Information Concealment in Images Using Least Significant Bit and Pixel Selection Function

Digvijay Singh Sengar [1], Aditya Shrungi [2], Anand Singh Kamlesh [3], Roshan John [4]
[1, 2, 3, 4] SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.

Abstract – Steganography is the process of hiding a secret message within a cover object/message and obtaining it when required. Steganography takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will be unable to know it contains encrypted data. Images are the most popular cover objects for Steganography and are one of the most widely used media which further helps the concealment. In this paper the existing LSB (Least Significant Bit) replacement technique is being improved upon by creating another layer of selection which can be made by the user. LSB replacement is simplest one to understand, easy to implement and results in stegno-images that contain embedded data as hidden. The disadvantage of Least Significant Bit is that it is vulnerable to steganalysis. This aspect is being improved on by replacing LSB in the pixel selected by user-given function.

Index Terms – Steganography, cryptography, Least Significant Bit (LSB), Steganalysis, Stegno-image.

1. INTRODUCTION

In this age of information, it has become essential to store information securely and safely. The information maybe a backup seed for 2FA (2 factor authentication) or keys to a cryptocurrency. Encryption provides a good way to secure information but it isn't perfect and subject to strength of the key used and the encryption method used. The goal of Steganography is to hide the existence of the hidden message in the first place. The approach of information hiding has recently become popular in a number of application areas and has its effectiveness. Images are one of the most widely used media and act as good cover object for steganography as an altered image with a little variation in its pixels will be hard to differentiate visually from the original image by a person.

There are several ways to implement steganography in images using Least Significant Bit, Masking and filtering, algorithms and transformations. In this paper we discuss on variation of Least Significant Bit Replacement using user-given function. The extra layer of encryption is also used to ensure the security of data and acts as a fail-safe. The process to obtain the information would require three steps

1) Identification of the stegno-image
2) Obtaining the encrypted message or information by successfully obtaining and matching the user given function.
3) Decrypting the message to obtain the information.

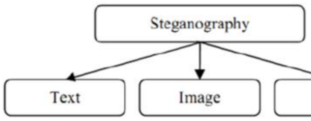
In addition, the image is first split into R, G, B plane to perform the LSB Replacement, the process is explained further in the following segments.

Through the whole barrage of processes which the image undergoes, its visually unaffected and remain indistinguishable from the original to a human being. The encryption isn't even visible which is why it's all the more effective. Any secure encryption algorithm can be selected for the process which follow the Unicode thus making sure there is no error during user to user communication or machine to machine communication.

2. RELATED WORK

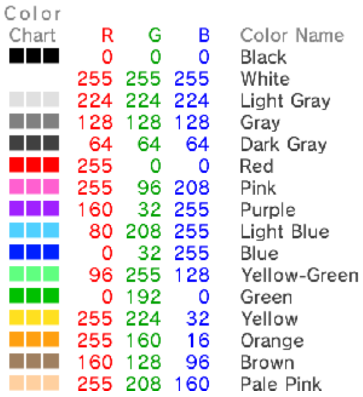
There have been various techniques proposed for concealing information within the image, i.e. Image Steganography. Each technique has its own advantages and disadvantages and have their own significance.

For simple Least Significant Bit replacement (LSB) suggested by Champakamala. B.S et al [1], the focus is on simplicity and ease of implementation but lucks in efficiency. Using more techniques such as encrypting the information prior to hiding helps in securing the information, even if the hidden encrypted data is revealed, the original information is not exposed [4]. Dilpreet Kaur et al [4] also recommended the compression of secret data to reduce its size and key-pixel cipher, which makes it secure against RS detection attack. Some technique focuses heavily on the encryption part [3] so that steganographic information is hard to identify. The steganography is not just limited to audio, images or texts, Dawen Xu et al [11] implemented an algorithm to embed additional data in encrypted H.264/AVC bitstream using the technique of code word substitution.



Audio steganography focuses on hiding the information in the digitalised audio signal, the changes made to the audio is so subtle that its undetectable by human ears. It should be noted that human hearing is between 20 Hz – 20 kHz. The techniques of spread spectrum, phase coding are also used to implement it.

