AN INNOVATIVE MODEL FOR SECURE

ENVIRONMENT USING STEGANOGRAPHY

G .NaliniPriya  
Professor , Department of IT ,  
Saveetha Engineering college,Chennai, Tamil Nadu  
dr.g.nalinipriya@gmail.com

Hemaroshini.M Jayathraa.V Reethika.R  
UG, Department of IT, UG, Department of IT, UG, Department of IT,   
Saveetha Engineering college, Saveetha Engineering college Saveetha Engineering collegeChennai, Tamil Nadu Chennai, Tamil Nadu Chennai, Tamil Nadu hemaroshini711[@gmail.com](mailto:keerthivasan.ravi14@gmail.com) jayathraa07@gmail.com reethureethika2002@gmail.com

***Abstract***—***Steganography is a form of safety approach through obscurity, and it's the art of hiding the message among sender and the intended recipient. it is used to cover secret messages in various varieties like documents and also digital images, video and audio. it works through hidden information in the sort of way that nobody can suspect . this is the far method to shield sensitive or mystery information from spiteful assault. photo Steganography is the method of hiding the secret message which can be textual content, photograph or video inside stegno image in the way that is not visible to the human eyes. In this paper, we are using steganography technique to hide a secure image, we use virtual environment by using powershell tool.***

***Keywords***—***Information hiding, Steganography, Stegno-image, Encryption, Decryption, Powershell.***

I.INTRODUCTION

Steganography is the art of hiding records and that stops the detection of hidden messages. Invisible inks, microdots, person association, virtual signatures, covert channels, and unfold spectrum communications are a number of the methods in it. Steganography and cryptography are cousins in the spycraft circle of families .Steganography is one that hides the message so it can not be seen and Cryptography is one which scrambles a message so it can't be seen or understood. It also applies to other media, which includes text, voice, communique channels and binary report.

II.RELATED WORKS

We had gone through many papers that use the data hiding technique in steganography and we have found certain paper related to our concept. Roy and Changder [1] developed this method by means of presenting a technique called confidential mapping which is primarily based at the common succeeding. This technique is sturdy towards the brute-force cracking and additionally provides a favourable concealing capability.

In another paper, S.Samima et al.[2] developed a method for steganography,that is photograph recognition steganography, that is totally based on comfy key. It recruits image discernment regardless concealing the image. A mapping technique called matrix mapping is used for concealing the name of the game message and is sturdy against statistical and brute-force cracking inclusive of the analysis of watermarked image .Wu and Tsai in [3] carried out a photograph steganography method known as PVD . The quilt photo is divided into well separated blocks in this method.And the variation in each block inbetween each two pixels is calculated and some of these dissimilarites are categorized under a few degrees.

Another paper by Valandar et al.[4] proposed a remodel area steganography scheme.This techique used a chaotic map and for vitual pix,it is based on the integer wavelet transform (IWT).Bhardwaj and Sharma [5] proposed a steganography approach which is totally based on LSB technique. To lessen the changes that is wanted for the duration of the implant section, the pixels are primarily based on the second and third bit values.Valandar et al[6] designed two processes called uprooting and embedding.The privacy of the steganograpy scheme is increased by these twoprocesses. Sahu et al. [7] developed many similar double layered primarily based on RDH techiques by the use of altered LSB. Examining the chance of appealing our encoding technique to enhance the concealing capability of RDH technique, we depart for destiny paintings.

In another paper Kumar et al. [8] developed the other compacting techniques, consisting of low involution image compressing algorith.The pleasant of the stego picture can be enhanced using this algorithm.C.-K. Chan and L. M. Cheng[9] designed a scheme which calculates the distinction among pixels within the stego and the cover photo. The clearness of the steganography method can be enhanced by adjusting the concealed bits.

I. Hafi et al. [10] carried out a technique for photographic steganography called hybrid fuzzy method.Bit trimming and pixel correction are used. K..J.Devi[11] changed some bits of LSB to make the distinction between original picute and stego image very hard to identify. One of the challenges of this algorithm is coverting massive number of bits within the original image.There may be lo alternate inside the original image at few instances while the capacity of the message is concealed.

III**.**SYSTEM ARCHITECTURE

This paper presents building a secure data hiding technique in digital images. The advantage of limited power of human visual system (HVS) is taken by the image steganography technique. Image is used as cover media for embedding secret message. image steganography technique. Image is used as cover media for embedding secret message.

Secret message

Encryption process

Stego-image

Key

Secret message

Decryption process

**Fig. 1.** Proposed system architecture for hinding image using steganography

Fig 1. explains the proposed system architecture for hiding photo the usage of steganography. The sender desires the message i.e. the records to remain personal. it could be ciphertext, plain textual content, password or other photo and is known as as stego-key, which guarantees that simplest receiver who knows the suitable decoding key can be capable of extract the message from a cover- object.oposed system architecture for hiding image using steganography. The sender wishes the message i.e. the data to remain confidential. It can be ciphertext, plain text, password or other image and is called as stego-ke*y*, which ensures that only receiver who knows the appropriate decoding key will be able to extract the message from a cover- object.

