VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
(SCOPE)

November 2019

CSE4019 - Image Processing

FINAL PROJECT REPORT

Image Steganography: Implementation and Analysis of different algorithms for Hiding Data

Under the guidance of,
Prof. Don S

Submitted By:
Divam Kesharwani (17BCE0541)

SLOT: F1+TF1

Image Steganography: Implementation and Analysis of different algorithms for Hiding Data

Name: Divam Kesharwani
Registration No.: 17BCE0541

1 Abstract

Steganography is the craft of concealing the way that correspondence is occurring, by concealing data in other data. A wide range of transporter document arrangements can be utilized, however advanced pictures are the most prevalent on account of their recurrence on the Internet. For concealing mystery data in pictures, there exists a vast assortment of steganographic methods some are more unpredictable than others and every one of them have separate solid and feeble focuses. Diverse applications have distinctive necessities of the steganography method utilized. For instance, a few applications may require outright intangibility of the mystery data, while others require a bigger mystery message to be covered up.

In the following project we are concentrating on least significant bit of the image and modifying it in spatial domain. We have broken down and concluded about the variations of this algorithm as far as efficiency and hiding capacity of an image. Viability of the algorithm is estimated by client assessments deciding so, all things considered change to the pictures wound up evident.

2 Keywords

Image Steganography, Bit Plane, Encryption, Least Significant bit, Colour Map, Threshold, Metadata manipulation, PNG Chunk.

3 Introduction

"Steganography is the craftsmanship and investigation of imparting in a way which shrouds the presence of the correspondence. As opposed to Cryptography, where the foe is permitted to identify, block and adjust messages without having the capacity to damage certain security premises ensured by the spread message with the inserted cryptosystem. The objective of Steganography is to conceal messages inside different innocuous messages in a way that does not enable any foe to try and identify that there is a second message present"[1]. In picture steganography the data is covered up solely in pictures.

The thought and routine with regards to concealing data has a long history. In Histories the Greek student of history Herodotus composes of an aristocrat, Histaeus, who expected to speak with his child in-law in Greece. He shaved the head of a standout amongst his most confided in slaves and inked the message onto the slave's scalp. At the point when the slave's hair became back the slave was dispatched with the concealed message [2]. In the Second World War the Microdot strategy was created by the Germans. Data, particularly photos, was decreased in size until it was the span of a composed period.

Amazingly hard to recognize, a typical spread message was sent over an unreliable channel with one of the periods on the paper containing shrouded data [3]. Today steganography is generally utilized on PCs with advanced information being the carriers and networks being the high speed delivery channels.

Information security issues can emerge from a wide scope of sources, for example, social insurance records, criminal equity examinations and procedures, money related establishments and exchanges, natural qualities, home and geographic records and ethnicity. Information security or information protection has turned out to be progressively critical as an ever increasing number of frameworks are associated with the Internet. There are data security laws that spread the insurance of information or data on private people from purposeful or inadvertent exposure or abuse. Along these lines, concealing the information in a sort of structure, for example, inside a Steganography Algorithm to Hide Secret Message inside an Image is indispensable so as to ensure that security or protection of the vital information is ensured.

Steganography depends on concealing undercover message in unsuspected interactive media information and is commonly utilized covertly correspondence between recognized gatherings. Steganography is a strategy for encryption that conceals information among the bits of a spread record, for example, a realistic or a sound document. The strategy replaces unused or unimportant bits with the mystery information. Steganography isn't as vigorous to assaults since the installed information is powerless against annihilation.

Watermarking has the component of heartiness against assaults. Regardless of whether the presence and strategy for installing the information is known, it might be hard to wreck the concealed information. Information stowing away and information implanting can be named strategies among steganography and watermarking.

4 Related Work/Literature Review

G. Prashanti and K. Sandhyarani(2015) have done review on late accomplishments of LSB based picture steganography. In this review creators talk about the upgrades that improve the steganographic results, for example, high vigor, high installing limit and un-perceptibility of shrouded data. Alongside this overview two new methods are additionally proposed. First strategy is utilized to insert information or mystery messages into the spread picture and in the second method a mystery dark scale picture is installed into another dim scale picture. These strategies utilize four state table that produce pseudo irregular numbers. This is utilized for inserting the mystery data. These two strategies have more prominent security since mystery data is covered up on irregular chose areas of LSBs of the picture with the assistance of pseudo arbitrary numbers produced by the table.

Savita Goel(2014-2015) proposed another technique for implanting mystery messages in spread picture utilizing LSB strategy utilizing distinctive movements. Creators contrast the nature of stego picture and regard to cover picture utilizing number of picture quality parameters, for example, Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), histograms and CPU time, Structure Similarity (SSIM) record and Feature Similarity Index Measure (FSIM). Their investigation and test results demonstrates that their proposed technique is quick and exceptionally productive when contrasted with essential LSB strategies.

Bingwen Feng, Wei Lu, and Wei Sun(2015) in their paper "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture" purposed a best in class approach of twofold picture steganography. This strategy is proposed to limit the bending on the surface. In this technique for steganography initially the pivot, supplement and reflecting invariant surface examples are separated from the double picture. They likewise proposed an estimation and dependent on this proposed estimation this methodology is for all intents and purposes executed. Reasonable outcomes demonstrate that proposed steganographic approach has high factual security with high stego picture quality and high inserting limit.

Amitava Nag(2014) present a novel steganographic method of LSB substitution. Their procedure fundamentally centers around high security, bigger inserting limit and worthy dimension of stego picture quality. Right off the bat Huffman tree is delivered to encode each 8 bits of mystery picture. In the wake of encoding, they isolate the encoded bits into four sections and have 0 to 3 decimal qualities. Area of implanting a message in spread picture is dictated by these decimal qualities. Test results demonstrate that it is troublesome for assailant to extricate the mystery data on the grounds that Huffman table abatement the span of the spread picture. Proposed methods simply have satisfactory dimension of PSNR qualities and lie between 30 dB to 31dB.

