VIDEO STEGANOGRAPHY USING LSB TECHNIQUE BY UNIQUE FRAME SELECTION METHOD TO INCREASE THE SECURITY

Project submitted in partial fulfilment of the requirement for the degree of Bachelor of Science In Computer Science

Under the Guidance of

Bibek Ranjan Ghosh

By

ANISH SI (6CMSA16R007)

SOUMYADEEP BANIK (6CMSA16R008)

Department of Computer Science

Ramakrishna Mission Residential College (Autonomous), Narendrapur

University of Calcutta

ACKNOWLEDGEMENT

We have immense pleasure in expressing our sincerest and deepest sense of gratitude towards our guide Prof. for the assistance, valuable guidance and co-operation in carrying out this Project successfully. We have developed this project with the help of the Faculty members of our department and we are extremely grateful to all of them. We also take this opportunity to thank Head of the Department Prof. Siddhartha Banerjee, and Principal of Ramakrishna Mission Residential College (Autonomous), Narendrapur, Swami Bhudevananda Maharaj for providing the required facilities in completing this project. We also like to thank our lab assistant Shree Shyama Prosad Chakraborty for assisting us in the lab whenever we needed him. We also like to thank the Librarian of our College for supplying books whenever we needed. We are also greatly thankful to our parents, friends and faculty members for their motivation,guidance and help whenever needed.

Name and signature of team Members:

1. Anish Si
2. Soumyadeep Banik

Abstract:

It is an art of hiding an information within other such that the change in the cover information cannot be detectable. In this paper we have provided security for an image using the concept of video steganography. A secret information is to be hidden in the randomly chosen unique video frame. Here we use the LSB method to hide that image into multiple video frames. Here frames are generated by some pseudo random number generator. Eight bits of secret images are divided into 8 bit-planes .As we first resize the image equal to the cover frame along with the bit-slicing method ,exactly 8 cover frames are needed to embed the secret image. An application of this technique is also presented here.

Keywords:*Bit-plane slicing, Pseudo random number generator, LSB,*

1. *Introduction*:

Steganography is the method where messages can be identified only by the sender and receiver. Steganography is the combination of two different words such as “Stego” and “graphy”. “Stego” means “Covered or concealed” and “graphy” means “writing and drawing”. Steganography is the method to block the survival of communication. So, in steganography messages should be hidden in some other files. The files may be an image, an audio file, video file etc. Hidden data may be any important text, Image, audio, or even a video. There are two methods for hiding data into other. They are

1. Cryptography
2. Steganography

Basically Steganography is none other than cover writing while cryptography relies on secret writing and is used only for data protection. So by Steganography secret communication can be easily done. So Steganography refers to conceal the existence of the message. On many occasions, encryption can be added to it. It means it can work like cryptography.

Though Steganography is less popular than cryptography, it has more benefits as outsiders can not notice the secret data. According to the cover media Steganography has different names such as audio steganography, image steganography, text steganography, video steganography etc.

1. Audio steganography means hiding the data inside an audio.
2. Image steganography means hiding the data inside an image.
3. Text steganography means hiding the data inside a text

4. Video steganography means hiding the data inside a video.

Video Steganography can hide an image, text, audio and even another video as well. It is more prominent as videos are large in size and consist of audio and many running images. So in video large amounts of data can be hidden. In video Steganography, image and audio Steganography techniques can also be employed. So it is imposing a high security.

In video steganography, the original video file is known as cover video while the video after embedding the secret data is known as stego-video. In this project we are interested in manipulation of selected video frames of the cover video file to hide a secret data or message into them.

2. LITERATURE SURVEY:

Steganography has been started in various forms from the past 2500 years. It is vastly used in World War 2 to secretly pass one information to the others by hiding from the opponent. Then it is done by microfilm, micro-drops and some chips. So the concept of steganography is very old.

Now -a-days, the main motto of steganography is to hide intellectual protection. So it has been often seen that people emphasize the digital steganography system rather than doing micro concepts. So there become a concern about steganography.

As this concept is very old, there are many methods to be done for doing this steganography method. Mainly they are

- Pure steganography
- Public-key steganography
- Private-key steganography

As there are many steganography types, there should be some different approaches. They are mainly divided by two domain categories:

- Spatial domain or substitution domain technique
- Transform or frequency domain technique

Spatial domain mainly substitutes the redundant part of the cover image with that secret information by operating pixel or blockwise. On the other hand, in the transformation domain steganography is done by embedding the secret information in the transformed space of the signal.* So, messages are also embedded in that transform coefficient.

