Image Steganography for Secure Communication

Y.Lalitha,N.Vineela,S.Akash,S.Charan
Dr.T.Sathish Kumar
Hyderabad Institute of Technology and Management

Abstract: Most military and other research organisations must transmit and receive critical text information such as weaponry blueprints, schematics, and satellite data. If the SMS is delivered on a frequent basis, hackers may be capable of intercepting this and import data. Data is concealed under images to prevent unauthorised access.This approach employs a both plain text and a file. We'll have a letter as well as a document with a cover picture. The pixel in the header picture will be the next consideration. Each hidden text snippet will be inserted there. This procedure will be continued until the final piece of hidden text is discovered.It is accompanied by information being concealed underneath the picture. Following that, we will give this picture file. The data is concealed under the image. After getting this image file from us, the client will utilise reverse engineering to retrieve the original text from of the image. In cyber security, there are several approaches and tactics for concealing data. In this project, the Least Significant Bit approach was applied. Each approach is significant in its own way. (LSB).

Keywords: data, hiding, encode, security, image.

INTRODUCTION:

In recent years, technology has improved significantly, resulting in widespread usage of video for data transfer, particularly in relation to the Internet of Things (IoT). Often, transmission occurs across insecure network routes. The usage of the internet, in particular, for transferring digital files, has grown in popularity. People, private enterprises, organisations, and governments all share data using various multimedia data transmission technologies. Although it offers many advantages, one important disadvantage is the lack of data security and confidentiality. The availability of multiple widely accessible technologies capable of damaging the confidentiality, integrity of data, and safety of the information being transferred has raised the possibility of hostile threats, espionage, and other subversive operations. Encryption process is a typical way for converting data it in to a cypher text domain to use an encryption key. At the receiver end, a decryption key is used to convert the cypher text to plain text. The application of data security. The actual data is not accessible, yet cypher text is viewable to human eyes in a jumbled form, arousing suspicion and demanding more

DOI: 10.55041/IJSREM19136

research. Steganography, a fresh research topic, has gained popularity in this context for concealing information that is not apparent to human eyes.

Although information hiding methods have been used for a long period of time, their importance has recently increased. The major cause is an increase in social media as well as internet data traffic.

Steganography, a technique used to conceal information, allows for the usage of a wide variety of concealed information types, including picture, text, audio, video, and files. Digital watermarking, which integrated sensitive information, is another method for asserting ownership. Although encryption is the most extensively used method of concealing information, steganography has grown in prominence in recent years.

Steganography is the method of hiding a tiny amount of multimedia data within a much larger amount of multimedia data, such as an image, text, file, or video [1]. Image steganography is a technique for hiding one picture within another. Image steganography manipulates the cover picture so that the hidden data is not visible, makes it less conspicuous than encryption.

Steganalysis, on the opposite hand, is used to detect the presence of any hidden message inside the image and to extract the secret data. Steganalysis can help you determine whether a photo is a stego image or a conventional image. In addition to categorising the image, extra study is conducted to establish the location and contents of the hidden image inside the cover image.

LITERATURE SURVEY:

A. Genetic Algorithm for Hiding Text in Images A.L. Sanchez, A. Conci, and A. Behlilovic in Brazil in 2011. Because of the study of the Internet, more individuals are linked, which raises the demand for exchanging private information. As one means of securing data received over the internet, the relevant data can be concealed inside a conventional picture to disguise it from hackers. To efficaciously solve this problem, they suggested using a hybrid heuristic that integrates a genetic algorithm and the path relinking metaheuristic. In this way, the addition of a path relinking procedure can considerably enhance the effectiveness of an evolutionary algorithms for the issue under discussion.

A. B. Image and audio protection Bhowal, In 2011, K. Sarkar, D. Biswas, and S. Sarkar developed the Audio concealing approach to ensure secure data transfer between parties, as is common in the internet community. The authors of this paper give a new, logical answer to the challenges that remain in the replacement approach for audio concealment. At the basic level, writers take picture data out of an image file. The visual data is then embedded into audio data using a powerful LSB (Least Significant Bit) technique based on a GA in the second step (Genetic Algorithm). Picture data bits are included into relatively high LSB levels and randomized layers in this method, which increases noise addition resistance. GA processors, on the opposite hand, help to reduce distortion. The results show that if we give a somewhat successful first GA, we can modify the output and add further protection to prevent information from being accessed by a third party or accessible by someone without authority.

