Digital Innovations & Contemporary Research in SCIENCE, ENGINEERING & TECHNOLOGY
Vol. 12. No. 1, 2024 Series

Article Citation Format
*Abiola, O.A., Ojugbeli, M. & Akinola, S.O. (2024): Concealment of Secret Information In Digital LSB Steganography In Colour and Grey Scale Images. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology. Vol. 12, No. 1. Pp 63-74.
dx.doi.org/10.22624/AIMS/DIGITAL/V11N4P5
www.isteams.net/digitaljournal.

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received 19th January, 2024
Review Type: Blind Peer
Final Acceptance: 29th March 2024

Concealment of Secret Information in Digital LSB Steganography in pColour and Grey Scale Images

***Abiola Oladimeji A, Ojugbeli Mercy & Akinola Solomon O.**
[1,2,3]Department of Computer Science
University of Ibadan
Ibadan, Nigeria.
E-mail: * oladimejiarowolo@yahoo.co.uk mercyojugbeli5@gmail.com, solom202@yahoo.co.uk
[1,2,3]07055535539, 09077610697, 08169748281

ABSTRACT

Modern communication system needs an exceptional way of security, especially on computer networks. The network security is becoming more paramount as the number of data being exchanged on the internet increases. Steganography is the art of hiding information in a cover image without causing statistically significant variations to the cover image. Different types of carrier file formats can be used, but digital images are the most popular ones because of their frequency on the internet. This research work gives an overview of image steganography, it's uses and techniques, basically, to store confidential information within images such as details of working strategy, secret missions, criminal and confidential information in various organizations that work for national security such as military, FBI, DSS, Nigerian police etc. The desktop application has been developed that incorporates Advanced Encryption Standard for encryption of the original message, and Spatially Desynchronized Steganography Algorithm for hiding the text file inside the image. Least Significant Bit (LSB) technique was used in hiding messages in an image. The system enhanced the LSB technique by randomly dispersing the bits of the message in the image and thus making it harder for steganalyst to extract the original message.

Keywords:. LSB, Cryptography, Encryption, Image Processing, Security

1. INTRODUCTION

The Internet of Things (IoT) represents a cutting-edge information technology paradigm—a dynamic network that facilitates communication and interaction among self-configuring, intelligent devices and human users (Cao, et.al., 2021). In this age of internet, the security of information has also been one of the most challenging factors of information technology and communication. Huge volume of data is transferred every second in the internet via e-mails, file sharing sites and social networking sites.

As the number of internet users rises, the concern on the credibility of the services is also on rise, so the concept of internet security has become the important research topic nowadays. The competitive nature of the computer industry has forced the web services into the market at a breakneck pace giving a very little time for audit of system security.

Image steganography is the process of concealing secret contents in a cover image. Thus, the secret contents are hidden in such a way that it is not perceptible to the human eyes (Kaur, et. al., 2022). Different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. Steganography is not to be confused with Encryption, which is the process of making a message unintelligible—Steganography attempts to hide the existence of communication and the message embedding capacity can be increased due to a wider edge area (De Rosal, 2022). The basic structure of Steganography is made up of three components: the "carrier", the message, and the key. Carrier is also known as cover-object, in which the message is embedded and serves to hide the presence of the message. The carrier can be a painting, a digital image, an mp3, even a TCP/IP packet among other things. A key is used to decode/decipher/discover the hidden message. This can be anything from a password, a pattern, a black-light, or even lemon juice. In this project our focus is on implementing digital image steganography, Bitmap image (BMP) using LSB Substitution, although the properties of Image Steganography may be substituted with audio mp3's, zip archives, and any other digital document format.

Basically, our focus is on implementing digital image steganography as shown in Figure 1.1. The Message is the data that the sender wishes to remain confidential. It can be plain text, ciphertext, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as stego-key, which ensures that only recipient who knows the corresponding decoding key will be able to extract the message from a cover-object. The cover-object with the secretly embedded message is then called the stego-object. Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message. Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message.