Munasinghe[1] et al. proposed a method to hide a video in a visual file in which LSB of each byte of the cover file is changed to embed the secret data. This method only changes the least significant bits. So there will not be any change in size of the cover file. Hence the existence of the data can not be detected.

Rehana[2] et al. proposed LSB based video steganography which uses genetic algorithm visual cryptography for secure data hiding and transmission over networks. This approach uses the genetic algorithm to shuffle the pixel location of the stego image and visual cryptography to create the shares. Since visual cryptography is used, it suffers from the requirement to represent every pixel within the original frame by multiple pixels in every share, leading to a contrast deterioration problem called ***pixel expansion.***

J.K.Mandal[3] et al. proposed a hash-based least significant technique for video steganography. The proposed technique takes 8-bits of secret data at a time and conceals them in LSB or RGB pixel value of the cover frames in 3,3,2 order respectively. Such that out of 8-bits of message 6-bits are inserted in the R & G pixel and remaining 2 bits are inserted in B pixel. The embedding positions of the eight bits out of 4 available bits of LSB is obtained using a hash function of the form , **k=p%n** where k is LSB bit position within the pixel, p represents the position of each hidden image pixel and n is number of bits of LSB.

Video steganography in recent days has also gained quite significance for researchers. Various techniques of LSB exist where [4] proposed the data is first encrypted using a key and then embedded in their career AVI video file in LSB keeping the key of encryption in another file called key file. Another video steganography scheme based on motion vectors and linear block codes has been proposed. [5]

3. ALGORITHMS:

3.1 Algorithm of image embedding:

- Step 1: read the image file
- Step 2: resize that image into the size of the cover video.
- Step 3: divided the images into bit-slicing method [9]
- Step 4: input the cover video
- Step 5: split that video into frames
- Step 6: select 8 frames where a bit sliced image will be embedded.
- Step 7: find that LSB bit of the cover frames.
- Step 8: embed those bit planes into that image frames and return those frames into its previous position.
- Step 9: regenerate video frames.

3.2 Algorithm of extraction:

- ❖ Step 1: input the stego video
- ❖ Step 2: extract frames from the video
- ❖ Step 3: find those frames by the specified key
- ❖ Step 4: find LSB of those frames.
- ❖ Step 5: extract those bits from those stego frames.
- ❖ Step 6:merge those bits to form the final image.

4. PROPOSED METHOD:

In this section, we proposed an algorithm which consists of random selection of frames, LSB method, and resizing an image file. The architecture is shown in the figure downwards. As previously, we also know video steganography can be done by audio or image steganography method, here we choose image steganography logic to implement video steganography.

Here we take the video-path and the hiding image path as the input and also the key of the hidden technique method must be inputted.

4.1 *Bit-Slicing* :

In this section, the information, needs to be hidden is taken for processing. This process includes image bit slicing and division of that image into 8 different bit-planes.

The pixel values of each image are converted to its corresponding 8-bit binary values. Every **i^{th}** bit is taken from each byte of pixel values to form the **ith bit-plane image**.

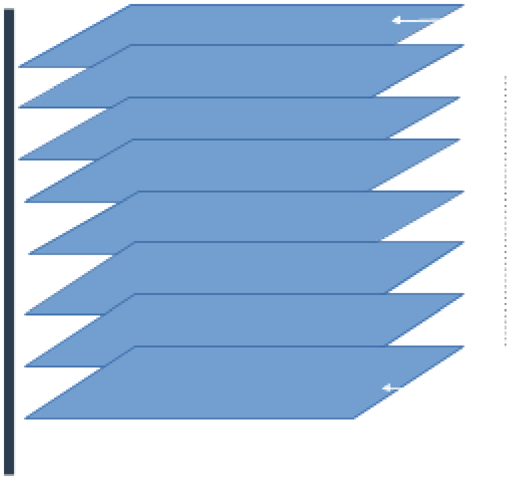


Fig no:**1**

The first bit-plane constructed from every first bit is called MSB plane while the last one is called LSB plane.

