Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 6, No.4, June : 2024

REVIEW ON DEEP LEARNING BASED SECURE DATA TRANSFER OVER INTERNET USING IMAGE STEGANOGRAPHY AND IOT

Mr.Sharath Babu CG,Assistant Professor,Dept Of Computer Science And Engineering Sri Siddartha Institute Of Technology Tumkur
Dr.Komala K,Associate Professor,Dept Of Electronics And communication Engineering Sri Siddartha Institute Of Technology Tumkur

Abstract
The application of optimisation methods in steganography—the practice of concealing confidential information in other data—is examined in this review study. Shown that optimisation strategies work well to enhance steganography systems' performance, especially when it comes to maximising the quantity of secret data that can be concealed while minimising the influence on the cover data. The most recent optimisation methods for steganography like genetic algorithms, particle swarm optimisation, ant colony optimisation, and fruit fly optimisation, are thoroughly reviewed in this study. The advantages, drawbacks, and possibilities for future advancement of these approaches are also covered in this study. Additionally, the PSNR (Peak Signal to Noise Ratio), payload capacity, SSIM (Structured Similarity Index), and other metrics were compared between the state-of-the-art techniques. The significance of optimisation approaches in steganography and their possible influence on the creation of more effective and safe steganography systems are highlighted in the review's conclusion.
keyword; Secure data transfer; Image Steganography; Versatile Applications of Steganography;

1 Introduction

These days, information technology has had a huge effect on the types of online business possibilities that are available. New technologies have many benefits, but they can also put some businesses at risk when it comes to information protection. Because of this, safe data sharing is becoming more and more important [1]. This study aims to come up with a strong answer to this problem using image steganography, a powerful way to hide protected data within pictures to keep it safe from prying eyes [2]. Steganography is a safe way to send secret messages over networks and the internet. Because of this, it is very useful in many places, like the military and secret companies. When cryptography [3] and steganography[4] are used together, they add an extra layer of security that makes moving secret information safer.

The Imperative for Secure Data Transfer:

Making sure data transfers are safe has become very important for all types of businesses because cyberattacks are happening more often and are getting better. Traditional ways of encrypting data are useful, but they might not be enough to stop skilled attacks. [5] Because of this, extra steps like steganography are becoming more and more necessary to protect private data from people who shouldn't have access to it and people who want to steal it.

Image steganography is a strong way to keep information safe.

Secret info in pictures is a great way to keep it safe when using computers. [6] Steganography hides secret data by weaving protected data into. This makes it almost impossible for people to find it. [7] This secret layer of security makes the information being sent more private and secure, keeping it safe from possible breaches.

Versatile Applications of Steganography:

Steganography is very useful in many situations, but it is especially useful in military activities. [8] When dealing with private companies, steganography makes it easier for clients and service providers to send and receive private information safely, protecting both privacy and trust. People in the military use steganography to send secret messages to each other. This defends national interests and makes missions safer.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 6, No.4, June : 2024

Adding to existing cryptographic methods to make them safer:

Data that is encrypted can't be read by people who shouldn't see it. Steganography adds another layer of security, making it hard to find data that is hidden. [9] By using these two steps, you can make sure that doing business online is safer and that your important info is safer as well. Digital steganography is often used to show who owns multimedia content. Powerful steganography is needed to hide data in a safe and secure way in many multimedia programs. Figure 1 uses terms that are unique to this field of study to show the most common ways that steganography is used. Watermarking is an important part of steganography because it hides an owner's mark right into multimedia files so that the real owner can be found. [10] A stamp (W) is added to the source media (X) to make the marked picture (X'). The stamp acts as a secret mark that lets you know who owns the paper. It should be impossible to find and impossible to attack or change for the watermarking process to work. But sometimes, extra needs may mean that you need watermarking that is clear or simple to get rid of. [11] A general plan for steganography is shown in Figure 2. It reveals how the stamp is hidden in the original file. During this step, a key can be used to create a better mark, which in turn makes the information that is put in safer and more private. With digital steganography in multimedia programs, you can hide information, protect intellectual property, show who owns something, make sure the information is real, and track down changes that have been made. Today, strong steganography techniques are needed to protect intellectual property rights and make sure the accuracy of multimedia content.