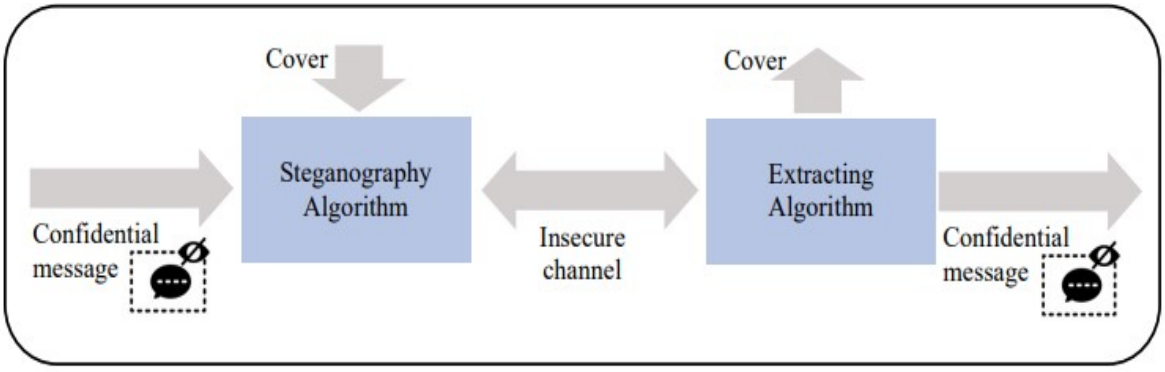

Figure 1; General Scheme of Steganography, (Source; Alqahtany, et.al., 2023)

1.1 Classification of Information Hiding

Hiding information take different forms in term of placing data within media, there are three main forms considered when talking about data security (Inas J. K et al, 2019). Cryptography is changing the data itself by scrambling under certain condition, as if he was openly challenging and no need to hide secret coding because power of encryption method. Watermarking to a certain extent look like steganography and main different by choosing the media of cover and secret. In steganography, many hosting media used to cover secret message as shown in Figure 2. Each cover media has advantage and disadvantage in text media imperceptibility is good but gain less capacity due to text can carry less amount of data while video and audio can use large amount of data accompanied by a few of security exactly the contrary with protocol that has high degree of security with less capacity.

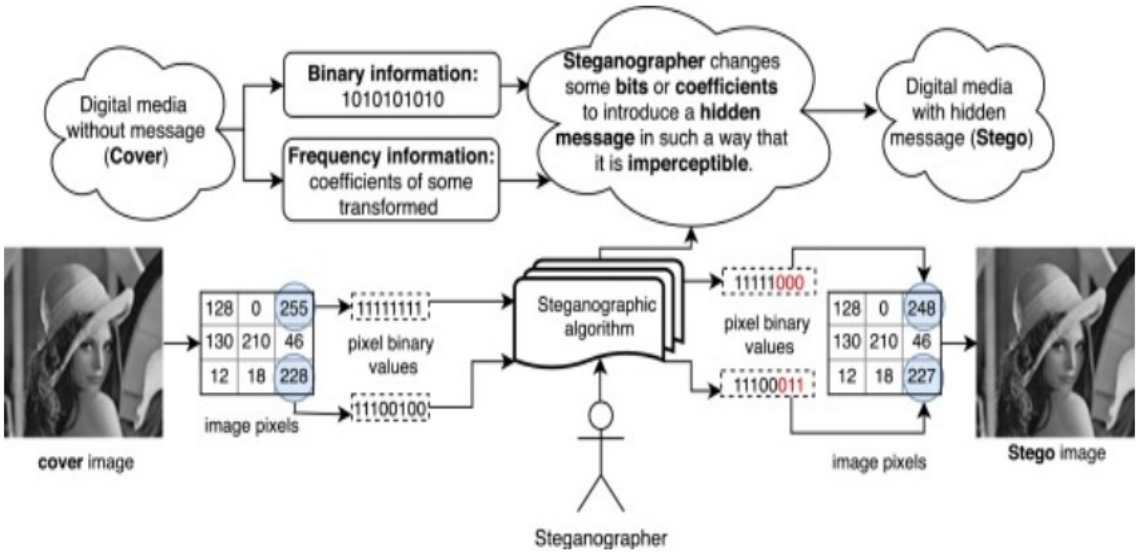

Figure 1.2 Steganography process
(Source; PanelReinel, et.al., 2020)