10010011	10110101	10100101
01100101	11001100	11001101
11010101	10100011	10010111
11011011	10101100	01001101

1	1	1
0	1	1
1	1	1
1	1	0

bit-array of 1st bit plane

0	0	0
1	1	1
1	0	0
1	0	1

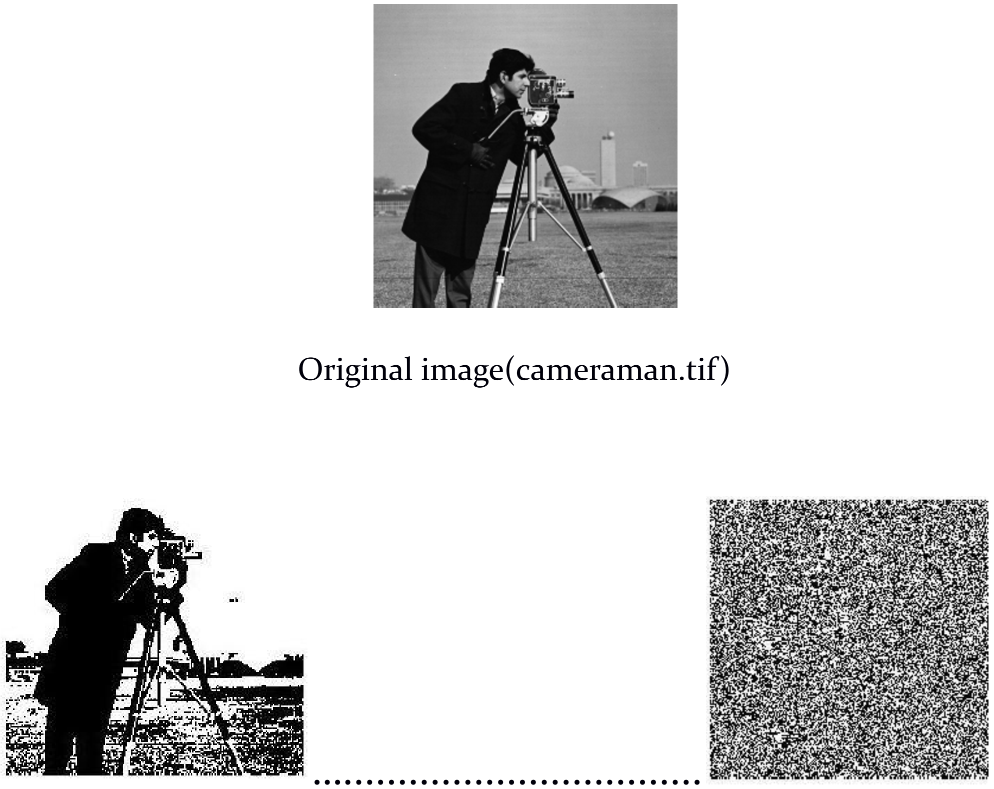
bit-array of 2nd bit plane

....

1	1	1
1	0	1
1	1	1
1	0	1

bit-array of 8th bit plane

Fig no. **2**



Original image(cameraman.tif)

MSB plane image **LSB image(8th bit image)**

Fig No. 3

4.2 LSB Technique:

First of all the video file is converted into frames.Generally, in small video .AVI, .MPEG, .MP4 video at least 20-25 frames can be generated per second . A frame in the video is actually an image consisting of a collection of pixel values(color and intensity) in a matrix form or in a list formation. The 24 - bitmap RGB image has 24 bits values for each pixel, 8-bits for each 3 color channels. The RGB is most suitable as there are lots of information where we can hide secret messages, with one bit change for each byte.

Each component is of one byte i.e. 8-bits in which the first one is the most significant bit. In LSB technique (Least Significant Bit) is used for hiding secret information resulting in the change in the last bit of each byte of the component.

Substitution of the least significant bit results in human imperceptibility. We all know the first and foremost requirement of steganography is the invisibility of the changes in the cover frames. The strength of steganography lies in its ability to be unnoticed by the human eye.

For hiding three bits of the data in every pixel's color, we used a 24-bit image. Human eye can not easily differentiate between 21-bit color and 24-bit color.

4.3 Frame selection:

In the embedding process of this algorithm involves selecting frames randomly from the cover video in which the data is to be hidden. Here we used a random function which generates random numbers within a given range. We also used a **seed-value** which is also the **Key** for retrieving the data, given by the user. By using this seed value selected frames can be selected and those frames are unique for that particular seed value.

