INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 1024-1027

e-ISSN : 2583-1062

Impact Factor : 5.725

STEGANOGRAPHY ALGORITHM TO COVERTLYCOMMUNICATE A SECRET MESSAGE IN AN IMAGE

R. Mohanraj[1], M. Elango[2]

[1,2]M.sc Computer Science, Sri Krishna Arts & Science College, Coimbatore

ABSTRACT

The authors of this study suggest a brand-new algorithm for employing steganography to conceal data inside images. Binary codes and the pixels in a picture are used in the suggested approach. To maximise the amount of data thatmay be stored inside an image, the zipped file is employed before the image is converted to binary codes. The proposed algorithm is used to create a system known as the Steganography Imaging System (SIS). The proposed algorithm is then tested on the system to determine its viability. The photos contain data of various sizes, and for each of the examined images, the PSNR (Peak signal-to- noise ratio) is also recorded. The stego image has a greater PSNR than the otherimages, according to their PSNR values.

Keywords: Data Retrieval, Image Processing, Secret Key, And SteganographyAlgorithm.

1. INTRODUCTION

In this paper, a new approach for employing steganography to conceal data inside of images is proposed. To safeguard the privacy of the data, an algorithm is created to disguise all the data inputted within the image. Then, a novel steganography algorithm is used to construct the system. The suggested system offers a text box for adding text and an image platform for users to enter images. Once the suggested algorithm has been modified, a user can send a stego image to another computer user in order for the recipient to be able to readand extract the data that is concealed in the stego image using the suggested system. Thus, the information can be safeguarded without distributing the contents to others.The Steganography Imaging System (SIS) is a device that can conceal data inside of an image.The system employs two levels of security to protect the confidentiality of user data. Data security is the process of preventing unauthorised access and data corruption. Data security is centred on maintaining privacy while safeguarding individual or corporate data. Contrarily, privacy is the ability of a person or organization to keep their identity or information about them a secret and only divulge it when necessary. The link between data gathering and dissemination, technology, public expectations of privacy, and legal considerations is known as data privacy or information privacy. Health records, criminal justice investigations and processes, financial institutions and transactions, biological features, domicile and geographic records, and ethnicity are just a few of the many data sources that may give rise to privacy concerns. As more and more systems are linked tothe Internet, data security and privacy have taken on greater significance. Data or information on private individuals is protected against intentional or unintentional disclosure or misuse by information privacy regulations.Therefore, concealing the data in some manner, such as within an In order to safeguard the confidentiality or privacy of the sensitive data, image is essential.

2. ADDITIONAL WOR

Data hiding is the process of incorporating data into digital content without impairing perception. Three well-known approaches can be applied to data concealing. They are cryptography, steganography, and watermarking. Greek writing is concealed via steganography. It covers all operations involving data or data included within other data. Steganography, according to conceals the existence of a message by including information into a variety of carriers. The main goal is to avoid secret information being discovered. When the ancient Greeks tattooed a secret message on a messenger's shaved head and allowed hishair to grow back before sending him through hostile territory, the latency of this communications system was measured in months. Research on the steganography technique was conducted during this time. The most well-knowntraditional steganography technique dates . and involves marking a document with a secret, invisible ink that resembles lemon juice to conceal information.Another technique is to create a pattern or signature by poking holes through specific characters in a document. However, the majority of computerised steganography's creation and application only started in 2000 . The primary benefit of the steganography algorithm is due to its straightforward security mechanism. The steganographic communication is concealed and mergedinvisibly inside other safe sources.Without knowing the presence and the proper encoding technique, it is quite difficult to decode the message. The least significant bits (LSB), bit-plane complexity segmentation (BPCS), batch steganography, permutation based steganography, chaos-based spread spectrum image steganography, and others are among the steganography techniques used to conceal data. (CSSIS). Numerous academics have studied the use of steganography to concealdata inside images, as seen in. In order to conceal data, Warkentin et al. suggested a method utilising audiovisual files. This study makes advantage of a concept El-Emam first proposed. To conceal the data, a bitmap (bmp) image will be employed. The pixels will be used to incorporate data inside the image.The secret data within the image can then be retrieved by accessing the pixels ofthe stego image. There are two steps involved. The first step is to create a new steganography technique that will allow the data to be concealed inside the image, and the second step is to create a decryption algorithm that will allow thehidden data to be recovered from the stego image.