In digital formats such as JPEG, PNG, etc. the images are represented using RGB colour palette, where the intensity of the each of the Red, Green and Blue colour is used to determine the colour of each pixel.



Color Chart	R	G	B	Color Name
⬛⬛⬛	0	0	0	Black
⬜⬜⬜	255	255	255	White
⬜⬜⬜	224	224	224	Light Gray
⬛⬛⬛	128	128	128	Gray
⬛⬛⬛	64	64	64	Dark Gray
🟥🟥🟥	255	0	0	Red
🟪🟪🟪	255	96	208	Pink
🟪🟪🟪	160	32	255	Purple
🟦🟦🟦	80	208	255	Light Blue
🟦🟦🟦	0	32	255	Blue
🟩🟩🟩	96	255	128	Yellow-Green
🟩🟩🟩	0	192	0	Green
🟨🟨🟨	255	224	32	Yellow
🟧🟧🟧	255	160	16	Orange
🟫🟫🟫	160	128	96	Brown
⬜⬜⬜	255	208	160	Pale Pink

The value of each part of R, G, B varies from 0-255 in 8-bit colour palette. The change of colour by +/- 1 bit isn't recognisable to human eye and that is the concept being exploited in most image steganography works. RGB colour code are widely used and are universally accepted hence its easier to work around them.

Vikas Verma et al [2] focused on enhancing the Least Significant Bit technique by using a mid-point circle technique. The idea was to improve the efficiency of the Least Significant Bit technique by using the centre of the image to replace LSB instead of starting from the first pixel continuously. The techniques for image steganography as mentioned in the above references focus on continuous pixel selection and are void of randomness in pixel selection. The lack of randomness can cause predictability and that's not word which needs to be associated with stenography or encryption.

3. PROPOSED WORK

The techniques used in the method is a combination of Least Significant Bit Replacement supported by Encryption which acts as a fail-safe for the steganography and the Pixel Selection Function for the selection of each pixel which can be selected by the user based on his choice.

ENCRYPTION & PLANE SEPARATION

Encryption

The first step is the encryption of the information or the message. Any encryption algorithm can be used such AES (Advanced Encryption Standard), DES (Data Encryption Standard) and their variations or RSA algorithm (Rivest-Shamir-Adleman) or any other standard and secure algorithm which uses characters in the Unicode. The encryption acts as a fail-safe, thus even if the steganographic image was extracted, there would still there be need for decryption using brute force if the key is not known.

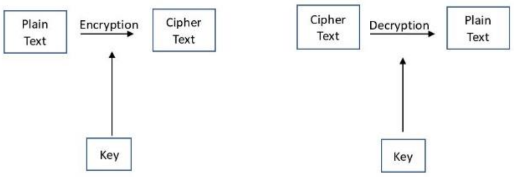


Fig.1. A simple flow chart for encryption and decryption.

Plane Separation

For the purpose of embedding the encrypted message onto the image, we first split the image into its Red, Green & Blue components i.e. their RGB components.

The result is three 3 different images, i.e. one of each R, G & B plane for the image.

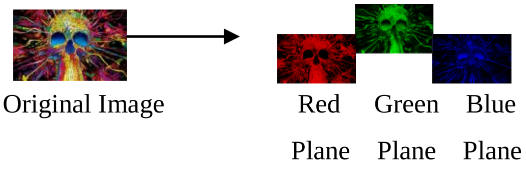


Fig.2.Plane Separation of the Image

Any changes in the colour of pixel, either in R, G or B segment will not have a visible change in the steganographic image. The plane separation allows us to interact with each segment individually thus simplifying the process a little.

LEAST SIGNIFICANT BIT REPLACEMENT & PIXEL SELECTION

Text steganography is hard and ineffective, it can be done by altering the text formatting, or by altering characters in the texts as in Vignere Cipher. Hiding secret messages in text can be a very challenging task because the text files contains very little redundant data and therefore reliable decoding and minimum visible change are somewhat conflicting.

Line-Shift Coding, Word-Shift Coding and Feature Coding are examples of text steganography.

Image steganography is the most popular technique being used in digital world of today. This is because of limited power of human visual system. Any kind of text whether it is plain text or cypher text can be hidden inside a cover image. An image consists of hundreds if not thousands of pixels and an increase or decrease in the brightness of colours by one or two points does not make much difference to a human eye. Most common steganography is Least Significant bit apart from masking and filtering techniques.

