# AN APPROACH TO HIDE DATA IN VIDEO USING STEGANOGRAPHY

**Deepak Kumar Sharma[1], AsthaGautam[2]**

[1]*Student, School of Computer Science &Engineering, Bahra University, Himachal Pradesh, India*
[2]*Student, School of Computer Science &Engineering, Bahra University, Himachal Pradesh, India*

## Abstract

*In this paper, we have proposed a new video steganographic algorithm that is used to hide any sort of data or information inside the video with the help of hash function technique. A video steganography is an approach to hide the data inside the video. In general, video is a set of moving frames, so we here are selecting a frame and then applying a hash function technique to choose a pixel for the purpose to hide the information. A double hash function technique is used to select the pixel from row and column. It might happen that the pixel after applying hash function may not found in the frame, this type of problem can occur, so a collision resolution technique is used. A quadratic probing technique is used for solving the problem of collision where we are adding a prime number with the existing hash value instead of linear search. A division method technique is used to point out the pixel in a frame that is pixel's location in row and column in a frame. When pixel is found, the character of information that is to hide, a binary value of that single character is replaced by original pixel's red component, then second frame is to select and second character's binary value is replaced by the original pixel's green component, this will continue until the all binary characters of the information are hidden.*

***Keywords:*** *Collision, Embedding, Extraction, Video Frame, Steganography.*

----------***----------

## 1. INTRODUCTION

Steganography is the art and science of hiding information by embedding messages within other. Steganography is made up of Greek words "stegno" and "graphie". Here stegno means "covered or protected" and graphie means "writing". Steganography is the art or practice of concealing a message, image or within another message, image or files [1].

Early steganography was messy. Before phones, before mail, before horses, messages were sent on foot. If you wanted to hide a message, you had two choices: have the messenger memorize it, or hide it on the messenger. In fact, the Chinese wrote messages on silk and encased them in balls of wax. The wax ball, "la wan," could then be hidden in the messenger.

Some steganographic methods also use steganography with cryptography where sender encrypts the message and receiver decrypts the message to get original message. This technique is used to prevent the message from the intruders [9].

The primary objective of steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this objective that has been planned to achieve the security of the secret message because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message[7][8].

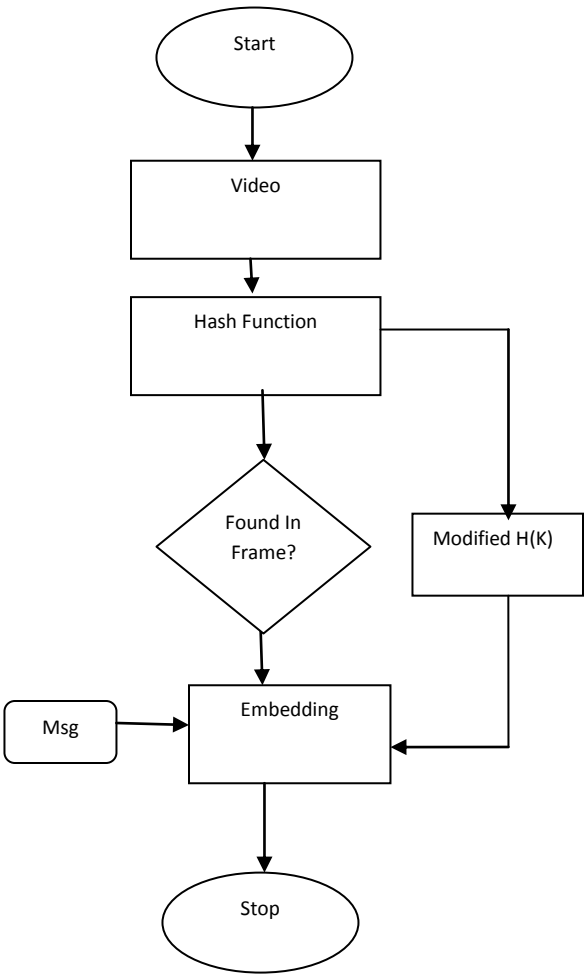
## 2. VIDEO STEGANOGRAPHY

It is a technique to hide any kind of files into a carrying video file. The use of the video based steganography can be more eligible than other multimedia files because of its size and memory requirements.