2. RELATED WORKS

Steganography is the practice of concealing a message within another message or a physical object. In computing/electronic contexts, a computer file, message, image, or video is concealed within another file, message, image, or video. From (Ganiev, *et. al*., 2020) the word steganography comes from Greek steganographia, which combines the words steganós, meaning "covered or concealed", and -graphia meaning "writing". Yan, *et.al*., (2021), reported that steganography sends out secret messages by embedding them into an innocent cover with the goal of conceal the hidden channel using the public channel. The hidden messages appear to be (or to be part of) something else: images, articles, shopping lists, or some other cover text which may be in invisible ink between the visible lines of a private letter. Some implementations of steganography that lacks a shared secret are forms of security through obscurity, and key-dependent steganographic schemes (Pallavi et al, 2018).

Duta et al, (2020), expatiated the advantage of steganography over cryptography that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent and its contents.

2.1 Steganography Vs. Cryptography

Cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from malicious people, whereas steganography even conceals the existence of the message. Steganography must not be confused with cryptography, where we transform the message so as to make its meaning obscure to malicious people who intercept it. Therefore, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message. Natiq and Zahir (2022), expatiated steganalysis as the art and practice of detecting secret material or messages in a digital image (cover) and distinguishing between stego-object and the clean-cover object with little or no understanding of the steganography techniques. The aim of steganalysis is to gather some evidence indicating the existence of an encoded message and it is the inverse of the process of steganography

Cryptography today guarantees that the data sent are protected with the final aim of ensuring the receiver can get to this information from registered roots; cryptography can be regarded as an old technique that has been implemented up to now (panelDilip, et.al., 2022). In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something.

A steganographic scheme with less distorted stego image is more secure than one with a highly distorted stego image, because it does not attract the attention of intruders. An ideal steganographic scheme should have a large embedding capacity and the visual qualityof stego objects should be excellent (panelPranab, et.al., 2020). Steganography does not alter the structure of the secret message, but hides it inside a cover-image so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an “invisible” message created with steganographic methods will not. In other words, steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical steganography systems relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated.

It is possible to combine the techniques by encrypting messages using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique and detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message.

3. METHODOLOGY

LSB Algorithm:

LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image, its simple approach for embedding messages into the image. The Least Significant Bit insertion varies according to the number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message and for a 24 bit image, the colors of each component like RGB (red, green and blue) are changed. LSB is effective in using BMP images since the compression in BMP is lossless. Randomization of bit algorithm in LSB to read in user message, the process takes a large amount of time to process, because bit streams takes too long to process, since the bit algorithm statement needs to order entire message bits that is growing all the time, and by 5 thousand words it takes over 1.5 seconds.

