Digital Steganography

[1]Ariba Khan, [2]Vaishnavi Jivarakh, [3]Akshada Unde, [4]Divya Gadhe

Students
Department of Computer Engineering
G.H.Raisoni college of Engineering and management Ahmednagar

***Abstract*: The privacy and security of data is of utmost importance to individuals whose critical data can be leaked out and used for illegal purposes. The data needs to be secure and precautions needs to be taken whenever it gets transmitted from one place to another. In the preceding years, chaotic systems are erratic but definite in nature. The data encrypted using this system is so sensitive, that, changes in one of the coordinate positions leads to data being encrypted in other coordinate positions. So the proposed paper involves an image encryption algorithm.**

***Keywords*: steganography Vs Cryptography, Uses of Steganography, Steganography under Various Media**

Introduction

Maintaining secrecy is very important in a largecorporation and because of the intelligent of the hackersitbecomes tedious. Already we have crypto graphy for transmitting secret information. Even though crypto graphy successfully transmitting secret information, it will give a suspicion to the hackers and it affects unintended users.

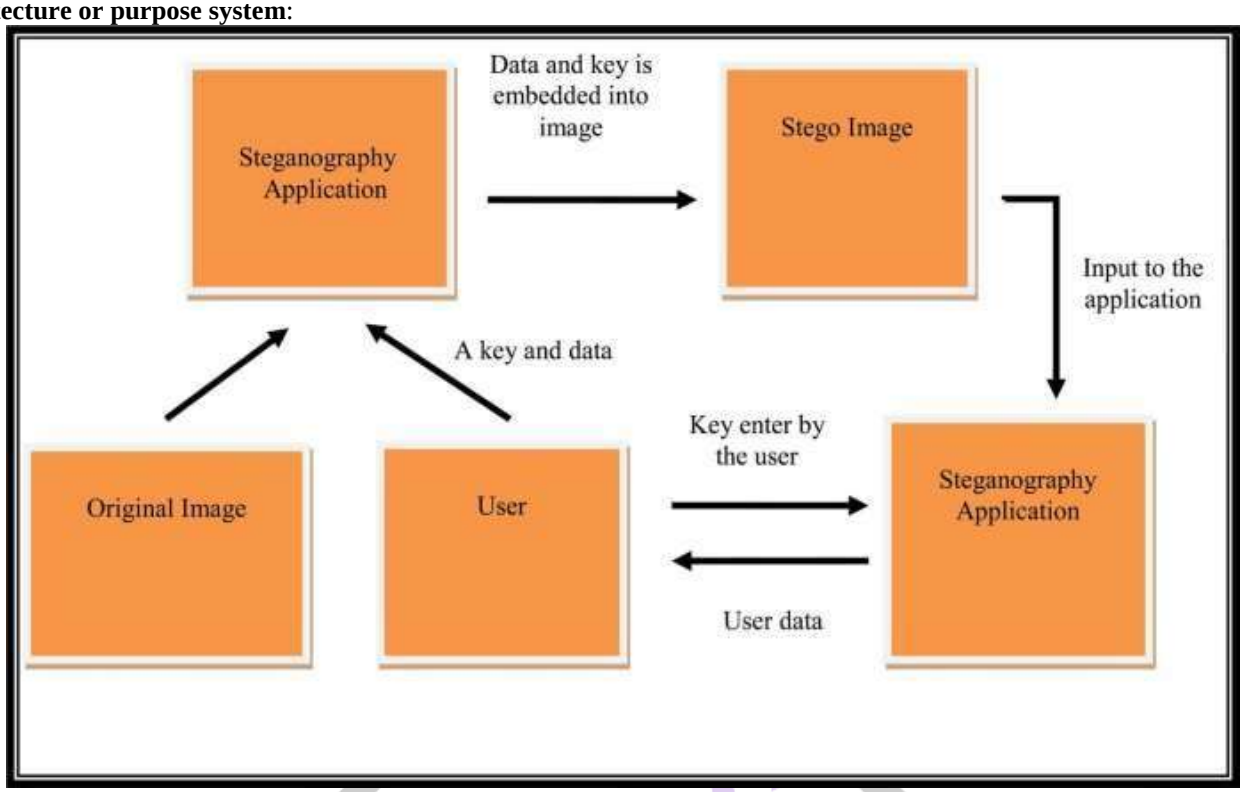
Our project, **DIGITAL STEGANOGRAPHY** overcomes this factor and it gives a solution for transmitting secret formation with out affecting unintended users. Steganography uses multimedia data as a covering medium (Covering secret information). By using steganography data (secret information) can hided with in data (multimedia data, here multimedia data is an image) and it can be sent anywhere to transfer the message easily without giving any suspicion to others.