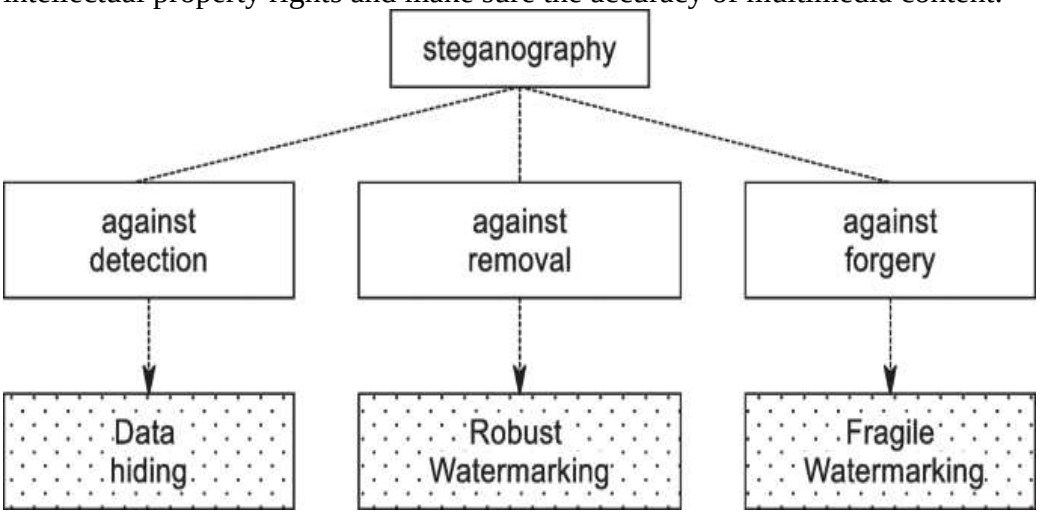

FIGURE 1 How to use steganography and the different terms for it [14]

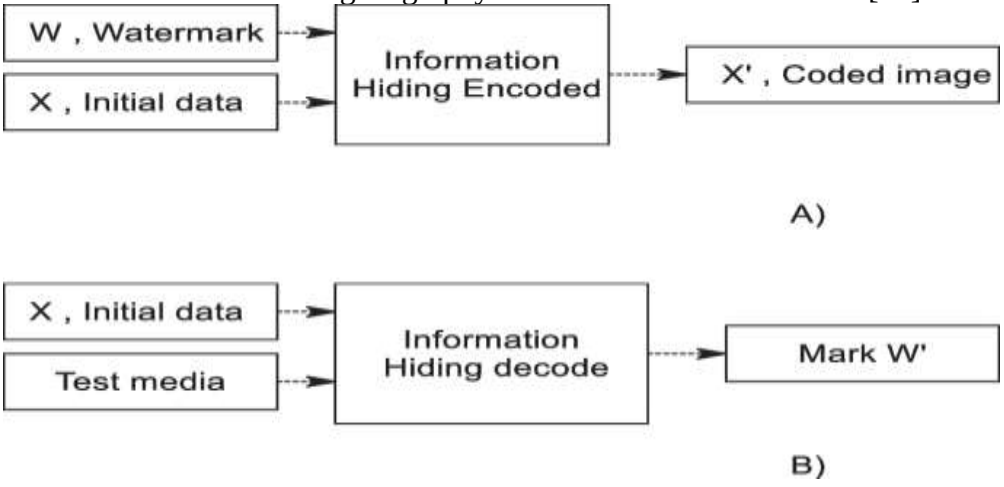

figure 2 Block diagram of how to hide data: encoder (A) and decoder (B) [13]

A key that is used for steganography can also be used for cryptography. This gives the hidden message an extra layer of protection. Figure 1B [14] shows that once the receiver gets the stego picture X', it has to figure out what the message means and put the steganography process backwards to find the

secret mark W'. The following equations (1) and (2) show how the original cover picture X maps to the marking W. This helps us show the ideas behind steganography formally. When a key is used, it is shown between the quotes. The key is a big part of figuring out where the replacement bit goes, which makes the embedded message safer overall.

$$X^{'} = E\left(X, W, [Key]\right)$$

$$W^{'} = \mathrm{D}\left(\mathrm{X}', [\mathrm{X}], [\mathrm{Key}]\right)$$

In equation (1), X' is the marked image that was moved. It is made by adding the stamp W to the cover picture X. It is possible to attack the system even if the key is used because it is an extra input that guides the steganography process and helps describe where the new bit goes. The signature that was found on the stego picture X' is shown by W' in equation (2). The extraction process is easy when the key is used, and the secret mark is always found properly. I'm going to call the first cover picture X a "cover" image and the marked image that was moved a "stego" image. The ideas behind steganography are clearer when you use these mathematical notations. This makes it easier to understand and use properly. By using both steganography and cryptography together, information can be safely added to and taken out of multimedia material. They are mostly used to solve problems with multiple goal functions that are at odds with each other.