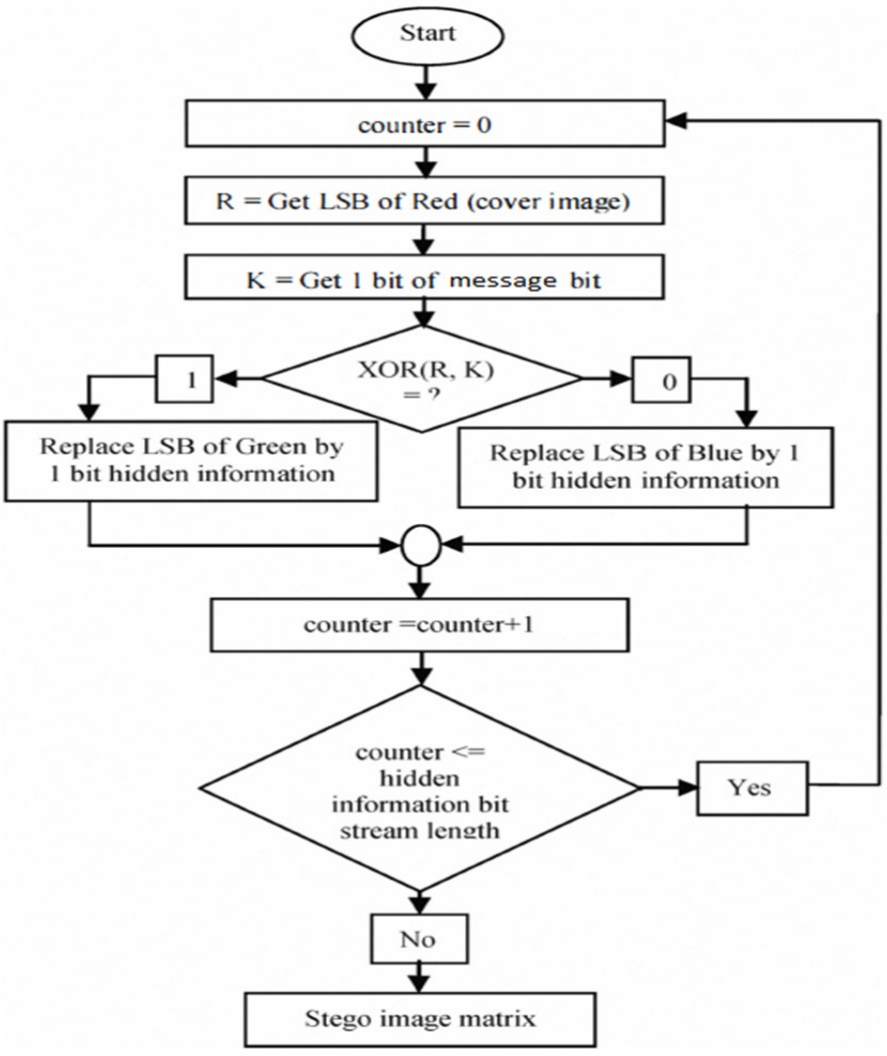

Figure 3. 1 Flowchart to Conceal Information Into A Cover Image

An alternative variant, which generated random bits without ordering the entire message, but by fetching LSB as a random number, took 0.00086 seconds, boosting the input speed. In the future, we recommend the introduction of machine learning in the encryption and decryption process to maximize the bit arrangement process. Least significant bit (LSB) coding is the simplest way to embed information in a digital Image or Audio file. By substituting the least significant bit of each sampling point in Audio and each pixel in Image with a binary message, LSB coding allows for a large amount of data to be encoded. In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHZ.