3. PROPOSED METHOD

Two levels of security are used in our suggested technique, to keep the data accurate, private, and confidential. The framework for the system's entire process is depicted in Fig. 1. The system has the ability to bothhide data inside a picture and retrieve data from an image.According to Fig. 1, a username and password are necessary before using the system in order to hide the data. The user can utilise the information (data) andthe secret key after logging into the system to conceal the data inside the selected image. These data will be incorporated and concealed inside the image using a cutting-edge steganography method with essentially no distortion to theoriginal image. A secret key is needed to unlock the data that has been hidden inside the image in order to retrieve it. The information in the image cannot be obtained without the secret key. This protects the data's confidentiality and integrity.

Fig. 2 depicts the steganography algorithm for embedding the hidden message inside the image. A secret key is required for the purpose of recovering the message from the image after the message has been embedded inside the image.

From Fig. 2, the retrieved secret message from the system is first transferred into a text file. The text file is then zipped up and stored in the zip file. The conversion is then performed using the zip text file. Because the zipped text fileis more secure than the unzipped version, that is why it is necessary to zip up text files. The contents of the packed file will be very difficult to find and understand. Additionally, the key and the compressed text file's series of binary codes are lengthy random codes that only contain the numbers one and zero.

```
Begin
    Input: Cover_Image, Secret_Message, Secret_Key;
    Transfer Secret_Message intoText_File;
    Zip Text_File;
    Convert Zip_Text_File to Binary_Codes;Convert
    Secret_Key into Binary_Codes; Set BitsPerUnit to Zero;
    Encode Message to Binary_Codes;Add by 2 unit for
    bitsPerUnit;
    Output: Stego_Image;
End
```

```
Begin
    Input: Stego_Image, Secret_Key;Compare
    Secret_Key;
    Calculate  BitsPerUnit;
    Decode All_Binary_Codes;
    Shift by 2 unit for bitsPerUnit;
    Convert Binary_Codes to Text_File;
    Unzip Text_File;
    Output Secret_Message;
End
```

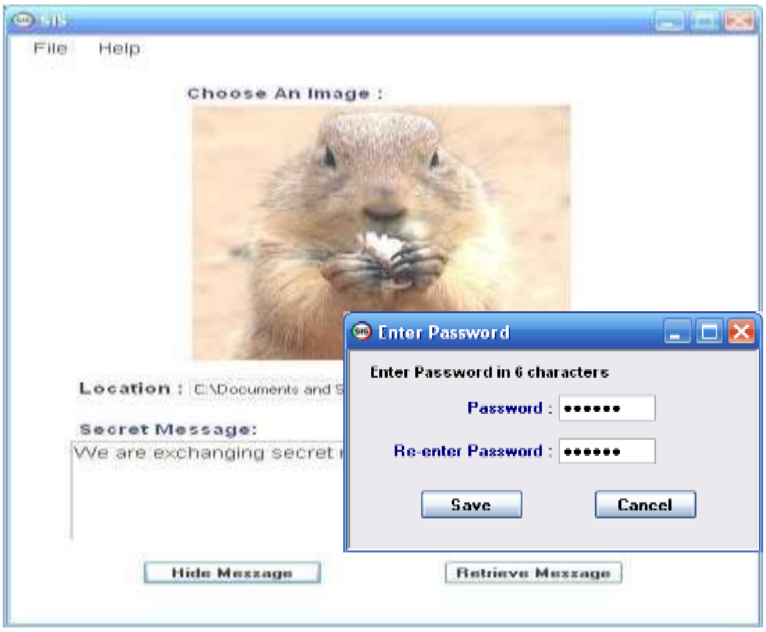
DATA-EMBEDDING ALGORITHM FOR IMAGES

The location of the key serves as a locker for the secret message, which can be locked or unlocked. Each pixel in the image has its final two bits encoded in order to use the data concealing approach. This will guarantee that there won't be too many alterations made to the original image.The message can be recovered from the stego image once it has been concealed inside the image. The algorithm for removing the hidden message from the stego image is shown in Fig. 2. A secret key is required for the purpose of verification in order to recover the proper message from the image.

According to Fig. 2, a secret key is required for the data extraction procedure to determine whether The key matches the key used to decode a series of binary codes. The method then moves on to convert the binary code to a zipped text file, unzipping the text file, and transferring the secret message from the text file to recover the original secret message after the key is matched.