These methods are based on natural processes and make it easy and quick to solve difficult optimisation problems. One problem with them is that it's not always possible to reach global optima [15]. This paper describes a new way to improve the Peak Signal-to-Noise Ratio (PSNR) in picture steganography that is based on bio-inspired methods. One major goal of this method is to keep the quality of the picture while it is being steganographed. The tests showed that the suggested way does raise PSNR, which means that after steganography, the picture quality is better kept. Along with that, the study looks into the best order to use the chosen bio-inspired algorithms in order to get the best outcomes. These bio-inspired algorithms can be used together to make the picture steganography process better and more effective. We can use their best features and get around their flaws. Exploring different combos helps us find the best ones, which improves the quality of steganographically changed pictures and makes the whole system work better.

Related works

LSB, pixel value differencing, randomised, circular, and other ideas have been put forward for digital steganography over the last few decades. Each has its own pros and cons. In particular, the LSB technique5 is the most well-known and commonly used way to hide a message inside a cover media. [16] This method is widely used because it is easy to understand and follow. Let's figure out what RGB and HSI models mean, though. The tone of something is one of its most important parts.

People usually use variety in picture handling because of two main reasons.

A colour is a strong way to describe a scene because it makes it easier to find things and understand what they look like.

People can tell the difference between thousands of different colour shades and levels, while there are just too many shades of grey.

The second one is mostly important for actual picture analysis, which is done by people. Having a colour model or colour system makes it easier to describe colours in a way that everyone agrees on when you're working with images, which is what image processing is all about. [17] The HSI model is what this work is mostly about. You can freely switch between the HSI colour model and the RGB and CMY models17 while making colours in the RGB model. This colour system worked great for device applications. Although the human eye is naturally drawn to red, green, and blue colours, the RGB system works well with them.

People name things that are colored by their shade, strength, and shine. [18] The shade of a color, like yellow, red, and orange, makes it clean. On the other hand, saturation shows how much white light changes the color of a clear color. One thing that is hard to measure, though, is desire. The HSI model splits the part of a color picture that deals with intensity from the part that deals with color (hue and saturation). The HSI color model is a great way to find easy-to-understand ways to process pictures based on color descriptions. We think RGB is the best tool for making colors, but it's not great for talking about colors. The HSI color model is a great way to hide important data. In RGB, all the planes are clearly linked, but this is not the case. It costs a little less to work with a picture in the HSI model when using LSB-based methods, etc., because each one is different. [19] The process of LSB is to hide the hidden message in the pixels of the LSB cover picture. This can be done at random or in a certain order, as seen in Fig. 3. Shows how the embedding process works in Equation (1).

$$S^{IM}_{(i,\ j)} = C^{I}_{(i,\ j)} - C^{I}_{(i,\ j)} \mathrm{mod}_2^K + S^{M}_{(i,\ j)}$$