2012: In this creator proposes an upgraded LSB calculation for picture steganography. In this proposed work they just insert mystery data in blue part of the RGB shading space. In their method first MN measure spread picture is chosen. After choice of spread picture just blue part is utilized for implanting mystery data. They likewise utilize pixel channels to get to the best districts to insert data in spread picture to get 5 most ideal rate. Exploratory outcomes demonstrate that this procedure diminishes the twisting dimension of spread picture and stego picture has extremely great unmistakable quality and changes in spread picture are careless to Human Visual System (HVS). This strategy lessens the jump in shading scale on the grounds that just blue segments are utilized to implant the mystery data.

2010: On the bases of Human visual framework (HVS) X. Qing proposed another system in which delicate data is implanted in all planes of RGB parts of a picture. In this method numerous arrangement bit is utilized with versatile nature of data concealing calculation. This proposed technique has high installing limit than conventional LSB strategy and low computational multifaceted nature. Proposed framework likewise has great nature of stego picture.

H. Yang(2009) displayed another versatile LSB based strategy for picture steganography. It utilizes the pixel change procedure for better stego picture quality. This versatile LSB substitution results in high shrouded limit. LSB based picture steganography strategy is proposed. To conceal the information regular piece design is utilized. As indicated by the message and the example bits LSB's of pixels are adjusted. This technique has low shrouded limit.

5 Proposed Methodology

5.1 Least Significant Bit (LSB)

Least critical piece (LSB) inclusion is a typical, basic way to deal with implanting data in a spread picture [4]. The least critical piece (at the end of the day, the eighth piece) of a few or the majority of the bytes inside a picture is changed to a touch of the mystery message. When utilizing a 24-bit picture, a touch of every one of the red, green and blue shading segments can be utilized, since they are each spoken to by a byte. As it were, one can store 3 bits in every pixel. A 800600 pixel picture, would thus be able to store an aggregate sum of 1,440,000 bits or 180,000 bytes of inserted information.

5.2 Bit Plane

Rather than featuring dark dimension pictures, featuring the commitment showed up by explicit bits may be wanted. Assume that every pixel in a picture is spoken to by 8 bits. Envision the picture is made out of 8, 1-bit planes running from bit plane 1-0 (LSB) to bit plane 7 (MSB).In terms of 8-bits bytes, plane 0 contains all least request bits in the bytes involving the pixels in the picture and plane 7 contains all high request bits. Isolating an advanced picture into its bit planes is valuable for breaking down the relative significance played by each piece of the picture, suggesting, it decides the sufficiency of quantities of bits used to quantize every pixel, helpful for picture pressure.

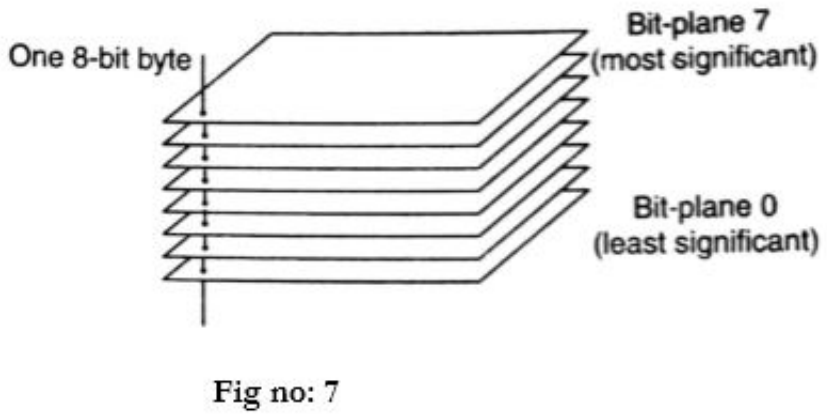


Figure 1: Bit Plane

5.3 Spiral Embedding

The Spiral Embedding orders the pixels of the picture in a winding example to keep the inserting from being as effectively decoded. The Spiral Embedding has two primary thoughts that enable it to be decoded effectively and help upset visual assaults. The first is that metadata about the picture's substance are implanted into known areas. This data makes it conceivable to interpret the stego object and recover the mystery message. The second is that the information is serialized and implanted in an example that obliterates the capacity to disentangle the message in a visual attack.The Spiral Embedding starts by structure a vector containing every one of the information that will be inserted into the spread including the metadata and the message substance. The elements of the message are inserted losslessly into the initial 32 positions in the vector as

unsigned 16-bit whole numbers. A bit speaking to the vector's substance is composed into the LSB of the spread in a winding example from the outside in, pixel by pixel.Decoding a stego object made with the Spiral Embedding is essentially a procedure of perusing in the put away measurements and after that following a similar winding example that represented the inserting. The estimations of the LSBs of the stego object are perused into a vector. At the point when the installed information has been perused completely, the vector is apportioned to make another picture with the message's unique measurements. The aftereffect of this inserting would then be able to be shown:

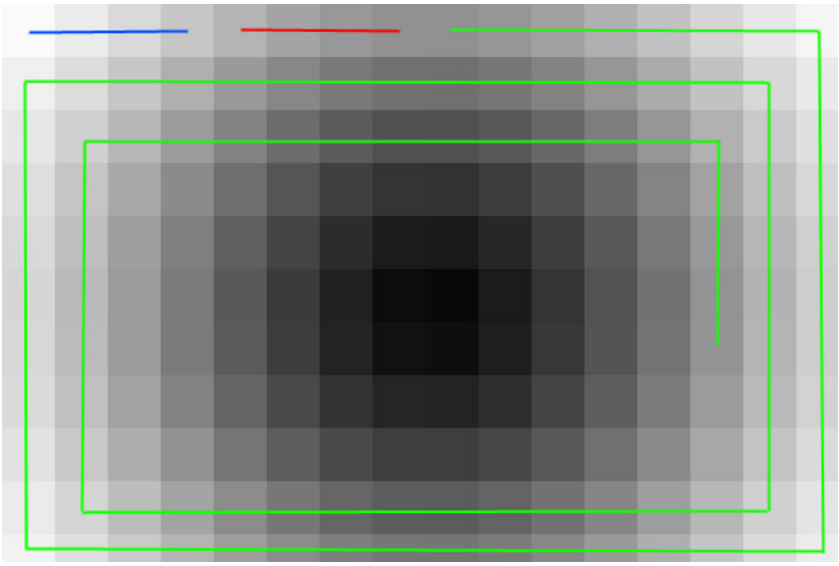


Figure 2: Spiral Embedding Pattern

5.4 Metadata Manipulation

Metadata is essentially information about information. In the event that we think about a picture document as our information, metadata would incorporate data, for example, the name of the picture, the title, measurements, width, stature, Video and sound records contain similar kinds of information.

The Exchangeable Image File (Exif) position is a standard utilized for account data about picture and sound documents made with a computerized camera. There are numerous information handle that can be utilized to conceal data. On the off chance that we right snap on a spared .jpg record and select properties, we will see a little subset of those fields.

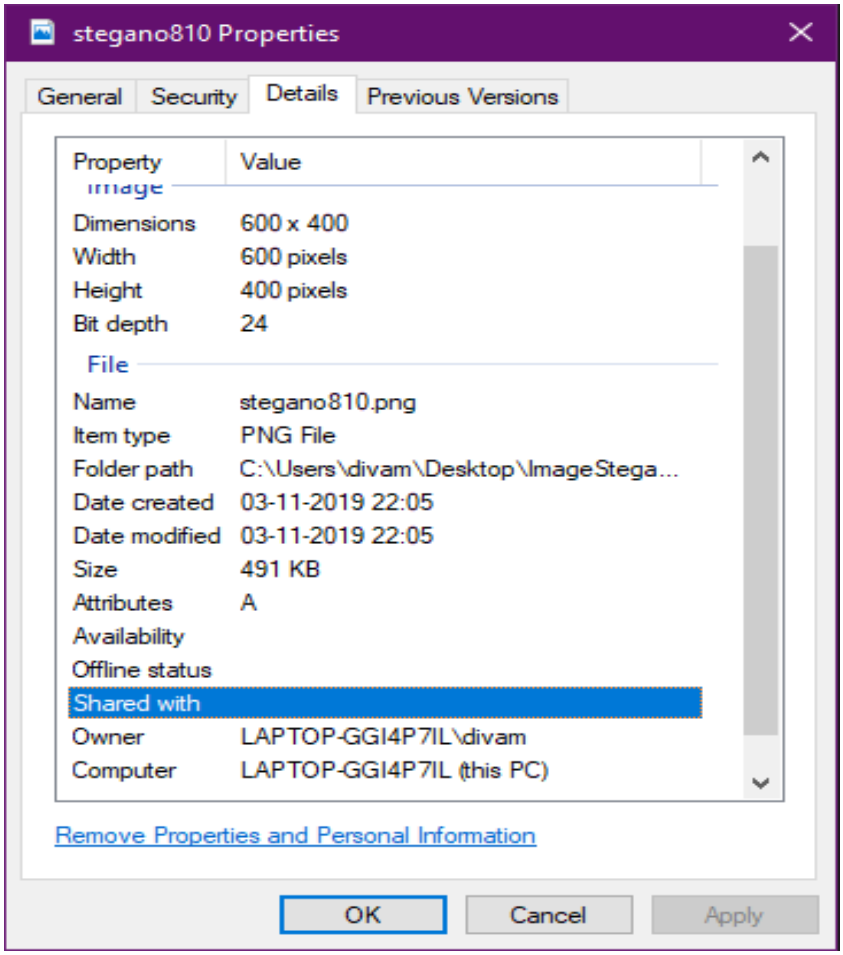


Figure 3: Metadata using File Properties window

5.5 Altering Threshold

Thresholding is the least difficult strategy for picture division. From a grayscale picture, thresholding can be utilized to make parallel pictures. The least complex thresholding strategies supplant every pixel in a picture with a dark pixel if the picture force is not exactly some fixed steady T or a white pixel if the picture power is more noteworthy than that consistent.

5.6 Appended Data

A straightforward and normal steganography strategy is to add information toward the finish of picture record. This strategy works on the grounds that most picture watchers disregard any attached information and thus a stego message stays covered up. Linux 'feline' direction can be utilized for annexing information toward the finish of picture document.

5.7 PNG Chunk Analysis

A PNG record begins with a 8-byte signature. After the header comes a progression of lumps, every one of which passes on certain data about the picture. Lumps proclaim themselves as basic

or auxiliary, and a program experiencing a subordinate piece that it doesn't comprehend can securely disregard it. This structures the premise of steganography. Information can be inserted in obscure auxiliary lumps and it will be overlooked by picture watchers or decoders.

A piece comprises of four sections: length (4 bytes, huge endian), lump type/name (4 bytes), piece information (length bytes) and CRC (cyclic excess code/checksum; 4 bytes). The CRC is a system byte-request CRC-32 registered over the lump type and piece information, yet not the length.

Piece types are given a four-letter case touchy ASCII type/name; look at FourCC. The instance of the distinctive letters in the name (bit 5 of the numeric estimation of the character) is a bit field that furnishes the decoder with some data on the idea of lumps it doesn't perceive.