Technology has blitz scaled over the past years leading to a wide usage of multimedia for transferring data, especially Internet of Things (IoT). Usually, the transfer happens over insecure network channels. In particular, the internet has gained accelerated popularity for exchanging digital media and individuals, private companies, institutions, governments use these multimedia data transfer methods for exchanging data. Though there are numerous advantages attached with it, one prominent disadvantage is the privacy and security of the data. The availability of numerous readily available tools capable of exploiting the privacy, data integrity and security of the data being transmitted has made the possibility of malicious threats, eavesdropping and other subversive activities. The prominent solution is data encryption where the data is converted into a cipher text domain using encryption key. At the receiving end, the cipher text is converted into plain text using a decryption key. Using data encryption associate editor coordinating the review of this manuscript and approving it's for publication was Li. He original data is not visible, however, cipher text is visible in a scrambled form to human eyes leading to suspicion and further scrutiny. A new research topic, steganography, has gained acceptance in this context to hide the data that is not perceptible to human eyes.

Information hiding techniques have been available for a long time but their importance has been increasing recently. The main reason is the increase in the data traffic through the internet and social media networks. Though the objectives of cryptography and steganography are similar, there is a subtle difference. Cryptography makes the data unbreakable and unreadable but the cipher text is visible to human eyes. Steganography, which is used to hide the information in plain sight, allows the use of wide variety of the secret information forms like image, text, audio, video and files. Digital watermarking is another method where confidential information is embedded to claim ownership. Cryptography is the popular method used for information hiding, but, steganography is gaining popularity in recent times. Steganography can be defined as the process of hiding a secret small multimedia data inside another but much larger multimedia data such as image, text, file or video [1]. Image steganography is a technique to hide an image inside another image. In image steganography, the cover image is manipulated in such a way that the hidden data is not visible thus making it not suspicious as in the case of cryptography. Inversely, Steganalysis is used to detect the presence of any secret message covered in the image and to extract the hidden data [2]. Steganalysis helps in classifying if the image is either a stegoimage on normal image. Apart from classifying the image, further investigation is carried out to detect the location and the content of the secret image inside the cover image.

The main goal of this paper is to review the available methodologies, present trends and discuss the challenges that are currently available in the studies. Along with these studies, the datasets that are publicly available and commonly used, the evaluation metrics considered are also discussed. Finally, a comparison on the performance among the methods and a possible discussion identifying the gaps in the present studies, pros and cons of the methods are elaborated. The remaining paper is organized as follows. Section II summarizes the working principle of the methods grouped into three categories - Traditional methods, CNN-Based methods and GAN-Based methods. Datasets used commonly are elaborated in section III along with evaluation in section IV. A table with the comparisons of the results from the different methods are provided with the
Experimental set-ups generally used in section IV. Finally, the challenges faced, a brief discussion, and conclusion
are added in section V, VI and section VII respectively.

Architecture or purpose system:



***Literature survey*:**

Savita Goel et al. in [20] proposed a new method of embedding secret messages in cover image using LSB method using different progressions. Authors compare the quality of stego image with respect to cover image using number of image quality parameters such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), histograms and CPU time, Structure Similarity (SSIM) index and Feature Similarity Index Measure (FSIM). Their study and experimental results shows that their proposed method is fast and highly efficient as compared to basic LSB methods.

David & Deitel in (1999 have done survey on recent achievements of LSB based image steganography. In this survey authors discuss the improvements that enhance the steganographic results such as high robustness, high embedding capacity and un-detectability of hidden information. Along with this survey two new techniques are also proposed. First technique is used to embed data or secret messages into the cover image and in the second technique a secret gray scale image is embedded into another gray scale image. These techniques use four state table that produce pseudo random numbers. This is used for embedding the secret information. These two methods have greater security because secret information is hidden on random selected locations of LSBs of the image with the help of pseudo random numbers generated by the table.

