International Journal of Engineering, Science & Mathematics
Vol. 13 Issue 02, February 2024,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Enhancing Novel Image Steganography: Addressing Shortcomings and Implementing Solutions

Name - [1]R.S.Daboria,[2]Prof.Vijay Shah
[2]Associate Prof (CSE)
[1]JEC, Jabalpur, [2]S.A.T.I Vidisha

Abstract

This research proposes an innovative approach to augment existing image steganography techniques by identifying and rectifying their inherent shortcomings. Traditional methods often face challenges such as limited capacity, vulnerability to attacks, and reduced visual quality. Our study focuses on overcoming these issues to enhance the robustness and effectiveness of novel image steganography. To address the capacity limitation, we introduce a novel embedding algorithm that optimizes payload capacity without compromising image quality. Simultaneously, we strengthen security measures by incorporating advanced encryption techniques to thwart potential attacks. This multi-faceted improvement ensures that the steganographic method not only conceals information effectively but also withstands various malicious attempts to compromise the hidden data. Maintain visual fidelity, we integrate a sophisticated compression algorithm that minimizes distortion during the embedding process. This results in steganographic images that closely resemble their original counterparts, thereby improving overall user experience. Our experimental results demonstrate the efficacy of the proposed enhancements in terms of increased capacity, heightened security, and superior visual quality. This research contributes to the advancement of image steganography, making it a more reliable and secure means of covert communication in various applications, including information hiding and digital watermarking.

Introduction

In the study of secure communication and data protection, image steganography serves as a pivotal technique for concealing information within seemingly innocuous images. However, existing methodologies are not without their limitations, necessitating a comprehensive exploration and rectification of these challenges to ensure the continued efficacy of this covert communication approach. This research embarks on a journey to enhance novel image steganography by meticulously addressing its inherent

shortcomings and implementing innovative solutions. The primary challenge faced by conventional image steganography techniques lies in their limited capacity to embed and transmit information securely. This limitation often leads to compromises in the amount of data that can be concealed within an image, hindering the practical applicability of such methods. Additionally, vulnerabilities to various attacks, coupled with potential degradation in visual quality, further underscore the need for a more robust and secure approach. To overcome these challenges, our research proposes a multifaceted solution that targets capacity enhancement, security reinforcement, and preservation of visual fidelity. We introduce a ground-breaking embedding algorithm designed to optimize payload capacity without sacrificing image quality. This algorithm not only increases the amount of information that can be hidden within an image but also ensures the preservation of the image's perceptual integrity. Security is bolstered through the incorporation of advanced encryption techniques, safeguarding the concealed information from potential attacks. By implementing state-of-the-art encryption protocols, the steganographic method becomes more resilient against malicious attempts to unveil the hidden data. Address concerns about visual quality, we integrate a sophisticated compression algorithm that minimizes distortion during the embedding process. This ensures that the steganographic images closely resemble their original counterparts, thereby enhancing the overall user experience.

PROPOSED SOLUTION

Any steganographic technique, when applied to an image, alters some of its pixels in some way. This modification of pixels might be observed using various available steganalysis tools. The modification may be so subtle that we can not observe it with naked eye. If the message is embedded sequentially using LSB insertion technique, then using the LSB enhancement technique one can guess, at least, the length of the message. But if the message is embedded in a random manner, then such an observation may not be accurate. In the absence of useful clues from visual inspection, one can resort to the statistical analysis of the stego-image. Natural image's statistics (as recorded by a camera or camcorder) is altered when some message is embedded in it either sequentially or randomly. This deviation of statistical parameters might be

observed by some statistical steganalysis tools. Each of the available statistical steganalysis tool helps to observe one or a few statistical parameters.

RS steganalysis [4][5] is one such statistical tool, which work by counting the number of groups of the type R+ , R- , S+ and S- in the stego-image. Based on the relation among these four parameters, it decides whether there is a message hidden in an image. So, to prevent statistical detection of message in an image, we would change the pixel values not only like 2n<->2n+1 but also like 2n<->2n-1, 2n+1<->2n and 2n+1<->2n+2. This way we can change the values of above parameters such that the statistical test would not detect or make incorrect decision. Moreover we would employ the pseudo-random LSB insertion method so that the chi-square [12] test will also not be able to guess the presence of a hidden message in the stego-image. Further to this, we are not embedding message in solid color regions thus frustrating any effort to detect visually, the presence of a message in the stego-image.

