Video Steganography Based on Linked hopping and preprocessing frame

Pranav S. Raut, Dhanashree S. Phulkar, Sourabh S. Pukale and Kiran Kamble,

Department of Computer Science and Engineering,
Walchand College of Engineering, Sangli, Maharashtra, India

pranavr7700@gmail.com,
dphulkar@gmail.com,
souravp7777@gmail.com,
kirankamble5065@gmail.com

Abstract. Data Security has emerged to be the utmost priority in recent decades. To send data from one place to another place securely, different techniques have been proposed. One of them is Video steganography, it is an art of hiding information inside the video by manipulating pixels of the frame. In this paper we have provided a steganography algorithm based on linking of text inside the frame and preprocessing the frame to reduce the alteration of original data by finding if some pixel already has that data, then maintaining a link to that pixel and if failed to find the required pixel, replacing the pixel with the minimum of absolute difference between both the pixels. Link is maintained by hiding the x, y co-ordinates in the vicinity of the previous frame data found. The PSNR value obtained by this approach is about 71. The obtained PSNR value has been compared with various techniques and the results have been encouraging.

Keywords: Video Steganography; Cryptography; Lease Significant Bit (LSB); Linked Hopping;

1 Introduction

The increase in the interest of the sleuths in the important data being transferred over the communication network demands the increase in security of that data. Information Security regarding the military of the country is of the utmost priority for any country. This information needs to be transferred over the communication network in a disguised way which should bypass every snoop waiting to fetch the data in between.

Steganography is the art of sending hidden messages in a particular way that no one can apart from the sender and the receiver suspects the existence of a message. The word steganography literally means covered writing as derived from Greek **[3]**. Image Steganography is the process in which we store an important text that we want to send in the pixel

values in the image by overriding the original pixel value of the image. It was considered to be one of the secured ways to send data in the early 2000's but as the time passed cracking of the data from the image became easy as we have to process only one frame, which led to the beginning of Video Steganography. Video Steganography explains a way of disguising the important data behind a carrier Video. Cryptography prevents an unauthorized intruder to recognize the information by transforming the information to a not understandable form.
Here in Video Steganography we have two parts.

1. Message: The data to be send to the opposite end.
2. Cover Video: The video in which we have to hide the data.

Video Steganography along with Cryptography can be used to provide better results. As the quality of video increases the amount of the redundant bits where the data can be hidden increases **[1].**
Applications of Video Steganography vary from military, industrial applications to copyright etc. **[1]**.There are many problems in the existing systems such as the size of the video increases **[3]**. The Peak to Signal Noise Ratio is less The Security is increased by first compressing the information to be hidden in a lossless format proceeding with proper encryption and then hiding the data in the carrier video.
Section 2 describes previous work with respect to video steganography, Section 3 elaborates about the algorithm being proposed, Section 4 shows the results obtained by the algorithm, Section 5 compares the PSNR values and gives the conclusion and section 6 mentions thereferences.

2 Literature Review

There have been many interesting and efficient algorithms proposed earlier for video steganography.

Munasinghe **[3]** proposed a method for video steganography in which Least Significant Bit of each byte of cover file is changed. This method does not increase the size of the video. But the security provided is very low. This is the basic approach to video steganography.
Sudeepa K **[2]** proposed a method which uses encryption first toprovide an additional level of security and also exploits the property of randomization and parallelization. But the technique to hide the data remains the same.

Koushik Dasgupta **[1]** proposed a Hash based Least Significant Bit (HLSB) technique. A spatial domain technique where the secret information is embedded in the LSB of the cover frames. Eight bits of the secret information is divided into 3, 3, and 2 and embedded into the RGB pixel values of the cover frames respectively. A hash function is used to select the position of insertion in LSB bits. This method has only been proposed for .avi files. Embedding is done directly without any preprocessing.

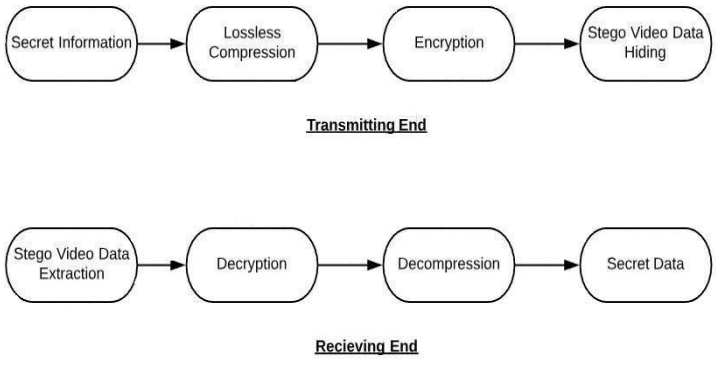
Pooja Yadav **[4]** proposed a technique where each frame of secret video will be broken into individual components then converted into 8-bit binary values, and encrypted using XOR with secret key and encrypted frames will be hidden in the least significant bit of each frames using sequential encoding of Cover video. Each bit of secret frames will be stored in cover frames following a pattern BGRRGBGR. But the sum of absolute difference was not the less.