Pixel Selection

An Image of the resolution for e.g. 480x360 consists of 1,72,800 pixels. The pre-existing methods use continuous Pixels and alter their least significant bit for replacement purpose, which is easy to implement but isn’t highly secure and doesn’t fully utilise the available pixels. The method suggested here is using a user-given function to select the pixel to be modified.

Generally pixel is represented in the form of [x,y] where x and y are x and y co-ordinates respectively.

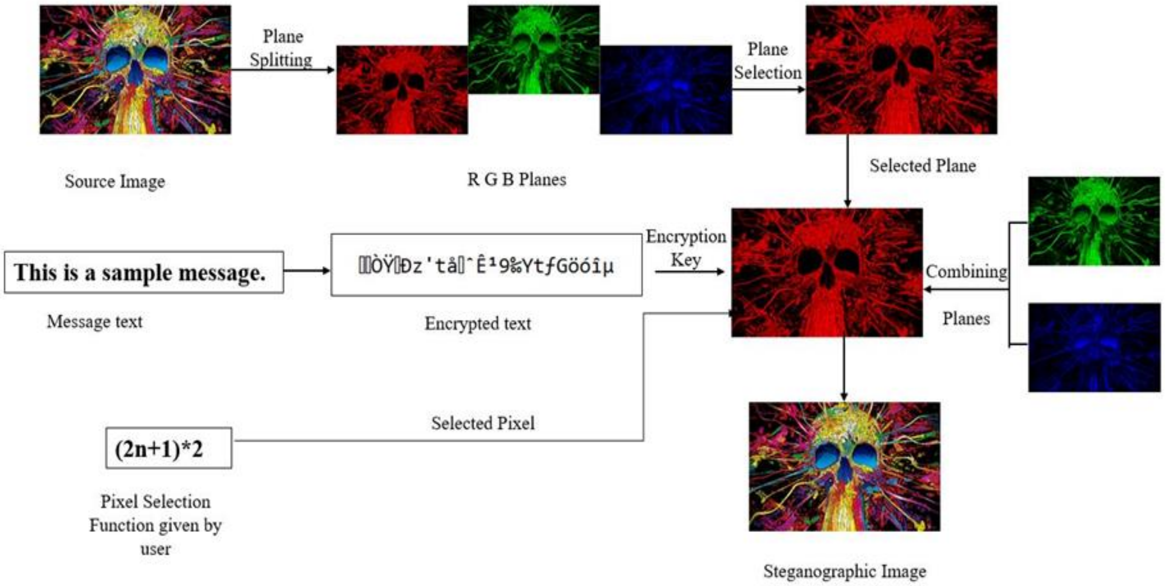
To make it simpler for the user to select a pixel, we can count the horizontally and assign each pixel a number.

The function can be anything mathematical expression simple enough to be computed easily.

For e.g. x=n*2;

x=(2n+1)

x=10*log(n+1)



where n=1,2,3……. up to number of pixel required for the steganographic embedding.

In order to obtain only integer values for the pixels the functions such as floor or ceil can be used. In order to validate a function, the function is checked and seen if it generate unique integers for the number of pixels required.

For a single character in Unicode, 8 bits are required which requires 8 pixels. Therefore for 10 characters, 80 pixels would be required. In addition, all the function’s modulus is taken to account for any negative value for the generated pixel value. The user can use a simple function such as x=n or a complex function such as x=log((n)^2+1). It’s up to the user to choose the function based on his requirement, it should be noted that this function is required during the extraction of the message or information from the image. This function shall be referred from here on as Pixel Selection Function.

Based on the function a wide variety of pixels can be selected. The selected values will look like 23 or 450 or 1250 1090 or 107200, etc. In order to convert this value into pixel co-ordinates, we need to perform the following steps.

For an image of resolution mxn and generated pixel value p,

For the x co-ordinate value, (p/m)+1

For the y co-ordinate value, (p%m)+1 i.e. the remainder of p/m.