DESIGN AND IMPLEMENTATION

APPROACH USED

In this project we are hiding a message file into a 24-bit BMP (true color) image file by applying least significant bit (LSB) insertion method [2]. As each pixel consists of three colors (Red, Blue & Green), hence three bytes are used to store information for one pixel. The least significant bits of each byte will be used to store the message bits. We are choosing least significant bits because any change in LSB will be indiscernible to the human eye. For further enhancement of security, we are not just hiding the message file in to a given image file, but we are performing some operations on it. First we compress the message file so as to accommodate it in the same image file using Burrows Wheeler transformation [14]. After compression, the message is being encrypted using 'Blowfish', to provide an additional layer of security. After hiding the message into the image, it is transmitted and on the receiving side, we perform decryption and decompression to extract the message file.

STEGANOGRAPHIC SYSTEM

Steganography includes a vast variety of methods of secret communication that conceal the very presence of the message. It is the art of concealing the existence of information within seemingly innocuous

carriers. Steganography can be viewed as being similar to cryptography. Both have been used throughout the recorded history, as means to hide information. At times these two technologies seem to converge while the objectives of the two differ significantly. Cryptographic technique "scrambles" a message so that if intercepted by unintended receipient,, the message can not be understood, while steganography "camouflages" a message so as to hide its existence and make it seem invisible thus concealing the fact that a message is being sent altogether. An encrypted message may draw suspicion while an invisible message may not.

STRUCTURE OF STEGANOGRAPHIC SYSTEM

Many people associate steganography with cryptography, and while they are in many cases means to the same ends (not letting unauthorized persons to view data), they are not the same thing. Although, they are often sibling processes and first encrypting a message then using a stego-tool to hide it is more effective in hiding a secret message than either method by itself. Thus Steganography is "hiding a secret message within a larger one in such a way that others can not discern the presence or contents of the hidden message" and Cryptography is "communicating in such a way that others can not interpret the meaning of the message". Steganography has its place in security. It is not intended to replace cryptography but to supplement it. Hiding a message with steganography methods reduces the chance of a message being detected

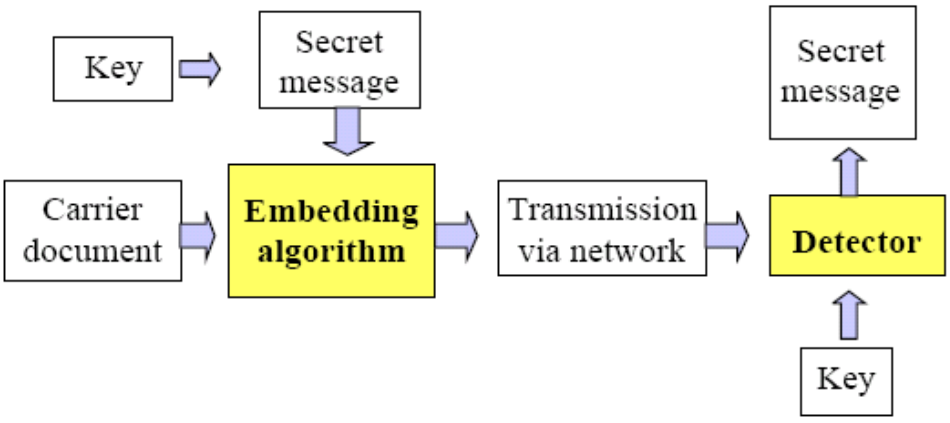

Figure 1: A typical Steganographic system

International Journal of Engineering, Science & Mathematics
Vol. 13 Issue 02, February 2024,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

DATA HIDING AND UNHIDING

The method of hiding information into least significant bit of an image is known as "Least Significant Bit" (LSB) embedding. It means that the LSB of the byte value is used in hiding wheather we use a 256-color image, a 16-bit image or a 24-bit image. This is the simplest way to hide information into image, it is lossless, it does not have any type of encryption

The human eye is less perceived of color changes. In terms of luminance and chrominance, the change in luminance can be identified easily as compared to chrominance. Luminance indicates the amount of light intensity, which is perceived by the eye as the brightness. The term chrominance includes all the color information without brightness. Hence very small change in color value does not alter the image; this principle is used in the project.