Nirmalya Kaur **[5]** suggested the video steganography technique using linear congruential generator (LCG) and chaotic map. LCG and chaotic maps helps to keep the data in randomized order which helps to increase security of data. This produces good results but still no preprocessing is done which results in increase of sum of absolute difference.

Jasleen Kour **[9]** reviewed the different security and data hiding techniques that are used to implement a steganography such as LSB, ISB, and MLSB etc. in the research paper.

Bharti Chandel **[10]** analyzed fundamental concepts, performance metrics and security aspects of video steganography. Different methods used for protecting secret information by using a video as cover media are explored. Comparisons between different video steganography techniques are also provided.

3 Proposed System



This section proposes an algorithm for video steganography based on linked hopping and preprocessing. The proposed algorithm takes a binary string of encrypted information and carrier video as input. The algorithm is divided in 5 stages:

Algorithm:

1) Selection of order of frames in which data is to be embedded.
2) Calculate the initial seed value using a polynomial equation.
3) Find next Coordinates by fetching data from 12 bits each from one pixel in right and upward direction corresponding to X and Y coordinate respectively.
4) Go to previous frame and embed the position of data hidden.
5) Calculate number of hops for next character of secret key and go to step iii, till all characters are to be hidden.

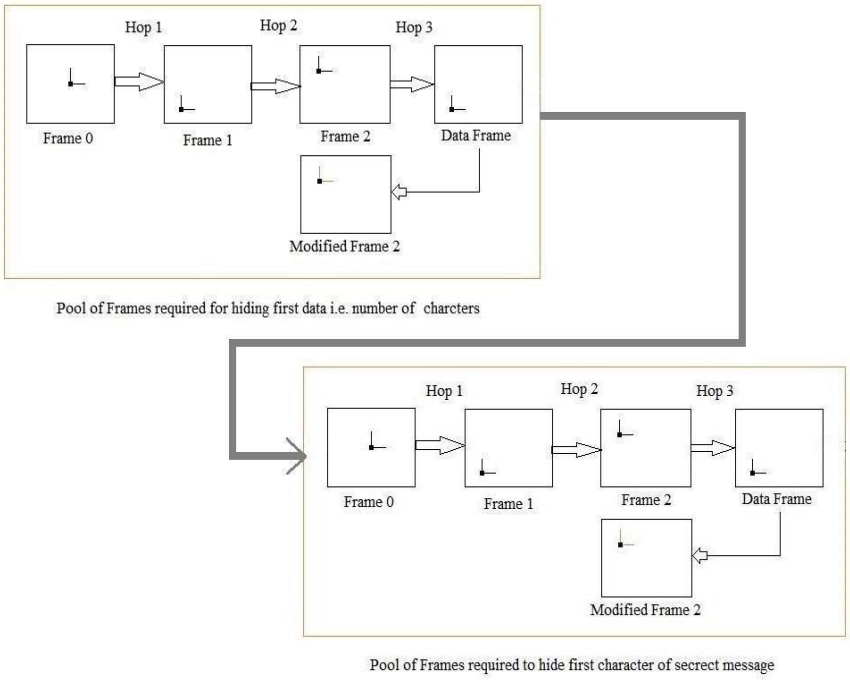


Figure explains the working of the algorithm proposed.

The detailed algorithm is as follows:

3.1 Selection of Frames

In this stage we use any polynomial equation to choose the frames in which the data has to be embedded. Polynomial expression should be known to transmitter and receiver side in order to receive the data with no noise.

Considering polynomial equation,

$$\boldsymbol{seed = a * seed + b} \quad \textbf{(1)}$$

Here a, b are constants and seed is the value that determines the frame number to be chosen for data hiding. The frame value will be,

$$\boldsymbol{seed} \,\%\, \boldsymbol{M} \quad \textbf{(2)}$$

Where M = number of frames in the video.

Seed can be passed as a key but we propose to calculate the seed value by adding all the pixel values of the first frame we get in the video by our expression and taking mod of the value with a prime number. This reduces the overhead of passing an extra key to the receiver. The frame being chosen is distinct as the secret data may get overwritten.