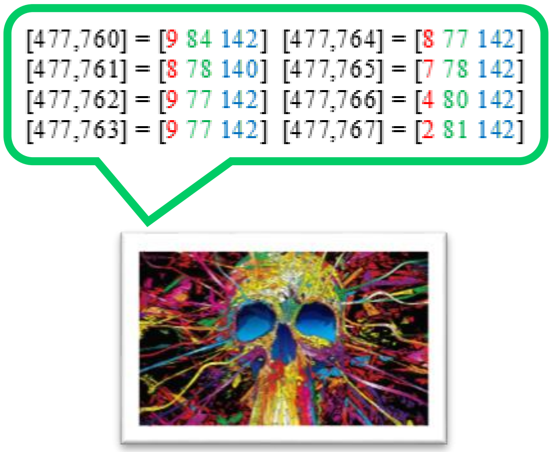
After we successfully obtain the pixel co-ordinates required to be modified, we can perform the process of replacement least significant bit from R, G or B plane based on our choice.

It should be noted that the above-mentioned process is really complex and thus any effort to brute force and access the data will face a lot of resistance and may even be impossible to crack since it deals with various levels of security and encryption using algorithms and functions. This is just an added benefit from the steganographic process.

Least Significant Bit Replacement

Pixel: A pixel is the fundamental unit of digital image. It is the smallest point whose colour can be controlled. An image is made of pixels in rows and columns. More the number of pixels, better is the resolution or clarity of image.

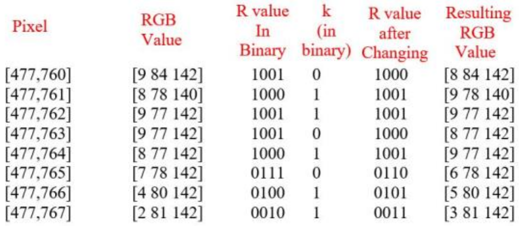
Colour: In a digital system, colours are represented as additive combination of three basic colours - RED, GREEN, and BLUE known as RGB system. Each of these primary colours is assigned a value from 0 to 255 (8-bit RGB colours).



[477,760] = [9 84 142] [477,764] = [8 77 142]
[477,761] = [8 78 140] [477,765] = [7 78 142]
[477,762] = [9 77 142] [477,766] = [4 80 142]
[477,763] = [9 77 142] [477,767] = [2 81 142]

Fig 3. Representing a part of the images pixel co-ordinates and their values.

Table 1. Representing the changes in R component of selected pixels after embedding the letter ‘k’



Pixel	RGB Value	R value In Binary	k (in binary)	R value after Changing	Resulting RGB Value
[477,760]	[9 84 142]	1001	0	1000	[8 84 142]
[477,761]	[8 78 140]	1000	1	1001	[9 78 140]
[477,762]	[9 77 142]	1001	1	1001	[9 77 142]
[477,763]	[9 77 142]	1001	0	1000	[8 77 142]
[477,764]	[8 77 142]	1000	1	1001	[9 77 142]
[477,765]	[7 78 142]	0111	0	0110	[6 78 142]
[477,766]	[4 80 142]	0100	1	0101	[5 80 142]
[477,767]	[2 81 142]	0010	1	0011	[3 81 142]

For the encryption & embedding process, the user needs to provide 3 inputs.

Source Image

Encryption Key

Pixel Selection Function

The user also needs to select the desired plane for embedding (i.e. R, G or B plane)

The steganographic generated when compared to the original is indistinguishable to a human being.