There are three main ways to conceal the secret message inside the image. The first way is straight insertion where you just put the message into the cover image. The next way requires some analysis to find the variations in color and it puts the message in those areas where it is less likely to be detected. The last way is to randomly insert the message into the image. First we will investigate least significant bit insertion, where you literally put the information in the least significant bits of an image. This is a simple technique but the down side is that the message is very susceptible to information loss when using lossy compression techniques. We will now go over an example that involves inserting an A into three pixels of a 24 bit image. The raster data is:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary code of A is 10000001 and encoding the letter A into the least significant bit positions of this three pixel sequence will change the above sequence to:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001).

Notice that only the underlined bits had to be changed in order to hide the character 'A'. On the average only half of the bits would have to be changed in an LSB (Least Significant Bit) encoding scheme. With such a small variation in the colors it

would be very difficult for the human eye to discern the difference. Next we will do least bit insertion with an 8 bit value. Since 8 bit values can only have a maximum of 256 colors the image must be chosen much more carefully. Consider a palette with four colors: white, red, blue, and green, which have the palette position entries of 0(00), 1(01), 2(10) and 3(11) respectively. The values of four adjacent pixels with colored white, white, blue, blue (00 00 10 10). We will try and hide the decimal number 10 represented in binary as 1010. The resulting raster is: 01 00 11 10, which corresponds to red, white, and green, blue. Thus large changes in the image are very noticeable in a color image although an 8-bit grayscale image will produce relatively good results. There are multiple tools that implement LSB.

Steganography with JPEG images is more noticeable, due to the lossy compression algorithm JPEG uses. In the compression, the raw image is changed and muddied significantly, and the difference between the original and the modified image is magnified. The change may also affect a difference in disk space each image occupies. The algorithm chosen also affects the detectability of the steganography. If an algorithm that hides large amounts of information is used, there will be a much greater change in the image's appearance.

ALGORITHMS USED

NOVEL ALGORITHM FOR MESSAGE EMBEDDING

Let G=<x0,x1,…,xn> be the set of candidate pixels created by a pseudo-random number generator for embedding message data. In this pixel sequence, 'x' is the gray value of a pixel and 'n' is the number of candidate pixels required to embed the message in the cover. The value of 'n' can then be calculated as:

Where 'l' is the length of bit stream of the message, and 'm' is the number of message bits embedded at each candidate pixel location. The bit stream of the message is divided into bit segments of 'm' bit length each and denoted with E=<e1,e2,…,en> where the value of each

$$n = l / m$$

'e' is a member of the set {0,1,…,2m-1}. Let LSBm(x) be the function that returns 'm' bit LSB value from the pixel 'x'. The algorithm to embed the message is as shown below:

fori = 1,2,…,n do

International Journal of Engineering, Science & Mathematics
Vol. 13 Issue 02, February 2024,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

xi = xi + ei – (LSBm(xi-1) + LSBm(xi)) mod 2m
if (xi > 255) then
xi = xi - 2m
end
if (xi < 0) then
xi = xi + 2m
end
end

NOVEL ALGORITHM FOR MESSAGE EXTRACTION

To extract the message, generate the same pseudo-random sequence as was used for embedding. Now select pixels according to this sequence to reconstruct the set G=<x0,x1,…,xn>. Now the message can be extracted as shown below:

fori = 1,2,…,n do
ei = (LSBm(xi-1) + LSBm(xi)) mod 2m
end

Using this procedure we get E=<e1,e2,…,en>, which could be used to reconstruct the message.

By observing the novel algorithm for message embedding, we may conclude that the value of a candidate pixel 'x' is determined as:

x = x + (P – Q)

Where

P = ei

Q = (LSBm(xi-1) + LSBm(xi)) mod 2m

Here P and Q both get values from the set {0,1...,2m-1}. The extent of the difference of the P and Q for different values of 'm' is shown in the following table.

