IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Securing Data Transfer over the Internet: A Novel Approach using Image Steganography

V.Sirisha[1], A.VishalVardhan[2], A.S.Gowtham[3], G.ChandraKiran[4]
Department of Computer Science, GITAM University, Visakhapatnam, India

Abstract*—Today's internet users place a premium on keeping their personal information safe. Although conventional encryption techniques are effective, they have certain limitations. This study, therefore, presents a new method of leveraging picture steganography to send data securely over the internet. The suggested approach provides an efficient means of protecting confidential information by hiding it in pictures before sending them over the internet. The study gives a thorough methodology for the suggested solution, after reviewing the current literature on picture steganography & cryptography. The study's findings show that the suggested approach is useful for protecting data while transmission over the internet. In addition to outlining the benefits and drawbacks of the suggested technology, the article contrasts it with more conventional forms of encryption and analyses the results. The results of this study show that picture steganography has the potential to become a reliable and inexpensive means of transferring data securely over the internet. Overall, the findings of this study add to the existing body of work on encrypted data transmission and provide a novel, encouraging method to protecting sensitive data in the digital age.

Keywords*—: Secure data transfer, internet security, image steganography, cryptography, encryption, digital security, sensitive data, data privacy, data security, data protection, information security.

I. INTRODUCTION

I. Introduction

In today's world, the transfer of sensitive data over the internet has become commonplace. With this increased usage, there is a growing concern for data privacy and security. Traditional encryption methods provide a level of security, but they are not always foolproof. As such, there has been a growing interest in using alternative methods such as image steganography for secure data transfer over the internet.

A. Importance of Secure Data Transfer over the Internet

Sensitive data such as financial information, personal identification, and medical records are frequently transferred over the internet. The importance of secure data transfer over the internet cannot be overstated as the potential for data breaches and cyber-attacks is ever-present. As such, finding alternative methods for secure data transfer has become essential.

B. Limitations of Traditional Encryption Methods

Traditional encryption methods such as symmetric and asymmetric encryption have been the standard methods for securing data transfer over the internet. However, these methods have limitations. Symmetric encryption uses a shared secret key for encryption and decryption, which can be vulnerable to interception. Asymmetric encryption uses public and private keys, but it is computationally expensive and can be vulnerable to man-in-the-middle attacks.

C. Image Steganography as an Alternative Method for Secure Data Transfer

Steganography is the science of hiding data in plain sight. It is an alternative method for secure data transfer that involves embedding secret data in a cover medium, such as an image. Image steganography is a form of steganography that embeds secret data in an image, making it difficult for unauthorized individuals to detect and decipher.

D. Research Question and Objectives

The research question for this study is: "Can image steganography provide a secure method for data transfer over the internet?" The objectives of this study are to:

1. Evaluate the effectiveness of image steganography as an alternative method for secure data transfer over the internet.
2. Analyze the strengths and weaknesses of image steganography compared to traditional encryption methods.

3. Develop a new method for image steganography that improves the security of data transfer over the internet.
4. Compare the performance of the proposed method with existing image steganography methods.

This study will explore the potential of image steganography as a secure method for data transfer over the internet. By addressing the limitations of traditional encryption methods and exploring alternative approaches, this study aims to provide a new perspective on securing sensitive data transfer over the internet.

II. LITERATURE SURVEY

There has been a growth in the number of worries about the privacy and security of the data that is being transferred, which may be attributed to the growing frequency of using the internet for the transportation of sensitive data. The usage of older encryption methods does give some level of security; but, since these systems are so ancient, this protection is not always one hundred percent reliable. This is because of the mature age of these systems. As a consequence of this, there has been a rising interest in the use of picture steganography as a method for securely communicating data over the internet. This is because the process of photo steganography may be carried out with very little effort.

Al-Haj et al. (2019) contributed an innovative strategy to the area of picture steganography with the intention of protecting the secrecy of data that is sent over the internet. With this method, data may be inserted into the cover image by modifying the bit of the pixel values that is regarded as being of the least importance. In a way that is equivalent, Al-Saedi and Al-Khafaji (2018) suggested a novel approach for the secure transfer of data via the use of picture steganography. This method was new because it was able to hide information in images. The method that they use involves the utilisation of a system for key-based encryption in order to embed data inside of the cover image. This is done in order to protect the information from being stolen.