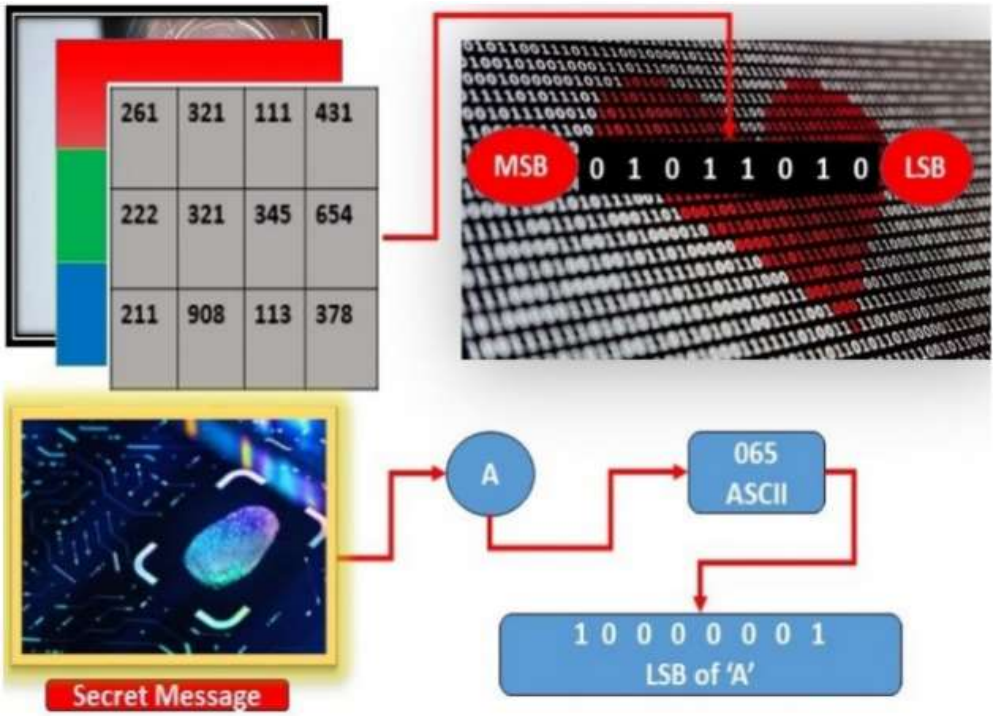

Figure 3 The basic concept of least significant bit (LSB).

The stego image i is shown by SIM (i, j), the cover image is CI, and the secret message is SM. where j stands for column and row. [20] Anyone with an open eye can see or guess that any smooth part of a picture hasn't changed much24. Putting the picture on top of the secret message can be done at random or in a set order. Different types of picture steganography are changed so that the right amount of information can be hidden in the right cover objects25.

Randomization was used by Khan et al. to come up with a cyclic image-based steganography method. It was hard for the people who wrote this to make sure that all of the basic requirements were met. They also added 4–8 KB secret notes to the text. Not all attacks can be stopped, like ones that change the size, add noise, crop, etc., but this is a better way to hide pictures.29.

Rustad et al. came up with a new way to hide images that makes them more clear to the human eye. The LSB method is turned around and an adaptable pattern is used.

When Cheng and Huang changed the interpolation picture and the histogram, they came up with a new way for encrypted image-based steganography to work both ways. As part of this study, the author changed the positions of the pixels in a picture using the double scrambles method. The test results showed that the anchoring ability and security were high31.

Shwe Sin et al. come up with a way to hide things using LSB and Huffman codes. The research showed that the method had a high ability for embedding and better security32.

Even so, the way that was mentioned can be made better for HC, on top of these benefits. [23] The suggested work is built on LBP, so it doesn't see the surface and smooth pictures clearly when the EBs are added.

[24] The results were surprising when it came to the area that had been changed and the plans that could not be carried out. Later, the work that was suggested can be linked to getting the changed bits back on your own and making more room for change and moving things around even more. Steganography with images has been used in a number of known works. Table 1 shows some studies that have been done on the way things are done now.

Table1. Image steganography criteria are used to evaluate the pros and cons of different current methods.

Techniques	Pros	Cons	Measuring algorithm				
			Capacity	Security	Transparency	Temper protection	Computation
Canny edge detector[16]	High strength and safety	Low quality and payload	No	Yes	No	Yes	Yes
Huffman Encoding[17]	A high capacity and a good ability to blend in	Secure less	Yes	No	Yes	Yes	No
Huffman coding and the LSB replacement[18]	Embedding ability, safety, and invisibility	Can’t resist against attacks and time consuming	Yes	Yes	Yes	No	No
Adaptive Huffman code mapping (AHCM)[19]	More safe payload	Low quality image	Yes	Yes	No	No	Yes

To sum up, Table 1 showed a study of the different ways that are already out there using the basic measure of steganography. It also went into detail about the methods used, their pros and cons, major goal, integration process, and what each method couldn't do. Choosing the right cover object and making sure it meets the most important steganography criteria. Because some people tried to make a reliable method but only got one or two factors right. They also broke the other criteria and the trustworthiness between the criteria, which is an important part of steganography. [25] However, the

suggested algorithm is made in a way that shows which picture size is best for which secret message size. This is done to meet these important goals and make a reliable method. But in the next part, we'll talk about the suggested algorithm's whole process in more depth.

3. Proposed Algorithm

This section describes about the encryption and the decryption methods. **Encryption Method (Sender's End): Step 1**: Pick out the text file where the first message was written. Use the RSA method and the receiver's public key to encrypt the text file's information. Step 3: Choose a good cover picture (.jpeg file). The fourth step is to read the image's title and tail from an array file. Add the protected data to the end of the picture tag. Step 6: Both the sender and the user are connected with the internet figure 4.