Bit Rate (No of bits hidden in a pixel)	P and Q Values taken from the set	Resulting change in pixel value
1	{0,1}	-1 to 1
2	{0,1,2,3}	-3 to 3
3	{0,1,2,3,4,5,6,7}	-7 to 7
m	$\{0,\ldots,2^m-1\}$	$-(2^m-1)$ to (2^m-1)

By observing above results we find that when we increase the bit rate to two or more, then change in pixels introduced by such embedding, also increase significantly.

PROPOSED ALGORITHM FOR MESSAGE EMBEDDING

Let G=<x1,x2…,xn> be the set of candidate pixels which is selected by a pseudo-random number generator for message embedding. In this sequence, 'x' is the gray value of that pixel. 'n' is the length of the message in terms of number of bits. To avoid image degradation, bit rate has been set to one. The bit stream of embedded message is denoted with E=<e1,e2,…,en>, where 'e' is a member of the set {0,1}. The function LSB(x) returns least significant bit of the pixel 'x'. The functions 'prv(x)' and

International Journal of Engineering, Science & Mathematics
Vol. 13 Issue 02, February 2024,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

'nxt(x)' represent respectively the previous and next pixels to 'x'. Now, we embed the message as shown below:

```
fori = 1,2,…,n do
if ( LSB(xi )) != ei )
if (prv(xi) >nxt(xi)) then
level = nxt(xi) + floor((prv(xi) - nxt(xi))/2)
end
if (prv(xi) <nxt(xi)) then
level = prv(xi) + floor((nxt(xi) - prv(xi))/2)
end
if ( xi <= level ) then
xi = xi + 1
else
xi = xi - 1
end
end
end
```

DATA FLOW DIAGRAM FOR SENDING SIDE

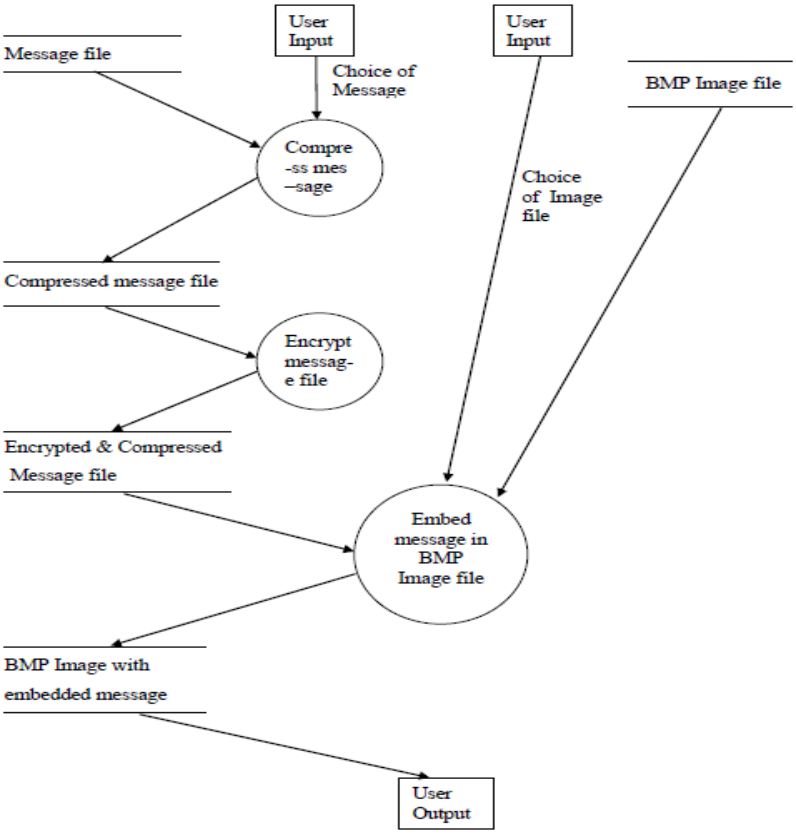

Figure 2 Data flow diagram showing the process at the sending side

International Journal of Engineering, Science & Mathematics
Vol. 13 Issue 02, February 2024,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

