**Synopsis Report**

**On**

**STEGANOGRAPHY**

*Submitted in partial fulfilment of the Requirement for the Degree of*

**Bachelor of Technology**

**In**

**Computer Science and Engineering**

*Submitted BY*

*KRISHAN BHADANA-1/14/FET/BCC/2/055*

*NAWEEL ANWER-1/14/FET/BCC/2/040*

*Under the supervision of*

*Ms. MEENAKSHI MOZA*

****

**Department of Computer Science and Engineering**

**Faculty of Engineering & Technology**

**Manav Rachna International University, Faridabad**

**JAN 2017**

**Introduction**

Steganography is the practice of hiding private or sensitive information within a file that appears normal to the user. Steganography is often confused with cryptography because the two are similar in the way that both are used to protect important information. The difference between two is that steganography is used in hiding information without leaving any doubt or hint. It usually appears that no information is hidden at all. If a person views that file which contains a hidden information, it will appear to be normal and the person would not be able to figure it out, therefore the person will not attempt to decrypt the information.

In short, the most common use of steganography is to hide a file inside another file.

There are many different file formats used in steganography but image files are most popular among them.

This project report intends to give an overview of the Steganography, its uses and techniques. It also attempts to reflect which steganographic techniques is more suitable on which application.

Steganography is used for hiding the fact that communication is taking place, by hiding information in other information

**Existing system**

The existing system for securing the communication while sharing the information is either encrypting the information using cryptographic techniques or creating a virtual private network.

In symmetric key cryptography the information or file is locked by the sender and unlocked by the receiver with a key which is private.

In asymmetric key cryptography the sender locks the message with public key of the receiver and the message is afterwards unlocked by the private key of the receiver.

The only limitation of the above technique is that the person who is looking to steal the information knows where to steal from or where the information is present, he/she will make efforts to get the information and might succeed . If the person does not even know that there is something hidden, there will be no reason to be worried about information security.

**Proposed system**

User needs to run the application. The user has two tab options – encrypt and decrypt. If user selects encrypt, application give the screen to select image file, Text and option to save the image file. If user selects 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 secret information is hidden within a image file.

Decryption is getting the secret information from image file.

**Hardware/Software requirement**

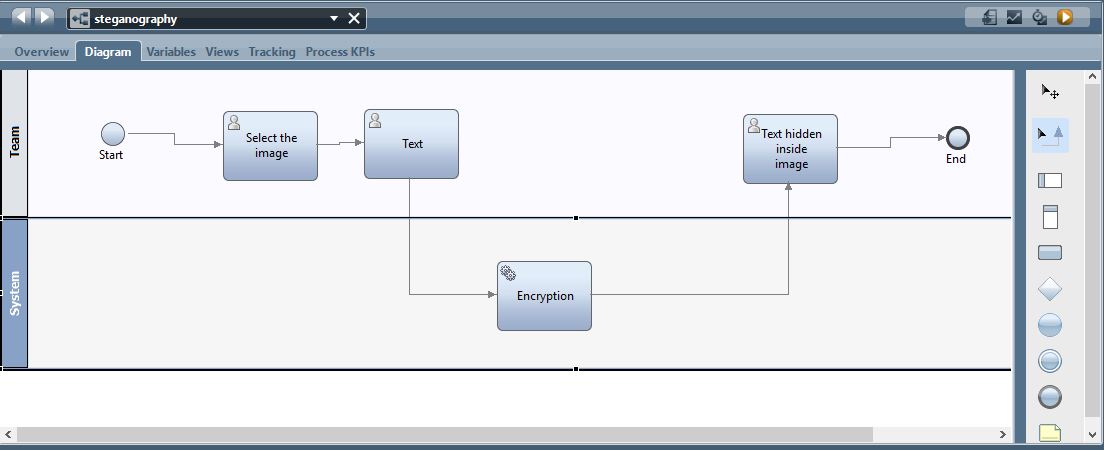
The development of this software will require a desktop computer with specifications:-

* 64 bit operating system (windows)
* 1GB ram
* 160GB storage
* Min clock speed 1.5Ghz
* Visual Studios

**Project scope**

The scope of this project is to enable a user to hide sensitive/secret information inside another file format making it harder to trace or steal. A third person will never able to know that there is being some information transferred in the network. This technique very useful in a scenario where the user wants to communicate in a network without creating any suspicion.

**Encryption Process**



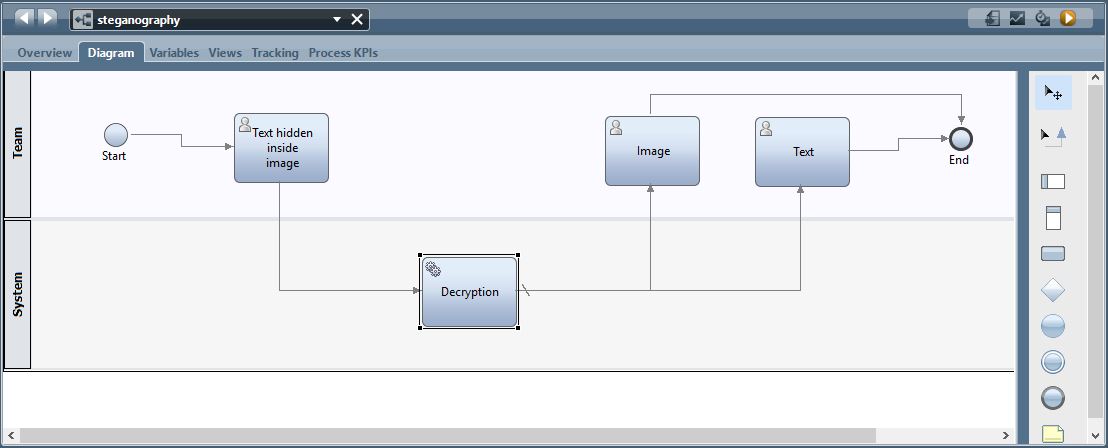
**IMAGE FILE**

 **TEXT**

**BMP FILE**



**Decryption Process**



**BMP FILE**



  **IMAGE FILE**

**TEXT**

**References.**

* The new boston (yotube c# tutorials)
* <http://www.google.com>
* http://www.wikipedia.org