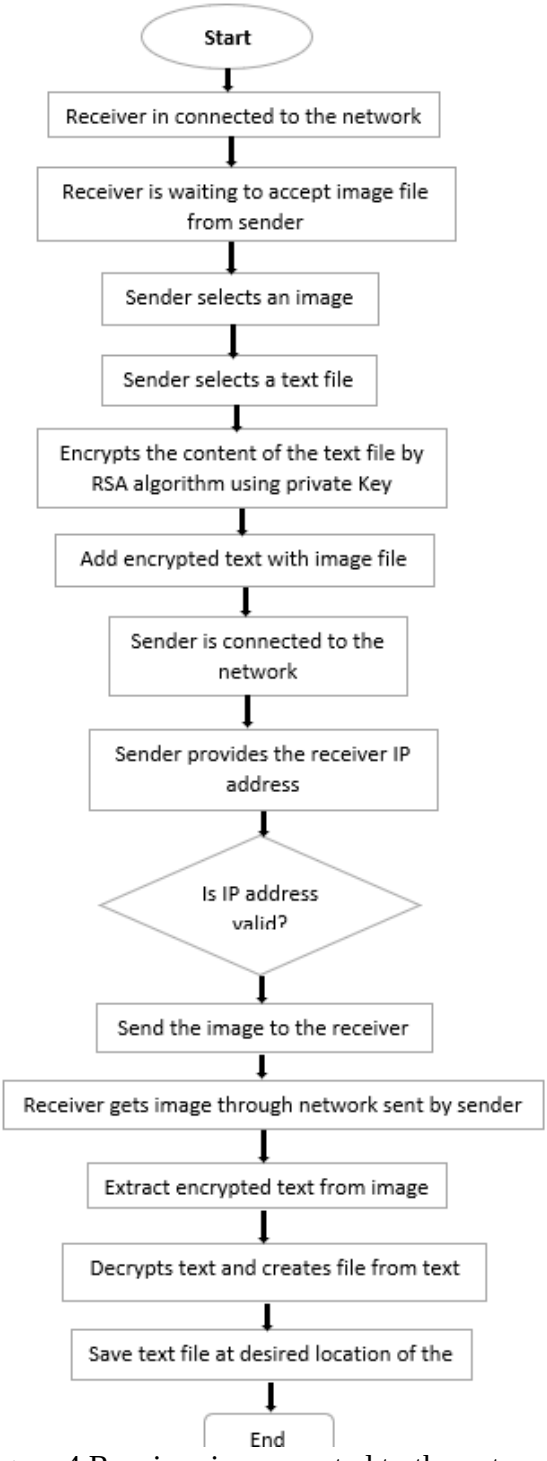

Figure 4 Receiver in connected to the network

Step 7: When the sender knows the IP address of the user, they can send the Stego-image if the IP address is correct. On the receiver's end, the decryption algorithm is: Step 1: Get the picture of the Stego. Step 2: Read the header of the picture to get the hidden message from the end of the stegoimage. Step 3: Make the secret key, decrypt the message that was taken, and then save it as a text file. Step 4: Save the written file where you want to.

CONCLUSION

Sharing information and talking to each other over the internet is an important part of every business and every part of life today. The idea behind our suggested method is to use a safe communication system to make a spread link that will protect this communication. This algorithm hides encrypted text using the RSA algorithm inside a JPEG image. The encrypted image file is then sent over the network. In this way, we combine the ideas of cryptography and steganography to trick hackers into thinking that the sender is sending a safe media file. Since a picture file shows up on the network as a normal media file, hackers don't see it as a security risk. As a cypher text, cryptography protects the data in this method, and steganography hides the cypher text in a picture file so that only the person who is supposed to see it can read it. Here, we've put the protected text at the bottom of the JPEG file that was picked. Going forward, our main goal will be to insert text into picture pixels. We will also try to solve the problem of lossy compression in JPEG images and expand our work to other image forms, such as.BMP, GIF, and others.