The instance of the primary letter demonstrates whether the lump is basic or not. On the off chance that the principal letter is capitalized, the piece is basic; if not, the lump is auxiliary. Basic pieces contain data that is important to peruse the document. On the off chance that a decoder experiences a basic lump it doesn't remember, it must prematurely end perusing the record or supply the client with a suitable cautioning. The instance of the second letter shows whether the lump is "open" (either in the determination or the vault of uncommon reason open pieces) or "private" (not institutionalized). Capitalized is open and lowercase is private. This guarantees open and private piece names can never struggle with one another (albeit two private lump names could strife). The third letter must be capitalized to comply with the PNG detail. It is saved for future development. Decoders should treat a piece with a lowercase third letter equivalent to some other unrecognized lump. The instance of the fourth letter shows whether the lump is sheltered to duplicate by editors that don't remember it. On the off chance that lowercase, the piece might be securely replicated paying little mind to the degree of alterations to the document. On the off chance that capitalized, it might possibly be replicated if the changes have not contacted any basic chunks[6].

5.8 Changing Color Map

In registering, recorded shading is a strategy to oversee advanced pictures' hues in a restricted manner, so as to spare PC memory and document stockpiling, while at the same time accelerating show revive and document exchanges. It is a type of vector quantization pressure.

At the point when a picture is encoded along these lines, shading data isn't legitimately conveyed by the picture pixel information, however is put away in a different bit of information called a palette: a variety of shading components. Each component in the cluster speaks to a shading, filed by its situation inside the exhibit. The individual passages are now and then known as shading registers. The picture pixels don't contain the full determination of its shading, however just its list in the palette. This strategy is here and there alluded as pseudocolor or aberrant shading, as hues are tended to by implication. This method can be abused to conceal information in picture utilizing appropriate palette or shading map. To unravel information we should attempt diverse irregular shading maps.

6 Implementation

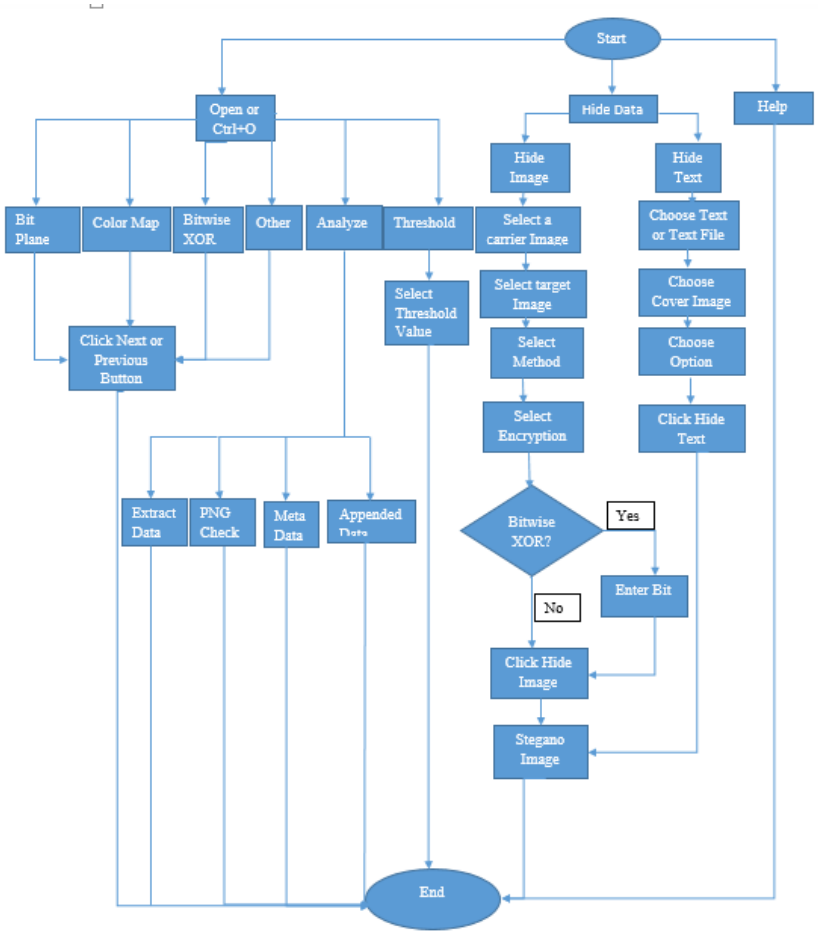


Figure 4: Flow Chart of the Project

Algorithm For Hiding Text
1. Read the input cover image(png)
2. Select the text file to be inserted.
3. Enter the text to be inserted in image
4. Select the bit plane to be used for hiding
5. Calculate new pixel value for each of the but in the corresponding bit
6. Create a new png image and save the new image.

Algorithm For Recovering Text
1. Open the image in recover text part software
2. Select the bit that had the text hidden.
3. Perform reverse arithmetic for the pixel and extract the text form the pixel.
4. Show the text.

Algorithm For Hiding Image
1. Select the carrier image(png)
2. Select the target image(png)
3. Image is cropped to resolution of the carrier image in case target image has larger size
4. Select bit plane in which image has to be hidden.
5. Calculate the new pixel value for bit plane.
6. Select the encryption to be inserted.
7. Create new image and save the image(png)

Algorithm For Encryption Using Java
1. Read Input that is to be Encrypt.
2. Encryption key is calculated using SecretKeySpec. SecretKeySpec's constructor take user defined bytes array generate Key.
3. Create Cipher's object basis on key.
4. It encrypts string data and Encodes using Base64Encoder and return encrypted message.