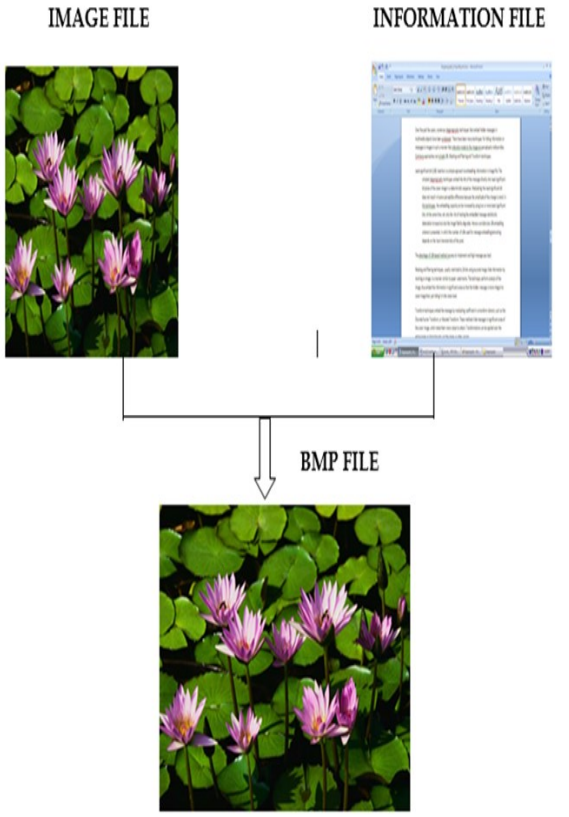

Figure 3. 2 Encryption Process

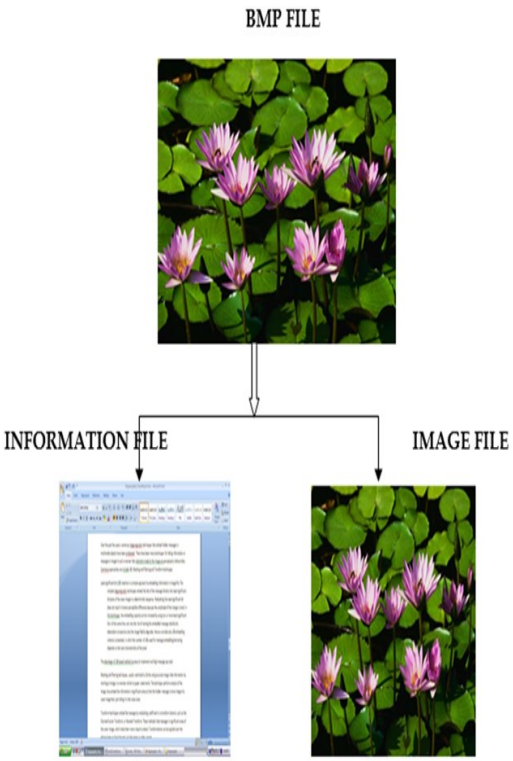

Figure 3.3 Decryption Process

3.3 Encryption and Decryption of short Message

This layout shows the short message encryption and decryption page of the system. With this page, the user can encrypt messages as a file or type a message using the “Type Message” feature. The user can also select a cover image file and encrypt the message. This is shown in figures 3.4, 3.5 and 3.6.

Figure 3.4 image before encryption

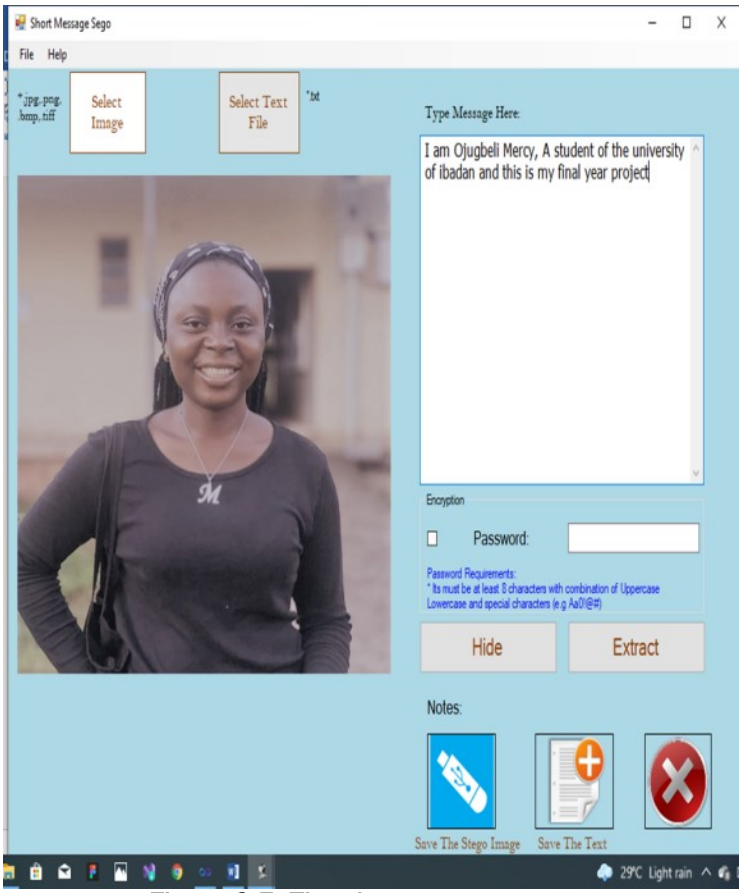

Figure 3.5 The short message page

Figure 3.6 Image after encryption

Encoding

Algorithm For Encoding

1. *STEP 1. //Information from Stegno Key*
2. *Input the key in string datatype;*
3. *//Apply Arithmetic coding to the string key float num = Arithmetic_coding(key); num=num*100;*
4. *x=10*(1st digit of num); y=10*(2st digit of num);*
5. *STEP 2. //converting Plain Text into Bit Stream*
6. *//Input Text to be hidden in string datatype; string plaintext;*
7. *//apply encription algorithm on this string*
8. *string ciphertext = Vigenere_cipher(plaintext); convert ciphertext ASCII form;*
9. *convert ASCII form Bit_stream;*
10. *STEP 3. //Hiding bitstream of input text in Image or Audio file*
11. *int n = length(plaintext);*
12. *//HIDING IN IMAGE FILE*
13. *get_resolution(image) pxq; if (p==odd)*
14. *p=p-1; if(q==odd) q=q-1;*
15. *R value of 1x1 pixel = n; int g =1;*
16. *int h=1;*
17. *int m= bit lodation in Bit_stream; char C= R or G or B;*
18. *for(int i=0;i<8n;i++)*