D. Samidha and D. Agrawal [32] in their research paper "Random Image Steganography in Spatial Domain" study various image steganographic methods and proposed a LSB based steganography method using random bit selection. In their techniques least significant bit is selected randomly for embedding the secret information inside the cover image. They also proposed some more techniques based on random pixels of cover image and secret information is embedded in randomly selected bits of random pixels. Intensity values, location of pixels etc. parameters are used for this purpose.

Roger S.Perssman, Software Engineering in their research paper "Random Image Steganography in Spatial Domain" study various image steganographic methods and proposed a LSB based steganography method using random bit selection. In their techniques least significant bit is selected randomly for embedding the secret information inside the cover image. They also proposed some more techniques based on random pixels of cover image and secret information is embedded in randomly selected bits of random pixels. Intensity values, location of pixels etc. parameters are used for this purpose.

Author proposes an enhanced LSB algorithm for image steganography. In this proposed work they only embed secret information in blue component of the RGB color space. In their technique first M×N size cover image is selected. After selection of cover image only blue component is used for embedding secret information. They also make use of pixel filters to access the best regions to embed information in cover image to obtain best possible rate. Experimental results show that this technique reduces the distortion level of cover image and stego image has very good visible quality and changes in cover image are negligent to Human Visual System (HVS). This method reduces the leap in color scale because only blue components are used to embed the secret information

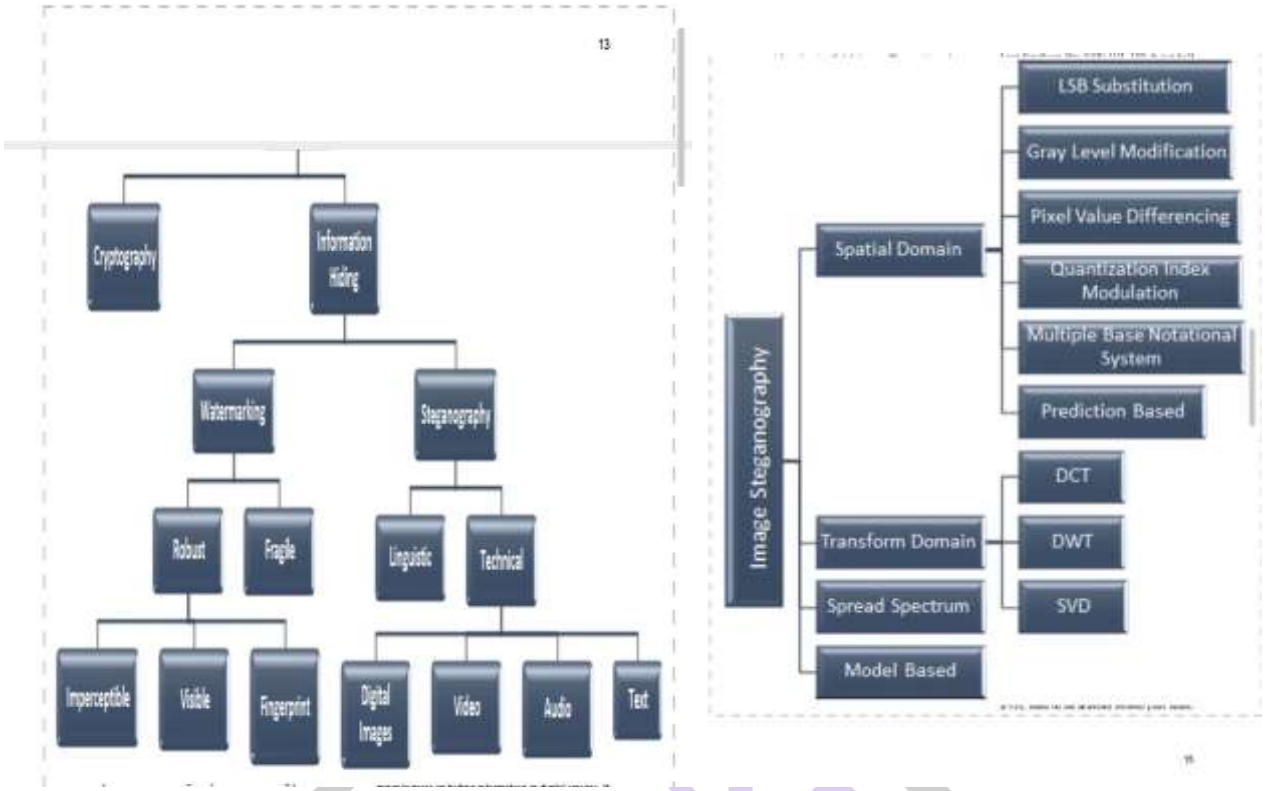


Fig.Classification of image steganography techniques

Proposed Algorithm:

Our proposed algorithm is using two layers of security Steganography Algorithm to Hide Secret Message inside an Image 104 to maintain the privacy, confidentiality and accuracy of the data. Fig. 1 shows the framework for the overall process of the system. The system is able to hide the data inside the image as well as to retrieve the data from the image. From Fig. 1, for hiding the data, a username and password are required prior to use the system. Once the user has been login into the system, the user can use the information (data) together with the secret key to hide the data inside the chosen image. Using a novel steganography algorithm, these data will be embedded and hided inside the image with almost zero distortion of the original image. For retrieving the data, a secret key is required to retrieving back the data that have been embedded inside the image. Without the secret key, the data cannot be retrieved from the image. This is to ensure the integrity and confidentiality of the data. For the steganography algorithm, Fig. 2 shows the algorithm for embedding the secret message inside the image. During the process of embedding the message inside the image, a secret key is needed for the purpose of retrieving the message back from the image. From Fig. 2, the secret message that is extracted from the system is transferred into text file first. file. The zip text file then is used for converting it into the image text file is more secured if compared with the file that is without the zipped. The contents in the zipped file will significantly hard to be detected and read. Furthermore, this series of binary codes of the zipped text file and the key is a long random codes in which they only consist of one and zero figures. A data hiding method is applied by using this series of binary codes. By applying the data hiding method, the last two binary codes from the series are encoded into a pixel in image, then, next two binary codes are encoded to the next pixel in image, the process is repeated until all the binary codes are encoded. The secret key in this proposed steganography algorithm is playing an essential Secret Key Username and Password Cover Image Stego Image Secret Key Top Secret First Layer of Security Second Layer of Security Top Secret Data Hiding Data Retrieving A Novel the the system role where the key is acts as a locker that used to lock or unlock the secret message. For the data hiding method, each last two bit is encoded into each pixel in image. This will ensure the original image will not be tempered with too many changes. Once the message is hidden inside the image, this message can be extracted back from the stego image. Fig. 3 shows the algorithm for extracting the secret message from the stego image. In order to retrieve a correct message from the image, a secret key is needed for the purpose of verification. From Fig. 3, for the data extracting method, a secret key is needed to detect whether the key is match with the key that decodes from the series of binary code. Once the key is matched, the process continues by forming the binary code to a zipped text file, unzip the text file and transfer the secret message from the text file to retrieve the original secret message. Steganography

```
Begin
Input: Cover_Image, Secret_Message, Secret_Key;
Transfer Secret_Message into Text_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
```

Design Steganography Algorithm

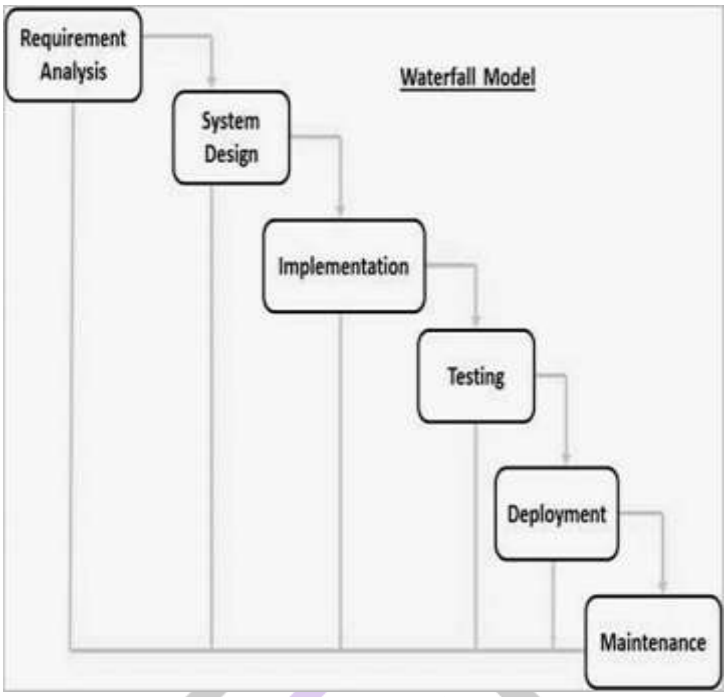
```
Begin
Input: Stego_Image, Secret_Key;
Compare Secret_Key; Calculate BitsPerUnit;
Decode All_Binary_Codes;
Shift by 2 unit for bitsPerUnit;
Convert Binary_Codes to Text_File;
Unzip Text_File;
Output Secret_Message;
 End
```

