SmallSEOTools

PLAGIARISM SCAN REPORT

Words	953	Date	August 12,2020
Characters	5823	Exclude Url	

0% Plagiarism	100% Unique	0 Plagiarized Sentences	46 Unique Sentences

Content Checked For Plagiarism

CHAPTER 1 Introduction- Steganography is a methodology of covert classified data within an ordinary or non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The steganography can be blended with encryption as a step for shielding data. Steganography extracted from the Greek term steganos, meaning covered or secret, and graphy (writing or drawing). In simple words, steganography is covert writing, whether it consists of invisible ink on paper or information hidden in a file like audio, image,etc. Cryptography scrabbles a message into a code to nullify its meaning, steganography hides the message entirely. These two covert communication technologies can be used individually or together—for example, by first encrypting a message, then hiding it in another file for transmission. steganography's role is gaining prominence. Steganography basically does is to exploit human behaviour, human senses are not trained to peep into files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography.) Steganography hides the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to information analysis. It is one of the methods employed to guard secret or classified data from malicious attacks. Cryptography and steganography are techniques used to hide and protect secret data. However, cryptography makes the data unreadable, or hides the meaning of the data, while steganography hides the existence of the data. In layman's terms, cryptography is similar to writing a letter in a secret language: people can read it but won't understand what it means. However, the existence of a (probably secret) message would be obvious to anyone who sees the letter, and if someone either knows or figures out your secret language, then your message can easily be read. If you were to use steganography in the same situation, you would hide the letter inside a pair of socks that you would be gifting the intended recipient of the letter. To those who don't know about the message, it would look like there was nothing more to your gift than the socks. But the intended recipient knows what to look for, and finds the message hidden in them. Similarly, if sender and receiver exchange media files over the internet, it would be more difficult to determine whether these files contain hidden messages than if they were communicating using cryptography. Cryptography is often used to supplement the security offered by steganography. Cryptography algorithms are used to encrypt secret data before embedding it into cover files. It is viable to alter graphic and sound files without losing their overall viability for the viewer and listener. With audio, one can use bits of the file that contain sound which is not audible to the human ear. With graphic images, one can remove redundant bits of colour from the image and still produce a picture that looks intact to the human eye and is difficult to discern from its original. These are those bits that stego conceal its data. A stego program uses an algorithm, to embed data in a file that could be an image, audio, etc , and a password scheme to allow you to retrieve information. In image steganography, covertness is achieved by embedding data into a cover image and publishing a stego-image. There are different types of steganography techniques each has its strengths and weaknesses. In this paper, we review the different security and data hiding techniques that are used to implement steganography such as LSB, ISB, MLSB etc. In this project, the algorithm that will be used is LSB (Least Significant Bit). A digital image is described using a 2-D matrix of the colour intestines at each grid point (i.e. pixel). Typically, grey images use 8 bits, whereas coloured utilizes 24 bits to describe the colour model, such as the RGB model. The Steganography system which uses a file as the cover, there are several techniques to conceal information inside cover-image. The techniques manipulate the cover-image pixel bit values to embed the secret information. The last bits are altered directly to the cover image pixel bytes. Consequently, the techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in image Steganography. The concept of LSB Embedding is simple. It works upon the level of precision in different image formats is far greater than that perceivable by average human vision. Therefore, a stego image with slight variations in its colour intensity will be indistinguishable from the average human vision. Therefore, a stego image with slight variations in its colour intensity will be indistinguishable from the original by a human being, just by looking at it. For making our data more secure we will be using a cryptographic algorithm because if the intruders uses Steganalysis (Detecting use of Steganography) and they gets to know that there is a data present inside the image then also the intruder can’t get his hand to the classified data as it will be encrypted by the most secure cryptographic algorithm know as Advance Encryption Standard (AES-256). The Advance Encryption Standard (AES) is based on substitution-permutation network. AES is a sub-set of Rijndael. It is a family of ciphers with different key and block sizes. In AES, the block size is 128 bits or 16 characters which means 16 characters can be encrypted at a time. It has three different key size variation: 128 bits, 192 bits and 256 bits. When hackers want to access a system, they will aim for the weakest point, which is not the encryption, but the key. AES-256 is most secure encryption technique and till now there is no report of its cracking.

Sources	Similarity