{
If (m%3==1) C=R;
If (m%3==1) C=G;
If (m%3==1) C=B
Least significant digit of C value of (g+x)x(h+y) th
pixel = Bit_stream[i];
g = g+x;
h = h+y;
}
//HIDING IN AUDIO FILE
string audio_stream= sampled audio
Byte_stream;
audio_stream[0]= n;
for(int i=0;i<8n;i++)
{
If (Bit_stream[i]==0) audio_stream[i++]=audio_stream[i++] AND "11111110";
If (Bit_stream[i]==1) audio_stream[i]=audio_stream[i] OR "00000001";
}
ALGORITHM FOR DECODING
STEP 1. //Information from Stegno Key
Input the key in string datatype;
*//Apply Arithmetic coding to the string key float num = Arithmetic_coding(key); num=num*100;*
x=10(1st digit of num); y=10*(2st digit of num);*
//from IMAGE file
STEP 2. //read stegno image
int n= R value of 1x1 pixel int g=0;
int h=0;
STEP 3. for(int i=1; i<=n;i++)
{
g=g+x;
h=h+y;
string Bit_stream;
char C;
If (i%3==1) C=R;
If (i%3==1) C=G;
If (i%3==1) C=B;
Bit_stream[i--]=least significant digit of C value of (gxh) pixel
}
// from Audio file
STEP 2. //read stegno audio
string audio_stream= sampled stegno audio Byte_stream; int n = audio_stream[0];
STEP 3. for(int i=1;i<8n;i++)
{
Bit_stream[i]=least significant digit of audio_stream[i];
}
STEP 4. //converting Bit Stream into Plain Text

65. *string ciphertext ;*
66. *convert Bit_stream ASCII form; convert ASCII form ciphertext;*
67. *//apply dencription algorithm on this string*
68. *string plaintext = inverse_Vigenere_cipher(ciphertext); PRINT plaintext;*
69. *Vigenere Cipher*