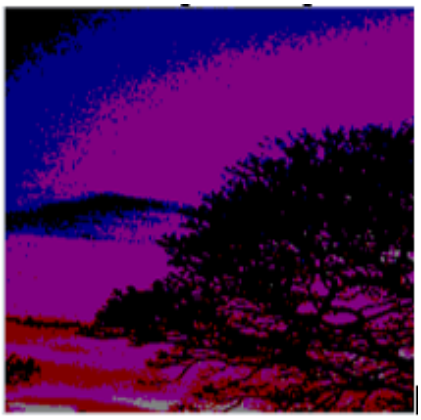
Algorithm For Decryption Using Java
1. Take string to be Decrypt.
2. Get key for decryption.
3. Create Cipher's object basis on key.
4. It decrypts string data and decodes and return decrypted message.

Algorithm for Extracting Image
1. Open the image that has the hidden image in it.
2. Browse the image through different types of extracting algorithm available if the type of encryption is not known.
3. If known directly select the method and find the image that has been hidden in the carrier image.

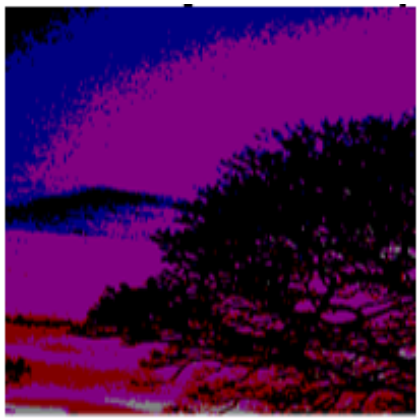
7 Results and Discussion

7.1 Comparing Hidden Image in different bit planes

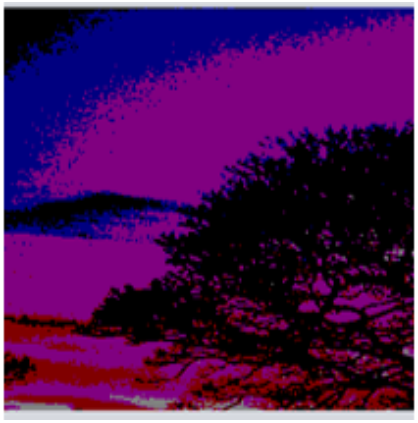
Figure 5: Cover Image for hiding Secret Image



(a) Secret Image Hidden in Oth bit Plane



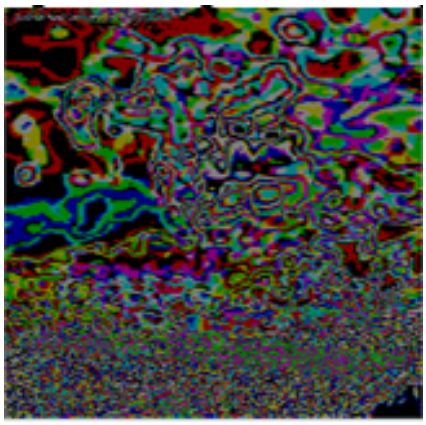
(b) Secret Image Hidden in 1st bit Plane



(a) Secret Image Hidden in 2nd bit Plane

(b) Secret Image Hidden in 3rd bit Plane

(a) Original Secret Image



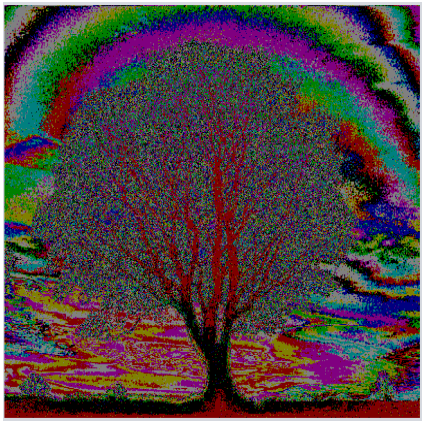
(b) Image in 4th bit plane when image is hidden in 3rd bit plane

Thus it is clear that image is only visible when the selected bit plane is same as the one which was used while hiding the image.

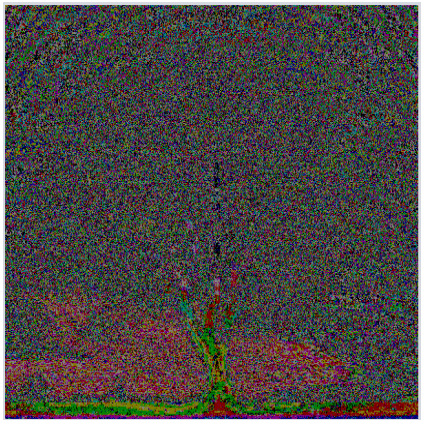
7.2 Different Bit planes of image having Hidden Text

Figure 9: Original RGB Colour Image

(a) 7th Bit Plane



(b) 4th Bit Plane



(a) 2nd Bit Plane

(b) Hidden Image in 0th Bit Plane

Thus it can be concluded that the hiden image was not visible until the image was not processed till 0th bit plane.

