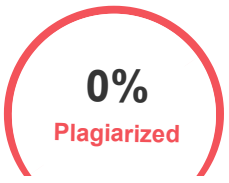
Dec 11, 2022

Plagiarism Scan Report



Characters:5780	Words:911
Sentences:38	Speak Time: 8 Min

Excluded URL None

Content Checked for Plagiarism

ABSTRACT The modern computing world revolves around the word “DATA”, but just what is so intriguing about it? In today’s world, data is the power and business start realizing it because data can predict customer trends potentially , get increased sales, and help the organization to achieve newer heights. The technology has become so advanced and our topmost priority is to secure data. Nowadays data sharing is increasing rapidly as there are thousands of messages and large number of data transmission taking place on the internet every day from one place to another. The secured data transmission is the primary concern of the sender, which is to protect data and it is really important to transmit our message in a secret way that only the receiver can able to understand.Steganography literally means hiding data in plainsight. In this project, we will understand what is image steganography and how can we implement it using a chat application in java. KEYWORDS: Steganography, Data security, java INTRODUCTION- Steganography The process of hiding a secret message within a larger one so that the contents or presence of the hidden message could not be known to anyone and this process is known as steganography. Steganography serves the main purpose which is to provide secret communication between two groups. Cryptography which can conceals only the contents of a secret message but steganography can able to conceal the fact that a message is communicated. Though there are some differences between steganography and cryptography, there are many analogies between them and some authors categorize steganography as a type of cryptography because hidden communication is a type of secret message. We can perform steganography on different transmission media like images, video, text, or audio. TYPES OF STEGANOGRAPHY Based on the way of transmission steganography can be classified into Text steganography, Image steganography, Video steganography, Network steganography, E-mail steganography, Audio steganography STEPS TO BE FOLLOWED TO PERFORM IMAGE STEGANOGRAPHY Obtain the secret information which is to be shared between sender and receiver Select an image in which you are going to encode the secret message Encode the secret message to the selected image The sender shares the message to receiver In receiver end, while decoding the secret information is extracted from the image So, in others point of view it is just an image but to the sender and receiver the secret message is successfully shared. My project is about network security (secured data transmission) by image steganography using Python. BASIC STEGANOGRAPHIC MODEL In this basic model of steganography, a cover file(image) and secret message is given to steganographic encoder and the stego object is communicated from sender to receiver and steganographic decoder decodes and only the secret message is obtained.

PROTOCOL FUNCTION UTILIZED BY STEGANOGRAPHY The various OSI RM layers that are related to steganography since it is mainly a data transmission between two parties Datalink layer In the Open Systems Interconnection (OSI) architecture model for a set of telecommunication protocols, layer 2 is the datalink layer. In this layer, data bits were encoded, decoded and organized before they are transported. The modified data bits are transported as frames between two adjacent nodes on the same WAN or LAN. Application layer The layer which specifies the shared communications protocols and the host's interface methods used in a communications network is known as application layer. It is otherwise known as abstraction layer. Both the standard models of computer networking, the Internet Protocol Suite (TCP/IP) and the OSI model uses the application layer abstraction. TOOL USED: JAVA(SERVER AND CLIENT WITH GUI AND OTP)FINAL CODE: JAVA is a very versatile programming language.We can use so many libraries,swing and so on for the GUI,OTP,Encoding,Decoding and so on! BASIC CONCEPT OF LEAST SIGNIFICANT BIT TECHNIQUE • We use the least significant bit technique to implement our steganography in the image. The data is converted to bits and modification in LSB doesn't affect the data much while MSB does. So, while encoding our secret message changes are made in LSB. STEPS TO BE FOLLOWED IN RUNNING THE CODE The JAVA code:- Run Server java file Immediately run Client java file GUI Opens up and connection is established Streams will be set and OTP will have to be used Then follow on screen functions! MERITS OF NETWORK SECURITY BY IMAGE STEGANOGRAPHY • It provides secured data transmission. • Up to now, cryptography plays a vital role in protecting the secret communication between the sender and the intended receiver. However, nowadays people use steganography techniques besides cryptography, because it adds more protective layers to the hidden data. • In comparison to cryptography alone, steganography uses a method that does not draw attention to the intended message. • It is difficult to detect only the intended receiver can be able to detect as it is pretty sneaky enough to slip through. • If we use large number of software's, it can be done faster. DEMERITS OF NETWORK SECURITY BY IMAGE STEGANOGRAPHY • Steganography is popular among cyber criminals. Recent attacks shows that the attackers used Steganography to embed the malicious code inside the file, which is found by security researchers that attackers use new malware campaign which uses image to hide the data • Image may become distorted. While compressing image such as JPEG, secret information may lost. When steganography is implemented properly, it can be difficult to detect, but not impossible. • Large number of data and large file size which is considered to be a disadvantage.

Sources