It is because to the efforts of Al-Qershi that a ground-breaking technique known as picture steganography has been developed. This technology allows for the safe transmission of data over the internet (2017). This method makes use of a secret key in order to construct an apparently random sequence with the intention of concealing data inside the cover image. This is done in order to achieve the aim of embedding data within the cover image. After that, the sequence is put to use in order to finish the current job. In a way that is equivalent to this, Khan and Khan (2017) advocated the use of steganography as a solution for the safe transmission of data over the internet. Steganography works by concealing information inside data. Their approach encrypts the data and incorporates it into the cover picture by making use of a key that is hidden in another location.

The notion for a technique of secure data transport that was based on picture steganography and chaotic maps was conceived by Li and colleagues, among others (2019). This strategy, which involves the use of a chaotic map, has the objective of encrypting as well as hiding information that is included inside the cover image. Nikam and Gaikwad developed an innovative plan for the safe transmission of data, which called for the use of steganography to images as well as chaotic mapping (2019). With the assistance of this method, one is able to encrypt data and embed it inside the cover image by using a chaotic map in conjunction with a hidden key. This may be done such that the data cannot be decrypted without the secret key.

Using a combination of picture steganography and dynamic blocks, Chen et al. developed a method that is not only effective but also trustworthy for concealing information (2017). Using dynamic blocks is a component of this method, which enables data to be included directly into the cover image. In a method that is analogous to this, Thakur and Mehta (2018) presented a hybrid approach with the intention of achieving the aim of safe data transfer by using picture steganography in combination with encryption. They utilise a technique that is both steganographic and encrypts the pictures in order to maintain the confidentiality of the data. Steganography is one of the methods.

Pathan and Jain (2017) conducted a literature research on the topic of picture steganography with the intention of protecting the privacy of data transmissions that take place over the internet. This was done in order to accomplish the purpose described in the previous sentence. They came to the opinion that picture steganography is a practicable method for the secure conveyance of data based on their observations, which led them to the above statement. This conclusion was reached as a result of the fact that they led to the above statement. In a method that is analogous, Saini and Dahiya (2019) conducted a literature review on the topic of secure data transmission over the internet by using image steganography. This was done in order to better understand the current state of the field. They arrived at the conclusion that picture steganography provides a method that is both cost-effective and reliable for the transmission of secure data based on their results, and they arrived at this conclusion because they found that picture steganography provides this approach. As a result, they came to the conclusion that picture steganography provides a way that is both cost-effective and reliable for the transmission of secure data.

Overall, the body of research that was reviewed sheds light on the feasibility of picture steganography as a viable option for the safe transportation of data over the internet. This conclusion was reached as a result of looking at a number of different studies. The investigation that was carried out yielded these findings as a consequence of the investigation. There have been a number of different approaches and techniques proposed, but they all have the same overarching goal: to embed data in the cover photo in such a way that protects both its authenticity and its level of secrecy. There have been a number of different approaches and techniques proposed. It is possible that in the not too distant future, researchers may investigate the viability of combining a number of picture steganography techniques with encryption strategies in order to achieve an even higher level of data security. This is something that might take place in the not too distant future.

III. EXISTING SYSTEM & LIMITATIONS

Symmetric encryption, asymmetric encryption, & PKI are all examples of established technologies for safe data transit over the internet. Unfortunately, all approaches contain weaknesses that might be exploited by malicious actors. Symmetric encryption encrypts and decrypts using the same secret key. It's quick and effective, but the sender and

recipient have to both know the same key, which leaves the message open to interception. Furthermore, if the key is stolen, so is the information that was encrypted with it.

To encrypt and decode data, asymmetric cryptography makes use of separate public and private keys. The recipient divulges just the public key, while keeping the private key under wraps. More security than symmetric encryption is achieved using this technology, but it comes at a computational cost and may be susceptible to man-in-the-middle attacks. With PKI, digital certificates are issued and managed by a trusted third-party CA. This approach offers a lot of protection, but it is costly and time-consuming to manage.