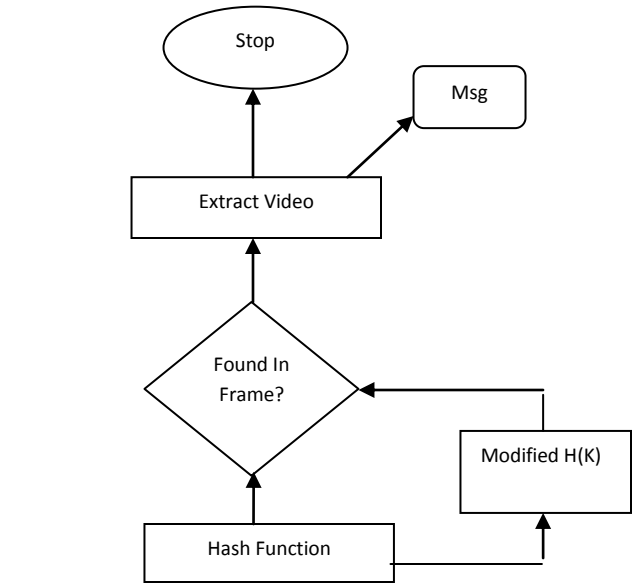
Videos are the set of images. Video is an electronic medium for the recording, copying and broadcasting of moving visual images. The number of still pictures per unit of time of video ranges from six to eight frames per second [1] It is 120 or more frames per second for new professional camera [3]. Aspect ratio describes the dimensions of video screen and video picture elements. All popular video formats are rectilinear and so can be described by a ratio between width and height [6].

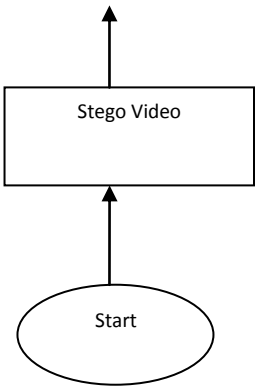
## 3. FLOW CHART OF VIDEO STEGANOGRAPHY:

### 3.1 Encryption:




### 3.2 Decryption:




## 4. PROPOSED ALGORITHM

The algorithm of video steganography is based on the fact that each pixel is represented by 3 bytes where each byte representing the intensity of 3 primary colors that is RGB (Red, Green and Blue).Size of image file is directly related to number of pixels and granularity of color definition[11].

Let the data to be hidden is word "ABC"
ASCII code of A=65
Binary code of A= 01000001
ASCII code of B = 66
Binary code of B = 01000010
ASCII code of C = 67
Binary Code of C = 01000011

Let the first pixel's RGB component be:

| RED | | | | | | | | GREEN | | | | | | | | BLUE | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |

Red component of pixel is replaced by binary values of 65 i.e A

| RED | | | | | | | | GREEN | | | | | | | | BLUE | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |

Let the second pixel's RGB component be:

| RED | | | | | | | | GREEN | | | | | | | | BLUE | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |

Green component of pixel is replaced by binary value of 66 i.e B

| RED | | | | | | | | GREEN | | | | | | | | BLUE | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |

Let the third pixel's RGB component be:

| RED | | | | | | | | GREEN | | | | | | | | BLUE | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |

Blue component of pixel is replaced with binary value of 67i.e C

| RED | | | | | | | | GREEN | | | | | | | | BLUE | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |

The resulted image pixel contains the text bits

Now one image contains a text bit.

As we know that video is a set of images, So we can hidemore number of data in other images that is consisted by video.After replacing the bits from one imageweincrement to the next video frame or image and again applying the same procedure of bits replacing operation.

## 5. CHOOSING THE PIXEL IN IMAGE TO REPLACE IN VIDEO

We here are using hash function to choose the pixel in image. The terminology which we are using in hashing will be oriented towards file management.

A hash function[4] is any algorithm that maps data of arbitrary length to data of a fixed length. The values returned by a hash function are called hash values, hash codes, hash sums, checksums or simply hashes.