From those frames, users can retrieve the data i.e. bit-planes embedded in those frames. Here we used the Python3 **random.seed(x)** method , where x is the seed value,for which the function generates a unique sequence of random numbers. So there will be no repetition of frames as we used the seed value in the random function.

As we divided the original image into 8-bit planes, so 8 frames are sufficient to embed those bit-planes. So here we used LCG(Linear Congruential Generator) which generates the residues of successive powers of a number i.e. pseudo-random numbers having good randomness properties.

$$x_n = a^n \bmod m \text{ which is equivalently } x_n = ax_{n-1} \bmod m^{[6]} \quad \ldots\ldots(1)$$

a = multiplier, m = modulus

Here we used $m=2^k$. As the above modulus function is cyclic after certain periods, here the maximum possible period is 2^{k-2}.

So our function to generate 8 sufficient frames without any repetition is

$$x_n=5x_{n-1} \bmod 2^5 \qquad \ldots\ldots\ldots\ldots\ldots..(2)$$

x_o be the initial seed value which is an odd integer. Thus random sequences of frames are generated from taking the first random number of the random sequences corresponding to the respective residues.

For instance, if we take the initial seed value 1 then from the above modulus function ,the generated sequence is 5,25,29,17,21,9,13,1 and their corresponding pseudo random numbers are 34,145,16,65,30,126,115,120 which are also the unique frame numbers.

4.4 Embedding :

A simple LSB insertion process is used for the embedding image in the cover video file frame. We replaced the least bits of each 24 bit pixel of the selected cover frames (target frames) by each bit plane image generated by the bit slicing method. Here we embedded every (8-i)th bit plane image into the i th frame of the randomly generated sequence.

4.5 Extraction:

In this section we are going to retrieve the hidden image from the embedded video which is called stego-video.

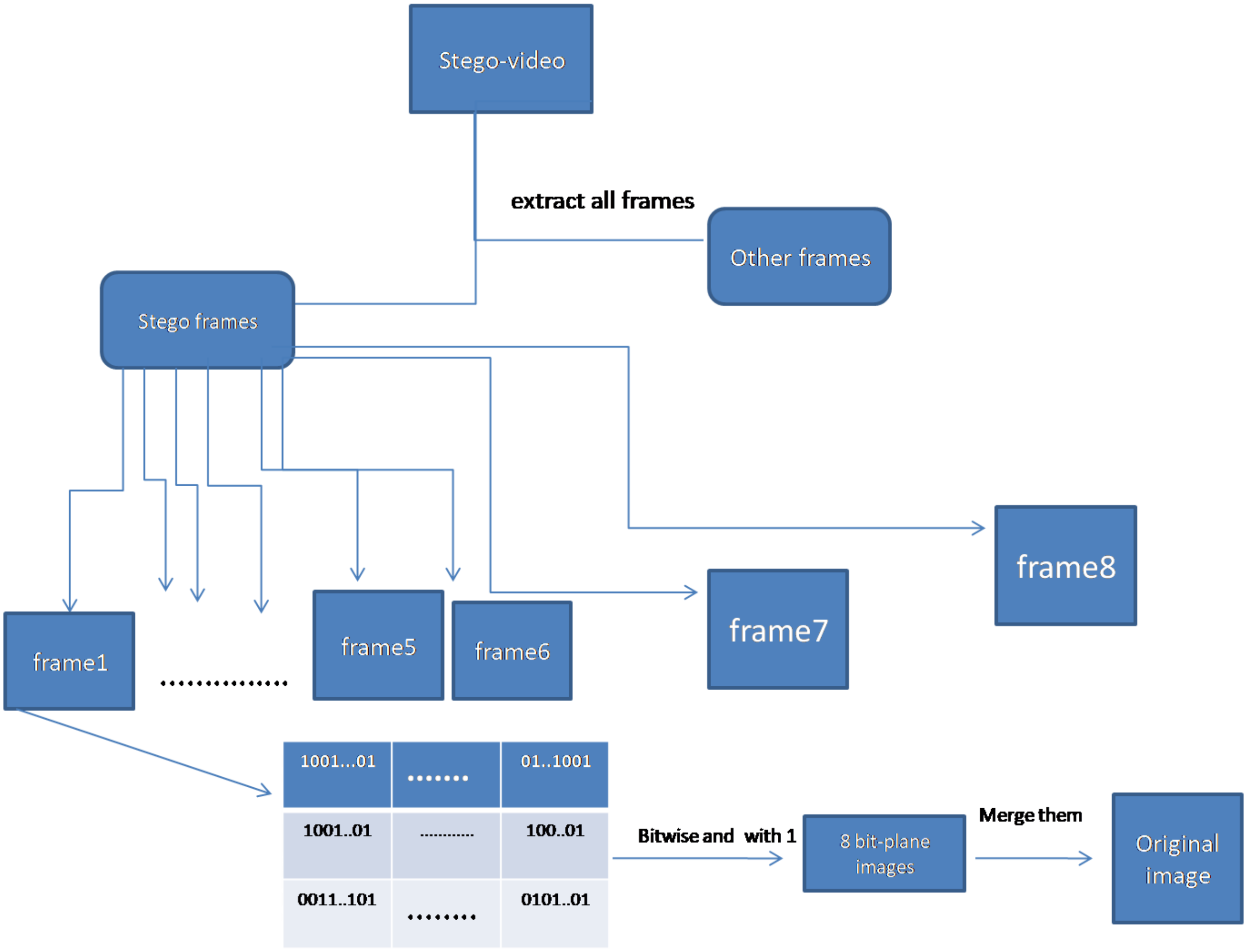
We used a very simple extraction algorithm to extract the secret image from the stego-video.