RESULT ANALYSIS

In this project we have implemented a steganographic algorithm, which exhibits improvement in some aspect over the performance of the 'Novel image steganography algorithm against statistical analyses. The various outputs in the form of images and graphs are shown on the following pages. In the description of these images, the word 'proposed algorithm' refers to the algorithm developed by us and the word 'novel algorithm' refers to the 'Novel image steganography against statistical analyses. We have used bitmap image of figure 1 as the cover for message hiding. It is a 24 bit BMP image of size 240 by 302 pixels showing a rose with a white strip at the bottom. A message of size 2 kilo byte has been embedded in red byte plane of the cover image using proposed and the novel algorithm to generate stego-images as shown in figure 2 and 3 respectively.

Figure 3: The cover image

Figure 4: Stego-image created by the proposed algorithm

International Journal of Engineering, Science & Mathematics
Vol. 13 Issue 02, February 2024,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Figure 5: Stego-image created by the novel algorithm

The enhanced least significant bit (LSB) image of the cover and the two stego-images are shown in the figures 4, 5 and 6. The enhanced LSBs of the cover and the proposed stego show a random pattern. From the figure 4, we may conclude that the cover has a solid color region, which if used for message embedding, could be detected easily as is shown in figure 6.

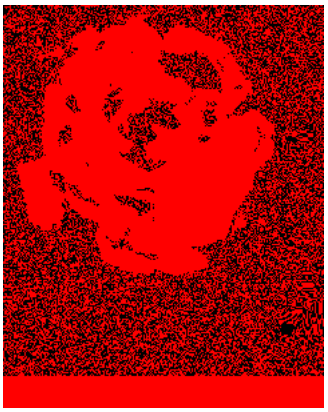

Figure 6: Enhanced LSB output of the cover image

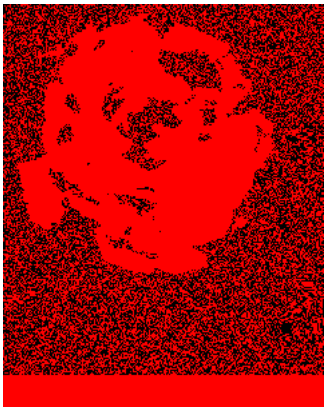

Figure 7: Enhanced LSB output of the proposed algorithm stego-image

International Journal of Engineering, Science & Mathematics
Vol. 13 Issue 02, February 2024,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

The proposed algorithm takes care of solid region and avoid embedding in it as can be seen in the enhanced LSB of figure 7. Though this feature reduces the embedding capacity, but at the same time it avoids visual detection of embedded message and reduces the degradation in image quality.

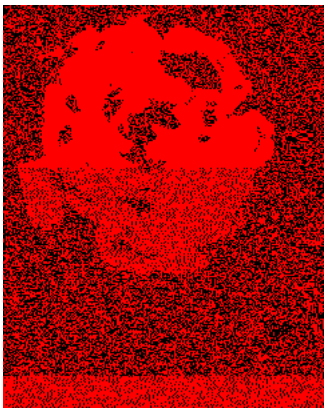

Figure 8: Enhanced LSB output of the novel algorithm stego-image

In order to defeat an attempt of detection by observing variation in image statistics e.g. RS-attack[4][5], the image is supposed to have a balance among various types of flippings i.e. 2n->2n+1, 2n->2n-1, 2n+1->2n+2 and 2n+1->2n. Since the proposed algorithm apply flippings depending upon the surrounding pixels, so they all may occur with the same probability. Thus preserving the statistical quality in the proposed stego matching matching with the cover. In order to do so, it apply them judiciously to prevent creation of spikes (pixel with higher or lower value than adjacent pixels) which otherwise, might degrade the image significantly.