We are considering 2 assumptions:

- First of all we are assuming that there is a file F of n records with a set K of keys which uniquely determine the records in F.
- Secondly, we are assuming that F is maintained in memory by a table T of m memory locations and that L is the set of memory address of the location T.

For notational convenience we have assumed that the key in K and address in L are integers.

The general idea of using the key is to determine the address of a record is an excellent idea but it must be modified so that a great deal of space is not wasted. This modification takes the form of a function H from the set K of keys into the set L of memory addresses.

Such a function H : K→L is called hash function or hashing function.

Unfortunately, such a function H may not yield distinct values, it is possible that two different keys K1 and K2 willnot be able to yield the appropriate hash address for resolving this problem we are using Quadratic probing of Collision Resolution Technique. If the resultant pixel is not found in frame then the value of H(K) is modified to K.

### 5.1 Quadratic Probing Technique:

Suppose a record R with key K has the hash address H(K)=h. then instead of searching the location with address h, h+1,h+2…… so on we linearly search the address location.
H(K) = H(K) + Prime number.

The two principle criteria used in selecting a hash function are:
Firstof all, the function H should be very easy and quick to compute.
Second, the function H should as far as possible uniformly distributes the hash addresses throughout the sat L so that there is minimum number of collisions.

Let, K=256and m=7

Then, H(256)=256(mod 7)
H(256)=4

So replace the 4th pixel from top of the frame.

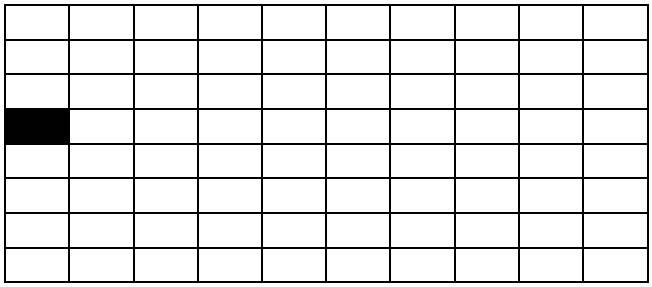


**Fig 1** Frame with selected 4th pixel

To make the change of pixel more efficient andunidentifiable we used two hash functions. One function isto choose from row and 2nd is to choose from column.

Two hash functions are:

- H(K)=K(mod m)
- H(L)=L(mod n)

Let K=256 and m=7

H(256)=256(mod 7)=4
Let L=118 and n=3

H(118) = 118(mod 3)=1

So, from 4th row we choose 1st column pixel to replace or to Implement algorithm.

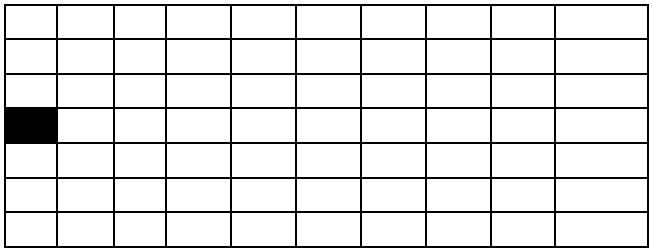


**Fig 2** Frame with selected 4th pixel by two hash function

## 6. Technique of hash Function

### 6.1 Division Method

Choose a number larger than the number n of keys in K.Hash function H is defined as :

$$H(K)=K(\text{mod } m)$$

Or

$$H(K)=K(\text{mod } m)+1$$

Where, K is a key and the value of K lie between image frame size (width or length) and m is any prime no.