3.2 Finding first pixel

The data to be hidden is in 8 bits in one frame. The first value of the pixel in the second frame by polynomial equation is fixed. In this frame the length of information to be sent is hidden. The data is divided in 3 parts of length 3-3-2. The pixel value with R, G, and B values matching with required data to be hidden is found i.e. the pixel with values of R being ended with the required 3 bits in the last, 3 bits of G and 2 bits of B is searched in the frame. If we don't get the pixel with the required value, the pixel having minimum absolute difference with data value to be hidden. The x, y co-ordinate value of this pixel is stored in an auxiliary storage by maintain the order.

3.3 Next pixel to be chosen

The data at the current pixel is fetched, values of R, G and B are summed up. This sum modulo a prime number gives us the number of hops we need to take to store the next data value. If the number of hops is 3 we have to skip 3 frames generated by the equation. But we do not blindly skip the frames. The next pixel value in the proceeding frame is taken from the 12 bits in the y-axis above the current data. The 12 bits above in the vertical direction gives the y co-ordinate of the next pixel in the next frame. Similarly the x co-ordinate is stored horizontally (towards right) of the current pixel in 12 bits, in the last bit i.e. 1 bit per pixel. If the row or column number goes out of bound it has to be circularly linked to go to the first column or row in the frame. After the hops are over and we arrive at the frame where we have to store data. We search for the pixel value matching with our data and store the x, y co-ordinates in the auxiliary storage.

3.4 Embed data position in previous frame

Repeat the traversal of the frames in the same order as before, and before every data frame i.e. last frame before data frame embed the x, y co-ordinate of the next pixel in the current pixel vicinity.

3.5 Retrieve the data

Traverse the frames in the same order as per the polynomial equation and the seed given by the first frame, the data value itself represents the number of hops when we mod it with fixed prime number. So we can get the data by first fetching the data followed by the hops which is again followed by data, this continues till we get the required length of data.

4 Result and Analysis

Performance Metrics:

(As per mentioned in [8])

1. MSE

MSE stands for Mean Squared Error and it is calculated by the comparison of the stego file and cover file with each of the bytes. We have the following equation to calculate MSE value.

$$\mathrm{MSE} = \frac{1}{(m * n)} * \sum_{i=1}^{m} \sum_{j=1}^{n} (\mathrm{Xij} - \mathrm{Yij})^2$$

Where, m = Width of the frame and n = height of the frame

The MSE value is calculated for each modified frame and average is noted for value of MSE for stego video.

2. PSNR

PSNR is the parameter of the video file that means Peak Signal to Noise Ratio. PSNR and MSE both are inversely proportional to each other and PSNR can be measured by the following equation.

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

Where, R is the maximum fluctuation in the input image data type.

3. RMSE

RMSE is a parameter that means Root Means Square Error which is calculated as the square root of MSE.

Table: The values of PSNR after inserting text information

Video Format	PSNR	MSE	RMSE
1. Mp4	71.1886	0.004946	0.07032
2. Avi	70.8144	0.005395	0.07345
3. Mov	71.0971	0.005051	0.07107
4. MPG	70.8733	0.005318	0.07292

All the values are computed for secret Message of variable lengths on different video formats covering all characters such as alphabets, numbers, whitespaces, special characters, etc. Different video formats of same video file is considered for calculating PSNR, MSE and RMSE values.