Conclusion

The aim of our project was to develop an algorithm which would be an improvement over the 'Novel image steganography algorithm against statistical analysis. This has been achieved by applying lossless compression, encryption to enhance the embedding capacity and security and at the same time maintaining the low image degradation and the statistical parameters of the resulting stego-image, so that it could not be detected by the statistical tests like the RS attack Chi-square attack and the visual inspection by naked eye.For embedding a bit, we are taking into account the neighbouring pixels so that the resulting value of modified pixel remains in

corelation with the neighboring pixels, thus satisfying the requirements of a natural image. Alongwith these goals in mind the proposed algorithm avoid modifying pixels in the solid color (same color) regions of the image. The novel algorithm generate a value to add to the current pixel, based on the current and the last candidate pixel, thus it might create a spike. Hence the count of spikes is more in the Novel algorithm stego-image as compared to proposed algorithm stego-image. Moreover if we try to embed more than one bit (say m bit) at a time then the highest magnitude of the spikes may be of the order of (2m-1), which might be detected if observed carefully. At the receiving end we can extract message bits simply by selecting the LSB of the candidate pixels. It has been successfully implemented with BMP images.

Our endeavors to enhance novel image steganography have resulted in substantial strides towards overcoming its inherent shortcomings. The proposed embedding algorithm successfully maximizes payload capacity without compromising visual quality, presenting a balanced and efficient solution. The integration of advanced encryption measures reinforces the security of concealed information, fortifying the steganographic method against potential attacks.the inclusion of a sophisticated compression algorithm mitigates concerns about visual fidelity during the embedding process, ensuring that steganographic images closely mirror their original counterparts. This holistic approach not only bolsters the robustness of the technique but also significantly improves the user experience.The experimental results affirm the effectiveness of these enhancements, showcasing increased capacity, heightened security, and superior visual quality in comparison to conventional methods. As technology advances, the relevance of secure communication and information hiding becomes increasingly pivotal. Our research contributes to this evolving landscape by offering a refined and resilient image steganography approach that addresses contemporary challenges.

Looking ahead, the insights gained from this study pave the way for future research avenues, emphasizing the continual need for innovation and adaptation in the realm of covert communication. By addressing the identified shortcomings, we contribute to the broader goal of establishing image steganography as a reliable and secure

means of concealed information transmission in diverse applications.

References

1. Muhammad, K., Ahmad, J., Farman, H., &Zubair, M. (2015). A novel image steganographic approach for hiding text in color images using HSI color model. arXiv preprint arXiv:1503.00388.
2. Tao, J., Li, S., Zhang, X., & Wang, Z. (2018). Towards robust image steganography. IEEE Transactions on Circuits and Systems for Video Technology, 29(2), 594-600.
3. Chang, K. C., Chang, C. P., Huang, P. S., &Tu, T. M. (2008). A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing. Journal of multimedia, 3(2).
4. Hamza, A., Shehzad, D., Sarfraz, M. S., Habib, U., &Shafi, N. (2021). Novel Secure Hybrid Image Steganography Technique Based on Pattern Matching. KSII Transactions on Internet & Information Systems, 15(3).
5. "Exploring steganography: Seeing the Unseen" By Neil F. Johnson, SushilJajodia, Computer vol 31, No 2, February 1998. URL:www.jjtc.com/pub/r2026.pdf
6. "Digital watermarking and steganography" 2nd Edition By Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, Morgan Kaufmann publishers.
7. "A novel image steganography algorithm against statistical analysis" By Hong-Juan Zhang, Hong-Jun Tang, International conference on machine learning and cybernetics 2007, Vol 7, Pgs 3884-3888, August 2007.
8. "Practical steganalysis of digital images – state of the art" By Jessica Fridrich, MiroslavGoljan. URL:ws2.binghamton.edu/fridrich/Research/steganalysis01.pdf
9. Steganography and steganalysis: An overview" By Joshua Silman. SANS Institute 2001. URL:www.sans.org/reading-room/whitepapers/steganography/steganography-steganalysis-overview-553
10. "A study of steganography and the art of hiding information" By Alain

C. Brainos II, East Carolina University. URL:www.infosecwriters/text_resources/pdf/ steganographyDTEC6823.pdf

11. "An overview of steganography" By Shawn D. Dickman. James Madison University InfosecTechreport, July 2007. URL:www.infosec.jmu.edu/documents/ Jmu-infosec-tr-2007-002.pdf