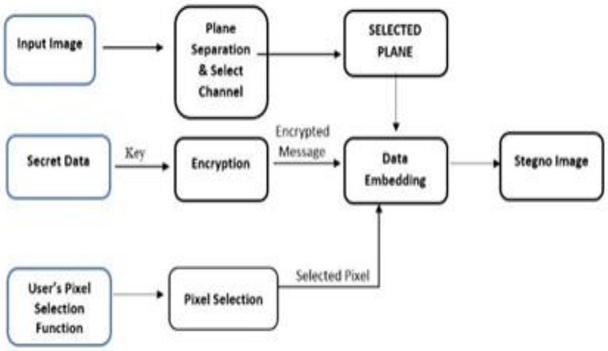


Fig 4. Process Flow chart for Encryption & Embedding

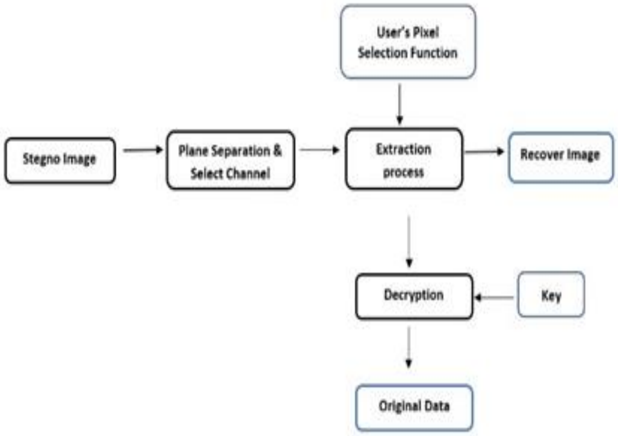


Fig 5. Process Flow chart for extraction and decrypting.

The extraction and decryption require 2 inputs from the user.

1. Decryption Key
2. User’s Pixel Selection Function.
3.

Fig 5. Original Image

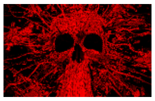


Fig 6.Red Plane

Fig 7.Steganographic Image After Embedding

4. RESULTS AND ANALYSIS

The technique has a lot of advantages as provides user with customization capability and also helps randomness in the selection of pixels being embedded for steganography. It also adopts the methods of using Least Significant Bit and encryption for added security. The technique can be used for formats such as JPEG, PNG, BMP, etc. and the changes made during steganography cannot be identified visually. It is also scalable, as the size/resolution of the image increases, more information can be embedded into.

5. CONCLUSION

As compared to the traditional LSB replacement technique, the proposed method offers flexibility and added layer of security against steganalysis. It’s level of complexity is also controlled by the user i.e. an advanced user could create much more effective way of utilising their image by choosing a complex pixel selection function. The recommended means of transmission is email/file sharing services because LSB is vulnerable to any form of image compression or cropping. Also converting the image to any another form and reverting it could also lead to data loss.

REFERENCES

[1] Champakamala .B.S, Padmini.K, Radhika .D., “Least Significant Bit algorithm for image steganography”, International Journal of Advanced Computer Technology.

[2] Vikas Verma, Poonam, Rishma Chawla, “An Enhanced Least Signifcant Bit Steganography Method Using Midpoint Circle Approach”, Interational Conference on Communication and Signal Processing, April 3-5, 2014, India.

[3] Vipul Sharma,Department , Madhusudan, “Two New Approaches for Image Steganography Using Cryptography”, 2015 Third Interational Conference on Image Information Processing.

[4] Dilpreet Kaur, Harsh Kumar Verma, Ravindra Kumar Singh, “A Hybrid Approach of Image Steganography”, International Conference on Computing, Communication and Automation (ICCCA2016).

[5] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, “Steganography Using Least Significant Bit Algorithm”, International Journal of Engineering Research and applications, vol.2, issue 3, pp. 338-341May-June2012.

[6] Atallah M. Al-Shatnawi, “A New Method in Image steganography with improved image quality”, Applied mathematical science, Vol. 6, no79, 2012.

[7] Vijay kumar sharma, Vishal Shrivastava, “A Steganography algorithm for hiding image in image by improved LSB substitution by minimize technique”, Journal of Theoretical and Applied Information Technology, Vol. 36 No.1,15th February 2012.

[8] S. S. Divya, M. Ram Mohan Reddy, "Hiding Text In Audio Using Multiple LSB Steganography And Provide Securit Using Cryptography," International Journal of Scientifc & Technology, research Volume I, Issue 6, July 2012 ISSN 2277-8616 68 , ijstr©2012

[9] Dawen Xu, Rangding Wang, and Yun Q. Shi, *Fellow, “*Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution”, IEEE

[10] Masoud Nosrati, Rona Karimi, Mehdi Hariri, "An introduction to steganography methods," World Applied Programming, Vol (I), No (3),ISSN: 2222-2510,August 201I 191-19

Authors

Digvijay Singh Sengar
UG Scholar
SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.

Aditya Shrungi
UG Scholar
SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.

Roshan John
UG Scholar
SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.

Anand Singh Kamlesh
UG Scholar
SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.