The secretly embedded message with the cover-object is called as the stego-object and that which may be embedded in a chunk movement which includes a copyright mark,a serial variety or a covert communique. mystery message is the data that is hid.it can be of any type like audio ,video and photo.Encryption manner is the facts protection is particularly essential.An encoding method is used to encryt the secret statistics a good way to be embedded into the quilt picture. Stego-picture may be defined as the output of the embedding technique is the stego photograph. Stego image carries the hid message both in optimally selected coefficients or in pixel values. Decryption system is developed to decrypt the encrypted stego photo ,we need to use the equal encryption algorithm and to extract the embedded message we should use the equal steganography set of rules.

## *A.PROPOSED ALGORITHM*

In the newly proposed steganography technique, the encrypted facts inside the photograph is in part hidden and we generate two keys with the help of the last part of the encrypted message.these two keys are mystery keys and those two keys need to be regarded by means of the receiver to retrieve the unique encrypted message.

Algorithm:

|  |
| --- |
| **Input:** Dataset  **Output:** Hiding a secret message inside a image  **Step1**: Start  **Step2:** Create a virtual env and install the requirements.  **Step3:** Merge and unmerge your files with powershell.  **Step4:** We want to apply the image module from the Pillow library.  **Step5:** The output photo from the merge in operation and the input photograph for the unmerge operation need to be in PNG layout.  **Step6:** Stop |

**Fig. 2.** Proposed Algorithm for embedding data from

Stegno image

*B. INSERTING IMAGE INTO COVER IMAGE*

The cover color image should be get. The cover image size is retrieved. Now, calculate the max index size(MIS=row\*columns\*3).Then, get the message length(L) and reshape the cover image to 1 column matrix.A private random key of indexes within the range 1 to MIS and length=L should be generated and the private key is saved.

*C.RESHAPE THE COVER MATRIX:*

The message is inserted into the cover matrix by using the indexes of the private key.The cover matrix should be reshaped again to 3 dimensional matrix.

*D.RETRIEVING THE MESSAGE FROM IMAGE:*

## Get the cover image and reshape it to 1 column

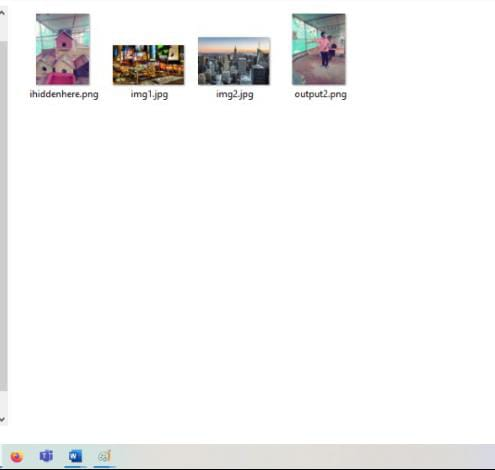
## matrix. The indexes of the message within the image

## is get using the private key . Retrieve the message.

## Implementation and result.

IV**.** IMPLEMENTATION

This approach is applied the usage of python. Python is an interpreter language.which means it executes the code line through line. Python offers a Python Shell, which is used to execute a unmarried Python command and show the result.

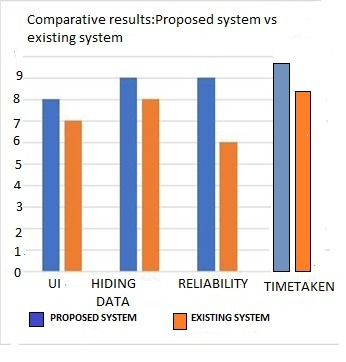


**Fig. 3**.Merged image of hiding in steganography

It is also known as REPL (examine, examine, Print, Loop), where it reads the command first after which evaluates the command, prints the end result, and loop it returned to read the command again together with your PowerShell command line open, input python to run the Python 3 interpreter. (some instructions choose to use the command py or python3, those ought to also work). you'll understand that you're a success due to the fact a >>>prompt with three more-than symbols could be displayed.

V**.**COMPARISON BETWEEN PROPOSED AND EXISTING SYSTEM

The proposed model has a limitation that the less secure app access has to be enabled by the sender in their gmail account. The sender should also provide the account credentials.