7.3 Finding hidden text using Colour Map

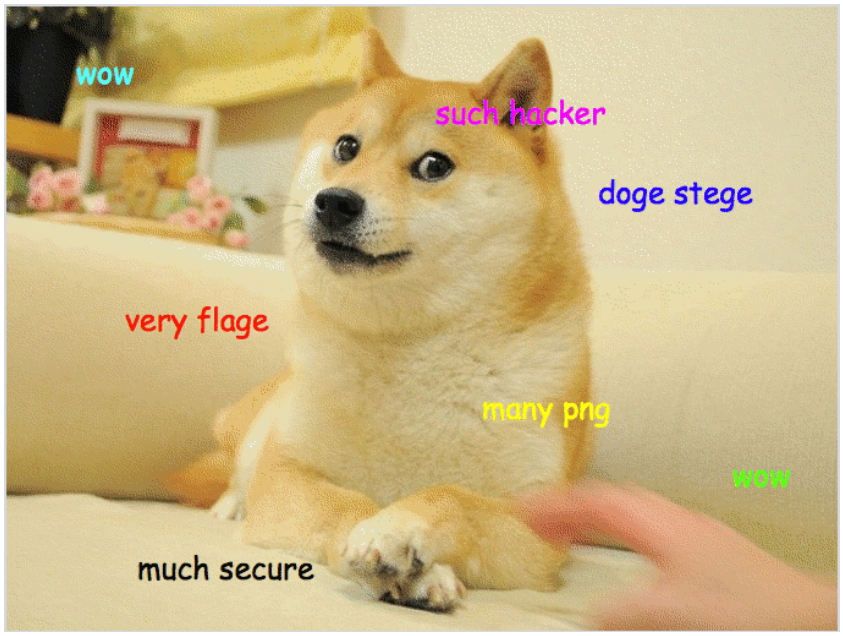
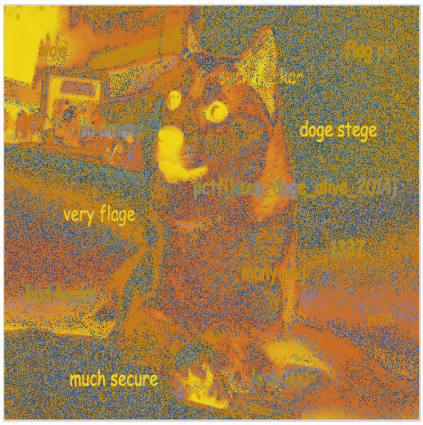
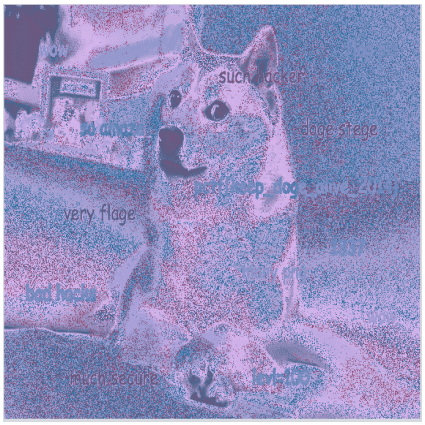


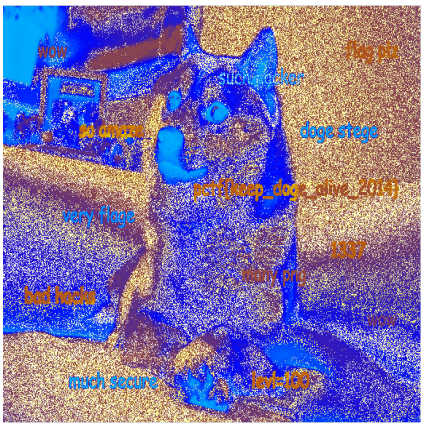
Figure 12: Original Index Image



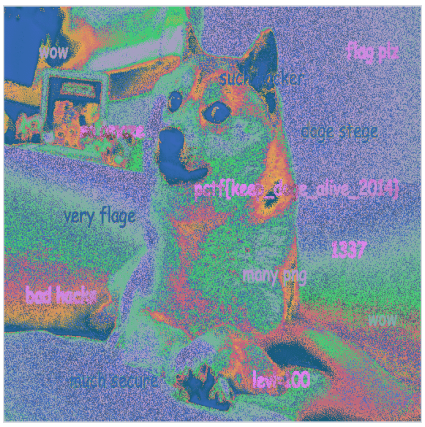
(a) Colour Map 0



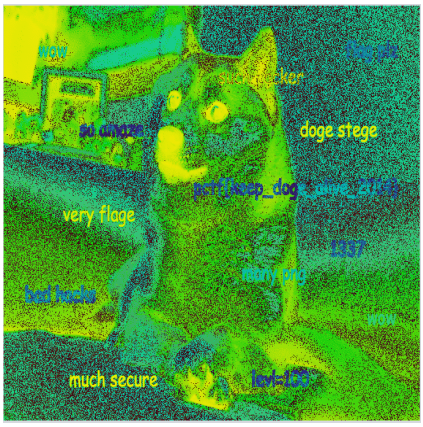
(b) Colour Map 1



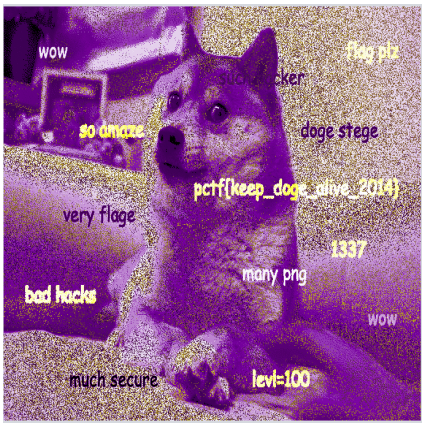
(a) Colour Map 2



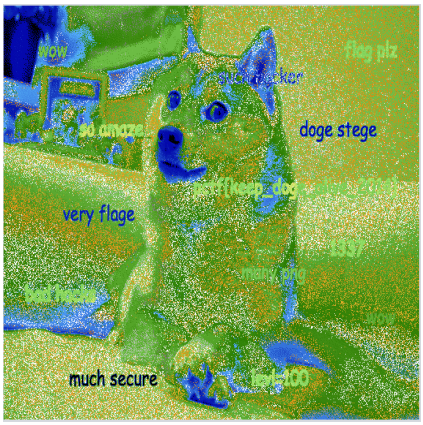
(b) Colour Map 3



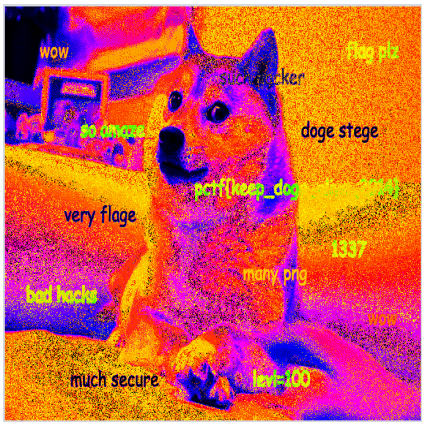
(a) Colour Map 4



(b) Colour Map 5



(a) Colour Map 6



(b) Colour Map 7

From the colour map 7 it can be clearly seen that there are more words visible in the image than the original indexed image.