## 7. EMBEDDING TECHNIQUE ON SENDER END

### 7.1 Encryption:

1) Begin
2) Select a text file to hide
3) Convert a text into binary form and calculate the number of bits in it
4) Select a video file for hiding purpose
5) Start sub iteration 1 until all frames covered
6) s = Calculating the number of frames in video
   = Rate of video frame(25fps) * Time length of video
7) For (i=1; i<=s; i++)
8) {
9) H(K) = 71(mod i)[for rows]
10) H(L) = 89(mod i)[for columns]
11) }
12) If ((H(K) || H(L) = 0) || (H(K),H(L))= NOT FOUND IN FRAME)
13) {
14) H(K) = H(K) +7
15) H(L) = H(L) + 13
16) }
17) Replaced Red component bit of pixel with 1st character
18) Replaced Green component bit of pixel with 2nd character
19) Replaced Blue component bit of pixel with 3rd character.
20)}

If video is of 4 minutes and of frame rate 25 frames per second then it means that 4 min video is equal to 240 second video which implies that it is having 25*240 framesthat is equal to 5100 frames, and we can replace 5100 frames pixel with 5100 characters

### 7.2 Decryption

1) Select the stego video
2) Start iteration until frames end
3) s= number of frames
4) For( i=1;i<=s; i++)
5) {
6) H(K) = 71(mod i)[for row]
7) H(L) = 89 (mod i)[for columns]
8) }
9) If ((H(K)|| H(L))=0 || (H(K),H(L))=not found in frame)
10) {
11) Collision resolution technique
12) H(K)=H(K)+7
13) H(L)=H(L)+13
14) }
15) Convert binary RGB bit value into ASCII and character values
16) }

## 8. CONCLUSIONS

As frame rate of video is 25 frames per second human eyeis not able to visualize any sort of alteration in a single pixel. Thus video steganography is a good technique to hide the data.

**Frame 1**
Pixel to choose in a frame to store 1st 3 characters that is 24 bits from text file

$$H(K1) = K(\text{mod } m1)$$

$$H(L1) = L(\text{mod } n1)$$

(H(K1), H(L1)) pixel

Replace (H(K1), H(L1)) pixel with 3 characters

Next

**Frame 2**
Choose pixel in a frame to store next 3 characters of text file that is 24 bits

$$H(K2) = K2 \text{ (mod } m2)$$

$$H(L2) = L2 \text{ (mod } n2)$$

(H(K2), H(L2)) pixels

Repeat till all the frames are used
As

Video length = 4 minutes
= 4*60 sec
=240 sec

Frame rate of video = 4 minutes

Total frame rate in a video is 25 * 240 frames = 5100 frames
Each frame consisting 3 characters.

No. of characters that we can hide in a video is 5100*3 characters= 15300 characters.

## FUTURE ASPECTS

We will implement this algorithm with the help of diffiehellman algorithm for embedding data bit into pixel bit. Further we are concerned with increasing the characters in video too. With the help of the concept or interpolation we will match the stego pixel with the original one.

## REFERENCES

[1]. en.wikipedia.org/wiki/steganography
[2]. strangehorizons.com
[3]. TayVoughan, Seventh edition, Multemedia: Making It Work, Tata McGraw Hill.
[4]. Seymour Lipschutz. 1st Edition, Data Structures, The McGrawHill, Schaum,sOutlins.
[5]. Vipul Sharma, Sunny Kumar, A New Approach To Hide Text In Images Using Steganography.
[6]. www.red.com/learn/red-101/video-aspect-ratios
[7]. H. Wu, H. Wang, C. Tsai and C. Wang, Reversible image steganographic scheme via predictive coding. 1 (2010), ISSN: 01419382, 35-43.
[8]. J, Corporation, Steganography. http://www.webopedia.com/ TERM/S/steganography.html. 2005.
[9]. A.A.Zaidan, B.B.Zaidan, AnasMajeed, "High Securing Cover-File ofHidden Data Using Statistical Technique and AES EncryptionAlgorithm", World Academy of Science Engineering and Technology(WASET), Vol.54, ISSN: 2070-3724, P.P 468-479.
[10].www.strngehorizons.com/2001/20011008,steganograhy.shtml#stools
[11] www.garykessler.net/library/steganography.html

## BIOGRAPHIES

Deepak Kumar Sharma, Mtech Student, Bahra University, Shimla Hills, Himachal Pradesh, Deepaksharma1810@live.com

AsthaGautam, Mtech Student, Bahra University, Shimla Hills, Himachal Pradesh, Gautam.aastha1@gmail.com