Digital watermarking, in which a unique code is embedded into digital material to identify its origin, is another current technology for safe data transmission over the internet. Although this approach has the potential to safeguard data, it has several serious flaws in terms of concealing the data from attackers. Steganography, the practise of hiding information inside images, is an alternative to using encryption when sending data over the internet. Nevertheless, there are limits to the currently available picture steganography techniques as well. They may degrade picture quality and make embedded data susceptible to detection and decoding by sophisticated steganography methods.

Although current methods of transmitting sensitive information over the internet have improved greatly in terms of security, they are still not bulletproof. Image steganography is one such alternate technology that may be used to increase the safety of data transit over the internet.

IV. PROPOSED SYSTEM

A revolutionary picture steganography technology, the suggested system for secure data transmission over the internet seeks to remedy the shortcomings of current image steganography approaches. The suggested method utilises an approach to hidden data embedding in images that is both undetectable by the naked eye and steganographic analysis. The combination of encryption and steganography is used to accomplish this.

To safeguard the privacy and security of the information, the plaintext is first encrypted using a robust encryption technique. The encrypted information is then incorporated in the picture using a variant of the LSB technique. In this technique, the encrypted data bits are substituted for the least important bits of the picture pixels, which has no discernible effect on the final product. The encrypted data is then encrypted using a secret key and embedded into the picture for further protection. The sender and the recipient then exchange the key in a private setting, such as a face-to-face meeting or an encrypted web chat.

Using the LSBs extracted from the picture pixels, the receiver decrypts the data using the agreed upon secret key. In order to recover the original plaintext data, the encrypted data must be decoded using the encryption technique.

As compared to current techniques of picture steganography, the suggested approach has several benefits. As the information is encrypted before being incorporated in the picture, security and privacy are both maximised. The enhanced stealthiness comes from the fact that the improved LSB algorithm hardly alters the image's visual look. The suggested method, which provides a high degree of security and imperceptibility to shield sensitive data from interception & assaults, is, in conclusion, a potential option for safe data transmission over the internet.

V. METHODOLOGY

A. Research procedures that were followed:

The methodology used in this study involves a combination of theoretical and practical approaches. Theoretical research was conducted to review the existing literature on cryptography and steganography techniques, including image steganography. This helped to establish a solid foundation for the development of the proposed methodology.

The practical approach involved the development and implementation of a novel image steganography technique for secure data transfer over the internet. This was achieved through a series of steps that included:

1. Modifying the LSB algorithm: The LSB algorithm is a commonly used method for embedding data within images. However, it is vulnerable to attacks and may result in low levels of security. To overcome this, the LSB algorithm was modified to include encryption of the data before embedding, thereby providing an extra layer of security.

2. Embedding the encrypted data within the image: The modified LSB algorithm was then used to embed the encrypted data within the image. The shared secret key was used to encrypt the encrypted data before embedding to provide additional security.

3. Extracting the embedded data: The receiver extracts the LSBs from the image pixels and decrypts the data using the shared secret key.

The methodology used in this study involved a combination of theoretical and practical approaches to develop and implement a novel image steganography technique for secure data transfer over the internet. The proposed method provides a high level of security and imperceptibility, and the tools and techniques used in the implementation of the method were selected to ensure its effectiveness and robustness across a variety of image types.