4. FINDING AND DISCUSSION

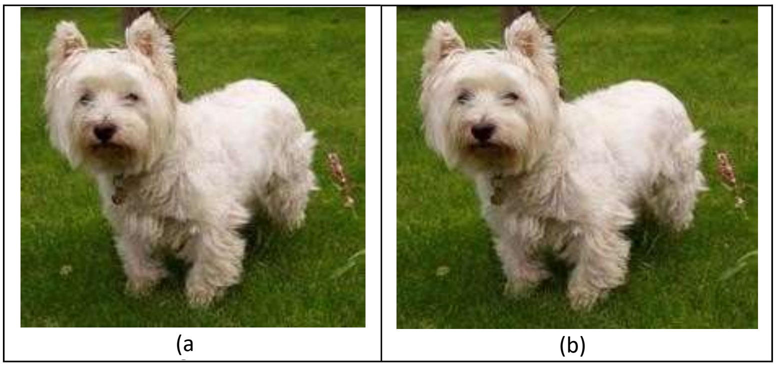
We create a straightforward system that executes the proposed algorithm based on the given algorithm. The system is known as the Steganographic Imaging System. (SIS). based on the system's visible frameworkSIS implemented two layers of security in Fig. 1. The second layer is for hiding and retrieving, and the first layer is for logging in. In [11], the system is introduced. The main interface for the system is depicted in Fig. 2. A box for thepicture and a box for the data that the user needs to conceal inside the image are the two main boxes in SIS. The text box is used to hide and retrieve the message to and from the picture, while the image box is used to fetch the image from any site. A secret key is needed for security reasons in order to disguise the data inside the image. The interface for the secret key, which must be 6 characters long, is shown in Fig. 2. It is necessary to enter the secret key twice for verification. The secret key is only 6 characters long for the sake of simplicity. Along with the data, this hidden key is also included in the image. Therefore, only 6 characters are utilised for the secret key in order to minimise the quantity of storage within the image. The new Stego image can be saved to a different image file after the data has been keyed in and the secret key has been inputted. Then, using this updated stego image.



Location : C:\Documents and S

Secret Message:
We are exchanging secret r

Enter Password in 6 characters
Password : ••••••
Re-enter Password : ••••••


(a

(b)

a) original image

b) steganography image

The method was then evaluated using the PSNR. (Peak signal-to-noise ratio). PSNR is a common parameter that is used in steganography to evaluate the efficacy of the stego pictures. The quality of the stego image will increase with increasing PSNR values.A cover picture C with a size of M x M and a stego image S with a size of N x N will each have pixel values (x, y) Range 0 to M-1 or 0 to N-1. , respectively. Next, the PSNR is determined as follows:The bitmap (BMP) format is the primary picture file format used in the suggested algorithm. Within the Microsoft Windows OS, graphics files are handled by the BMP file format. BMP files are typically huge since they are uncompressed. The ease of use and widespread acceptance of BMP files in Windows programmes are benefits of using BMP files. So, we decide to employthis kind of image in our suggested algorithm. The pixels in a BMP image are also proportionally larger since the BMP image is relatively greater in size. As aresult, it offers additional room for the encoding of binary codes. When reducing file size and enhancing security, the zip approach is employed to increase the number of characters that can be buried.We test different BMP picture sizes with the suggested algorithm to determine the different sizes of data stored in the image. Table 2 displays these diverse testfindings. By comparing various sizes of a BMP image with the suggested steganographyalgorithm, Table 2 illustrates the comparison. These BMP pictures serve as cover pictures.to encrypt the zip file contained therein. Typically, an image weighs 3.14 MB. The largest size of a zipped file that can be concealed within and extracted from a 3.14 MB BMP image using the suggested algorithm is 6.93 KB. This means that the size of the image can encode 27287 characters with spaces (or 4478 words or approximately 10 pages of words) beneath theimage with almost no distortion.

5. CONCLUSIONS

A new steganography algorithm with two layers of security was suggested in this study. Utilizing the suggested algorithm, SIS (Steganography Imaging System) has been created as a system. We put few photos with varied sizes of hidden data to the test. We discovered that the stego image does not exhibit anydiscernible distortion while using the proposed approach. (as seen by the naked eyes). We also used PSNR value to test our stego photos. The stego image has agreater PSNR value than the other images, according to their PSNR values. In order to effectively hide the data inside the image, this new steganography technique was developed. A variety of users can make use of SIS to conceal data inside an image without disclosing it to third parties.

The data are kept private, discreet, and accurate by SIS.

6. REFERENCES

[1] M. Chen, N. Memon, E.K. Wong, Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: InformationScience Reference, 2008, pp. 438-450.

[2] D.C. Lou, J.L. Liu, H.K. Tso, Evolution of information – hiding technology, in H. Nemati (Ed.), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: InformationScience Reference, 2008, pp. 438-450.

[3] Schneider, Secrets & Lies, Indiana:Wiley Publishing, 2000.

[4] E. Cole, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Indianapolis: Wiley Publishing,2003.

[5] T. Jahnke, J. Seitz, (2008). An introduction in digital watermarking applications,principles and problems, in: H. Nemati (Ed), Premier Reference Source– Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 554-569