Algorithm for embedding data inside image

Model:

The sequential phases in Waterfall model are −

- **Requirement Gathering and analysis** − All possible requirements of the system to be developed are captured in this phase and documented in a requirement specification document.
- **System Design** − The requirement specifications from first phase are studied in this phase and the system design is prepared. This system design helps in specifying hardware and system requirements and helps in defining the overall system architecture.
- **Implementation** − with inputs from the system design, the system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality, which is referred to as Unit Testing.
- **Integration and Testing** − All the units developed in the implementation phase are integrated into a system after testing of each unit. Post integration the entire system is tested for any faults and failures.
- **Deployment of system** − Once the functional and non-functional testing is done; the product is deployed in the customer environment or released into the market.
- **Maintenance** − There are some issues which come up in the client environment. To fix those issues, patches are released. Also to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment



METHODOLOGY:

User needs to run the application. The user has two tab options – encrypt and decrypt. If user select encrypt, application give the screen to select image file, information file and option to save the image file. If user select decrypt, application gives the screen to select only image file and ask path where user want to save the secrete file. This project has two methods – Encrypt and Decrypt. In encryption the secrete information is hiding in with any type of image file. Decryption is getting the secrete information from image file

RESULTS AND DISCUSSION:

The encryption and decryption algorithm that can blend the secret data with the cover image and secret key is extremely sensitive, that a change in the parameters in itself will lead to changes of the secret image being encrypted in different positions. A difference between the keys will provide a different encrypted images and only the specific key will be able to decrypt the output accurately. One should keep in mind that the key space needs to be large since the processing time required by the any third party attack will take some time till the actual secret key will be

***Conclusion*:**

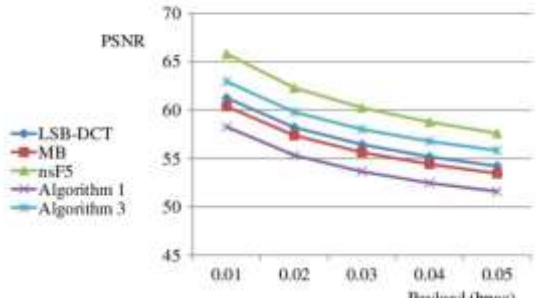
Steganography is **useful for hiding messages for transmission**. One of the major discoveries of this investigation was that each steganographic implementation carries with it significant trade-off decisions, and it is up to the steganographer to decide which implementation suits him/her best.

REFERENCES:

1. David & Deitel in (1999), they publish paper Java How to program Introducing Swing, Prentice Hall.
2. Roger S.Perssman was publish paper Software Engg A Practitioner's Approach Fifth Edition-McGraww Hill International Edition, Software Engineering Series.
3. The Complete Reference JSP2.0, was Tata McGraw-Hill publishing Company Limited, Phil Hanna
4. Wikipedia. (2020). Steganography. [Online]. Available: https://en. wikipedia.org/wiki/Steganography
5. https://www.clear.rice.edu/elec301/Projects01/steganosaurus/conclusion.html#:~:text=Conclusions,implementation%20suits%20him%2Fher%20best.

EXPECTED RESULT:

0.01	61.2	60.4	65.8	58.3	62.9
0.02	58.2	57.4	62.3	55.3	59.8
0.03	56.4	55.6	60.2	53.6	58.0
0.04	55.2	54.4	58.8	52.5	56.8
0.05	54.2	53.4	57.6	51.6	55.8



Future scope:

An ideal steganographic algorithm should have high precision, a higher level of security with good embedding capacity. Simplicity and cost-effectiveness should also be considered. Thus, it is necessary to investigate steganographic problems and solve with different approaches using different domains.

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Digital image steganography and its derivatives are growing in use and application.