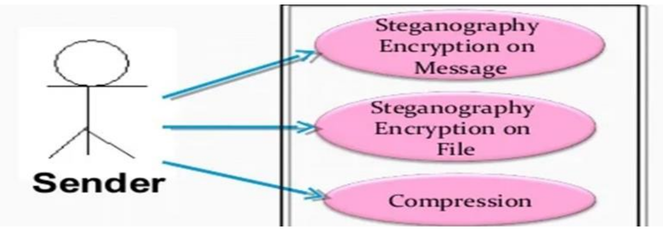
C. Picture Morphing-based Information Hiding Method

Qiangfu Zhao, Akatsuka, and M. Cheng Hsiung Hsieh proposed the study of a picture morphing-based approach for information concealment in 2012. The basic idea is to morphing an image from a secret image and another reference image to produce a morphed image that hides the hidden image. The ability to create spontaneously morphing images is required for this approach to be effective. To generate realistic morphed images, we must first choose a suitable feature point set (FPS). Given the multitude of possible FPSs, this works mechanically. They employed the interactive genetic algorithm (IGA) and performed trials to develop facial images in this study.

METHODOLOGY

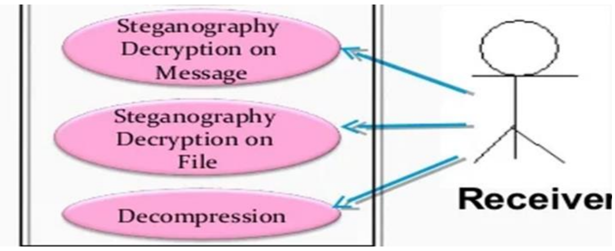
The suggested technique conceals the hidden picture in colour images. Initially, we will evaluate our communication, which must be protected from illegal access, and then we will execute encryption.

ENCODING: This is done inside the encoding module. During the encoding module, the text message will be placed into the image file. The "Least Significant Bit" (LSB) technique will be used for encoding. The LSB technique encrypts the picture by replacing the least significant bits of the each pixel with significant bits of a written content. This replacement method is basic. and quick to retrieve the data, and the image clarity is improved, so it offers excellent security.


Sender
Steganography Encryption on Message
Steganography Encryption on File
Compression

DECODING:

The messenger image is received by receiver from transmitter via the medium of communication in the decoding module. The recipient then sends the carrier image to the decryption phase. In the decryption phase, the same Least Significant Algorithm is used to decrypt the least significant bits from the image and combine them to frame the original message bits. After effective organisation, the data is encrypted from carrier file and read as just an original text document.


Steganography Decryption on Message
Steganography Decryption on File
Decompression
Receiver

IMPLEMENTATION

The execution sequence is depicted in Figure 2. To start, the user should select the picture containing the data. It may be a photo in any format, such as.jpg or.jpeg. The user can alternatively input the information manually. The picture's data is preserved in a desktop property. At the following stage, the information must be encrypted using one of the available encryption algorithms and a sufficient key. Encryption is a technique used to generate cypher writing from plain text.

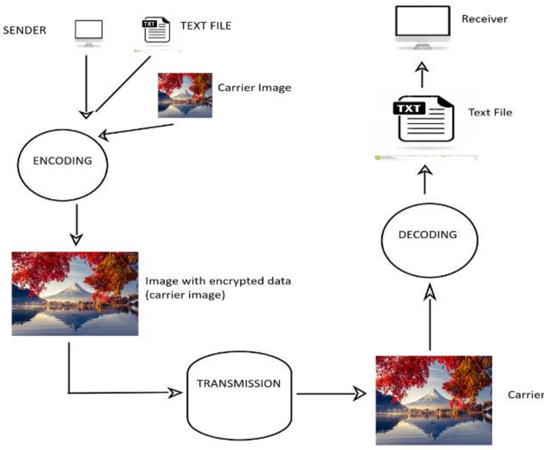


FIGURE-2

We deliver straightforward information in clear text. If the intruders look into it, they would quickly realise this information. The cypher content, on the other hand, is meaningless. Anybody who witnesses it will not comprehend it. It can only be understood if it has been decrypted with appropriate key. In the following stage in the encryption process, the encrypted cypher text is embedded into the image using the LSB modification method. The user must select a cover image and insert the cypher text into it. In order to put the cypher text onto the image, each character is picked and its bit format is constructed. These bits are modified at the final three LSB positions of the particle's components Red, Green, and Blue.

Consider a pixel with a red component of 11011010, a green component of 10110111, and a blue component of 11110010. Let the ASCII value of the present inserted letter be 11001101. The LSB bits of the Red, Green, and Blue components have now been altered to 11011110, 10110011, and 11110001, accordingly. The character's first three MSB bits are substituted by the last three LSB bits of the Red component. The character's next three bits are replaced by the Green component's final three LSB bits. The final two LSB bits of the blue component are utilised to replace the symbol's remaining two bits. Hence, the LSB values of the three components of a single pixel encode one letter. This operation is continued until all of the characters in the information are merged into the image's pixels. This process has a strict limit on the number of characters allowed for input. The total amount of inserted characters cannot exceed the total number of pixels in the image. As a result, higher-resolution images should be utilised to disguise more letters.

