EFFICIENT STEGANOGRAPHY TECHNIQUE USING BIT STREAM DATA TRANSFER

Praveena.V, Saranraj.R, Sweatha.R, Vinayagamoorthy.P

Ms.Prashanthini K - *Assistant Professor*

Department of Computer Science and Engineering,

KGiSL Institute of Technology, Coimbatore, India.

ABSTRACT

Steganography is to hide messages in such a way that no one apart from the intended recipient knows that a message has been sent.This can be achieved by concealing the existence of information within harmless cover.It is used in Defense sectors, National Security where no details of high officials should be hacked.In the proposed system,we use Image-Stegano technique along with LSB based Advanced Encryption Standard algorithm for hiding messages with data stream. In this method we use a secret key to decrypt the hidden data. The secret key can be kept common for a series of data and can be used to decrypt the encrypted images related to the secret key.

1. INTRODUCTION

Steganography could be a Greek word which implies hid writing. The word steganos suggests that lined and graphical suggests that writing. this can be AN ancient technique utilized by many folks as well as kings to speak protected message to supposed recipient.Most of the time except sender and receiver nobody else comprehend existence of such message. it's terribly powerful technique to share vital messages as there square measure less possibilities of revealing of the content. Thus, steganography isn't solely the art of concealment information however additionally concealment the very fact of transmission of secret information. Steganography hides the key information in another get into such the way that solely the recipient is aware of the existence of message. In ancient time, the information was protected by concealment it on the rear of wax, writing tables, or scalps of slaves. One use of steganography includes watermarking that hides copyright data inside a watermark by overlaying files not simply detected by the optic.This prevents dishonorable actions and offers copyright protected media additional protection.But these days most of the individuals transmit the information within the sort of text, image, video, and audio over the medium. so as to securely transmission of confidential information, the transmission object like audio, video, image square measure used as a canopy sources to cover the information. Steganography is outlined because the study of invisible communication. Steganography typically deals with the ways that of concealment the existence of the communicated information in such the way that it remains confidential. It maintains secrecy between 2 communication parties.Steganography is most frequently related to the sophisticated selection, wherever information is hidden inside alternative information in AN electronic file. for instance, a Word document can be hidden within a picture file. this can be typically done by exchange the smallest amount vital or most redundant bits {of information|of knowledge|of information} within the original file-bits that square measure hardly uncomprehensible by the human eye or ear with hidden data bits. the concept behind image-based Steganography is extremely easy. pictures square measure composed of digital information (pixels), that describes what’s within the image, typically the colours of all the pixels.In this project we've been mistreatment image steganography technique that has high capability to carry data to speak one to a different. this can be been planned to be implement in defence sectors for higher official meeting and schedules to be followed over there. In Image-Steganography, secrecy is achieved by embedding information into cowl image and generating a stegano-image. Drawback Statement within the existing system, this deals with Defense, National security exchange information mistreatment Image-stegano with providing a secret key .The system can hold personal data, uses LSB primarily based Advanced encoding formula as its computes on bytes instead of bits.Image-stegano and secret key generation are processed by AES that doesn't have packet losses whereas causing information.

2. PROBLEM STATEMENT

In the existing system, this deals with Defense, National security exchange data using Image-stegano with providing a secret key .The system will hold non-public information, uses LSB based Advanced Encryption algorithm as its computes on bytes rather than bits. Image-stegano and secret key generation will be processed by AES that does not have packet losses while sending data.