7.4 Finding hidden text using Threshold

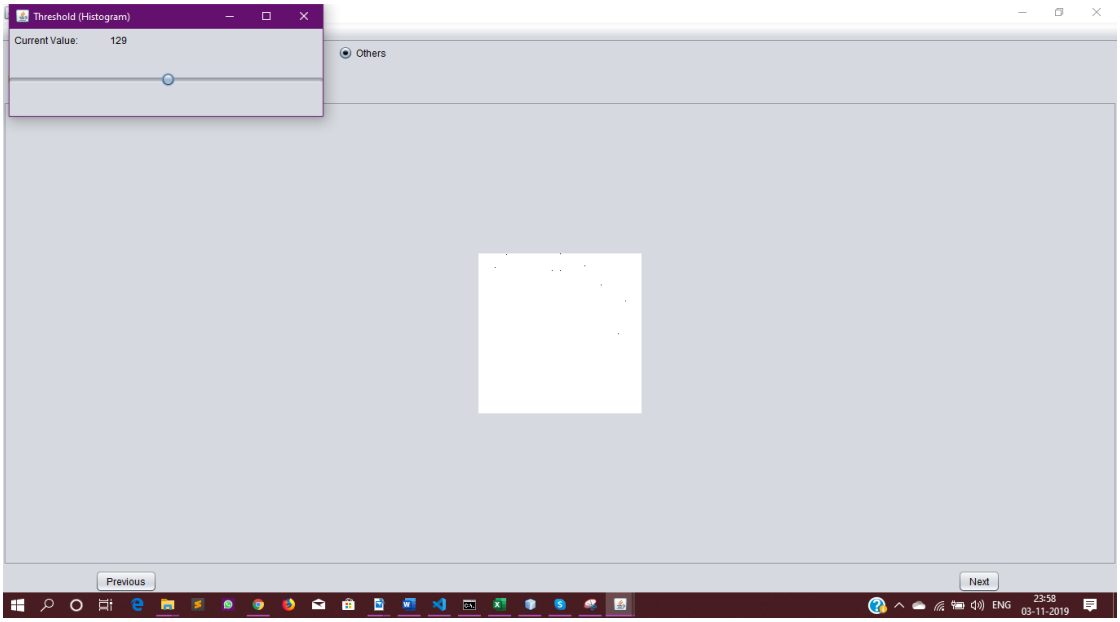


Figure 17: Image before applying threshold

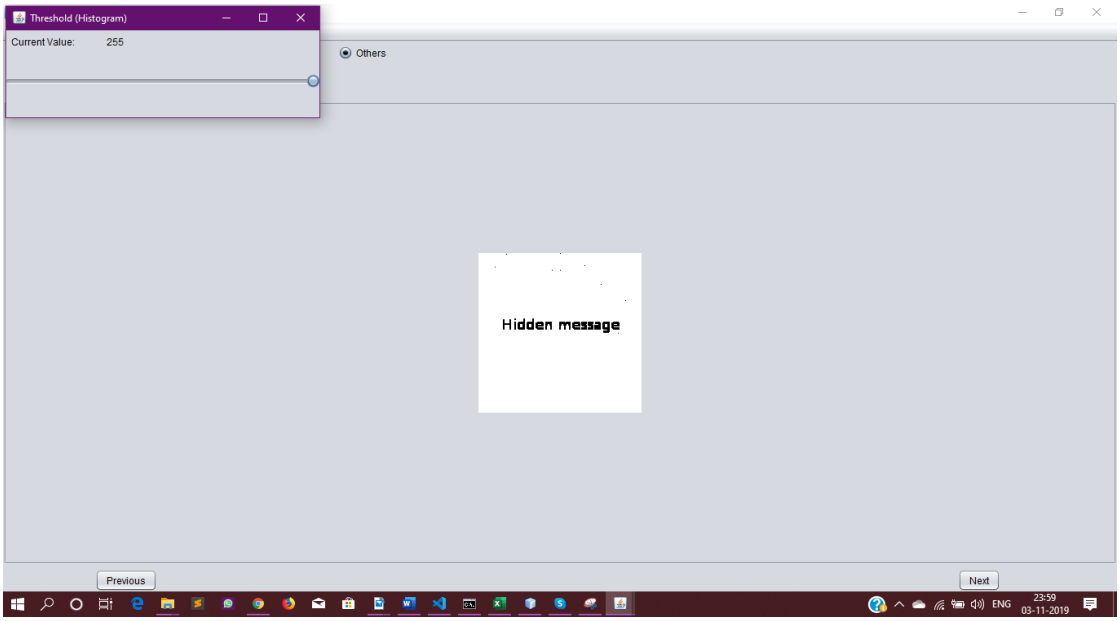


Figure 18: Image after applying Threshold

7.5 Hide Text

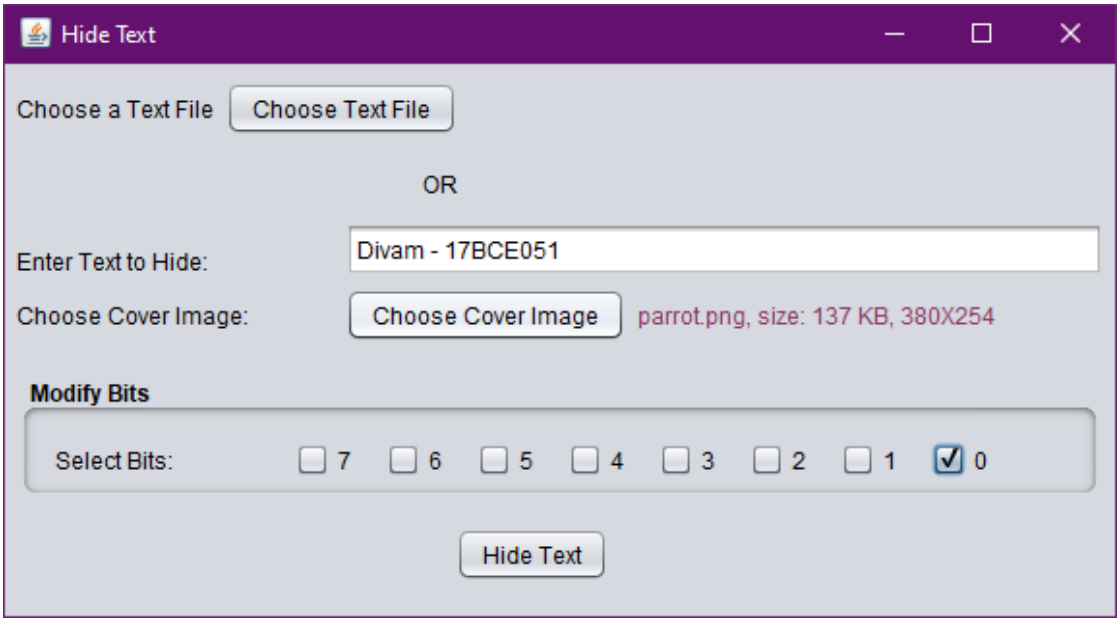


Figure 19: Hiding text in an image

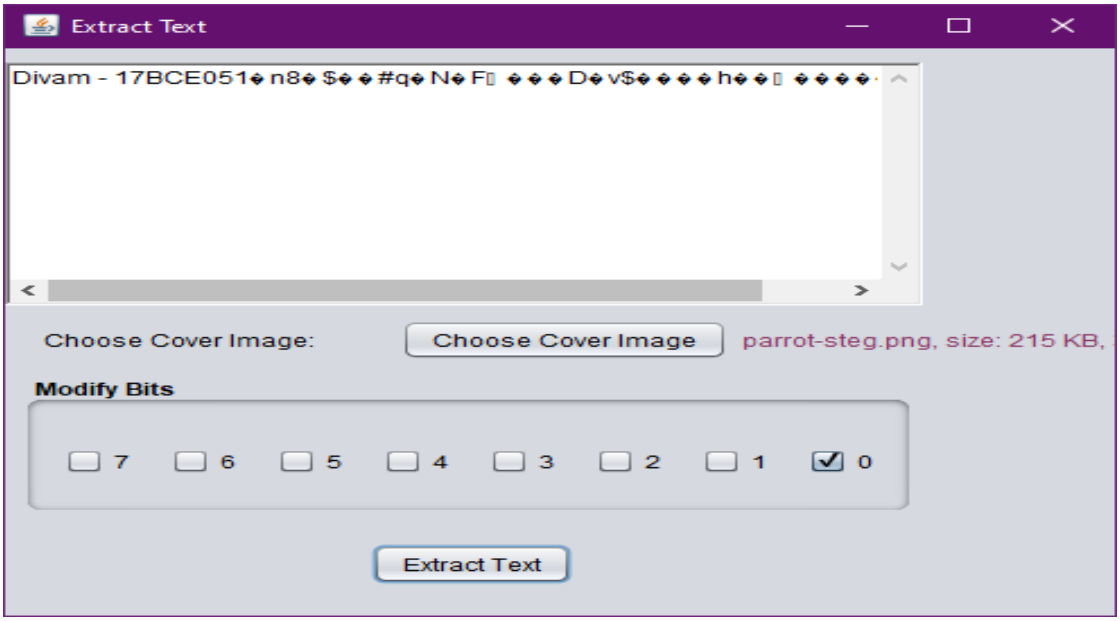


Figure 20: Extracting text from an image

8 Conclusion

The product made can be utilized by people/association. This instrument is stage free and is convenient for investigating regular steganography strategies. In spite of the fact that there are a few others steganography apparatuses accessible yet the new programming can be said as blend of numerous instruments and since it is open source so new functionalities will be included after some time by volunteer givers. Other than practical necessities, we have likewise centered around non-useful prerequisites (Nice UI and UX, Efficient). The device has constraint that it doesn't acknowledge jpeg pictures as bearer picture to conceal information. Likewise this apparatus does not utilize pressure and encryption of payload.

References

[1] B. Saha and S. Sharma, "Steganographic Techniques of Data Hiding using Digital Images", in Defence Science Journal, vol. 62, no. 1, 2012 January, pp. 11-18.

[2] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.

[3] Jamil, T., "Steganography: The art of hiding information in plain sight", IEEE Potentials, 18:01, 1999.

[4] Johnson, N.F. Jajodia S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.

[5] Sei-ichiro Kamata, et al: Depth-First Coding for Multi-Valued Pictures Using Bit-Plane Decomposition, IEEE Trans. on CT, Vol.43, No.5, pp.1961-1969, May, 1995.

[6] https://www.w3.org/TR/PNG-Chunks.html