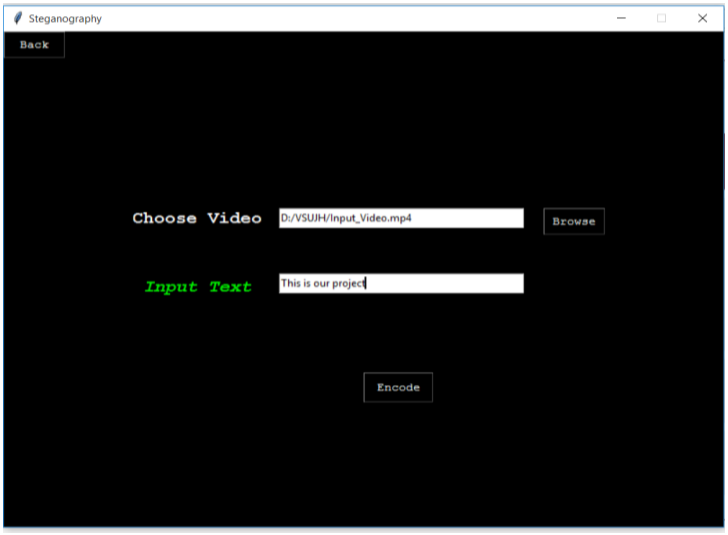
5 Conclusion

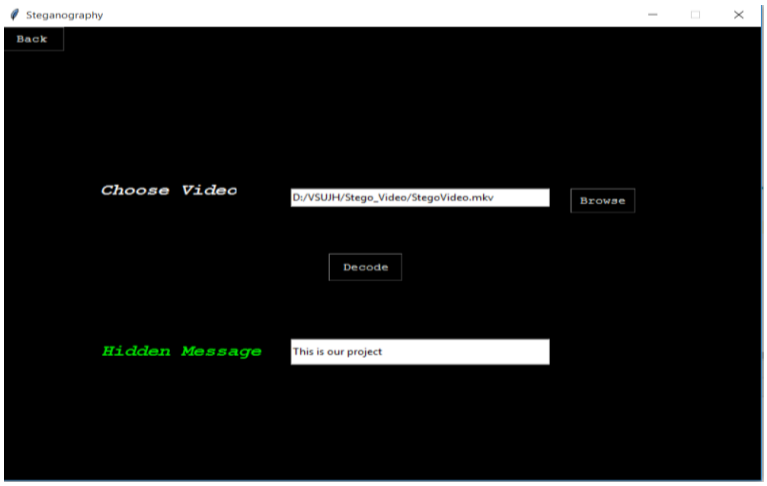
In this paper an algorithm for video steganography is put forth that use Hash based LSB along with linked hopping by saving distances in the vicinity of the last frame. The Security level is been increased by minimum altering the data, the sum of absolute difference for data values is the minimum. Even if we have a considerable minimum sum

of absolute difference for co-ordinate position. It is very less as only 24 bits are being altered i.e. 1 bit per pixel so the maximum absolute difference in the frames cannot increase more than 1 bit. Additionally the alternating hops and data make it difficult to recognize between data frame and hop frame.

Video Steganography using linked hoping and preprocessing frames is successful in reducing Mean Squared Error and increasing PSNR values. As per mentioned in Paper [1], average value of PSNR and MSE found using LSB technique is 48.56, 0.34 respectively. And the average values of PSNR and MSE obtained by Linked hoping and Preprocessing frames is 70.9933, 0.0051775 respectively.

Video Steganography using Linked hoping and Preprocessing frames can be applied to many file formats such as mp4, avi, mov, mpg, mkv, etc.





The above images show the project implemented by following the approach of video steganography by linked hopping and preprocessing frame.

6 References

[1] Koushik Dasgupta, J.K Mandal and Parmartha Dutta "Hash based least significant bit technique for video steganography" (HLSB), International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012

[2] Sudeepa K B, Raju K, Ranjan Kumar H. S. and Ganesh Aithal. **"**A New Approach for Video Steganography Based on Randomization and Parallelization". International Conference on Information Security and Privacy (ICISP) December 2015, Nagpur, India

[3] A. Munasinghe, Anuja Dharmaratne and Kasun De Zoysa, "Video Steganography", 2013 International Conference on Advances in ICT for Emerging Regions (ICTer), 2013,p.56-59.

[4] Pooja Yadav, Nishchol Mishra and Sanjeev Sharma, "A Secure Video Steganography with Encryption based on LSB Technique", IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2013

[5] Nirmalya Kar, Kaushik Mandal and Baby Bhattacharya "Improved chaos-based video steganography using DNA alphabets", The Korean Insitute of Communications Information Sciences, 2018

[6] Kunal Hossain and Ranjan Parekh, "An Approach towards Image", 2016 Second International Conference in Computational Intelligence and Communication Networks

[7] Kamred Udham Singh, "Text Hiding in Video by LSB Substitution", Kamred Udham Singh Int. Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 4, Issue 5 (Version 1), May 2014, pp.105-108

[8] Anamika Saini, Kamaldeep Joshi, Kirti Sharma and Rainu Nandal, "An Analysis of LSB Technique in Video Steganography using PSNR and MSE" , International Journal of Advanced Research in Computer Science, May-June 2017

[9] Jasleen Kour and Deepankar Verma, "Steganography Techniques A Review Paper", International Journal of Emerging Research in Management &Technology, Volume-3, Issue-5, May 2014

[10] Bharti Chandel and Shaily Jain, "Video Steganography: A Survey", IOSR Journal of Computer Engineering, Volume-18, Issue-1, Jan – Feb. 2016