography: a comprehensive review,” multimedia tools and applications, No.17 Vol.74, 2015, pp. 7063-7094.

[2] H.H.Soliman, H.E.Mostafa, E.A.E. Ahmed, “A Novel Algorithm for Hiding Information in Video using Spatial Domain,” Egyptian Computer Science Journal, 2014, No. 3,Vol .38, 2014, pp. 1-9.

[3] R. J. Mustafa and C. Bach, “Video Steganography: A Survey,” in IOSR Journal of Computer Engineering (IOSR-JCE) Issue 1, Vol.18, 2015, pp.11-17.

[4] Mansouri, J.Khademi, Morteza, “International Journal of Imaging Systems and Technology,” in International Journal of Imaging Systems and Technology, No.4, Vol.19, 2009, pp. 306-315.

[5] Hong,W.Chen,T.Shou, “A Novel data embedding method using adaptive pixel pair matching,” in Information Forensics and Security,IEEE Transactions, No.1,Vol.7, 2012, pp. 176-184.

[6] Z. Rongyue, et al., “A Novel Video Steganography Based on Non-uniform Rectangular Partitions,” Computational Science and Engineering (CSE), 2011 IEEE 14th International Conference on, Dailan, Liaoning, pp. 57-61, 2011.

[7] Chen, W. J. Chang, C. C. Le, T.H. Ngan.,“High payload steganography mechanism using hybrid edge detector,” Expert Systems with applications, No.4, vol. 37, pp. 3292-3301, 2010.

[8] Dasgupta et.al. “Optimized Video Steganography Using Genetic Algorithm (GA),” Procedia Technology, vol. 10, 2013, pp.131-137.

[9] Yuanzhi Yao,Weiming Zhang-Nenghai Yu-Xianfeng Zhao, “ Defining embedding distortions for motion vector-based video steganography,” in Multimedia Tools and Applications, October 01- 05, 2015,pp.11163-11186.

[10] Po-Chyi Su, Ming-Tse Lu, Ching-Yu Wu, “A practical design of high-volume steganography in digital video files,” Multimedia tools and applications, No.2, Vol.66, 2013, pp.247-266.

[11] B. D. Lucas and T. Kanade, “A High Payload Video Steganography Algorithm in DWT Domain Based on BCH Codes (15, 11),” in 2015 Wireless Telecommunication Symposium (WTS), at New York, 2015, pp. 1-8.

[12] A.R .Rayappan, J.B. Balaguru, “An intelligent chaotic embedding approach to enhance stego-image quality,” Information Sciences, Vol.193, 2012, pp. 115-124.

[13] L. Guo-Shiang and T. Tung-Sheng, “New Approaches to en encryption and steganography for digital videos,” in Multimedia Systems, No. 3, Vol.13, 2007,pp.191-204.