****

**Fig 4.** UHRT Algorithm for proposed system vs exiting system

The above fig.4 explains the UHRT set of rules for proposed gadget.x-axis is described by means of attributes consisting of hiding data,reliability,and the time taken to cover a picture and y-axis is also described and The comparative evaluation of proposed gadget with existing hiding information in steganography is defined in the above fig. We in comparison this paper with many literature papers with the opposite stegno papers referred to within the literatures [2][3] [7], our Proposed machine operates properly in phrases of attributes along with UI, and reliability. The reliability of current gadget noted inside the literature [3][9] are comparatively much less than our proposed work. This steganography sytem designed for communique to hide a message from a third birthday party is the cause of steganography. Steganography is different from cryptography, the artwork of mystery writing, which makes a message unreadable with the aid of a third birthday celebration however it does not conceal the lifestyles of the secret verbal exchange. This bar chart indicates how the proposed system is miles a head compares to all the prevailing. It also proves to the greater dependable, long lasting and extraordinarily scalable. actual time records switch between different users and also effective communique taken place can de taken from stegno paper mentioned in the literature[5] .

VI**.**RESULTS AND DISCUSSION

Information hiding has a huge extent that brings in researching interest which is the primary motive of steganography is incomes greater attraction to the secure infromation and data though the network communication. This observe abridges in the present days image of steganography strategies in spatial area and it additionally examined distinct problems and the drawbacks of each and every method that had been innovated from the past few years. No techniques are similar, each technique differs from every different technique. Few of them work on security or data hiding ability even as others work on better image quality. All those techniques can give more attempts and they're essential for futhure studies purposes in steganography.

Fig. 5 Explains use case diagram for the proposed steganography method for clear expertise. The use case diagram is used to discover the number one factors and techniques that shape the system. The primary factors are actors and this methods is called use cases.

Authenticator

Embedding message

User

Embedding file

Retrieve message

Retrieve file

**Fig 5.** Use case diagram for proposed system

VII. CONCLUSION

However the only a few of the primary image steganographic methods were mentioned in this paper, you may see that there exists a huge selection of techniques to hide information in pix,There is a unique methods of hiding messages for every photo file and layout, with distinct susceptible and robust factors respectively . If one method lacks in robustness ,the other alternative lacks in payload ability for as an example, the patchwork method has completely high stage of robustness, however it may conceal simplest and the small amount of data. Least significant bit (LSB) in both BMP and GIF makes up for this, but each methods bring about suspicious files that increase the possibility of detection within the presence of a warden. as a result for an agent to determine on which steganographic set of rules to apply,they might have to determine on the form of software they wanted to use as a set of rules for and if there willing to compromise on a few capabilities to ensure the security of others.hence we used steganography technique to hide a secure image,we use virtual environment by using powershell tool and also implemented succesfully.

REFERENCES

[1] R. Roy and S. Changder, “Image realization steganography with LCS based mapping,” in *Proceedings of the 2014 7th International Conference on Contemporary Computing (IC3)*, pp. 218–223, Noida, India, 2014.

[2] S. Samima, R. Roy, and S. Changder, “Secure key based image realization steganography,” in *Proceedings of the 2013 IEEE 2nd International Conference on Image Information Processing (ICIIP)*, pp. 377–382, Shimla, India, 2013.

[3] D.-C. Wu and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[4] M. Y. Valandar, P. Ayubi, and M. J. Barani, “A new transform domain steganography based on modified logistic chaotic map for color images,” Journal of Information Security and Applications, vol. 34, pp. 142–151, 2017.

[5] R. Bhardwaj and V. Sharma, “Image steganography based on complemented message and inverted bit LSB substitution,” *Procedia Computer Science*, vol. 93, pp. 832–838, 2016.

[6] M.Y Valandar, M. J. Barani, P. Ayubi, and M. Aghazadeh, “An integer wavelet transform image steganography method based on 3D sine chaotic map,” Multimedia Tools and Applications, vol. 78, no. 8, pp. 9971–9989, 2019.

[7] A. Sahu, G. Swain, and G. Swain, “Dual stegnography imaging based reversible data hiding using improved LSB matching,” International Journal of Intelligent Engineering and Systems, vol. 12, no. 5, pp. 63–73, 2019.

[8] R. Kumar, S. Singh, and K.-H. Jung, “Human visual system based enhanced for color image compression using interpolation,” in *Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 903–907, Noida, India, 2019.

[9] C.-K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognition, vol. 37, no. 3, pp. 469–474, 2004.

[10] I. Hafi, M. Noman, M. Gohar et al., “An adaptive hybrid fuzzy-wavelet approach for image steganography using bit reduction and pixel adjustment,” *Soft Computing*, vol. 22, no. 5, pp. 1555–1567, 2018.

[11]K. J. Devi, “A secure image steganography using lsb technique and pseudo random encoding technique,” Department of Computer Science and Engineering, National Institute of Technology, Rourkela, India, 2013, Ph.D. thesis.