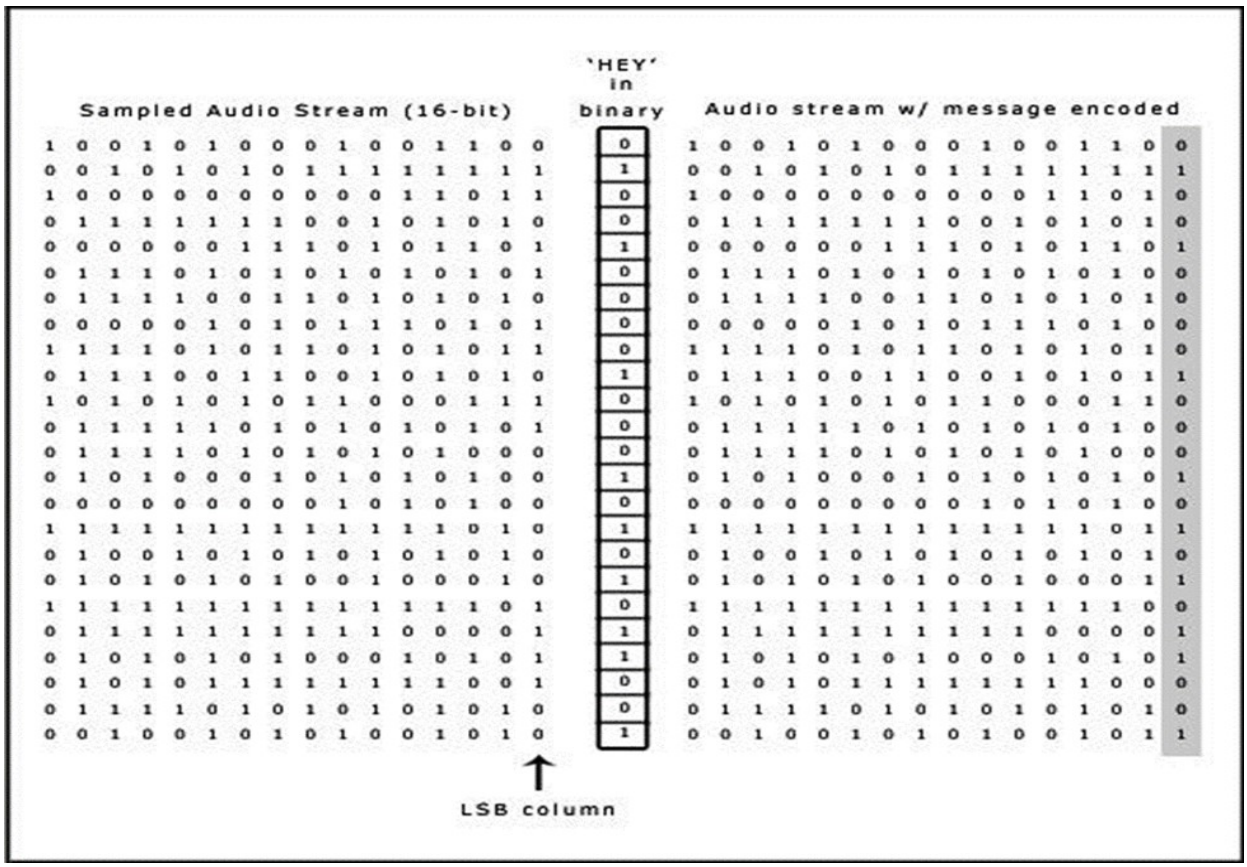

Fig 3.7 LSB method

The above diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method. This page handles the encryption process of the system. It offers the user the platform to encrypt the file. There are two ways to encrypt the message. One of the ways is to load the image and load the already prepared file or load the image and prepare the message on the platform.

3.5 Calculation of Bit Weight

Bit weight calculation is one of the ways to measure its popularity. The calculation of bit weight is focused on creating a labeled weighted graph, where each vertex and edge is associated with a value or several values, like width, weight, length. Vertex weight is calculated based on the number of incoming and outgoing message bits.

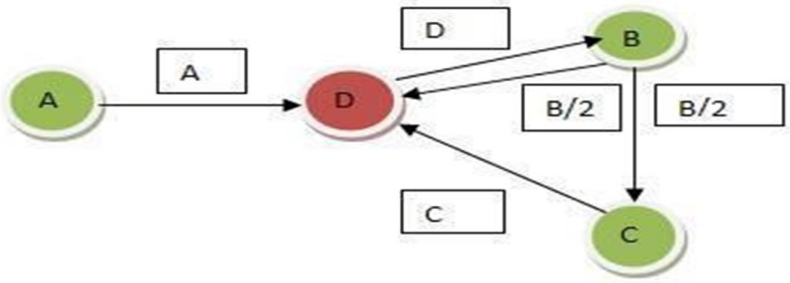

Figure 3.8 Computation Example

Every algorithm has its differences and from Figure 3.8, simplified Bit Rank done with nodes which have some variable ranks (named after vertex names). Every directed edge give a surplus of its weight to a vertex it is pointing to, ergo vertex B has some bit rank B that is equally divided between all edges. It is clear that if A gives entire bit rank to D, then A would have 0 bit rank, which is not exactly a right thing, that's why a limiting factor was introduced – damping factor, which basically states that some part of vertex weight stays with the source. This can be seen as the observer's physical limitation of viewing bits with unlimited depth and statistically is introduced as 15 %.The calculation of A, B, C, D real values can be done iteratively and be represented as a matrix. In the calculation process the new bit rank does not depend on its previous value.

4. RESULTS AND DISCUSSION

This research introduced an alternative approach to information security based on image steganography, which proved to be useful in communication between two entities by ensuring information security. This System enables us to perform remote operations such as data analysis and data compression at the source before data is transmitted over the network. This allows for more intelligent encryption techniques. The architecture used in this research work was medium scaled which was not subjected to the influence of a single selection policy. This system allows user to upload an existing message file or type a new message from scratch in the system. Code optimization was done by finding bottleneck areas of code that need optimization. In order to do this, the entire process was divided by time markers, which should tell us at the end of the process and what part of the code took the most amount of time. The lacks in generalization was made up for in specialization, which would in turn give speed and higher data processing capability. The software is able to insert a text file and an image file in the process of encrypting the image from more than one message input medium.