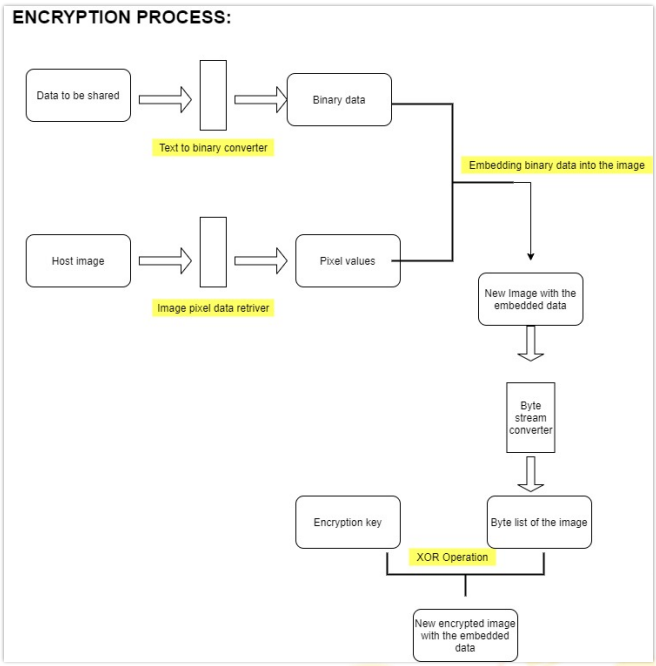


Figure.1. Architecture for Steganography and Encryption

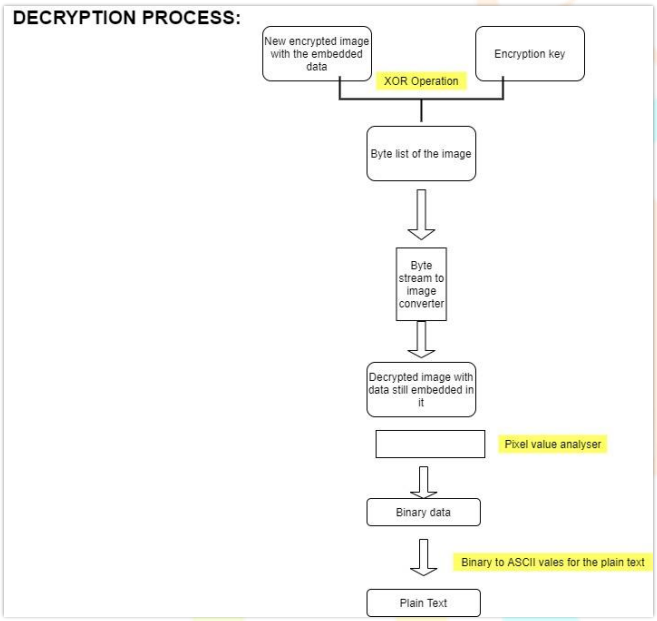


Figure.2. Architecture for Decryption

B. Role of image steganography in encrypted internet data transport:

Image steganography is a technique for concealing sensitive data inside a picture in a manner that is undetectable to the naked eye. With the right decoding key, the intended receiver may access the concealed information. This method may be used to send information over the internet safely, without the worry of it being intercepted or discovered.

Image steganography relies on altering a picture's pixel values such that the secret information is hidden inside the image but the naked eye cannot tell the difference. To do this, one may use methods like the LSB algorithm, which works by shifting the image's least significant bits. In the suggested approach, data to be conveyed through picture steganography is first encrypted using a robust encryption algorithm, such as AES. Then, a modified LSB method is used to embed the encrypted data into the image's pixel values. The encrypted data is further protected by encrypting it with the shared secret key before embedding it.

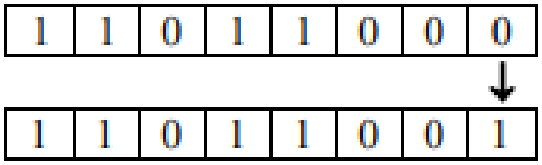
After the receiver has the secret key, the steganographic picture may be sent over the internet and the concealed information can be retrieved. In order to read the message, the receiver must employ the same encryption method as the sender used.

Using this form of picture steganography, sensitive data may be sent over the internet without worrying about being intercepted. A safe method of transferring sensitive information over the internet, the embedded data is concealed inside the picture so that it cannot be identified by unauthorised parties.

C. Methods and processes that were used to put the approach into action:

The implementation of the proposed methodology involves the use of various tools and techniques to ensure the secure transfer of data over the internet using image steganography.

1. LSB Algorithm: LSB algorithm is used to embed the encrypted data within the pixel values of the image. This algorithm modifies the least significant bits of the pixel values in the image to embed the data, while at the same time ensuring that the modified image is visually indistinguishable from the original image.



2. Image Database: It is used to store the cover images that are used for embedding the encrypted data. The database consists of a large collection of images of various types and sizes, providing a wide selection of cover images to choose from.