Step1: First of all we extracted frames all frames from the video

Step2: Select the stego frames using the above mentioned frame selection method .

Step3: As the secret image is embedded into the least significant bits of every stego-frames , so we simply do the logical and operation between 1 and every bytes of the carrier frames to get the bit-array of LSBs which is actually the bit-array of one of the bit-plane images.

At this stage we have 8 bit-plane images of the original image.To recover the original image those 8 bit-plane images must be merged according to the order by which they are inserted into the cover frame sequences.



1001...01	....	01..1001
1001..01	....	100..01
0011..101	....	0101..01

Block diagram of extraction algorithm (Fig No. 4)

5. Experimental results:

The proposed method is implemented in opencv-python. A steganography technique is mainly characterized by it's imperceptibility. The performance of the proposed method is evaluated using a video streams (drop.avi) and the secret image (cameraman.tif).The perceptual imperceptibility of the embedded data is indicated by comparing original video to it's stego video so that their visual differences can be determined(if any).

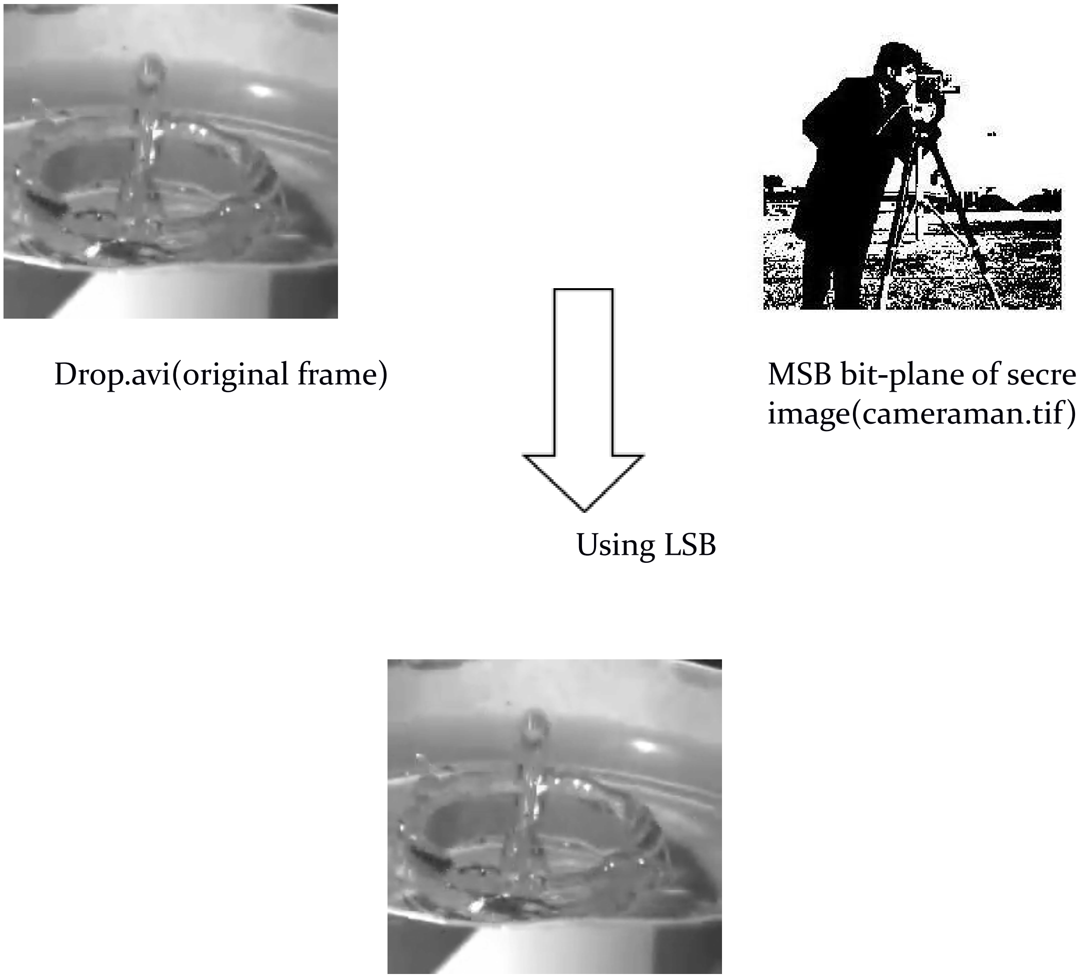
An additional measurement MSE (mean square error) and PSNR(peak signal to noise ratio) can be done to check the imperceptibility between the stego frame and corresponding cover frame.