Reference

[1] Soomro ZA, Shah MH, Ahmed J (Apr.2016) Information security management needs more holistic approach: a literature review. Int. J. Inf. Manage. 36(2):215–225
[2] Kaur M, AlZubi AA, Singh D, Kumar V, Lee H-N (2023) Lightweight biomedical image encryption approach. IEEE Access 11:74048–74057. https://doi.org/10.1109/ACCESS.2023.3294570
[3] Zeng J, Tan S, Li B, Huang J (2018) Large-scale JPEG image steganalysis using hybrid deep-learning framework. IEEE Trans. Inf. Forensics Secur. 13(5):1200–1214
[4] Tripathy, Gyananjaya, and Aakanksha Sharaff. "AEGA: enhanced feature selection based on ANOVA and extended genetic algorithm for online customer review analysis." The Journal of Supercomputing (2023): 1-30.
[5] Jafari R, Ziou D, Rashidi MM (2013) Increasing image compression rate using steganography. Expert Syst. Appl. 40(17):6918–6927
[6] Denemark T, Fridrich J (2017) Steganography with multiple JPEG images of the same scene. IEEE Trans. Inf. Forensics Secur. 12(10):2308–2319
[7] Valandar MY, Ayubi P, Barani MJ (2017) A new transform domain steganography based on modified logistic chaotic map for color images. J. Inf. Secur. Appl. 34:142–151
[8] Kanan HR, Nazeri B (2014) A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Syst. Appl. 41(14):6123–6130
[9] Denemark TD, Boroumand M, Fridrich J (2016) Steganalysis features for content-adaptive JPEG steganography. IEEE Trans. Inf. Forensics Secur. 11(8):1736–1746
[10] Zhang X, Zhao Z, Wang J (2014) Chaotic image encryption based on circular substitution box and key stream buffer. Signal Process. Image Commun. 29(8):902–913
[11] Guo L, Ni J, Su W, Tang C, Shi YQ (2015) Using statistical image model for JPEG steganography: uniform embedding revisited. IEEE Trans. Inf. Forensics Secur. 10(12):2669–2680
[12] M. Saritha, V. M. Khadabadi, and M. Sushravya, “Image and text steganography with cryptography using MATLAB,” in 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016, pp. 584–587.
[13] H.-C. Huang, F.-C. Chang, Y.-H. Chen, and S.-C. Chu, “Survey of bio-inspired computing for information hiding,” J. Inf. Hiding Multimed. Signal Process., vol. 6, no. 3, 2015.

[14] De Vleeschouwer C, Delaigle J-F, Macq B (2002) Invisibility and application functionalities in perceptual watermarking an overview. Proc. IEEE 90(1):64–77
[15] Roy R, Laha S (2015) Optimization of stego image retaining secret information using genetic algorithm with 8-connected PSNR. Procedia Comput. Sci. 60:468–477
[16] 6. Sharda S, Budhiraja S. Image steganography: A review. Int. J. Emerg. Technol. Adv. Eng. (IJETAE) 2013;3(1):707–710. [Google Scholar]
[17] Upendra Raju K, Amutha Prabha N. Dual images in reversible data hiding with adaptive color space variation using wavelet transforms. Int. J. Intell. Unmanned Syst. 2023;11(1):96–108. doi: 10.1108/IJIUS-08-2021-0095. [CrossRef] [Google Scholar]
[18] Inan, Y. Quality metrics of LSB image steganography technique for color space HSI. in 11th International Conference on Theory and Application of Soft Computing, Computing with Words and Perceptions and Artificial Intelligence-ICSCCW-2021, 67–74. (Springer, 2022).
[19] Hassan FS, Gutub A. Improving data hiding within colour images using hue component of HSV colour space. CAAI Trans. Intell. Technol. 2022;7(1):56–68. doi: 10.1049/cit2.12053. [CrossRef] [Google Scholar]
[20] Kumar A, Rani R, Singh S. A survey of recent advances in image steganography. Secur. Privacy. 2023;6:e281. doi: 10.1002/spy2.281. [CrossRef] [Google Scholar]
[21] Tang L, Wu D, Wang H, Chen M, Xie J. An adaptive fuzzy inference approach for color image steganography. Soft. Comput. 2021;25(16):10987–11004. doi: 10.1007/s00500-021-05825-y. [CrossRef] [Google Scholar]
[22] Elshoush HT, Mahmoud MM, Altigani A. A new high capacity and secure image realization steganography based on ASCII code matching. Multimed. Tools Appl. 2022;81(4):5191–5237. doi: 10.1007/s11042-021-11741-y. [CrossRef] [Google Scholar]
[23] Hemeida F, Alexan W, Mamdouh S. A comparative study of audio steganography schemes. Int. J. Comput. Dig. Syst. 2021;10:555–562. doi: 10.12785/ijcds/100153. [CrossRef] [Google Scholar]
[24] Setiadi DRIM. PSNR vs SSIM: Imperceptibility quality assessment for image steganography. Multimed. Tools Appl. 2021;80(6):8423–8444. doi: 10.1007/s11042-020-10035-z. [CrossRef] [Google Scholar]
[25] Zhang, Y. J. Image engineering. in Handbook of Image Engineering, 55–83. (Springer, 2021).