REFERENCES

1. Kaur, S., Singh, S., Kaur, M. et al. (2022), A Systematic Review of Computational Image Steganography Approaches. Archives of Computational Methods in Engineering (: 14June, 2022 pp. 1-23 https://doi.org/10.1007/s11831-022-09749-0.
2. Alqahtany, S.S.; Alkhodre, A.B.; Al Abdulwahid, A.; Alohaly, M. (2023). A Dynamic Multi-Layer Steganography Approach Based on Arabic Letters' Diacritics and Image Layers. Appl. Sci. 2023, 13, 7294. https://doi.org/10.3390/

3. De Rosal Ignatius Moses Setiadi (2022), Improved payload capacity in LSB image steganography uses dilated hybrid edge detection, Journal of King Saud University - Computer and Information SciencesVolume 34Issue 2Feb 2022 pp. 104–114 https://doi.org/10.1016/j.jksuci.2019.12.007.
4. Natiq M. Abdali, , Zahir M. Hussain (2022), Reference-free differential histogram-correlative detection of steganography: performance analysis, Indonesian Journal of Electrical Engineering and Computer Science, Volume 25, No. 1, January 2022, pp. 329~338, ISSN: 2502-4752 http://doi: 10.11591/ijeecs.v25.i1.
5. Mohammed Mahdi H., Suhad Hasan R., Ali Abdulwahhab A. and Adnan H. Ali (2020), Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography, August 2020 IOP Conference Series Materials Science and Engineering 881(1):012120, DOI:10.1088/1757-899X/881/1/012120.
6. Ganiev, A. A., & Mavlonov, O. N. (2020). The analysis of text steganography methods. ISJ Theoretical. & Applied Science, 22 Jul 2020 (87), 85-88. http://oaji.net/pdf.html?n=2020/679-1608415676.
7. Chaudhari Pallavi, Dhadge Snehal and Rajale Aishwarya (2018), Steganography Based On Embedded System, JournalNX, 2018, pp. 155-157.
8. Pinky Saikia Dutta and Sauvik Chakraborty (2021), Image based Steganography in Cryptography implementing different Encryption-Decryption Algorithm International Journal of Scientific Research in Computer Science, Engineering and Information Technology,© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307 DOI : https://doi.org/10.32628/CSEIT2063191745.
9. Inas J. Kadhima, Prashan P. Peter J. Viala and Brendan Hallorana (2019), Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research, Neurocomputing. Volume 335, 28 March 2019, Pages 299-326, https://doi.org/10.1016/j.neucom.2018.06.075.
10. panelReinel Tabares-Soto, Raúl Ramos-Pollán, Gustavo Isaza, Simon Orozco-Arias, Mario Alejandro Bravo Ortíz, Harold Brayan Arteaga Arteaga, Alejandro Mora Rubio, Jesus Alejandro Alzate Grisales.(2020). 12 - Digital media steganalysis, Digital Media Steganography Principles, Algorithms, and Advances,2020, Pages 259-293.
11. panelDilip Kumar, Sharma, Ningthoujam Chidananda Singh, Daneshwari, A Noola, Amala Nirmal oss, Janaki Sivakumar Matrialstoday, (2022). A review on various cryptographic techniques & algorithms. Proceedings, Volume 51, Part 1, 2022, Pages 104-109
12. Cao, B., Zhang, Y., Zhao, J., Liu, X., Skonieczny, Ł, & Lv, Z. (2021). Recommendation based on large-scale many-objective optimization for the intelligent internet of things system. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3104661.
13. Yan Ke, Minqing Zhang, Jia Liu, Tingting Su, Xiaoyuan Yang (2021). Generative Steganography with Kerckhoffs' Principle. arXiv:1711.04916.
14. PanelPranab K. Muhuri, Zubair Ashraf, Swati Goel(2020). A Novel Image Steganographic Method based on Integer Wavelet Transformation and Particle Swarm Optimization. Applied Soft Computing,Volume 92, July 2020, 106257