$$\text{MSE}= \frac{1}{H*W} \sum_{i=0}^{H} \sum_{j=0}^{W} (P(i,j) - S(i,j))^2$$

Where MSE is Mean Square Error,H and W are height width and P(i,j) represents the original frame and S(i,j) represents the corresponding stego frame.

$$\text{PSNR}=10\log_{10}\frac{L*L}{MSE}$$

Where, PSNR is peak signal to noise ratio,L is peak signal level for an image which is taken as 255.



Drop.avi(original frame)

MSB bit-plane of secret image(cameraman.tif)

Using LSB

Stego-frame(drop.avi)

Fig No. **5**

5.1 Cover video file:

Video name	Resolution	Frames /sec.	No. of frames	Secret image size
drop.avi	240*256	30	182	512*512

6. Conclusion:

A simple LSB technique for video steganography has been proposed in this paper. Basically we focused on the frame selection method,which is very unique and can play an important role in LSB steganography or any other techniques for steganography. The LSB technique utilizes selected cover video files in spatial domain to hide the presence of sensitive data regardless of its format.

The proposed technique is applied on several types of file(.avi,.mpeg,.mp4 etc.).

7. References:

1. A Munasinghe ,Anuja Dharmaratne and Kasun De Zoysa, "Video Steganography",2013 "International Conference on Advances In ICT for Emerging Regions.

2. Rehana Begum R.D. and Sharayu Pradeep, "Best Approach for LSB based video steganography using genetic Algorithm and visual Cryptography for secured data hiding and transmission over networks", International Journal of Advanced Research in Computer Science and Software Engineering,2014.

3.Koushik Dasgupta, J.K.Mandal and Paramartha Dutta , "Hash-based Least Significant Bit Technique for Video Steganography(HLSB)" Internatioanl Journal of Security , Privacy and Trust Management, 2012.

4.Mritha Ramalingan, Stego Machine Video Steganography using Modified LSB Algorithm, in World Academy of Science, Engineering and Technology,2011

5.Feng Pan , Li Xiang , Xiao-Yuan Yang and Yao Guo , video steganpgrapy using motion vector and linear block codes, in Proceedings of The International Conference on Image Processing, June 2002.

6. https://www.cse.wustl.edu/~jain/cse567-08/ftp/k_26rng.pdf

7. https://www.geeksforgeeks.org/image-based-steganography-using-python/

8. https://towardsdatascience.com/steganography-hiding-an-image-inside-another-77ca66b2acb1

9. https://www.geeksforgeeks.org/print-kth-least-significant-bit-number/

10. https://www.youtube.com/watch?v=7hsNFtsVahI