Once the embedding technique is completed, the picture with the hidden data is created. There is no obvious difference between the original image and the version with hidden information. As a consequence, this image may be shared without attracting the attention of hackers and intruders. In this example, the fundamental limitation is the medium utilised to convey the image. The transmission should have no effect on or distort the image. The medium must not handle or modify the image's real size, quality, or any other feature. At the receiver, the data from the received image should be extracted at the first step. To obtain the character encoded, the LSB bits of the three pixel components must be merged in that pixel. For example, suppose the Red, Green, and Blue components of a received pixel are 11011110, 10110011, and 11110001.

The letter embedded in that pixel is then 11001101. This is obtained by combining the three LSB bits of the Red component, three The Green component has two LSB bits, and the Blue component has two LSB bits. This doesn't necessitate the same design as before. The components are able to be utilized in any order during integration. The final three LSB bits are also able to replace any character bit sequence. When the characters are retrieved from the image, the resultant text is the cypher text. This cypher text needs be translated back to plain text in order to get the original communication content. To retrieve the plain text, use the decryption procedure to the cypher text while using the correct secret. Only by using the correct key can reliable data be produced. An incorrect key generates incorrect and worthless data.

REQUIREMENTS

EQUIPMENT REQUIREMENTS

The following general and particular minimum hardware specifications are required for the application's creation and deployment:

Minimum Component Requirement:

Processor and Rate64-bit, four-core processor with a minimal clock speed of 2.5 GHz per core

RAM size of 8 GB for research and testing

Hard disc 10GB for creation and testing, with a total capability of 1TB

TECHNICAL REQUIREMENTS FOR SOFTWARE

The following general and particular minimal software prerequisites are required for the creation and deployment of the application:

Minimum Component Requirement

Windows 7 is the operating system.(64-bit)

Java IDE is a programming tool.

Database NetBeans 7.4MYSQL

A functional precondition defines the objective of a software system or a software system component. A function is defined as a set of inputs, actions, and results. A text tries to convey as much information as possible. As a result, the rate of textual input should be substantial. Textual data should be kept private and only accessible to those who need it. This is referred to as textual data security. This is performed by employing encryption passwords.

Textual information is a significant part of data. It must withstand signal processing as well as information manipulation. There is also malicious tampering that attempts to remove the content. This is referred to as the resilience criteria. While textual material should be irremovable, it should also be undetected. It should not alter or deteriorate the material's integrity. Typically, the grade reduction is much less than 1%. The digital watermark's initial parts may or may not be employed inside the watermark recovery technique. Input design prioritises limiting the quantity of input required, managing mistakes, preventing delays, eliminating unnecessary processes, and making the process simple. The input is designed to provide security and convenience while keeping anonymity.

The following factors were taken into account by Input Design:

- What data should be provided as input?
- How should the data be arranged or coded?
- The dialogue that will assist the operating employees in giving input?
- Methods for creating data validations, as well as actions to take when an error occurs

QUALITY REQUIRMENT

A performance requirement is a declaration that specifies how well a work must be done. A performance requirement is often described using adjectives like degrees, rate, amount, quality, and timeliness. A performance requirement may additionally define the conditions under which the task must be completed.

Every data security system's efficacy may be judged by the speed with which it hides data, as well as the quality and security of the data it offers. When it comes to safety requirements, the problem emerges when data is transferred from one end to another. The hacker may try to penetrate the system and get the data via Steganalysis. Other dangers, such as virus attacks, can harm data, so it should be secured against them with powerful antivirus software.

- The usability of any data security system is critical; the software ought to be adaptive for shifting information from one side to the other. It should serve as a friendly connection between the client as well as the user.

- Scalability is an important factor to consider when designing software for large institutions where privacy is paramount. Certain technologies cannot provide high-level safety when the data to be embedded is large. In this case, scalability is critical.
- Several organisations, such as the military, utilise data security software or apps to safeguard important information, financial organisations to secure equities and trading information, and so on. To avoid alterations, the application ought to be consistent when utilised in other apps and give greater security.
- Keeping unauthorised persons away from critical information. The application should be protected from unauthorised alterations and should only be available to authorised users. The application should be versatile, easily available, and interoperable with any operating system.

CONCLUSION

This article addresses the use of steganography to conceal information. It is the safest method of transmitting sensitive information via the web. The LSB alteration approach, in particular, has gained much interest. This method's main advantages are its adaptability and efficacy. It also has the benefit of being a method for geographical domains.Complex transform domain algorithms do not need to be memorised. The picture steganography approach may be used to conceal sensitive passwords and keys from prying eyes. Digital artists may also utilise it to safeguard their reproduction rights by integrating their information within the piece.

REFERENCES

[1] https://ieeexplore.ieee.org/document/9104072

[2] https://link.springer.com/article/10.1007/s11042-017-5308-3

[3] http://java.sun.com

[4] http://en.wikipedia.org/wiki/java

[5] http://www.computerworld.com/securitytopics/story/0,10801,71726,00.html