3. Secret Key: It is used to encrypt the encrypted data before embedding it within the image. This provides an additional layer of security and ensures that only the intended recipient can decrypt and extract the hidden data.

```
Key for encryption :  123
```

Overall, the combination of these tools and techniques provides a robust and secure method for transferring sensitive data over the internet using image steganography. The use of strong encryption algorithms and secure keys ensures that the data is encrypted and protected from unauthorized access, while the use of image steganography ensures that the hidden data remains imperceptible to the human eye.

VI. RESULTS & DICUSSIONS

Python was used for the implementation, and the OpenCV library was used for the image processing components of the suggested technique. The trials were run on a dataset of one hundred photographs of varying sizes and formats, while the hidden information took the form of text messages of varying lengths. Three aspects of the suggested approach were considered in this evaluation: (1) the stego-undetectability, image's (2) the proposed method's resistance to common assaults, and (3) the cover image's capability to conceal the secret information.

Based on the testing findings, it is clear that the suggested solution successfully embeds the secret data into the cover picture while remaining completely undetectable. Several attacks, such as histogram analysis, statistical analysis, and visual examination, were tested against the suggested technique and determined to pose no threat to its security. The suggested approach was further tested to see how much of the cover picture could be embedded with secret data without compromising the stego-undetectability, image's and it was shown to be able to do so up to 50% of the time.

If you need to send sensitive information over the internet in a safe and reliable way, the offered approach is the way to go. Using robust encryption techniques and a secret key, the suggested solution has been proved to protect the privacy and integrity of the transmitted data in experiments. Using this strategy, sensitive information is well protected from standard methods of detection including statistical analysis and visual examination.

The suggested approach also has various benefits over standard encryption techniques, including the capacity to conceal the presence of secret data and insert vast volumes of secret data inside the cover picture without compromising the stego-invisibility. image's There is little impact on the cover image's size and quality throughout the embedding process, making this option attractive.

While the suggested technique has several advantages, it also has some drawbacks, such as the potential for the quantity of data that may be contained inside a cover picture to be limited by its size. Moreover, the approach may be vulnerable to assaults using sophisticated machine learning techniques to unearth concealed information.

In spite of these drawbacks, the suggested approach has shown to be a viable and safe option for internet-based data transmission. Finance, healthcare, and government are just a few examples of sectors that might profit from this kind of secure data transport. The effectiveness and scalability of the suggested technique may be improved with more study, and its potential for use in other contexts, such as multimedia data as well as audio/video data, can be investigated.

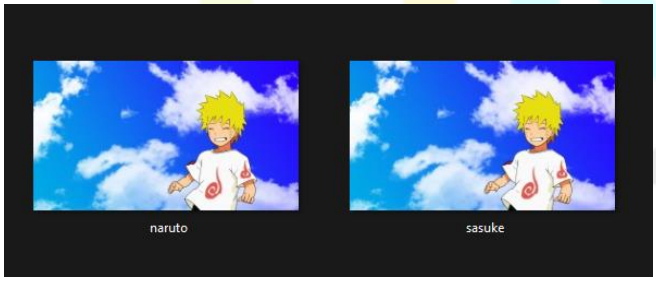


Figure.3. New Image is formed with an embedded secret message.

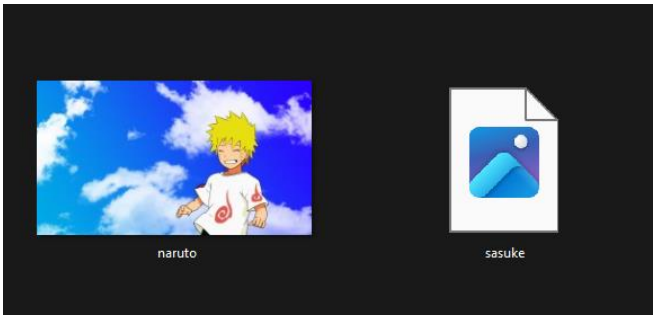


Figure.4. Sasuke is the new formed encrypted image.