3. PROPOSED WORK

The planned system need to overcome all the disadvantages of the prevailing system. Some prevailing system is not functioning well form of not exploitation algorithmic rule and by validation of 1 sort watchword, that the planned system need to overcome the problems. This project is been developed exploitation python that could be a high level language, has some secure sources in engineered that creates the system sturdy to urge far from intruders.Steganography have found usage in several applications. Steganography is another methodology for privacy and security. rather than encrypting, we will hide the messages in alternative innocuous trying medium carrier in order that their existence isn't disclosed. LSB-Steganography is a steganography technique in that we have a tendency to hide messages within a picture by replacing Least important bit of image with the bits of message to be hidden. LSB substitution could be a well-liked technique to insert knowledge on to digital pictures. we all know that a picture are keep within the variety of bytes. during this reasonably encryption, by exploitation the LSB of every computer memory unit, 1-bit info are often keep within the image as secret message . consequently 1-bit per computer memory unit are often keep in 8-bit pictures whereas 3-bits are often keep in 24-bit pictures for each 24-bits. relying upon the colour palette of a canopy image, a secret message are often keep in 2 LSB's that can't be known by human sensory system (HVS) .This system uses python language as a face and hypertext markup language ,css for front. LSB primarily based Advanced cryptography customary algorithmic rule is employed during this system, the a lot of well-liked and wide adopted radially symmetrical cryptography algorithmic rule probably to be encountered today is that the Advanced cryptography customary.The LSB primarily based Advanced cryptography customary algorithmic rule is employed within the project to convert knowledge into bit stream knowledge because it is simple to cover within the image .The bit stream knowledge has been keep in pixels of the image. Least important bit of image with the bits of message to be hidden. LSB substitution could be a well-liked technique to insert knowledge on to digital pictures. we all know that a picture are keep within the variety of bytes. during this reasonably encryption, by exploitation the LSB of every computer memory unit, 1-bit info are often keep within the image as secret message. This project deals with one to 1 communicators, doesn't holds public info. Not used for multiple users as some systems has been developed for multiple users by verifying just one occasion passwords as seen intruders might passes and in some systems no secret key generation was there to decipher the info hidden within the image.

3.1 ENCRYPTION MODULE:

Encryption allows information to be hidden so that it cannot be read without special knowledge such as a password.Data encryption is basically a strategy to make the data unreadable, invisible or incomprehensible during transmission by scrambling the content of data. Image encryption method prepared information unreadable.By using python it is quite easy to encrypt the image on the basis of AES algorithm.

- In this module, the data gets encrypts into the image using AES algorithm. Encryption or encoding the file into the cover image is the first process in steganography technique. The image that holds secure data is said to stegano-image.

- The data are changed into bit stream conversion once it gets encrypted into the cover image. In this project AES is used convert the data into bit stream while encrypting

- The process of converting information or data into a code, especially to prevent unauthorized access.

3.2 SECRET KEY GENERATION MODULE:

Key generation to the stegano-image is sort of a watchword to secure the file. secret is used for each encrypting and decrypting the file from the image. during this project whereas transfering the file from the drives it asks to enter the key therefore to upload and decode it firmly. The key contains a size to enter as compiled within the program.A secret key is the piece of data or parameter that's accustomed cipher and decode messages during a even, or secret-key, encryption. The key is accustomed cipher and decode information regardless of the information is being encrypted or decrypted. Symmetric-key algorithms use one shared key; keeping data secret requires keeping this key secret. during this module, Secret secret is generated exploitation python language, that is employed for each encoding and secret writing. whereas encrypting the image with the information secret secret is generated as coded. within the online page to transfer the file we want to enter the key as watchword then it must enter whereas decrypting the encoded image.

3.3 DECRYPTION MODULE :

The conversion of encrypted knowledge into its original type is called Decryption. it's typically a reverse method of coding. It decodes the encrypted data so a certified user will only decrypt the knowledge because decryption requires a secret key or arcanum.Decryption is the method of remodeling encrypted data so it's intelligible once more. This term can be accustomed describe a way of unencrypting the information manually or unencrypting the information mistreatment the right codes or keys.To decipher the image ,the same key given for uploading the image must enter during a given filed given during this project and so the transfer choice gets enabled .By that the file gets decrypted from the image .Hence the information is hided LSB formula this has file changing measures to open the file from the situation it's hold on. The users will retrieve the information as per their convenient.

4. CONCLUSIONS

We have proposed a Image Steganography . This allows the user to perform some basic operations to hide data in the image and pass from one communicator to another communicator. Our implementation could help for communication, process between one to one. Using this project image steganography will be more efficient while it is been put into practice and it helps the customers to easily communicate with each other. Steganography is to create secrete communication, in addition to this stegano way of embedding gives us higher end of security using LSB algorithm. Even if the person gets both stegano and cover image he/she needs key to retrieve the data, without the key one can't recover the data. So user will have no issues in using this image steganography process.

5.REFERENCES :

- Google
- Wikipedia
- IEEE papers
- https://www.engpaper.com/steganography-2017.html
- https://www.cis.upenn.edu/~cis110/13fa/hw/hw04/steganography.html#steganograpy
- https://www.sans.org/reading-room/whitepapers/stenganography/steganography-past-present-future-552
- https://null-byte.wonderhowto.com/how-to/steganography-hide-secret-data-inside-image-audio-file-seconds-0180936/

YouTube videos:

- https://programmer2programmer.net/live_projects/project7./steganography.aspx