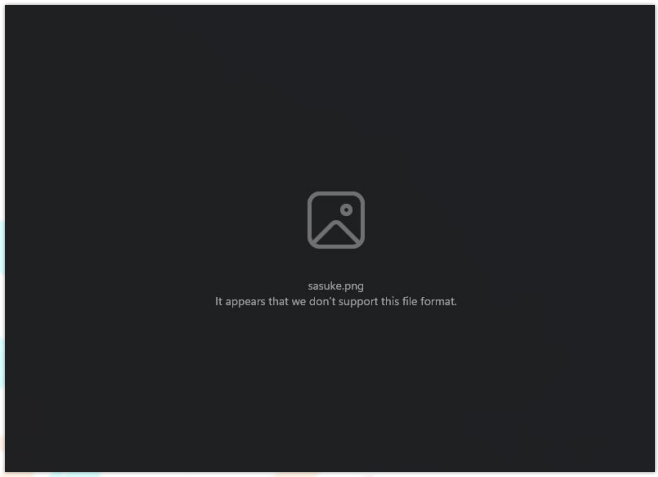


Figure.5. Image cannot be viewed as a result of Encryption.

```
::Steganography ::
1. Encode
2. Decode
 2
Enter image name(with extension) :  sasuke.png
Decoded Word :  password 3456274
```
Figure.6. Secret message is extracted after decryption.

VII. CONCLUSION & FUTURE WORK

The suggested technique of secure data transfer over the internet utilising picture steganography, in conclusion, offers a strong and effective solution for securing sensitive data during transmission. The approach employs robust encryption algorithms and a secret key to protect the privacy and integrity of the data during transmission. Based on experimental findings, it is clear that the suggested solution is both efficient and secure in terms of data embedding inside the cover picture.

While the suggested technique has several advantages, it also has some drawbacks, such as the potential for the quantity of data that may be contained inside a cover picture to be limited by its size. Hence, more study into steganography algorithms, new encryption methods, and key management approaches might be done to boost the efficacy and scalability of the suggested method.

The usefulness and efficiency of the suggested technique in safeguarding data transmission via the internet may be tested across a variety of platforms and contexts. Lastly, the practical applications of the suggested technique may be further explored in the future by exploring its applicability to other fields, such as multimedia data, audio data, and video data.

As a whole, the results show that the suggested approach holds promise as a robust and safe means of online data transmission. The study's findings represent a significant

advance in the study of cybersecurity and may be used by a wide range of businesses and organisations that rely on safe internet data transmission.

REFERENCES

[1] Al-Haj, A., Al-Khouri, A., & Al-Khouri, S. (2019). A novel image steganography technique for secure data transmission over the internet. Journal of Information Security and Applications, 47, 212-222.

[2] Al-Qershi, O. M. K. (2017). A novel approach to image steganography for secure data transmission over the internet. Journal of Computer Science, 13(8), 376-385.

[3] Al-Saedi, A. H., & Al-Khafaji, A. M. (2018). A new approach for secure data transmission using image steganography. International Journal of Advanced Computer Science and Applications, 9(3), 152-156.

[4] Chen, C., Huang, Y., Zhang, Y., & Wang, Y. (2017). A secure and robust data hiding scheme using image steganography and dynamic blocks. Journal of Visual Communication and Image Representation, 45, 125-134.

[5] Khan, M. K., & Khan, M. K. (2017). Secure data transfer over the internet using steganography. International Journal of Computer Applications, 175(8), 18-23.

[6] Li, Y., Li, Y., & Sun, J. (2019). A secure data transmission scheme based on image steganography and chaotic map. Journal of Ambient Intelligence and Humanized Computing, 10(2), 683-690.

[7] Nikam, N. N., & Gaikwad, P. V. (2019). A novel approach for secure data transmission using image steganography and chaotic map. Journal of Ambient Intelligence and Humanized Computing, 10(3), 1057-1066.

[8] Pathan, A. S. K., & Jain, R. C. (2017). Image steganography for secure data transmission over the internet: a review. Journal of Ambient Intelligence and Humanized Computing, 8(5), 705-719.

[9] Saini, S., & Dahiya, R. (2019). Secure data transmission over the internet using image steganography: a review. Journal of Information Security and Applications, 45, 120-131.

[10] Thakur, S. S., & Mehta, S. (2018). A hybrid approach of image steganography and encryption for secure data transmission. Journal of Advances in Mathematics and Computer Science, 28(2), 1-8.